



HYPER-UNIFIED STORAGE

Nexsan Unity Software User Guide

Firmware version: Unity v. 6.0
(Classic interface)

Copyright © 2010—2019 Nexsan Technologies, Inc. All rights reserved.

Trademarks

Nexsan® is a trademark or registered trademark of Nexsan Technologies, Inc. The Nexsan logo is a registered trademark of Nexsan Technologies, Inc. All other trademarks and registered trademarks are the property of their respective owners.

Patents

This product is protected by one or more of the following patents, and other pending patent applications worldwide:

United States patents US8,191,841, US8,120,922;

United Kingdom patents GB2466535B, GB2467622B, GB2467404B, GB2296798B, GB2297636B

About this document

Unauthorized use, duplication, or modification of this document in whole or in part without the written consent of Nexsan Corporation is strictly prohibited.

Nexsan Technologies, Inc. reserves the right to make changes to this manual, as well as the equipment and software described in this manual, at any time without notice. This manual may contain links to web sites that were current at the time of publication, but have since been moved or become inactive. It may also contain links to sites owned and operated by third parties. Nexsan is not responsible for the content of any such third-party site.

Contents

- Contents 3**

- Chapter 1: Introducing Unity 19**
 - New features and enhancements 20
 - Unity 6.0 20
 - Key features 22
 - Supported features by platform 26
 - Expansion options by next generation Unity Storage System 27
 - Expansion options by Unity 1.0 Storage System 27
 - FASTier caching by platform 28
 - Understanding multi-site implementation 28
 - Multi-site implementation characteristics 29
 - Multi-site implementation limitations 31
 - Typical Unity Storage System deployments 32
 - Unity2200 deployment 32
 - Unity4400 deployment 34
 - Unity6900 deployment 36

- Chapter 2: Setting up the site 39**
 - Step 1: Setting the password for the Nexsan Unity administrator 40
 - Step 2: Configuring the site information 40
 - Step 3: Configuring network settings 42
 - Step 4: Configuring IPMI settings 43
 - Allocating storage on the Unity 2000 43
 - Allocating storage on the Unity 4000 44
 - Allocating storage on the Unity 5000/Unity 6000 44
 - Step 6: Verifying configuration settings 46
 - Step 7: Viewing configuration results 47

- Chapter 3: Getting started with Nexsan Unity 49**
 - Starting Unity 50
 - Logging on to Unity 50
 - Navigating Unity 52
 - Tree view and nodes 52
 - Understanding nodes in Unity's tree view 53
 - System node 54
 - Storage Enclosures node 54

Cluster Settings node	56
n-Way node	56
Archive node	56
Storage Pools node	57
Incoming Replications node	58
Host Connectivity node	58
FASTier node	59
Node context menu	59
Properties panel	60
Global Toolbar	61
Tasks in progress panel	63
Viewing performance metrics with the Dashboard view	63

Chapter 4: Users and access rights 65

User authentication modes	66
Role-based administration in Nexsan Unity	66
Nexsan Unity roles and access rights	67
Managing users and access rights in the Manage Users and Groups panel	74
Opening the Manage Users and Groups panel	74
Users and Groups window	75
Access Rights, CIFS Permissions, and Group Membership window	78
Access Rights tab	78
CIFS Permissions tab	78
Group Membership tab	79
Viewing a user's or group's access rights	79
Viewing a user's or group's file system permissions	79
Viewing a user's group memberships	80
Viewing a group's members	81
Setting access rights	82
Giving Site Administrator access	82
Revoking Site Administrator access	84
Giving Pool Administrator access	85
Revoking Pool Administrator access	88
Managing users and groups with Nexsan Unity	90
Adding a user account	90
Adding a group	91
Adding a user to a group	92
Removing a user from a group	93
Deleting a user or a group	94
Changing a user's password	94
Changing the nxadmin password	95

Chapter 5: Storage Pools 97

Creating a storage pool	98
Before you begin	98
Mixing volumes with different RAID levels	98
Property settings order of precedence	99
Adding a storage pool	100
Step 1: Adding volumes to the storage pool	101
Step 2: Allocating FASTier cache devices to the storage pool	103
Step 3: Verifying settings	104

Step 4: Viewing configuration results	105
Scrubbing a storage pool	105
Performing a manual pool scrub	106
Modifying the scrub schedule for a storage pool	106
Adding volumes to a storage pool to expand capacity	107
Adding volumes to a replicated storage pool	109
Step 1: adding volumes to the primary storage pool	109
Step 2: adding volumes to the storage pool's replica	109
Step 3: Verifying settings	110
Step 4: Viewing progress	110
Replacing a volume in a storage pool	110
Storage Pool Properties Panel	112
Pool Properties tab	112
Scrub Schedule tab	112
System Notifications tab	112
Volumes tab	112
Administrators tab	112
VSS Client tab	112
Modifying the snapshot auto-deletion setting for a storage pool	112
Enabling data compression on the storage pool	113
Enabling the Access Time mode on a storage pool	114
Viewing space usage information for storage pools	115
Setting space usage notification thresholds for a storage pool	115
Moving a storage pool	116
Viewing and clearing storage pool errors	118
Deleting a storage pool	120
Chapter 6: File Systems	121
Overview of data management functions on file systems	122
Before you begin	122
Adding a file system using the Setup Wizard	123
Step 1: Creating a file system and configuring space usage	124
Step 2: Configuring the access method	126
Step 3: Enabling data replication and configuring snapshot scheduling	127
Step 4: Configuring your archive settings	129
Step 5: Verifying settings	131
Step 6: Viewing configuration results	132
Modifying file system properties	134
Renaming a file system	134
Disabling data sharing for a file system	135
Modifying a file system's sharing method	136
Modifying a file system's space usage settings	137
Modifying a file system's record size	138
Setting space usage notification thresholds for file systems	139
Enabling/disabling data compression on a file system	141
Enabling the Access Time mode on a file system	142
Setting up IP restrictions	143
Share IP permission precedence	145
Archive settings	146
Managing home directories	147
Viewing space usage information for file systems	149
Deleting a file system	149

Managing home directories	151
Creating file systems for home directories	152
Prerequisites	152
Step 1: Setting the name, storage pool, and space settings	153
Step 2: Assigning user groups	156
Prerequisites	156
Step 3: Assigning administrators	158
Prerequisites	158
Step 4: Selecting an access protocol	159
Step 5: Enabling data protection	160
Step 6: Configuring your archive settings	161
Verifying settings	163
Viewing results	164
Managing group assignments	165
Performing file system-level tasks for home directories	166
Example file system for home directories	167
Managing shares	168
Adding a share	168
Step 1: Setting the share's name	168
Step 2: Assigning access permissions to the share	170
Step 3: Verifying settings	171
Step 4: Viewing configuration results	172
Accessing shares	173
Accessing a CIFS share from Windows	173
Mapping a CIFS share to a drive letter	175
Accessing an NFS file system from UNIX/Linux	177
Using an NFS version 3 (NFSv3) client to access an NFS share with Microsoft Active Directory	178
Using an NFS version 4 (NFSv4) client to access an NFS share	179
Moving a share	182
Disabling data sharing for a share	183
Renaming a share	184
Viewing mount point information for file systems	186
Managing access permissions to shares	186
Understanding access permissions in Nexsan Unity	187
Read-only and Read/Write anonymous access	187
Windows and UNIX Access Control Lists (ACLs)	188
Giving share-level access permissions to a user or group	189
Modifying share-level access permissions	192
Revoking file system-level access permissions	193
Managing snapshots for file systems	194
Using the File Systems properties panel	194
Snapshots tab	194
Sorting the list of snapshots	195
Filtering snapshots in the grid	195
Searching for a specific snapshot in the grid	196
Snapshot Settings tab	197
Setting a schedule for automatic file system snapshots	197
Taking a manual file system snapshot	198
Browsing a file system snapshot	199
Stopping file system snapshot browsing	201
Rolling back the data in a share to a snapshot	202

Using the Windows Volume Shadow Copy service to roll back the data in a share	203
Configuring auto-deletion settings for file system snapshots	204
Manually deleting file system snapshots	205
Nexsan Unity n-Way Sync	207
Overview	207
Requirements	207
What is the CS organization?	207
Access Control	207
Network considerations	207
Server names:	207
Relay IP addresses:	208
Additional notes:	208
Preparing to create an n-Way file system	208
Creating an n-Way File system	209
Steps to sync an n-Way file system	209
Usage Notes	210
Working with links	210
Viewing link access information	211
Finding Users	212
Copying link URLs	212
Chapter 7: LUNs	213
Overview of data management functions on LUNs	214
Guidelines for adding and managing LUNs	214
Understanding disk space consumption	214
Adding a LUN	216
Setting the LUN name and block size	217
Configure space usage settings for the LUN	218
Enabling data replication and configuring snapshot scheduling	220
Selecting a Mask for the LUN	222
Add the LUN to a new LUN Mask	223
Verifying settings	224
Viewing progress	225
Modifying LUN properties	226
LUN Properties tab	226
Space Usage tab	226
VSS tab	227
Snapshots tab	227
Snapshot Settings tab	227
Renaming a LUN	227
Configuring client-side (host) settings for a LUN	228
Enabling VMware VAAI hardware acceleration for a LUN	228
Enabling client-side space usage notifications for a LUN	228
Modifying LUN space settings	229
Enabling/disabling data compression on a LUN	230
Disabling Read caching	231
Viewing space usage information for LUNs	232
Setting up host connectivity	233
Creating an Initiator group	234
Modifying an Initiator group	235
Deleting an Initiator group	236
Adding a LUN mask	237

Modifying a LUN mask	239
Deleting a LUN mask	242
Viewing LUN Masking information for a LUN	243
Adding an iSNS server	244
Removing an iSNS server	245
Managing snapshots for LUNs	245
Using the LUN's Properties panel to manage LUN snapshots	246
Introduction to snapshots	246
Snapshot concepts and terminology	247
Snapshots tab	249
Sorting the list of snapshots	250
Filtering snapshots in the grid	250
Searching for a specific snapshot in the grid	251
Snapshot Settings tab	251
Setting a schedule for automatic LUN snapshots	252
Taking a manual LUN snapshot	253
Browsing a LUN snapshot	254
Stopping LUN snapshot browsing	256
Rolling back data in a LUN to a snapshot	256
Deleting LUN snapshots manually	257
Setting auto-deletion settings for LUN snapshots	258
Using Windows VSS	259
Adding a CHAP user to the Management target	259
Installing the VSS Hardware Provider	260
Enabling the Microsoft VSS client for LUNs	263
Discovering your LUNs with the Windows iSCSI Initiator	264
Configuring the LUNs in Disk Management	268
Creating a VSS snapshot	270
Browsing a VSS snapshot	273
Viewing the VSS client information	275
Rolling back data to a VSS snapshot	276
Deleting a VSS snapshot	278
Using both Nexsan Unity and VSS Hardware Provider to manage LUN snapshots	279
iSCSI Functions	280
Configuring and managing CHAP authentication	281
Adding a CHAP user	281
Deleting a CHAP user	283
Modifying a CHAP user's secret	284
Setting the site-level CHAP user	286
Setting CHAP authentication for a target	287
Adding an iSCSI target	288
Step 1: Specifying the IQN and public alias for the iSCSI target	288
Step 2: Verifying configuration settings	289
Step 3: Viewing configuration results	289
Connecting to an iSCSI LUN from a Windows-based initiator	290
Deleting a LUN	291
Chapter 8: Clustering	293
Clustering overview	294
Unity 2000P/Unity 4000 Clustering	294
Unity 2000C/Unity 5000 Clustering	295
Unity 6000 Clustering	296

Unity2200 Clustering	298
Unity4400 and Unity6900 Clustering	299
Example of data access in a typical Unity cluster implementation	300
Viewing cluster health status and controller information	300
List of tasks and operations that you cannot perform when one of the controller nodes is down ..	302
Understanding heartbeats	302
Transient and persistent reservations with disk heartbeats	302
Transient reservation	303
Persistent reservation	303
Moving cluster resources	304
Restarting the cluster or individual controller nodes	306
Shutting down the cluster or individual controller nodes	307
Modifying IP configuration settings	309
Understanding IP address requirements	309
Understanding Network interfaces and required IP addresses	311
Network interfaces and required IP addresses	311
Understanding link layers	313
Setting up a secondary network interface	314
Setting or modifying IPMI settings	316
Accessing the IPMI web-based interface	317
Enabling jumbo frames	318
Enabling jumbo frames using the menu-driven nxadmin CLI	319
Enabling LACP	320
Requirements and guidelines for implementing LACP	320
Understanding link aggregation	322
Enabling LACP using Unity	323
Enabling LACP using the nxadmin CLI	323
Configuring TCP flow control	324
Chapter 9: Storage	327
Allocating new storage to the site	328
Step 1: Discovering new storage and configuring RAID settings	328
Step 2: Verifying settings	330
Step 3: Viewing results	330
Modifying IP settings for a Nexsan E-Series Storage System	330
Resetting the RAID configuration for storage	331
Renaming a storage enclosure	332
Adding new drives to a Nexsan storage enclosure	333
Removing a storage enclosure	335
Shutting down a Nexsan storage enclosure	335
Powering the systems back on	337
Using Self-Encrypting Drives (SEDs)	340
Disabling SEDs encryption	341
Chapter 10: Using Active Archive	343
Connecting to an Assureon Server	343
Managing Active Archive settings for file systems	344
Chapter 11: Site-level tasks	347
Modifying the site name	348

Disabling automatic FASTier write cache assignment	348
Modifying the time server	348
Setting NDMP configuration options	349
Modifying site preferences	351
Modifying the auto-refresh interval for the site	351
Manually refreshing site- or file system-level information	352
Scaling Unity to the screen resolution	352
Modifying the date and time formats displayed in Nexsan Unity	353
Modifying the Initial View	354
Modifying system preferences	355
Modifying background tasks settings	355
Modifying the date, time, and time zone settings	356
Adding a remote site for multi-site management	357
Disconnecting a remote site	360
Disconnecting sites in a multi-site implementation	360
Updating Unity	363
Upgrading to the latest firmware	364
Adding new features	366
Upgrading the cluster license	369
Modifying authentication settings	371
Joining an Active Directory Domain	371
Microsoft Active Directory domain requirements	371
Creating computer objects on the Active Directory server	373
Delegating control to the non-Administrator user account	376
Joining an Active Directory domain using Unity	380
Managing domain controllers	385
Discovering new domain controllers	385
Selecting alternate primary and/or secondary domain controllers	386
Enabling Kerberos for accessing CIFS file system	386
Adding a Reverse Lookup Zone in DNS Manager	387
Adding a host for each Resource Controller in DNS Manager	393
Configuring the host in Active Directory	393
Unjoining Unity from an Active Directory domain	396
Connecting to an LDAP Directory service	398
Setting up Unity authentication	400
Troubleshooting site-level warning and error conditions	401
Configuring NFS settings	402
Viewing APAL status	403
Viewing the Unity Vault Protection Module status	404
Viewing NVDIMM status	404
Enabling FTP support	405
Understanding the CallHome feature	406
How CallHome is triggered	407
Event-driven CallHome	407
Diagnostics-based CallHome	411
Enabling CallHome log collection settings	413
Enabling SSH connectivity for CallHome	413
Enabling Internet Connectivity	414
Connecting to the Internet using a Direct LAN link	415
Connecting to the Internet using an HTTP proxy server	415
Connecting to the Internet using a workstation	416

Chapter 12: Data replication	419
Data replication concepts and terminology	420
Asynchronous data replication	421
Asynchronous data replication features	421
Usage implementations	422
Before you begin	423
Setting up asynchronous data replication	424
Step 1: Add a remote site for asynchronous data replication	425
Step 2: Configuring a data replication schedule	428
Step 3: Selecting datasets to replicate	429
Step 4: Allocating FASTier cache devices to the storage pool's replica	430
Step 5: Verifying settings	431
Step 6: Viewing results	432
Modifying asynchronous replication properties and configuration settings	432
Modifying a storage pool's replication schedule	433
Disabling a storage pool's replication schedule	434
Enabling or disabling asynchronous data replication for a dataset	434
Setting a scrub schedule for a storage pool's replica	435
Performing a manual pool scrub on a storage pool's replica	436
Configuring Asynchronous Replication settings for the site	436
Configuring network settings for Asynchronous Replication	436
Configuring compression settings for Asynchronous Replication	438
Configuring encryption settings for Asynchronous Replication	438
Browsing replicated datasets and snapshots	439
Viewing and browsing replicated datasets	439
Viewing and browsing replicated snapshots on the remote site	441
Performing an offline replication	442
Performing a manual replication to a remote site	442
Performing an offline replication to a USB storage device	443
Importing data from the primary Unity	444
Importing data from a USB storage device	445
Configuring replication bandwidth settings for a storage pool	446
Enabling bandwidth throttling	446
Creating a bandwidth throttling schedule	447
Modifying a bandwidth throttling schedule	448
Disabling a bandwidth throttling schedule	449
Deleting a bandwidth throttling schedule	449
Disabling bandwidth throttling	450
Failing over to the remote site for disaster recovery	450
Failover vs. promote	451
Site failover vs. pool failover	451
Performing a failover of the entire site	452
Performing a failover of a storage pool	453
Promoting the remote site	454
Promoting a storage pool's replica	454
Demoting a site	455
Demoting a storage pool	456
Managing file system replication conflicts	457
Viewing a file system's replication conflicts	458
Enabling browsing for a difference share	460
Disabling browsing for a difference file system	461
Viewing the contents of a .diff file	462

Deleting a share's replication conflict	462
Removing asynchronous data replication for a storage pool	463
Synchronous data replication	465
Synchronous data replication features	465
Usage implementations	466
Before you begin	466
Setting up synchronous data replication for a storage pool	466
Step 1: Add mirror volumes	468
Step 2: Verifying settings	469
Step 3: Viewing configuration results	470
Promoting the mirrored storage pool	470
Removing synchronous replication for a storage pool	471
Chapter 13: System monitoring	473
Viewing performance metrics with the Dashboard view	474
Dashboard toolbar	475
Dashboard title bars	476
Dashlet title bars	476
Home dashboard	477
Performance dashboard	478
Managing dashboards	479
Configuring dashboard settings	479
Managing dashboard templates	480
Configuring autosave settings	485
Saving dashboard settings	485
Adding and configuring dashlets	486
Configuring a Site Health dashlet	488
Configuring a Space Usage dashlet	490
Configuring a Site Space Overview dashlet	492
Configuring a Performance Metrics dashlet	493
Configuring a Report dashlet	495
Configuring a Device List dashlet	496
Configuring an I/O Operations Per Second dashlet	497
Viewing and recording performance metrics with the Performance Monitor	499
Starting the Performance Monitor	500
Filtering live performance metrics	501
Taking performance snapshots	502
Taking a performance snapshot	502
Viewing a performance snapshot	504
Deleting a performance snapshot	504
Viewing historical performance data	504
Changing the duration to keep sampling data	505
Creating and viewing reports	507
Report types	507
Configuring report settings	508
Generating reports	509
Sending reports by email	513
Exporting reports	515
Printing reports	515
Deleting reports	516

Chapter 14: Event logging and notification	517
Viewing events	518
Using the Event Viewer	519
Layout of the Event Viewer	519
Event Filters section	520
Events section	520
Filtering events in the Event Viewer	522
Filtering events by site, source, and/or severity type	522
Filtering events according to a time period or a date	523
Filtering events in the Event grid	524
Searching for a specific event in the Event grid	525
Saving events	526
Emailing events	527
Clearing event logs	527
Collecting logs	528
Configuring logging options	529
Setting up notification	530
Setting up email notification for system events	531
Setting up system notifications	533
Configuring SMTP server settings for the site	535
Setting up SNMP notification	537
Chapter 15: Operating in mixed mode environments	539
Understanding how changing the mode of a file in NFS affects permission settings in CIFS	540
Understanding how using chmod in NFS creates allow and deny entries in CIFS ACLs	542
Deny access control entry added for owner and group	542
Deny access control entry added for group only	542
Examples of CIFS permissions after applying chmod in NFS	543
Example 1	543
Example 2	544
Example 3	545
Example 4	546
Mapping UNIX accounts on Unity to corresponding Microsoft Active Directory accounts	548
nstusermaps	549
Terminology	553
Index	577

About this document

This *Software User Guide* provides information and detailed procedures for configuring and managing your Unity storage infrastructure using Nexsan Unity. This guide assumes that you have installed Unity by following the steps mentioned in the *Nexsan Unity Hardware Reference Guide* for the corresponding Unity platform.

Audience

This guide has been prepared for the following audience:

- IT system administrators
- Engineers
- Technicians

Conventions

Here is a list of text conventions used in this document:

Convention	Description
<u>underlined blue</u>	Cross-references (both internal and to the titles of other documents), hyperlinks, URLs, and email addresses.
boldface	Text that refers to labels on the physical unit or interactive items in the graphical user interface (GUI).
monospace	Text that is displayed in the command-line interface (CLI) or text that refers to file or directory names.
monospace bold	Text strings that must be entered by the user in the command-line interface or in text fields in the graphical user interface (GUI).
<i>italics</i>	System messages and non-interactive items in the graphical user interface (GUI) References to Software User Guides

Notes, Tips, Cautions, and Warnings

Note Notes contain important information, present alternative procedures, or call attention to certain items.

Tip Tips contain handy information for end-users, such as other ways to perform an action.



CAUTION: In hardware manuals, cautions alert the user to items or situations which may cause damage to the unit or result in mild injury to the user, or both. In software manuals, cautions alert the user to situations which may cause data corruption or data loss.



WARNING: Warnings alert the user to items or situations which may result in severe injury or death to the user.

Contacting Nexsan

For questions about Nexsan products, please visit the [Nexsan support](#) Web page, and the Nexsan Unity [Documents and Downloads](#) page. If you are unable to find the answer to your question there, please see our contact information below.

Service and support

Nexsan's Technical Services Group provides worldwide assistance with installation, configuration, software support, warranty, and repair for all Nexsan products. A variety of service and support programs are available to provide you with the level of coverage and availability your operation requires.

Nexsan Unity Documents & Downloads page:

https://helper.nexsansupport.com/unt_downloads.html

Unity Online Help page:

https://helper.nexsansupport.com/unt_onlinehelp.html

Contact Nexsan Unity support:

https://helper.nexsansupport.com/unt_support

Worldwide Web site:

www.nexsan.com

Related documentation

The following Nexsan product manuals contain related information:

- *Nexsan Unity Hardware Reference Guide*
- *Nexsan Unity Hardware Maintenance Guide, Unity Next Generation*
- *Nexsan Unity Software User Guide*
- *Nexsan Unity nxadmin Command-line Interface Reference Guide*
- *Nexsan Unity nxcmd Command-line Interface Reference Guide*
- *Nexsan Unity Snapshots and Replication Guide*
- *Nexsan Unity Storage Expansion Reference Guide*
- *Nexsan Unity VMware Best Practices Guide*
- *Nexsan Unity NFS Interoperability*
- *Nexsan Unity Networking Best Practices Guide*
- *Nexsan Unity Performance Best Practices Guide*
- *Nexsan Unity Microsoft Best Practices Guide*

Safety notices

Always observe the following precautions to reduce the risk of injury and equipment damage:

- Computer components and disk drives are sensitive to static discharge. Take precautions to discharge any electrostatic charge from your person before and while handling components with your hands or any tools. Use an anti-static wrist-strap.
- The system only be installed in a clean, dry environment. The operating temperature is 10° to 35° C (50° to 95° F), with operating relative humidity at 20 to 95%, non-condensing.
- Do not install hardware in an enclosed cabinet or other small area without ventilation.
- Ensure correct lifting methods are used when handling hardware. Special care should be taken when removing hardware from its packaging and positioning it into its required location. When lifting hardware, two people at either end should lift slowly with their feet spread out to distribute the weight. Always keep your back straight and lift with your legs.
- When installing the system as a rack-mounted component, ensure that all Nexsan-supplied mounting fixtures are secure. All bolts and screws should be fully tightened. Failure to comply with this may result in the unit not being fully supported in the rack and could lead to the product falling from the rack causing personal injury or falling onto other rack components.
- Ensure that the rack is sufficiently stable by having wall anchors and/or stabilizing legs, and that the floor supporting the rack has sufficient strength for the overall weight loading.
- Only a fully-trained Service Engineer is authorized to disassemble any other part of the hardware, and then only when the hardware is powered off.
- The system has multiple power connections; as a result, you must remove all power leads to completely isolate the power and always use the IEC power cords which are supplied with the system.



CAUTION: All Nexsan Unity Storage Systems are hot-pluggable. However, new expansions must be powered on AFTER you connect it to the existing system.

Chapter 1

Introducing Unity

Welcome to Unity—Nexsan Technologies, Inc.'s patented web-based user interface for managing your Nexsan Unity storage infrastructure.

Unity 6.0 introduces the new Home Directories feature, including a setup wizard that automates creation of file systems dedicated to home folders for Active Directory users. Also, the Unity Firmware updater and Performance Monitor are now available in the new HTML5 user interface format. We also added fast Ethernet support, up to 40GbE, along with ACOU, version 2, with client triggered expiration, support for archiving access control lists (ACLs), and several other enhancements and bug fixes. Please see the Release Notes for details.

This guide provides procedures and guidelines to help you set up and manage Unity Storage Systems and Unity Storage Expansions.

Unity delivers unified NAS (CIFS/NFS) and block-level (iSCSI) storage with ground-breaking performance for mid-sized organizations looking for true enterprise-class features. Seamless, Enterprise n-Way file synchronization across distributed primary storage gives IT additional functionality to streamline processes such as data acquisition from remote locations, content distribution, business continuity, and disaster recovery. Unity features FASTier acceleration technology, which uses both DRAM and flash SSD to optimize block and file operations in a fault tolerant architecture.

Unity provides an easy-to-manage storage solution for protecting, managing, and sharing critical information across Microsoft Windows, UNIX, and Linux clients over a local area network (LAN) or wide-area network (WAN). Unity offers a streamlined design, an optimized embedded operating system (NestOS), and an intuitive web-based interface for easy installation, fast deployment, and administration. It adds high-capacity, high-availability storage within the framework of your current network infrastructure.

Unity provides CIFS and NFS shared folders as well as iSCSI volumes, with a comprehensive set of data management features—including: remote data replication with easy restore and failover capabilities, high-availability Active/Active Clustering with automatic failover, snapshots for point-in-time recovery of individual files or an entire file system, and NDMP (Network Data Management Protocol) backup support.

This section includes these topics:

New features and enhancements	20
Key features	22
Typical Unity Storage System deployments	32

New features and enhancements

This topic provides an overview of the new features, enhancements, and resolved defects by release.

Unity 6.0

The following new features and enhancements have been added in Unity 6.0:

Feature	Description
Home Directories	The Home Directories feature provides a wizard that enables you to automatically create a home folder for each user in the associated group on a client system. The Home Directories wizard steps you through adding administrators and user groups, and then instantly creates home folders for every user in the assigned user group. The feature requires that Unity and the client system be configured to use Active Directory for authentication.
Fast Ethernet connectivity, up to 40 GbE	To support faster Ethernet connectivity on Unity, we tested and qualified the Intel® XL710-QDA2 dual-port Ethernet Converged Network adapter, with supported speeds of up to 40 GbE.
Firmware updater and Performance monitor in HTML5	The Unity Firmware updater has been converted to the HTML5 UI format. Also, the Unity Performance Monitor now displays live and historical performance information in graphical format in the HTML5 UI. The Performance Monitor provides a visual display of built-in performance counters, featuring graphical and tabular views of the data.
Improvements for Assureon Client on Unity (ACOU), version 2	<p>We made the following enhancements for using the Assureon Client on Unity:</p> <ul style="list-style-type: none"> • client triggered expiration (CTE). • archiving Access Control Lists (ACLs). • control to limit shortcutting files based on size. <p>We also made improvements to the restore shortcuts mechanism and the real time mechanism, and added various enhancements and fixes that will improve ACOU performance and stability.</p>
Enhancements	
ATTO 10GbE NIC support	We added support for the ATTO FastFrame dual-port Ethernet adapter, with both RJ45 (copper) and SFP (fibre) connectivity.
ATTO 16/32GbE FC cards firmware upgrades	We tested and qualified a new firmware version for the ATTO 16/32 GbE Fibre Channel cards. This firmware improves performance and stability.
FW upgrade on the on-board SAS controllers	A new firmware version for the on-board SAS controllers was qualified on the Unity 2200, Unity 4400, and Unity 6900 Storage Systems. The new firmware provides stability and performance improvements.

Feature	Description
BIOS v 3.1 and IPMI v3.7 were qualified	New firmware releases of the BIOS and IPMI software were qualified for the Unity 2200, Unity 4400, and Unity 6900 Storage Systems. These new releases provide performance and stability improvements.
SMB/NFS joining Active Directory	This release removes the constraint to have SMB version 1 enabled on the Windows Active Directory for Unity to join the domain.
n-Way Sync	<p>We made the following improvements to n-Way Sync:</p> <ul style="list-style-type: none"> • added support to assist with initial data migration by allowing the replicator mechanism to obtain data from an alternate source (such as a storage expansion) rather than the replication partner. • resolved a potential deadlock situation. • stability and performance improvements.
E-Series firmware releases qualified	<p>We qualified and tested the following E-Series firmware releases with Unity:</p> <ul style="list-style-type: none"> • E-Series V/VT (6Gb) 1208.1 FW • E-Series P 1304 FW

Key features

Unity includes these features:

Active/Active Clustering

Unity has built-in Active/Active Clustering capability, whereby both controller nodes on Unity operate in active mode—that is, both controllers can actively serve data in parallel—in addition to providing full redundancy in the event that one of the controller nodes fails. Unity's Active/Active Clustering configuration provides both high-availability and load balancing for your Nexsan storage infrastructure.

For additional details and examples of Active/Active clustering, see [Clustering](#) on page 293.

All Ports / All LUNs

All Ports / All LUNs is a feature used in a dual-controller, active-active cluster to provide high-availability during failover. All LUNs can be accessed through all Fibre Channel ports. This feature also provides load balancing across the two controllers, thus improving the overall performance of the cluster.

Each controller hosts a set of LUNs, which can be accessed through the controller's Fibre Channel ports. The direct connection between the controller managing the LUNs and the host is referred to as the *Optimized Path*. The *All Ports / All LUNs* feature creates an additional access path from one controller to the set of LUNs hosted by the other controller; this is referred to as the *Non-Optimized Path*. As a result, this feature provides uninterrupted access to the LUNs by using multipathing.

Configurable RAID

Unity supports RAID levels 5, 6, and 10, and allows you to specify the RAID configuration during the initial setup of the system; it then automatically creates the corresponding number of volumes, based on your selection. Unity also allows you to specify the RAID configuration for each externally-connected storage device (Nexsan E18™, Nexsan E48™, Nexsan E60™, or the Nexsan Unity Storage Expansion).

Data replication (asynchronous and synchronous)

Unity provides intuitive, wizard-based configuration tools to help you set up asynchronous or synchronous replications of your data. With asynchronous data replication, you can set up an off-site (remote) Unity to protect your data when disaster strikes. The asynchronous replication feature delivers high-performance asynchronous replication of your data over both LAN and WAN networks, providing protection from site-specific and regional disasters. The asynchronous replication feature only replicates the data that changed since the last replication. It also includes a failover mechanism that allows you to seamlessly transition data access and system activity to the remote site when your primary Unity becomes unavailable. You can failover the entire site, or a subset of your storage pools, to the remote Unity.

The asynchronous data replication feature allows you to configure off-site data replications separately for each storage pool on the primary Unity. In addition, the asynchronous data replication feature allows you to manually transfer data on Unity to an external storage device for offline replications, and then import the replicated data on the remote site.

With the Synchronous data replication feature, you can mirror data between two Nexsan storage systems connected to Unity via Fibre Channel or SAS. The Synchronous data replication feature essentially mirrors all the data contained in a storage pool between a source Nexsan storage system and a target Nexsan storage system—both of which are connected to Unity via Fibre Channel or SAS.

Dedicated management interface

Unity provides a dedicated management network interface for managing Unity. The dedicated management interface allows the storage/network administrator to manage Unity storage infrastructure from a different subnet without the need for routing. The dedicated management network interface only carries management traffic; for example: access to Unity, SMTP, SNMP, and SSH. All network traffic related to data access

(access to shares and iSCSI LUNs) is restricted to the other interfaces.

FASTier Read/Write caching

Unity includes support for Nexsan's FASTier™ cache devices which provide non-volatile high-speed cache memory. The FASTier read, write, or read/write caching mechanism enhances the performance and speed for a storage pool.

- FASTier read cache stores frequently-read chunks of data to accelerate read operations on the system.
- FASTier write cache accelerates synchronous write operations to disk.
- FASTier read/write cache can be used for either read or write cache for the storage pool.

FASTier caching with NVDIMM

The Unity 4000 comes equipped with FASTier write cache. NVDIMM is the non-volatile memory used for FASTier write cache. In the event of a power failure, the NVDIMM's Power Management Unit (PMU) supplies sufficient power for the in-memory data to flush to the NVDIMM's non-volatile internal flash prior to powering off.

FASTier caching with SSD

The Unity 5000 supports read and write cache. FASTier cache devices are available for purchase as optional components for the Unity 5000. For more information, please contact your Nexsan reseller or Nexsan Support Representative.

FASTier caching with NVRAM

Many Unity Storage Systems come equipped with FASTier write cache. In the event of a power failure, the Unity Vault Protection Module provides power. When this occurs, the Unity System transfers in-memory cached data to an internal SSD in order to prevent data loss. Once power is restored, the system transfers the data stored on the SSD to disk. The system also mirrors in-memory cached data to the peer controller to protect against controller failure.

See [FASTier caching by platform](#) on page 28.

File System creation and management

Unity provides an intuitive wizard-based configuration tool allowing you to create shares and expose them to CIFS and NFS clients of Unity; it also allows you to allocate storage, manage space usage quotas, and configure user-level access permissions for each share that you create.

Home Directories

The new Home Directories feature enables you to quickly create a file system with Active Directory administrators and user groups, and automatically creates a home folder for each user in the associated group.

LUN creation and management

Unity provides an easy-to-use wizard-based configuration tool for creating iSCSI LUNs in storage pools. The wizard-based configuration tool lets you assign each LUN to an iSCSI target on the system; initiators can then connect to the LUN through its target. When creating a LUN, you can use the storage pool's default iSCSI target to assign the LUN to, or create up to 256 targets per storage pool. Nexsan Unity also supports CHAP authentication, both at the target- and LUN-level.

Multi-site management

Unity allows you to manage any number of sites within a single instance of Unity. Every Nexsan Unity site has its own set of resources independent from other sites. This functionality provides a global point of control for managing your Nexsan storage infrastructure across multiple geographic locations.

For details on multi-site management, see [Understanding multi-site implementation](#) on page 28.

n-Way Sync

Unity Enterprise n-Way Sync eliminates the difficulties of remote access to large files with automated persistent replication of datasets to one or many other remote sites. Users have access to data where they need it, when they need it, at LAN-access speeds, while leveraging the organization's secure infrastructure. This assures that information is in sync across multiple sites while data is secured with encryption at rest and in flight.

Report generation

The Unity Reports feature allows you to generate graphical reports detailing storage capacity across Unity infrastructure.

Reports are organized into six different types and provide detailed information about the storage resources in your environment, including space usage consumption for each share and/or iSCSI LUN on Unity, space usage consumption on a per user basis (with user quotas enabled), and overall storage pool capacity and used space. You can select the specific site, storage pool, shares, iSCSI LUNs, and users upon which you want to report.

For detailed information on reports, see [Creating and viewing reports](#) on page 507.

Snapshots

Unity provides continuous data protection with the Snapshots feature, which allows you to capture point-in-time copies of the data. The Snapshots feature includes a comprehensive set of snapshot management tools, including:

- customizable schedules for automatic snapshots;
- the ability to browse the contents of snapshots and restore individual files or folders;
- roll-back a file system and all its contents to a specific point-in-time;
- and configurable auto-deletion policies for snapshots.

Snapshots are explained in greater details in the *Nexsan Unity Snapshots and Replication Guide*.

SNMP and email alerts

Unity provides real-time notices of system events and errors. It keeps you informed of the status of your system via email or an SNMP management system. You can configure and manage SNMP and email alerts, and view system events.

Storage pool creation and management

Unity provides an intuitive wizard-based configuration tool allowing you to group underlying volumes into storage pools on Unity. Unity also provides pool management tools, such as pool scrubbing and customizable schedules for automatic pool scrubs.

Support for NDMP backup solutions

Unity includes an NDMP plug-in that allows you to back up data from Unity to an industry-standard backup and restore solution that supports NDMP. The plug-in preserves all access rights for CIFS and NFS shares on Unity, and uses background snapshots for fast backups.

To set up the NDMP plug-in, see [Setting NDMP configuration options](#) on page 349.

User management and security

You can configure Unity to join a Microsoft Windows Active Directory domain or connect to an LDAP (Lightweight Directory Access Protocol) Directory service. Nexsan Unity provides an intuitive user management tool allowing you to configure site-level, storage pool-level, and share-level access permissions on Unity, for all your corporate Microsoft Windows Active Directory or LDAP Directory service users and groups. Nexsan Unity also provides a mechanism for creating local user and group accounts on Unity if a

connection to a Microsoft Windows Active Directory or an LDAP Directory service is not required or available.

Volume management

Unity provides an intuitive wizard-based tool allowing you to easily replace an existing volume on Unity with a new volume—in the event of hardware failure or system maintenance; Unity automatically transfers your data and settings to the replacement volume.

VSS hardware provider

Unity includes a VSS (Volume Shadow Service) Hardware Provider, which enables VSS clients to create and manipulate shadow copies (point-in-time snapshots) of the data in iSCSI LUNs. Unity's VSS Hardware Provider supports Windows Volume Shadow Copy Service. Unity's VSS Hardware Provider serves as the interface between Windows Volume Shadow Copy Service running on a client system and Unity. Upon receiving instructions from a VSS client to create, mount, and restore snapshots, Unity's VSS Hardware Provider sends the appropriate commands to Unity and returns the result of these commands to the client. Unity's VSS Hardware Provider includes a Windows Shell extension that adds an Unity property page for managing shadow copies on the VSS client.

Web-based user interface

Unity includes Nexsan Unity, Nexsan's patented web-based user interface for managing Unity. Unity provides a hierarchical view of Unity, as well as wizard-based configuration tools for creating storage pools, shares, replication sites, and for performing other storage management tasks on the system.

▶ Related topics:

[Supported features by platform on the next page](#)

[Expansion options by next generation Unity Storage System on page 27](#)

Supported features by platform

This table describes the Unity platforms and their supported features.

Feature	Unity2200	Unity4400	Unity6900
Active/Active clustering	✓	✓	✓
All ports/All LUNs	✗	✓	✓
Configurable RAID	✓ Only after site setup	✓ Only after site setup	✓
Data compression	✓	✓	✓
Event logging and notification	✓	✓	✓
FASTier read cache	✓	✓	✓
FASTier write cache	✓	✗	✗
Fibre Channel	✗	✓	✓
Multi-site management	✓	✓	✓
Performance metrics	✓	✓	✓
Port redundancy (automatic failover for port failure)	✓	✓	✓
Replication: Asynchronous	✓	✓	✓
Replication: Synchronous	✓	✓	✓
Snapshots	✓	✓	✓
User management and security	✓	✓	✓
VSS hardware provider	✓	✓	✓

Expansion options by next generation Unity Storage System

This table lists the next generation Unity Storage Systems and their supported Unity Storage Expansions.

Nexsan Unity Storage Systems	Unity2200X	US224 Storage Expansion	US316 Storage Expansion	US424 Storage Expansion	US460 Storage Expansion
Unity2200	1, plus the front bay	x	x	x	x
Unity4400	x	Up to 3 of any combined Storage Expansions, plus the front bay	Up to 3 of any combined Storage Expansions, plus the front bay	Up to 3 of any combined Storage Expansions, plus the front bay	Up to 3 of any combined Storage Expansions, plus the front bay
Unity6900	x	Up to 8 of any combined Storage Expansions, plus the front bay	Up to 8 of any combined Storage Expansions, plus the front bay	Up to 8 of any combined Storage Expansions, plus the front bay	Up to 8 of any combined Storage Expansions, plus the front bay

Expansion options by Unity 1.0 Storage System

This table describes the Unity 1.0 Storage Systems and their supported Unity Storage Expansions.

	Unity 2000	Unity 4000	Unity5000	Unity 6000
Nexsan E-Series	x	✓ Up to 6 units (2 head units + storages)	✓ Up to 4 units (2 head units + Unity Storage Expansions) (Unity5300)	✓ Up to 9 units (3 head units + Unity Storage Expansions)
Nexsan US224X	x	x	✓ Up to 9 units (Unity5300)	✓ Up to 9 units
Nexsan Unity 2000XC	✓ 1 unit (Unity 2000C)	x	x	x

	Unity 2000	Unity 4000	Unity5000	Unity 6000
Nexsan Unity 2000XP	✓ 1 unit (Unity 2000P)	✗	✗	✗
Nexsan Unity5100X	✗	✗	✓ 1 unit (Unity5100)	✗

FASTier caching by platform

This table describes the Unity platforms and their supported FASTier caching device features.

PLATFORM / CONFIGURATION	FASTier READ CACHE	FASTier WRITE CACHE			
		Size	with NVDIMM	with SSD	with NVRAM
Unity2200	400 GB	8 GB		✓	✗
	400 GB to 800 GB	8 GB	✗	✓	✗
Unity4400	400 GB to 3.2 TB	8 GB		✓	✗
	800 GB to 3.2 TB	8 GB	✓	✓	✗
Unity6900	100 GB to 400 GB (read/write)	N/A	✗	✓	✗

Understanding multi-site implementation



Unity allows you to manage any number of sites within a single instance of Unity. Every Unity site has its own set of resources independent from other sites. This functionality provides a global point of control for managing your Nexsan storage infrastructure across multiple geographic locations.


When adding a site that is the primary site of a replicated site, its replicated counterpart is automatically added as well. The same applies when the site is a secondary site.

Likewise, disconnecting a site that is part of a replicated pair also disconnects the replicated site. If a site disconnects its own replicated site, then only the replicated site is disconnected. However, you must remove the replication beforehand to be able to disconnect a site.

Note If you connect to a site running an older Unity firmware version, you will only have access to features available in that version.

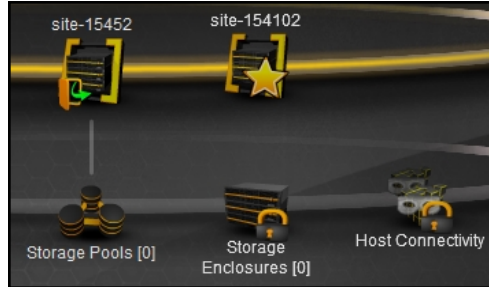
When you connect to a multi-site environment, Unity displays all sites that have been added to the current site, along with their replicated counterpart:

- the active site (the site you are currently logged in) is displayed with a star ;
- the added sites to which the current logged in user have access have regular icons .

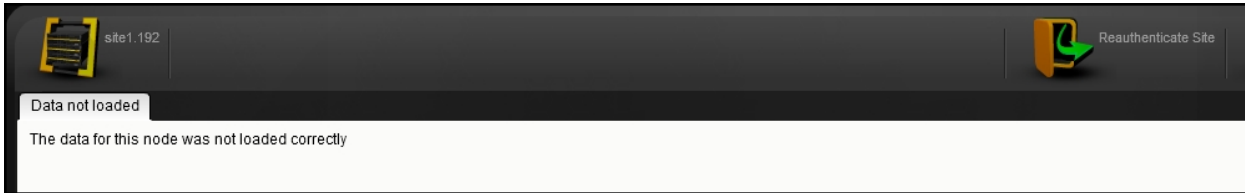
- the added sites that are not directly connected to the currently selected site appear grayed out .

Multi-site implementation characteristics

- If an added site is on a different domain and requires authentication with different credentials than the logged in user, you will see the Re-authenticate icon on the site's node.

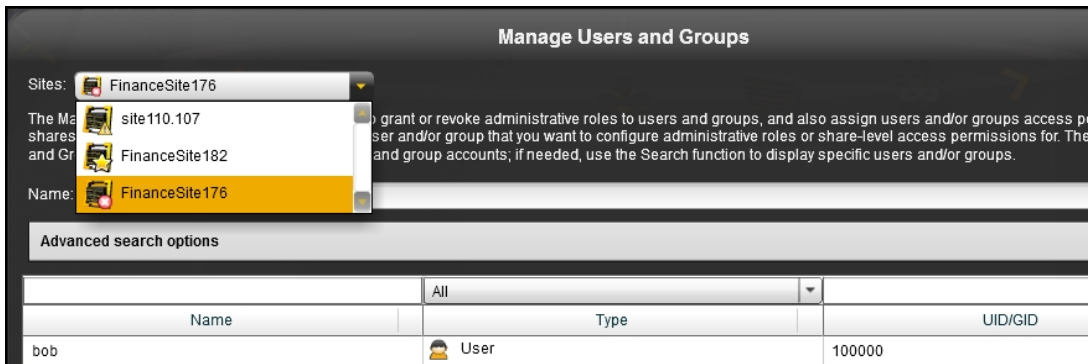


When you click on the Site, you are prompted to enter the credentials of the site. Click the **Re-authenticate** button on the Site's properties panel or use the context menu from the Site's node.



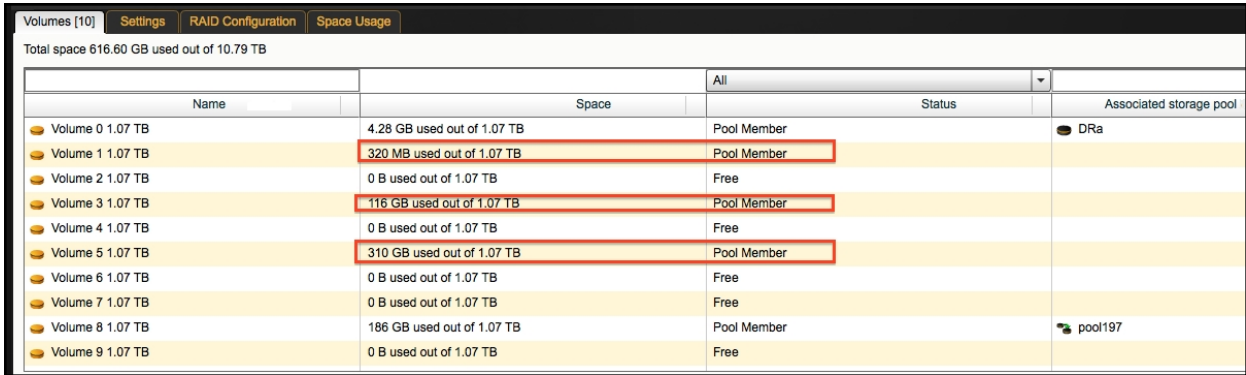
When you enter the credentials, you can store these credentials on Unity for future use. Subsequently, the stored credentials are used to automatically connect to this site.

- A Site Administrator becomes a Pool Administrator on the replicated site.
- If you modify the IP address of a site, Unity automatically reconnects to the new IP address.
- You can manage users and groups for all sites in your implementation from one site by selecting the site from the Manage Users and Groups panel.



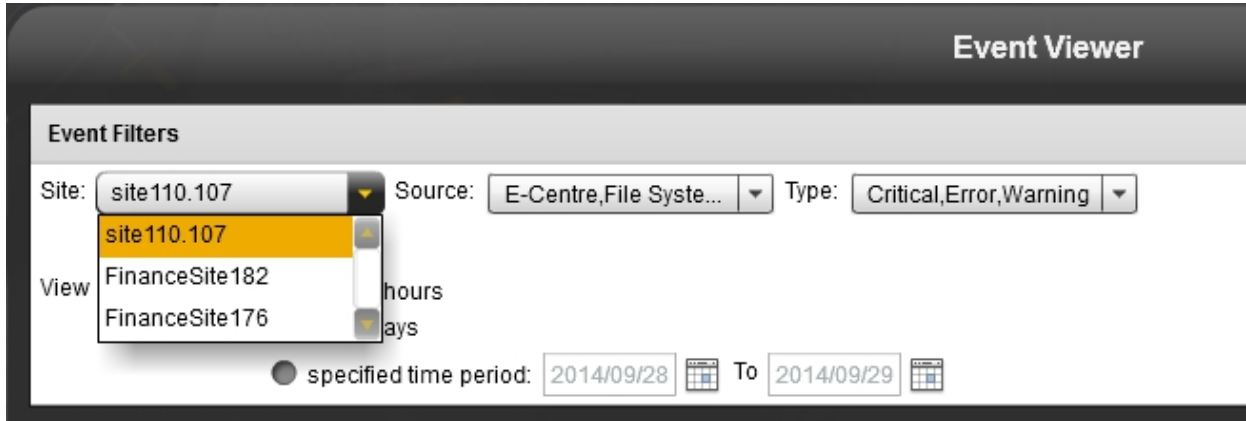
Key features

- On each storage enclosure, you can view space usage and volume information for storage pools in other sites.

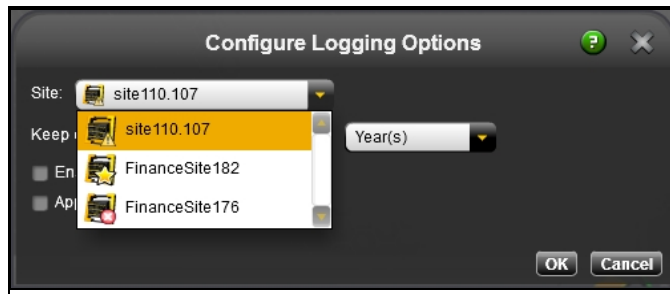


Name	Space	Status	Associated storage pool
Volume 0 1.07 TB	4.28 GB used out of 1.07 TB	Pool Member	DRa
Volume 1 1.07 TB	320 MB used out of 1.07 TB	Pool Member	
Volume 2 1.07 TB	0 B used out of 1.07 TB	Free	
Volume 3 1.07 TB	116 GB used out of 1.07 TB	Pool Member	
Volume 4 1.07 TB	0 B used out of 1.07 TB	Free	
Volume 5 1.07 TB	310 GB used out of 1.07 TB	Pool Member	
Volume 6 1.07 TB	0 B used out of 1.07 TB	Free	
Volume 7 1.07 TB	0 B used out of 1.07 TB	Free	
Volume 8 1.07 TB	186 GB used out of 1.07 TB	Pool Member	pool197
Volume 9 1.07 TB	0 B used out of 1.07 TB	Free	

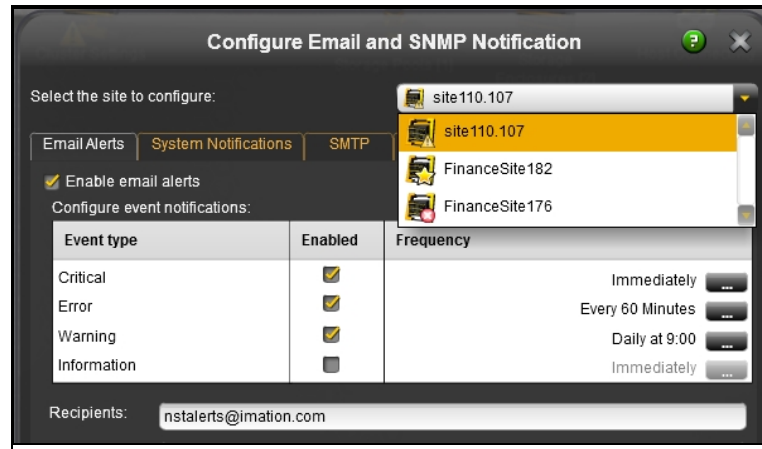
- The Event Viewer allows you to view events for all sites from one site. You need to filter events per site, then you can further filter events by source and type.



- You can configure logging options for all sites in your implementation from one site by selecting the site from the Configure Logging Options dialog box.



- You can configure email, system, SMTP, and SNMP notifications for all sites in your implementation from one site by selecting the site from the Configure Email and SNMP Notification panel.



Multi-site implementation limitations

- Firmware Upgrades cannot be performed from any site. To upgrade a site to the latest firmware version, you must log in to that site directly, then run the Unity Firmware Updater.
- CHAP users are managed per site. To create CHAP users for a specific site, you must log in to that site directly and open the Manage CHAP users panel from that site.
- The Performance Monitor does not allow you to view performance statistics for all sites. To view statistics for a site, you must click on that site's node, then launch the Performance Monitor from the **Tools** menu.
- You cannot completely remove a site connected to multiple sites at once. You must disconnect all sites connected to that site. For details, see [Disconnecting sites in a multi-site implementation](#) on page 360.

Typical Unity Storage System deployments

The following sections provide connection details and concepts for deploying Unity v. 6.0 systems.

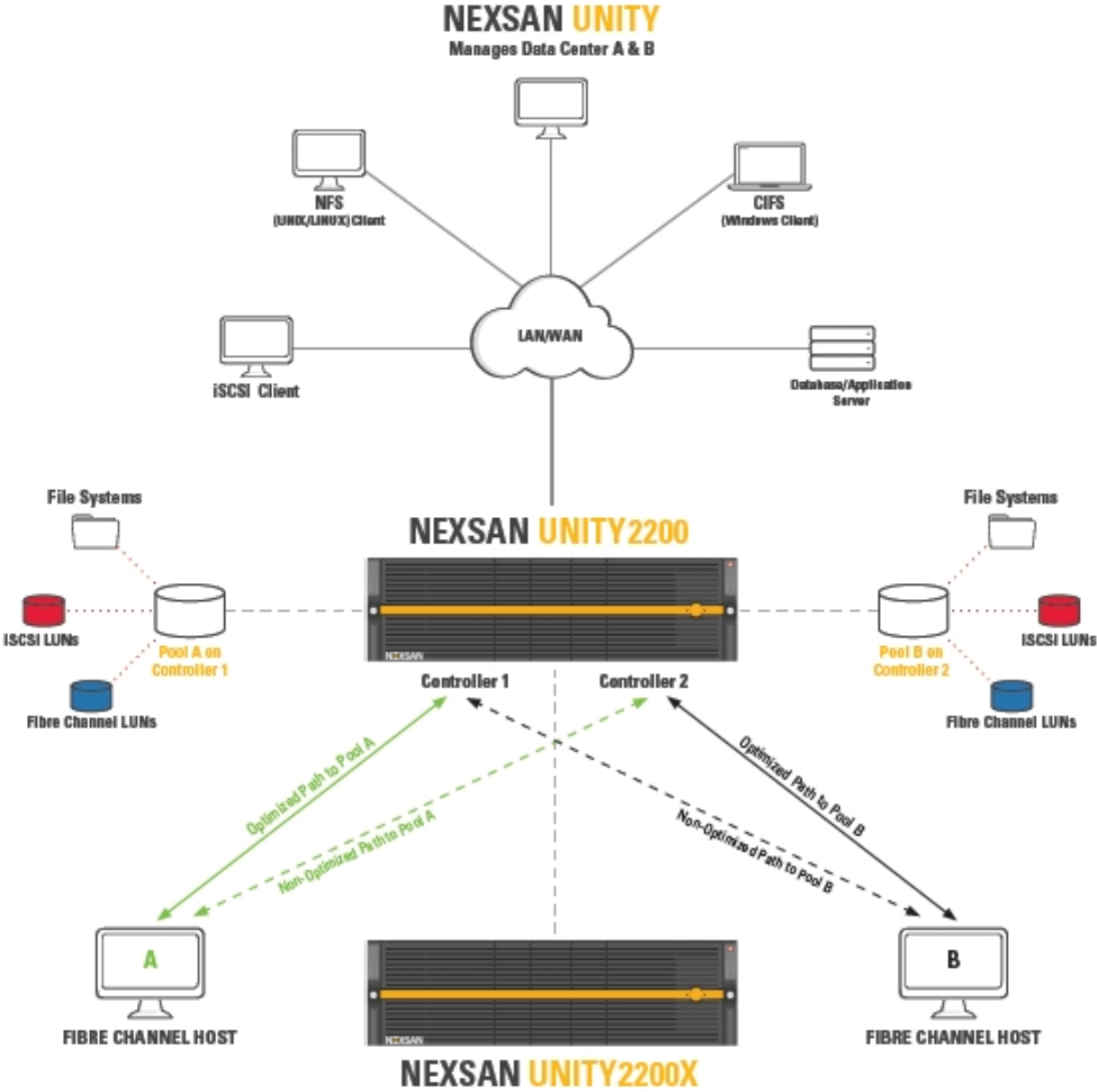
Unity2200 deployment

This diagram provides an example of Unity2200 deployment, with iSCSI and Fibre Channel LUNs. This deployment includes data replication within the same site. The configuration diagram illustrates expandable NAS (CIFS/NFS) and block-level (iSCSI and Fibre Channel) storage by connecting a Unity2200 to a Unity2200X Unity Storage Expansion via SAS.

The configuration diagram also illustrates chassis inter-connectivity to provide uninterrupted access to LUNs. The LUNs hosted by each controller can be accessed through the controller's Fibre Channel ports and iSCSI connections. The direct connection between the Unity2200 controller managing the LUNs and the Fibre Channel host is referred to as the *Optimized Path*. The *All Ports / All LUNs* feature creates an additional access path from one controller to the set of LUNs hosted by the other controller; this is referred to as the *Non-Optimized Path*.

For simplicity, the diagram below only shows one Fibre Channel host connected to the Unity2200, with a storage pool hosted on Controller 1 and a storage pool hosted on Controller 2. In this example, the *Optimized Path* to Storage Pool A goes directly to Controller 1, and the *Non-Optimized Path* goes through Controller 2 to go to Controller 1.

Figure 1-1: Typical Unity2200 deployment



1

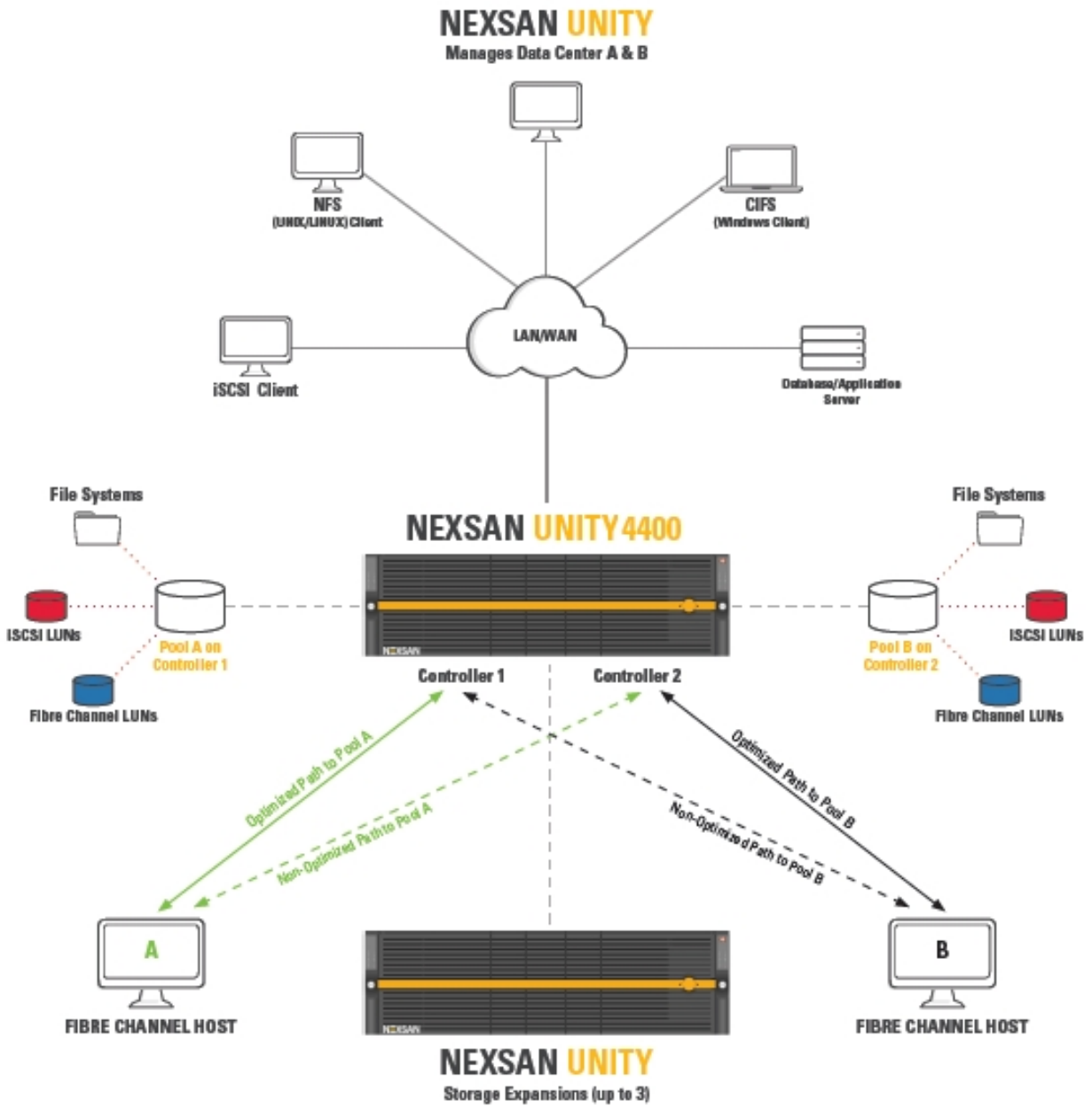
Unity4400 deployment

This diagram provides an example of Unity4400 deployment, with iSCSI and Fibre Channel LUNs. This deployment includes data replication within the same site. The configuration diagram illustrates expandable NAS (CIFS/NFS) and block-level (iSCSI and Fibre Channel) storage by connecting a Nexsan Unity Storage Expansion 316 via SAS to the Unity4400.

The configuration diagram also illustrates chassis inter-connectivity to provide uninterrupted access to LUNs. The LUNs hosted by each controller can be accessed through the controller's Fibre Channel ports and iSCSI connections. The direct connection between the Unity4400 controller managing the LUNs and the Fibre Channel host is referred to as the *Optimized Path*. The *All Ports / All LUNs* feature creates an additional access path from one controller to the set of LUNs hosted by the other controller; this is referred to as the *Non-Optimized Path*.

For simplicity, the diagram below only shows one Fibre Channel host connected to the Unity4400, with a storage pool hosted on Controller 1 and a storage pool hosted on Controller 2. In this example, the *Optimized Path* to Storage Pool A goes directly to Controller 1, and the *Non-Optimized Path* goes through Controller 2 to go to Controller 1.

Figure 1-2: Typical Unity4400 deployment



1

Unity6900 deployment

This diagram provides an example of typical Unity6900 deployment, with iSCSI and Fibre Channel LUNs. This deployment includes data replication within the same site. Both the primary and secondary controllers are connected to two Unity Storage Expansions.

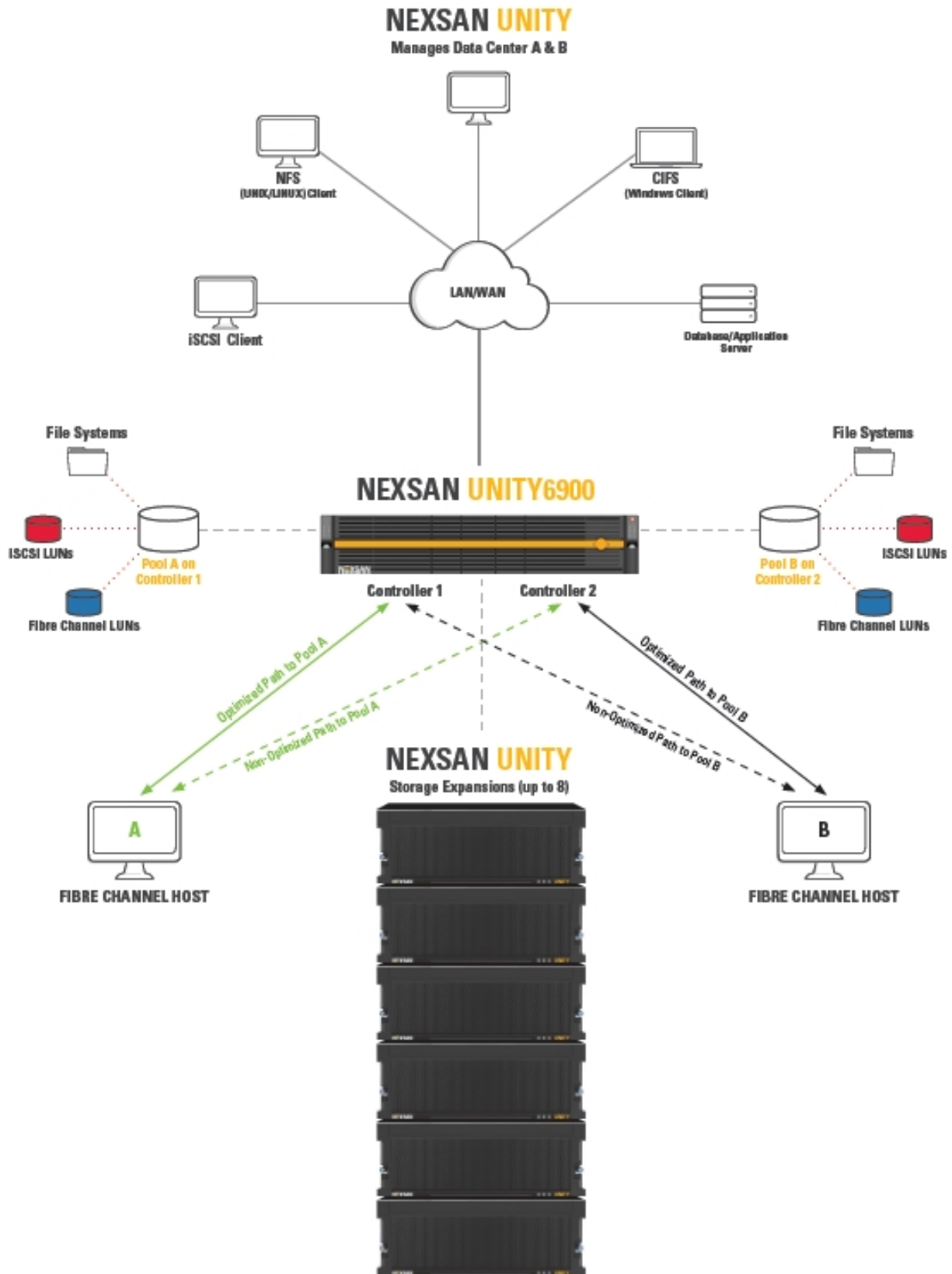
The Nexsan Unity6900 configuration diagram illustrates expandable NAS (CIFS/NFS) and block-level (iSCSI and Fibre Channel) storage by connecting Nexsan external storage via SAS to multiple Unity Storage Expansions.

The Nexsan Unity6900 configuration diagram also illustrates chassis inter-connectivity to provide uninterrupted access to LUNs. The LUNs hosted by each controller can be accessed through the controller's Fibre Channel ports and iSCSI connections. The direct connection between the Unity6900 controller managing the LUNs and the Fibre Channel host is referred to as the *Optimized Path*. The *All Ports / All LUNs* feature creates an additional access path from one controller to the set of LUNs hosted by the other controller; this is referred to as the *Non-Optimized Path*.

The Unity6900 comes equipped with FASTier write cache—non-volatile high-speed cache memory—which keeps a certain amount of I/O operations in memory in case of:

- power outage: the data gets written to disk.
- controller failure or network connection loss between the controllers: the data gets written to disk while the failover process occurs on the other controller.

Figure 1-3: Typical Unity6900 deployment



Chapter 2

Setting up the site

Before you can use Unity to manage your storage environment, you must perform its initial setup using the Unity Site Setup Wizard.

Note If you did not connect the Primary Data Network Interface (nx0) before running the Site Setup Wizard, you will need to validate nx0 in Unity to be able to use Unity.

▶ **To start the initial setup using a web browser:**

1. Open a web browser on a system that is installed on the same network (and subnet) as Unity.
2. In the web browser's address bar, type the Management Virtual IP address (that you set on the nx99 interface), and then press Enter. This starts the Site Setup Wizard.
3. Click **I accept the terms of the license agreement** and then click **Next**. The Nexsan Unity Site Setup Wizard displays the first step in the set up process.

▶ **To start the initial setup using the Discovery tool:**

1. In the Discovery Wizard, select Unity that you want to set up.
2. Click the Launch Nexsan Unity button.
The Nexsan Unity Site Setup Wizard opens and the end-user license agreement displays.
3. Click **I accept the terms of the license agreement** and then click **Next**. The Nexsan Unity Site Setup Wizard displays the first step in the set up process.

Step 1: Setting the password for the Nexsan Unity administrator	40
Step 2: Configuring the site information	40
Step 3: Configuring network settings	42
Step 4: Configuring IPMI settings	43
Allocating storage on the Unity 2000	43
Allocating storage on the Unity 4000	44
Allocating storage on the Unity 5000/Unity 6000	44
Step 6: Verifying configuration settings	46
Step 7: Viewing configuration results	47

Step 1: Setting the password for the Nexsan Unity administrator

Unity is shipped with the built-in Unity Administrator account, **nxadmin**. The Unity Administrator has unrestricted access to Nexsan Unity, including setting site and storage pool administrators for the system and accessing the Unity's nxadmin command-line interface (CLI). The Unity Administrator account cannot be removed from the system.

► **To configure the password for the Nexsan Unity Administrator:**


Set the Password for the E-Centre Administrator Account

This NST appliance is shipped with the built-in E-Centre Administrator account, nxadmin, which has unrestricted access to E-Centre. Please specify a password for the nxadmin account. If the NST appliance has a Nexsan Storage System(s) (Nexsan E18, E48, or E60) connected, E-Centre will set the storage system's administrator password to the same value as the nxadmin password.

Account:

Password:

Confirm password:



1. Type a password in the **Password** field.

The nxadmin password must contain a minimum of 6 characters and a maximum of 16 characters. It must contain one upper-case letter, one lower-case letter, AND one numeric character OR one of these special characters:

! \$ % & ' () * + , - . < > [] ^ _ ` { | } ~

For example, this is a valid password:

ITUnow\$

But this is not a valid password:

ITUnow

2. Type the password again in the **Confirm password** field.
3. Click the **Set Password** button to configure the password for the Unity Administrator.

When the password is configured, the Site Setup Wizard automatically moves forward to [Step 2: Configuring the site information](#) below.

Step 2: Configuring the site information

Unity allows you to manage multiple Unity sites from a single Unity session (multi-site management); the site name allows you to identify each Unity in a multi-site environment.

► To configure site information:

1. Type the site name in the **Site name** field; make sure that the new name adheres to these restrictions and conventions:

- Spaces are allowed
- The [site name](#) can contain up to a maximum of 16 characters—including spaces.
- The name must start with an (upper-case or lower-case) alphabetic or numeric character; and, with the exception of the hyphen (-), and period (.), the name can only contain alphanumeric characters, without spaces.

These characters are NOT allowed:

" / \ [] : ; | = , + * ? < >

2. (Optional) From the **Server Time Zone** drop-down list, select the time zone where Unity is installed. The default time zone setting is Eastern Time (US and Canada).

Regardless of the time zone setting that you set, when you access Unity from a client system using Nexsan Unity, Nexsan Unity automatically converts all date and time strings to the client's local time.

Note For the new time zone settings to take effect, reboot Unity after completing the Site Setup Wizard.

Step 3: Configuring network settings

- (Optional) Enable the CallHome log collection settings. The CallHome feature allows Nexsan Technical Support personnel to monitor the state of Unity using the collected system logs, without customer notification. You can enable this feature at a later time, using Unity or the nxadmin Command-line interface.
 - Enable autolog schedule:** The CallHome feature packages and sends all system logs based on a pre-defined schedule.

If the Autolog schedule has not been configured for the system, you can enable it later using the `autolog` command in the nxadmin CLI.
 - Enable event-driven CallHome to send system logs based on critical events:** This function sends system logs when major issues are detected, based on events and diagnostics.
- Click the forward arrow to continue to [Step 3: Configuring network settings](#) below.

Step 3: Configuring network settings

For more information about network interfaces and IP addresses, see [Understanding Network interfaces and required IP addresses](#) on page 311.

► To configure network settings:

Configure Network Settings

Please enter the appropriate network settings for this NST appliance. When you have finished, click Apply to set the network configuration on the system.

The screenshot shows a web form titled "Configure Network Settings" with three main sections. Section 1, "Primary Data Network Interface (nx0)", has a yellow highlight around the IP address field for Controller 1 (172.21.12.33) and a blue arrow labeled "1" pointing to it. Section 2, "Management Interface (nx99)", has a blue arrow labeled "2" pointing to the Controller 1 IP field (172.22.10.33). Section 3, "Gateway and DNS (for all network interfaces)", has a blue arrow labeled "3" pointing to the Default Gateway field (172.21.12.254). The form also includes fields for Controller 2, Intersite virtual IP, Pool Resource Group 1 and 2 virtual IPs, and Subnet Mask for both interfaces.

Field	Value
Management Interface (nx99) - Controller 1 (ES223344-001-01)	172.22.10.33
Management Interface (nx99) - Controller 2 (ES223344-001-02)	172.22.10.34
Management Interface (nx99) - Management virtual IP	172.22.10.200
Management Interface (nx99) - Subnet Mask	255.255.0.0
Primary Data Network Interface (nx0) - Controller 1 (ES223344-001-01)	172.21.12.33
Primary Data Network Interface (nx0) - Controller 2 (ES223344-001-02)	172.21.12.34
Primary Data Network Interface (nx0) - Intersite virtual IP	172.21.12.200
Primary Data Network Interface (nx0) - Pool Resource Group 1 virtual IP	172.21.12.203
Primary Data Network Interface (nx0) - Pool Resource Group 2 virtual IP	172.21.12.204
Primary Data Network Interface (nx0) - Subnet Mask	255.255.0.0
Gateway and DNS (for all network interfaces) - Default Gateway	172.21.12.254
Gateway and DNS (for all network interfaces) - Preferred DNS server	172.21.12.99
Gateway and DNS (for all network interfaces) - Alternate DNS server	

- Type the IP address for the primary data network interface (nx0) in the corresponding fields.
- Optionally, modify network settings for the management interface (nx99).
- Type an IP address for the Default gateway for Unity and for the preferred DNS server. (Optionally) Enter the IP address of the alternate DNS server. These settings are applied globally to all network interfaces on the system.
- Click **Apply** to set the network configuration.

- When the Site Setup Wizard successfully configures the network settings on the system, a confirmation message displays. Click **OK**. The site setup proceeds to [Step 4: Configuring IPMI settings](#) below.

Step 4: Configuring IPMI settings

This step prompts you to configure the Intelligent Management Interface ([IPMI](#)) settings. For more details, see [Setting or modifying IPMI settings](#) on page 316.

► To configure IPMI settings:

- Type the relevant IPMI IP address in the corresponding field for Controller 1.
- Type the relevant IPMI IP address in the corresponding field for Controller 2.
- Type the IP address of the IPMI subnet.
- Type the IP address for the IPMI gateway for Unity.
- Type a password in the **Password** field (required to access the IPMI web-based interface).
- Retype the password to confirm it in the appropriate field.
- Click the forward arrow to continue.

► What's next:

For Unity 2000, proceed to [Allocating storage on the Unity 2000](#) below.

For Unity 4000, proceed to [Allocating storage on the Unity 4000](#) on the next page.

For NST5000/NST6000, proceed to [Allocating storage on the Unity 5000/Unity 6000](#) on the next page.

Allocating storage on the Unity 2000

The Site Setup Wizard automatically discovers the Unity 2000XC or Unity 2000XP Unity Storage Expansion connected to Unity and the Storage Configurator opens.

The Unity 2000C is pre-configured for RAID6, with two RAID sets and no hot spare. The Unity 2000P is pre-configured for RAID10, with three RAID sets and one hot spare. You cannot change these settings during the site setup, but you can change them afterwards.

For information on RAID levels, see [Mixing volumes with different RAID levels](#) on page 98.

► To allocate storage:

Configure Storage

Select the RAID level and the number of RAID sets that you want E-Centre to configure on your storage.

NST2000C has 18 available drives.

RAID level: RAID6

Number of RAID sets: 1

Hot spares: 1


Friendly Name:

Summary:
1 RAID set will be created with 17 drives.
1 drive will be assigned as a hot spare.

OK Cancel

1. Click **OK** to close the Storage Configurator.
2. Click the forward arrow to proceed to [Step 6: Verifying configuration settings](#) on page 46.

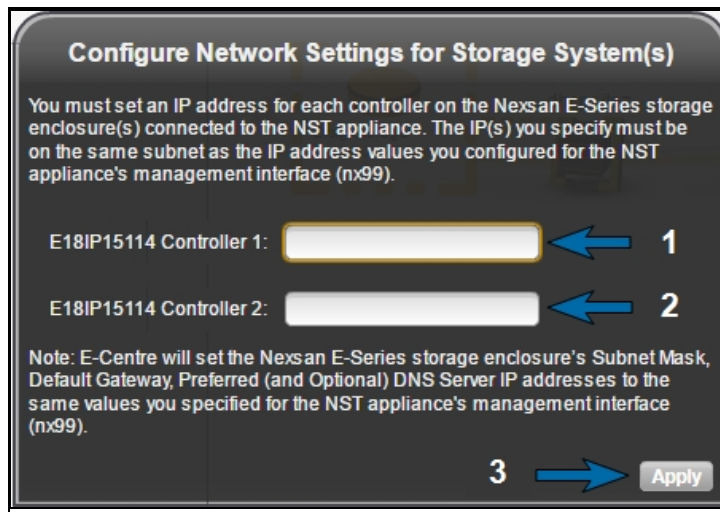
Allocating storage on the Unity 4000

If the Site Setup Wizard fails to discover the Unity Storage Expansion that you want to allocate to the site, make sure the Unity Storage Expansion is properly connected, and that it is powered on; then, click the refresh button .

RAID settings are preconfigured on Nexsan E-Series for the Unity 4000. You only need to set the IP addresses. The Nexsan E-Series storage enclosures have DHCP enabled by default. The Site Setup Wizard prompts you to specify a static IP address(es) for each controller on the E-Series storage enclosure.

For information on RAID levels, see [Mixing volumes with different RAID levels](#) on page 98.

► **To set static IP addresses for the Nexsan E-Series controllers:**




1. Type a valid IP address in the **Controller 1** field.
2. Type a valid IP address in the **Controller 2** field.
3. Click the **Apply** button to set the IP address(es) on the Nexsan E-Series storage enclosure. Nexsan Unity automatically sets the Subnet mask, Default gateway, and Preferred DNS server on the storage enclosure.
4. Repeat these steps for each storage enclosure connected to the Unity 4000 that you want to configure and allocate to the site.

Note If you selected multiple devices to configure in step 1, the Configure Network Settings for Storage System(s) dialog box automatically opens again for each enclosure.

When you finish setting the controller IP addresses for the Nexsan E-Series storage enclosures, the Site Setup Wizard automatically moves forward to [Step 6: Verifying configuration settings](#) on page 46.

Allocating storage on the Unity 5000/Unity 6000

The Site Setup Wizard automatically discovers all Nexsan E-Series storage enclosure(s) connected to Unity and then displays the Storage Configurator, where you configure RAID settings for the E-Series storage enclosure(s).

If the Site Setup Wizard fails to discover the E-Series storage enclosure that you want to allocate to the site, make sure the E-Series storage enclosure is properly connected to Unity, and that it is powered on; then, click the refresh button .

Notes:

- The Storage Configurator can only configure RAID settings for one storage enclosure at a time. If you select multiple storage systems in the **Available Storage Systems** list to allocate to the site, the Site Setup Wizard launches the Storage Configurator for the first storage system in your selection, and when you finish configuring the storage system, the Site Setup Wizard opens the Storage Configurator again for the next storage system in your selection, and so on.
- You are required to allocate at least one storage device to the site during the site setup process; you can add other storage devices later once the site is configured.

► To configure storage settings:

Allocate Storage

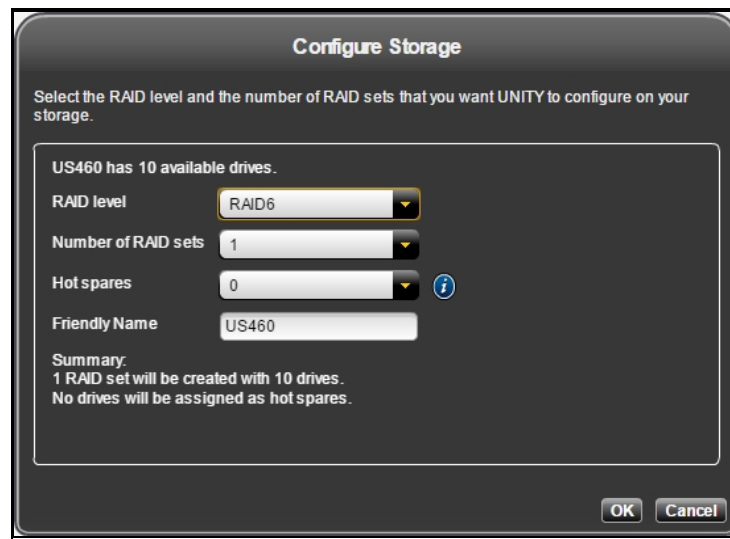
Allocate storage devices to the site by dragging devices to the area indicated below.



1. In the **Available Storage Devices** list, select the storage device(s) that you want to configure and allocate to the site and drag it to the area indicated. Hold down SHIFT or CTRL and click the left mouse button to select multiple devices; the Site Setup Wizard automatically displays Nexsan Unity's Storage Configurator.

Note If Unity has only one storage device installed or connected, the Storage Configurator opens automatically when this step displays.

Figure 2-1: Site Setup Wizard, step 7: Storage Configurator



2. From the **RAID level** drop-down list in the Storage Configurator, select the RAID level—5, 6, or 10—that you want Nexsan Unity to configure on your storage. The Storage Configurator automatically recommends the optimal RAID settings (**Number of RAID sets** and **Hot spares**) for the RAID level you select; you can adjust these settings, or keep the recommended (optimal) settings.
3. From the **Number of RAID sets** drop-down list, select the number of RAID sets. The Storage Configurator creates a volume for each RAID set that you specify.

For information on volumes and RAID levels, see [Mixing volumes with different RAID levels](#) on page 98.

4. From the **Hot spares** drop-down list, select the number of hot spare disks that you want the Storage Configurator to assign to the system. If a disk on the system fails, Nexsan Unity automatically replaces the failed disk with the hot spare, allowing the system to continue operating. Depending on your RAID level and RAID sets selections, and the number of disks available on the system, you may only be able to assign one disk as a hot spare.

Note The Storage Configurator automatically assigns any unallocated disks as hot spares. For example, if you have 2 hot spare disks available after setting the RAID level and RAID sets, and you select only 1 disk as a hot spare assignment, the Storage Configurator automatically assigns the second unallocated disk as a hot spare to the RAID array.

As you select the RAID level, the number RAID sets, and the number of hot spares to create on the storage device, the Summary section on the Storage Configurator panel automatically updates to display how your selections impact disk assignment on your storage.

5. (Optionally) Enter a friendly name for the storage device.
6. Click the **OK** button to save your selections and close the Storage Configurator.
7. Repeat these steps for each storage device connected to Unity that you want to configure and allocate to the site.

Note If you selected multiple devices to configure in step 1, the Storage Configurator automatically opens again for each device.

If Unity has a Nexsan E-Series storage enclosure connected to it—and it has DHCP enabled—the Site Setup Wizard prompts you to specify a static IP address(es) for the controller(s) on the storage enclosure. You **MUST** set a static IP address(es) for the storage enclosure.

► **To set a static IP address(es) for Nexsan E-Series storage:**

1. Type a valid IP address in the **Controller 1** field.
2. If applicable, type an IP address in the **Controller 2** field.
3. Click the **Apply** button to set the IP address(es) on the Nexsan E-Series™ storage system. Nexsan Unity automatically sets the Subnet mask, Default gateway, and Preferred DNS server on the storage system according to the values that you configured for Unity.

Once the Site Setup Wizard sets static the IP address(es) on the Nexsan E-Series™ storage system, the Storage Configurator opens, where you configure RAID settings for the storage system.

When you finish configuring and allocating storage, the Site Setup Wizard automatically moves forward to [Step 6: Verifying configuration settings](#) below.

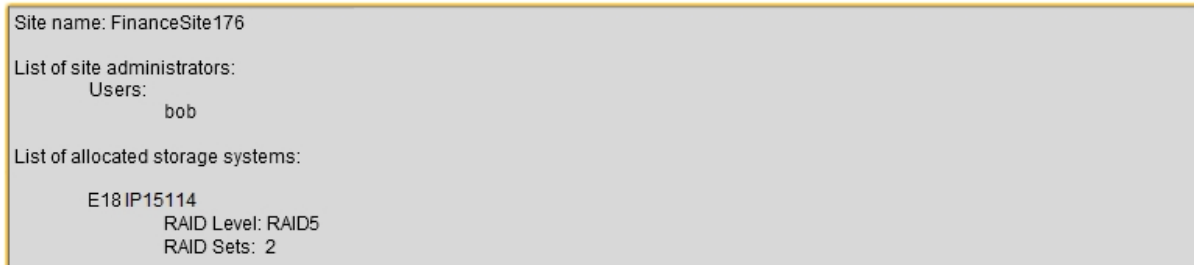
Step 6: Verifying configuration settings

This step of the Site Setup Wizard summarizes your configuration settings and applies them to the system. Review the summary carefully before applying configuration settings.

► **To change a configuration setting:**

Verify Settings

Please verify your configuration settings. If you want to change a setting, click the back arrow to navigate to the relevant configuration panel. Or, click the step identifier at the top of the wizard panel to go back to a specific step.



- Click the back arrow to navigate back to the corresponding configuration step.
Or
 - Click the step identifier at the top of the Site Setup Wizard panel to go back to a specific step. For example, if you want to change the site name, click **Step 2**.
- **To finalize the site setup:**
- If you are satisfied with the configuration settings, click the **Start** button at the bottom of the panel. The Site Setup Wizard automatically moves forward to [Step 7: Viewing configuration results](#) below, where you can view progress as the Site Setup Wizard configures Unity.

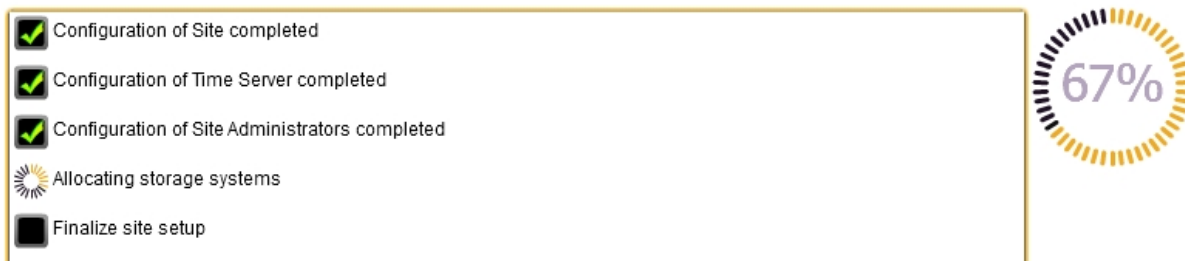
Step 7: Viewing configuration results

The Site Setup Wizard displays the progress of the setup process as the system applies the configuration settings.

The Site Setup Wizard displays any error events that the system encounters during the setup process. You can view more details about an error event by expanding the corresponding entry.

Configuration Results

Applying settings:



► **To view more details for an error event:**

- Click the plus (+) sign corresponding to the error event.

When the Site Setup Wizard successfully applies the configuration settings to Unity, it prompts you to create a storage pool:

- If you click **Yes**, the system automatically launches the Nexsan Unity Pool Setup Wizard. .
- If you click **No**, the system automatically logs you on to Nexsan Unity as the Nexsan Unity Administrator, nxadmin. You can then start managing Unity. To get started, see the *Nexsan Unity Software User Guide*.

Chapter 3

Getting started with Nexsan Unity

Once you install, discover, and set up the Unity Storage System, you use Nexsan Unity, our patented web-based user interface, to manage your storage infrastructure. Unity provides a hierarchical view of your Unity storage infrastructure. It includes wizard-based configuration tools for creating storage pools and file systems, setting up replication sites, managing data replication and snapshots, setting up and managing user accounts, and performing various other management tasks related to your Unity storage infrastructure.

This section includes these topics:

Starting Unity	50
Logging on to Unity	50
Navigating Unity	52

Starting Unity

There are two methods for starting Unity: from the Discovery Wizard and from a web browser.

Note For best screen resolution to view Unity, we recommend that your screen size resolution be set to 1280 x 720 minimum.

▶ To launch Unity from the Discovery Wizard:

1. Launch the Nexsan Unity Discovery Wizard and start the discovery process.
2. When the Discovery Wizard finds Unity that you want to manage, select the system in the Discovery Wizard.
3. Click the **Launch Unity** button. Nexsan Unity automatically opens in your default web browser, and displays the log on dialog.

▶ To launch Unity from a web browser:

Note For this method, you need the management virtual IP address of the Unity that you want to manage..

Unity supports the following desktop web browsers and browser versions:

Note Unless otherwise noted, only the latest released and/or patch level of each browser version is supported.

- Windows Internet Explorer 11
- Google Chrome 45.0.2454
- Mozilla Firefox 41.0
- Safari 8.0

1. Open a web browser on a system that is installed on the same network (and subnet) as Unity(s) that you want to manage..
2. In the web browser's address bar, type this URL, replacing <Management Virtual IP address> with Unity's management virtual IP address:

```
https://<Management Virtual IP address>/
```

3. Press Enter.

Unity's web-based interface launches and displays the log on dialog.

Logging on to Unity



You can log on to UnityNexsan Unity with a user account that has site- or storage pool-level administrator access, or as the UnityNexsan Unity Administrator account, nxadmin; for more information, see [Users and access rights](#) on page 65.

Unity's web-based user interface uses a self-signed SSL certificate to ensure a secure communication link between the Unity Storage System and the system where Unity is running. When you initially open Unity in your web browser, you are required to accept the certificate and/or add Unity to the browser's list of trusted sites before you can access the system.

Note When you log on to Unity for the first time, you can only log on as one of the Site Administrators that you added to the system during the initial setup of Unity. After the initial log on, you can add additional Site or Storage Pool Administrators, and use any of these Administrator accounts for subsequent log-ons to the system. For more information about adding user accounts, see [Users and access rights](#) on page 65.

► **To log on to Unity:**

1. Perform one of these actions:

For...	Do this
<p>Active Directory or LDAP implementation</p> 	<ol style="list-style-type: none"> 1. In the User name field, type your Microsoft Active Directory domain or LDAP Directory user name. 2. In the Password field, type your Microsoft Active Directory domain or LDAP Directory password. 3. From the Domain drop-down list, select the domain where the user account you are using to log on to Unity exists. 4. If you want to log on as nxadmin in addition to the domain authentication, type the nxadmin password in the Password field.
<p>Unity implementation</p> 	<ol style="list-style-type: none"> 1. In the User name field, type your user name. 2. In the Password field, type your password.

2. Click the **Log on** button. Unity starts loading site and configuration information and displays the main user interface.

Navigating Unity

Unity's tree view interface presents your Nexsan storage infrastructure in a hierarchical tree view with nodes representing storage components and data management functions.

Unity also includes built-in configuration wizards to help you easily accomplish complex data management tasks, such as creating storage pools and File Systems and setting up data replication. The configuration wizards guide you through these processes, while Unity automatically manages all the disk-level tasks in the background.

Note For best screen resolution to view Unity, we recommend that your screen size resolution be set to 1280 x 720 minimum.

Unity's dashboard view interface presents the same data as the property panels in the Unity's tree view, but for the entire site. The dashboard displays performance data, site health, I/O statistics, and space usage information in graphical format, using a dashlet for each category. Data shown in the dashboard cannot be modified. You must use the tree view wizards and property panels to change data configuration settings.

This section includes these topics:

Tree view and nodes	52
Viewing performance metrics with the Dashboard view	474

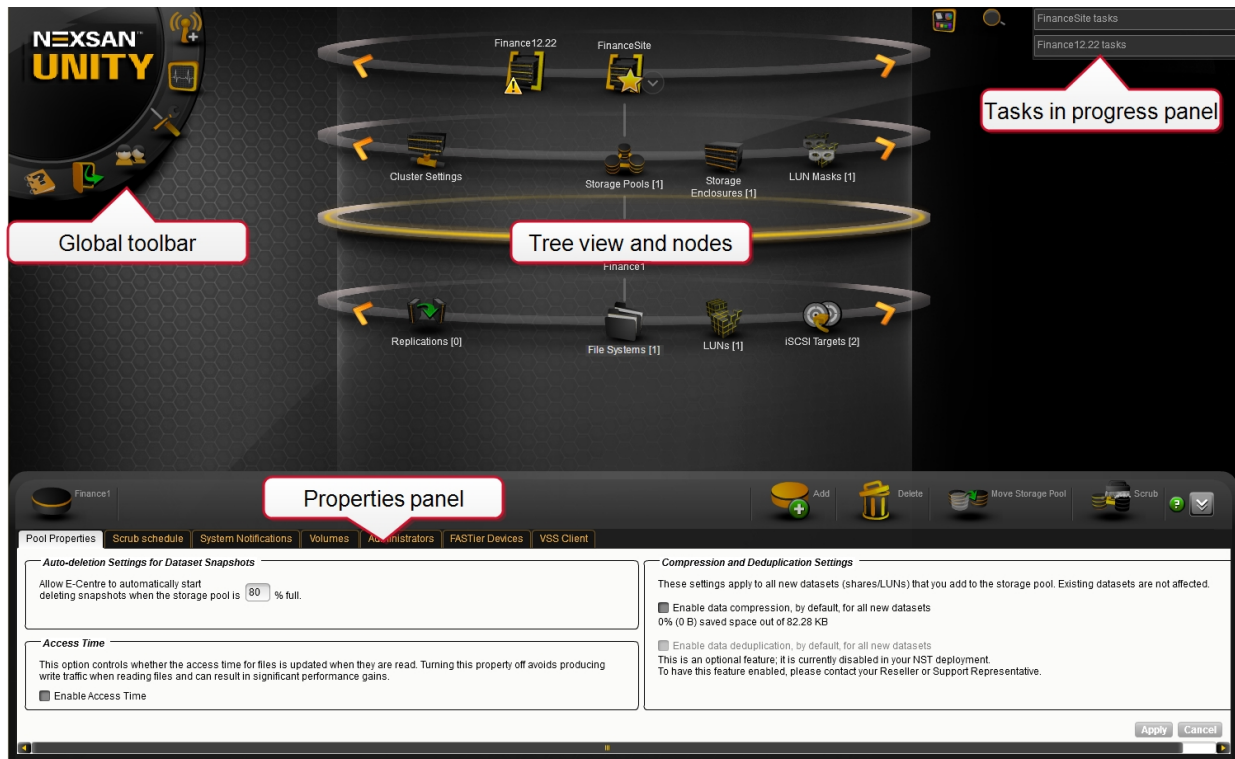
Tree view and nodes

Unity's tree view presents the Nexsan storage infrastructure in a user-friendly, hierarchical format. The tree view comprises a top level node—the site node—with sub-level nodes. Each sub-level node, under the site node, has its own set of child nodes—where, depending on the node, you can drill down in the tree to access additional child nodes. Each node in the tree represents either a component of the system that you configure, or a function that you use to manage your storage.

With the exception of the site-level nodes, all nodes in the tree are presented on a revolving bar that automatically moves a node into focus when you click it, and also displays its child nodes. You can also click the left and right arrows on the revolving bar to access nodes that are not visible on the bar; the revolving bar rotates and shuffles each node into focus as you click the left and right arrows.


Several nodes in the tree also display a node count value that informs you of the number of child nodes that exist under them. For example, if you have 3 storage pools on the system, the Storage Pools node appears as **Storage Pools [3]**.

Figure 3-1: Unity: Tree view



► **To switch to dashboard view:**

Perform one of these actions:

- Click the dashboard icon  next to the Task in progress panel, or
- Hover your mouse over the System Monitoring icon on the Global Toolbar and click the Dashboard icon.

The dashboard interface is described in [Viewing performance metrics with the Dashboard view](#) on page 474.

Understanding nodes in Unity's tree view

The System node, which is the highest-level node in Unity's tree view, is identified by the system name that you specify during the initial setup of Unity. If you configured data replication for Unity, or if you added one or more remote Unitys (multi-system implementation), Unity also displays the System node of each remote system configured on the system—but only if the user is currently logged on as:

- a System Administrator or a Pool Administrator on the remote system(s), or
- a Pool Administrator of a storage pool that is replicated to the remote system(s).

For example: System A has 2 storage pools configured, *Pool1* and *Pool2*, where only *Pool1* is replicated to a remote system, System B. System C has 2 storage pools, *PoolA* and *PoolB*, replicated to System B.

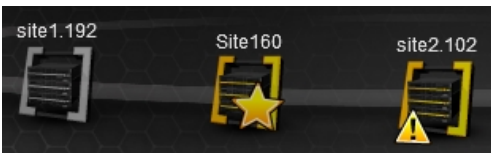
- A user logged as a System Administrator sees both System A and System B with their respective child nodes in the tree view.
- A user logged on as a Pool Administrator for *Pool2*, but not *Pool1*, sees System A.

- A user logged on as a Pool Administrator for *Pool1* (which is replicated to remote system B), sees both System A and System B with their respective child nodes in the tree view. However, the Pool Administrator only has access to *Pool1* on both Systems A and B, but not *Pool2*.
- A user logged on a System Administrator of System C sees System B and C. To access System A, that user must enter other credentials using the System node's properties panel and clicking the **Re-authenticate** button to log on.

The node for the active system is also displayed on the secondary system, where data is replicated; and the same access rules apply for Pool Administrators on the secondary system.

System node

This is the top node from which all nodes pertaining to this specific system are connected.

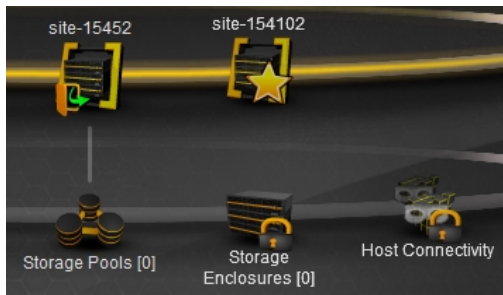


The System node can have these child nodes:

- Storage pools
- Storage enclosures
- Host connectivity
- Cluster settings
- n-Way
- Archive

In a multi-system environment, the System node has siblings, one node for each remote system.

In this example, *System160* is the primary system and it is identified with a star. It is connected to two peer remote systems, *system1.192* and *system2.102*. Since *system2.102* is currently selected, *system1.192* is gray because it is not the peer system of *system2.102*, but of *System160*.



In a multi-system environment, if the user currently logged on does not have access to the system, you will see the Re-authenticate icon on the system's node.

In this example, the user is not currently logged on to *system-15452*.

Storage Enclosures node

This node displays all storage systems connected to Unity.

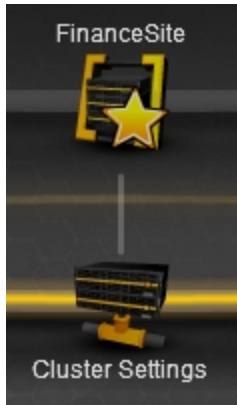


The Storage Systems node can have these child nodes, depending on the type of storage configured on the system:

- NST5100™—this refers to the disk drives installed in the front bay of the Nexsan NST5110™.
- A node for each Nexsan storage system attached externally (identified by model name and serial number); for example: E48X™ (serial #).

Cluster Settings node

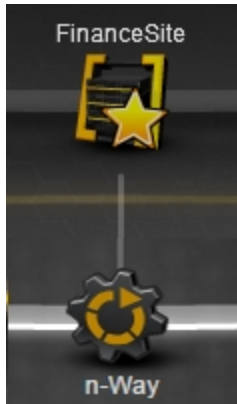
This node represents the storage controllers on Unity.



The **Cluster Settings** node has no child nodes.

n-Way node

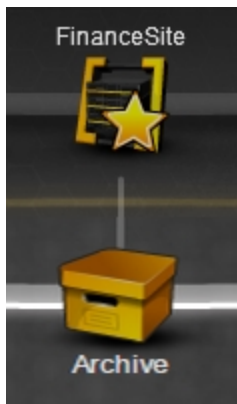
This node represents the n-Way Sync file systems on Unity.



The **n-Way** node has no child nodes.

Archive node

This node represents the file systems on Unity that are using Assureon's archiving capabilities.

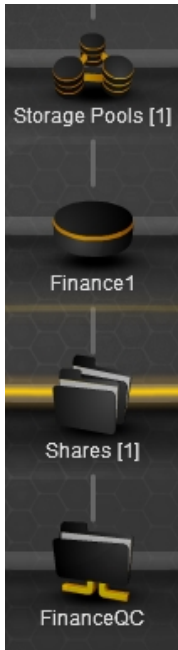


The **Archive** node has no child nodes.

3

Storage Pools node

This node displays the storage pools configured for the system.



A node for each storage pool configured on the system; each storage pool node has these child nodes:

File Systems node—has a child node for each file system that you create in the storage pool; each file system child node has these child nodes:

iSCSI Targets node—has a child node for each iSCSI target that you add to the storage pool, and the mgmt node.

Replications node—has a child node for the remote replication system.

- Node representing the secondary system(s)—this node is identified by the secondary system's system name. This node allows you to configure data replication for the storage pool.

Incoming Replications node

This node is displayed only if the system is designated as a remote replication system for another Unity.



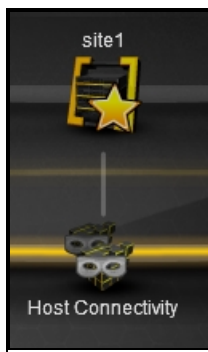
A node for each system that replicates data to the this Unity. Each system node is identified by its system name, and each node has these child nodes:

- The storage pool's node with these child nodes:
 - **Replicated File Systems** node—displays the file systems that are replicated to this Unity; it has a child node for each file system that is replicated.
 - **Replicated LUNs** node—displays LUNs that are replicated to this Unity; it has a child node for each LUN that is replicated.

3

Host Connectivity node

This node has a properties dialog box that displays the LUN Masks and Initiator Groups created for the system.



The Host Connectivity node has no child nodes.

FASTier node

This node displays the FASTier devices present on the system.

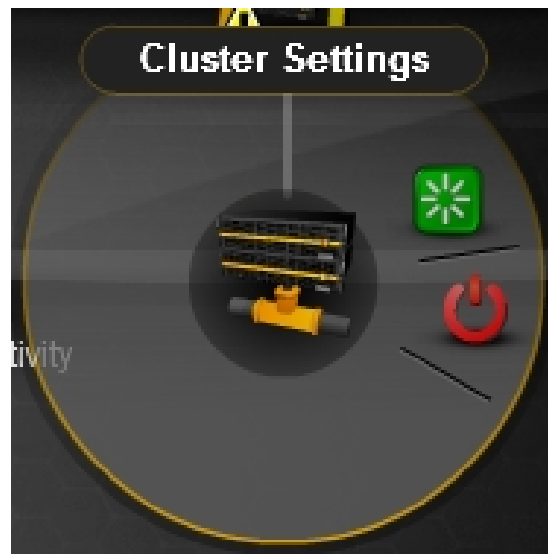


- A node for each FASTier device detected; this will display the FASTier device properties panel, where you can partition the device.
- A node for battery-backed cache, which is automatically present on Unity. This release allows to partition battery-backed cache as well. This device is used as a write cache only.

Node context menu

The node context menu provides easy access to node-level functions.

Figure 3-2: Node context menu



This example shows how to add a storage pool using the node context menu.

► **To add a storage pool:**

1. Under the site node, click the **Storage Pools** node.
2. Click the context menu button to open the node context menu.



3. When the node context menu opens, click the + icon to add a storage pool.

Tip You can also access a node's context menu functions in its [Properties panel](#) below.

Properties panel

The Properties panel, located at the bottom of the Unity user interface, displays node-specific configuration settings and functions for nodes in the tree. Each node, including the site node, has a Properties panel that is specific to that node. When you click a node, the contents of the Properties panel change automatically to reflect configuration settings and functions that are available for the node.

Figure 3-3: Example of the file systems node Properties panel

Name	Available space	User Data	Snapshots	Quota	Reserved Space	All	n-Way Sync Enabled	Compression
Pubs_001	118.50 MB	120 KB	13 KB				true	83.63% (879.63 KB)
Pubs_002	118.50 MB	26 KB	0 B				true	6.54% (1.82 KB)
s1	118.50 MB	20 KB	0 B				false	0% (0 B)

By default, the Properties panel is collapsed.

► **To expand the Properties panel:**

- Click the **Properties** tab located in the top-left corner of the panel.
Or
- Click the **Expand** button on the top-right corner of the Properties panel.
Or
- Position the mouse cursor at the top edge of the Properties panel; when the double-headed arrow displays, drag the Properties panel to the required height.

► **To collapse the Properties panel again:**

- Click the **Collapse** button on the top-right corner of the panel.
Or
- Click the **Properties** tab located in the top-left corner of the panel.
Or
- Position the mouse cursor at the top edge of the Properties panel; when the double-headed arrow displays, drag the Properties panel down to close it.

Note The Properties panel also contains functions available in a node's context menu. For example, to add a new storage pool, you can click **Add** in the Storage Pools node's context menu, or you can click the **Add** button in the Storage Pools' Properties panel.

Global Toolbar

Unity toolbar provides access to global system functions. You can collapse the Toolbar and hide the menu options, if needed; simply click the Toolbar to collapse it, and click it again to expand.

The toolbar includes these options.

Table 3-1: Global toolbar options

Global toolbar option	Description
System Monitoring	<p>This menu gives you access to Unity Event Viewer and also allows you to configure log settings for the active (local) site and any remote Unity(s) connected to the site. The System Events menu includes these menu options:</p> <ul style="list-style-type: none"> ● View: this option opens the Unity Event Viewer where you can view system events for the active (local) site, and for any remote sites connected to the site. ● Configure: this option opens the Configure Logging Options panel, where you configure log settings for system events for the active (local) site and any remote sites connected to the site. ● Generate reports: this option allows you to generate dashboard-type, graphical reports detailing storage capacity across the Unity storage infrastructure. ● Performance Monitor: this option opens the Performance Monitor window, where you can view real-time performance information for Unity in graphical format. ● Dashboard: this option opens the Dashboard view, which displays performance data, site health, I/O statistics, and space usage information in graphical format, using a dashlet for each category. It presents the same data as the property panels in the Nexsan Unity's tree view, but for the entire site.
Tools & Settings	<p>This menu includes these options:</p> <ul style="list-style-type: none"> ● Add a site: This menu option allows you to add a remote site to the active (local) site, for remote system management (in a multi-site environment). ● Notifications: select this option to open the Configure Email and SNMP Notification panel where you configure email and SNMP alerts for the active (local) site, as well as for any remote Unity connected to the site.

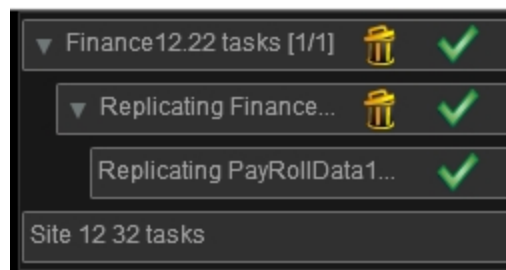
Global toolbar option	Description
	<ul style="list-style-type: none"> ● UnityPreferences: this option opens a dialog box where you can configure the auto-refresh interval for the site, date and time, and Performance Monitor settings. ● System Preferences: this option opens the Preferences panel where you can change date and time display settings, and modify the time zone on Unity. ● Refresh System Cache: Unity caches system-level configuration settings at the server-level, and then delivers cached information on demand at the management level through Unity. This ensures that the system performs optimally. You may be required, under certain circumstances, to manually refresh the system cache; for example, when Unity appears to be out of sync with configuration settings on Unity. When you select this option, a pop-up displays asking you to select the sites that you want to refresh the system cache for (in a multi-site environment). Select the corresponding site(s) and click OK. The process for manually refreshing the system cache can take time.
Security and Permissions	<p>This menu gives you access to user permission and security settings for the site; it includes these options:</p> <ul style="list-style-type: none"> ● Manage Users: select this option to open the Manage Users and Groups panel where you configure access rights and file system-level access permissions for user and user groups in your Microsoft Active Directory domain or LDAP Directory service—provided this feature is included with your deployment, and Unity is connected to a Microsoft Active Directory domain or LDAP Directory service. If Unity is configured to use Unity authentication, the Manage Users and Groups panel allows you to add or remove users and groups, and configure access rights and file system-level access permissions for your users and groups. ● Manage CHAP Users: select this option to add or remove CHAP (Challenge Handshake Authentication Protocol) users for the site. iSCSI initiators and targets prove their identity to each other using the Challenge Handshake Authentication Protocol (CHAP). You can use CHAP authentication to restrict iSCSI access to LUNs on Unity; only servers (initiators) that provide the correct user name and password (or secret) combination can connect to LUNs on Unity. ● Change My Password: displays a pop-up where you can change the password for the user currently logged on to the system. This option is only available if the user currently logged on is the Nexsan Unity Administrator (nxadmin), or a local user on a site configured to use Nexsan Unity authentication.
Help	<p>This menu gives you access to the Unity on-line help; it includes these options:</p> <ul style="list-style-type: none"> ● Download Software User Guide: select this option to copy the latest portfolio PDF of the Nexsan Unity documentation to a local disk. ● Help Topics...: opens Unity context-sensitive on-line help. You can also access topic-specific help from within any panel by clicking the help icon.

Global toolbar option	Description
	<ul style="list-style-type: none"> ● About Unity: this dialog box displays site, version, feature and copyright information. You can also open the Release Notes document and the read license agreement by clicking the corresponding button.
Check for Updates	This option opens the Unity Software Updater from where you can update Unity 's software components with the latest version of Unity. You can also use the Unity Software Updater to update software components on any remote Unity connected to the active (local) site; for more information, see Updating Unity on page 363.
Log off <user>	Select this option to log out of Unity; once the system logs you out, it displays the log on dialog again.

Tasks in progress panel

The Tasks in progress panel displays tasks that Unity processes in the background.

Figure 3-4: Tasks in progress panel



Background tasks include scheduled and manual data replications, scheduled and manual pool scrubs, recursive file system-level permission settings, site and storage pool failover operations, and so on. The Tasks in progress panel displays the progress of each background task; when a task completes successfully, the panel displays a check mark next to the task to inform you.

The title bar indicates the total number of tasks currently displayed in the Tasks in progress panel—this includes tasks that are still running and tasks that are complete; for example, if one background task is running, the title bar displays: **Task in progress [1]**.

You can continue working with Unity while background tasks are running.

You can remove tasks that have completed—either successfully or not—from the Tasks in progress panel.

► To remove a task from the Tasks in progress panel:

- Click the trash bin icon for task you want to clear. To select all tasks, click the trash bin icon on the top-level task.

You can also delete tasks automatically using the System Preferences menu. By default, five tasks are automatically deleted after one week. For details, see [Modifying background tasks settings](#) on page 355.

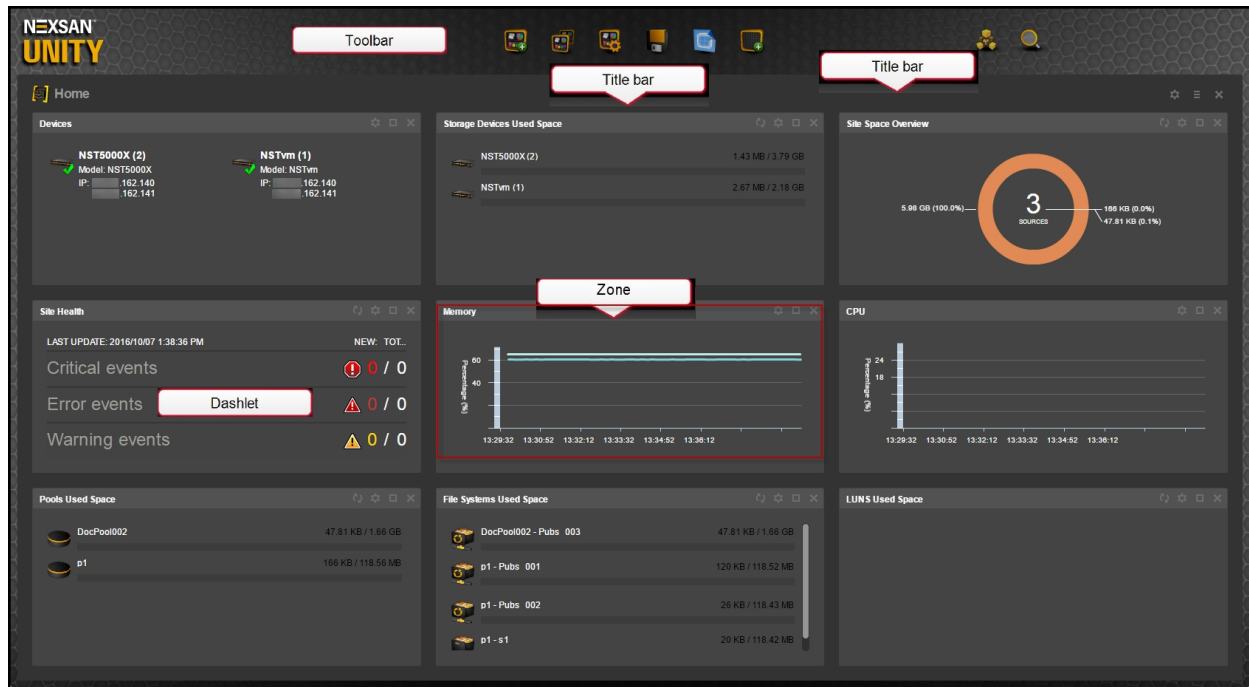
Viewing performance metrics with the Dashboard view

The [dashboard](#) consists of:

- a toolbar at the top
- a title bar

- zones that contain one or more dashlets

Figure 3-5: Dashboard view



3

To switch to Tree view, click the Tree view icon  on the top right corner of the screen; for a description of tree nodes, see [Tree view and nodes](#) on page 52.

This section includes these topics:

Dashboard toolbar	475
Dashboard title bars	476
Home dashboard	477
Performance dashboard	478
Adding and configuring dashlets	486
Managing dashboards	479

Chapter 4

Users and access rights

Unity provides role-based user authentication for Unity. Role-based authentication protects your site—including all your storage pools and underlying shares—from unauthorized access through a process of matching user accounts against the administrative rights and file-level access permissions that you set for those user accounts in Unity.

This section includes these topics:

User authentication modes	66
Role-based administration in Nexsan Unity	66
Managing users and access rights in the Manage Users and Groups panel	74
Setting access rights	82
Managing users and groups with Nexsan Unity	90

User authentication modes

During the initial setup of your site, you select the [user authentication mode](#) that you want to use with your Unity deployment. Unity supports three modes for user authentication:

- Microsoft Windows Active Directory domain
- LDAP Directory service (in UNIX/Linux environments)
- Unity authentication

To authenticate users against the user and group accounts stored locally on Unity, use the Manage Users and Groups panel; see [Managing users and groups with Nexsan Unity](#) on page 90.

To authenticate users against a Microsoft Windows Active Directory domain or an LDAP Directory service, use the user and group accounts that are maintained on the Microsoft Windows Active Directory server or LDAP Directory server.



CAUTION: RISK OF OUTAGE

Do not join Unity with Active Directory to Domain Controllers hosted on VMware. Domain Controllers used with Unity and Active Directory must either be a physical device or hosted externally to Unity.

Role-based administration in Nexsan Unity

Before assigning access rights and share-level access permissions to users and groups in Unity, it is important to understand the key concepts of [user](#) and [group](#) accounts in Unity, and the access rights of Unity administrative roles.

A role has certain access rights assigned to it—meaning things that members of the role are allowed to do in Unity. Another way of looking at it is that users can only manage resources that they are expressly given access to. Roles define that access.

Note Users can only log on to Unity if they are assigned an administrative role, or if they are a member of a group that is assigned a role.

- **Unity Administrator (nxadmin):** The Unity Administrator, or the **nxadmin** account, is a built-in administrator account that is preconfigured on every Unity. The Unity Administrator has full access to Unity. You cannot remove the Unity Administrator account from the system. The default password for the Nexsan Unity Administrator account is, **PASSWORD** (all upper-case); you are required to change the default password when you perform the initial setup of Unity. If you forget the password you configured for the Nexsan Unity Administrator account, it cannot be reset—but you can change the password, if needed; see [Changing the nxadmin password](#) on page 95.
- **Site Administrator:** Site Administrators have the same access rights to Unity as the Unity Administrator (**nxadmin**), except that Site Administrators cannot give or revoke Site Administrator access to other users or groups on the system; only the Unity Administrator can perform these operations. You give users and/or groups Site Administrator access during the initial setup of Unity. After the site is set up, you can give Site Administrator access to additional users or groups using the **nxadmin** account.
- **Pool Administrator:** Pool Administrators have pool-level access to the site. A user becomes a Pool Administrator if you authorize the user's account to manage a storage pool, or if the user is a member of a group that you authorize. Pool Administrators can ONLY manage the storage pools that you assign them to; this includes the ability to create, manage, and delete shares in the storage pools, perform data replication operations, configure and manage snapshots, and manage share-level access permissions. Pool Administrators can view information and settings about nodes and objects to which they are not authorized.

Nexsan Unity roles and access rights

This table lists the access rights for the **nxadmin**, Site, and Pool administrative roles.

Table 4-1: Nexsan Unity roles and access rights

Access rights	Unity Administrator (nxadmin)	Site Administrator	Pool Administrator
Perform the initial setup of the of Unity.	✓	✗	✗
Run CLI commands	✓	✗	✗
Site-level tasks			
Change network settings for the site	✓	✓	✗
Modify the Site name and the DNS entry for the site	✓	✓	✗
Enable the NDMP (Network Data Management Protocol) backup service and set the user name and password for the service	✓	✓	✗
Shut down/restart Unity	✓	✓	✗
Give Site Administrator access to users and/or groups	✓	✗	✗
Revoke Site Administrator access from users and/or groups	✓	✗	✗
Allocate new storage systems to the site	✓	✓	✗
Shut down/restart external storage systems	✓	✓	✗
Perform firmware updates (using Unity Firmware Updater)	✓	✗	✗
Customize date and time formats (using the Unity Preferences menu option in the Tools menu)	✓	✓	✗
Customize the server time and time zone (in the Site's properties panel)	✓	✗	✗
Access the Performance Monitor to view performance metrics for the system	✓	✓	✗

Access rights	Unity Administrator (nxadmin)	Site Administrator	Pool Administrator
Modify user authentication settings	✓	✗	✗
Create and edit Dashboard templates	✓	✓	✗
Set an NFSv4 Domain and modify NFS general settings	✓	✗	✗
Cluster-level operations (if Unity is configured with the Cluster package)			
Shut down/restart cluster nodes	✓	✓	✗
Switch the active node	✓	✓	✗
Change cluster network settings	✓	✓	✗
Change TCP flow control settings	✓	✗	✗
Enable Jumbo Frames	✓	✗	✗
Enable LACP	✓	✗	✗
Storage pool-level tasks, including:			
Create new storage pools	✓	✓	✗
Delete storage pools	✓	✓	✗
Give users and/or groups Pool Administrator access to storage pools	✓	✓	✗
Revoke a user's and/or group's Pool Administrator access	✓	✓	✗
Add volumes	✓	✓	✗
Replace a volume	✓	✓	✗
Perform scrub operations on storage pools and set a scrub schedule	✓	✓	✓ <i>Only on the pool</i>

Access rights	Unity Administrator (nxadmin)	Site Administrator	Pool Administrator
			<i>(s) to which the user has access</i>
Configure FASTier cache assignments for the storage pool	✓	✓	✓ <i>Only on the pool (s) to which the user has access</i>
File System tasks			
Create new file system	✓	✓	✓ <i>Only on the pool (s) to which the user has access</i>
Delete file system	✓	✓	✓ <i>Only on the pool (s) to which the user has access</i>
Modify a file system's name	✓	✓	✓ <i>Only on the pool (s) to which the user has access</i>
Adjust space usage settings	✓	✓	✓ <i>Only on the pool (s) to which the user has access</i>
Change the sharing method (CIFS, NFS, FTP, and/or anonymous access)	✓	✓	✓ <i>Only on the pool (s) to which the user has access</i> <i>For FTP sharing, only at share level</i>
Assign file system-level access permissions (Read, Read/Write, or Full, and Inherit) to users and/or groups	✓	✓	✓ <i>Only on the pool (s) to which the user has access</i>
LUN-level tasks			
Create new LUNs	✓	✓	✓

Access rights	Unity Administrator (nxadmin)	Site Administrator	Pool Administrator
Delete LUNs	✓	✓	✓
Create new iSCSI targets	✓	✓	✓ <i>Only on the pool (s) to which the user has access</i>
Change CHAP authentication for LUNs and iSCSI targets	✓	✓	✓ <i>Only on the pool (s) to which the user has access</i>
Manage CHAP authentication for the site, include adding new CHAP users	✓	✓	✗
Add, edit, and delete LUN masks	✓	✓	✓
Add and edit Initiator Groups	✓	✓	✓
Delete Initiator Groups	✓	✓	✗
Snapshots-related tasks			
Set schedules for snapshots	✓	✓	✓ <i>Only on the pool (s) to which the user has access</i>
Take manual snapshots	✓	✓	✓ <i>Only on the pool (s) to which the user has access</i>
Roll-back the data in a share to a specific snapshot	✓	✓	✓ <i>Only on the pool (s) to which the user has access</i>
Delete snapshots and configure auto-deletion settings	✓	✓	✓ <i>Only on the pool (s) to which the user has access</i>

Access rights	Unity Administrator (nxadmin)	Site Administrator	Pool Administrator
Start/stop snapshot browsing	✓	✓	✓ <i>Only on the pool (s) to which the user has access</i>
Data replication operations			
Add a secondary site and configure data replication for the site	✓	✓	✗
Synchronous data replication: configure a (destination) mirror for a storage pool	✓	✓	✗
Set data replication schedules (Asynchronous data replication)	✓	✓	✓ <i>Only on the pool (s) to which the user has access</i>
Perform offline replications (Asynchronous data replication)	✓	✓	✓ <i>Only on the pool (s) to which the user has access</i>
Import data from the secondary site or from a USB device (Asynchronous data replication)	✓	✓	✓ <i>Only on the pool (s) to which the user has access</i>
Failover all site-level operations to the secondary site (Asynchronous data replication)	✓	✓	✗
Failover a storage pool to the secondary site (Asynchronous data replication)	✓	✓	✓ <i>Only on the pool (s) to which the user has access</i>
Promote/demote the primary and/or secondary site (Asynchronous data replication)	✓	✓	✗
Promote/demote the primary and/or replicated storage pool (Asynchronous data replication)	✓	✓	✗
Promote a storage pool's mirror and make it a primary storage pool	✓	✓	✗

Access rights	Unity Administrator (nxadmin)	Site Administrator	Pool Administrator
Remove data replication for a storage pool (for both Asynchronous and synchronous data replication)	✓	✓	✗
Manage local users and groups (if the system is configured to use Unity authentication)			
Add local users and groups	✓	✓	✗
Delete local users and groups	✓	✓ Only for user or group accounts with Pool Administrator access	✗
Manage groups (for example, add and/or remove users from a group)	✓	✓	✗
Change a user's password	✓	✓ <i>Their own passwords and Pool Administrators' passwords; not other Site Administrators' passwords</i>	✓ <i>Only their own passwords</i>
Manage a remote site			
Add a remote site to manage	✓	✓	✗
View nodes and objects on the remote site	✓	✓	✓ <i>Only if the pool(s) that the Pool Administrator has access to is replicated to a remote site; or, only if the user has Pool Administrator access to a pool (s) on the remote site</i>
Configure/manage nodes and objects on the remote site	✓	✓	✓

Access rights	Unity Administrator (nxadmin)	Site Administrator	Pool Administrator
			<p><i>Only if the pool(s) that the Pool Administrator has access to is replicated to a remote site; or, only if the user has Pool Administrator access to a pool(s) on the remote site. In both cases, the user can only configure/manage nodes and objects on the remote site that belong to the pool to which the user has access</i></p>
Manage system events			
Retrieve and view system events	✓	✓	✓
Email and/or save event logs	✓	✓	✓
Configure event logging	✓	✓	✗
Manage SNMP and email alerts			
Configure SNMP alerts	✓	✓	✗
Configure email alerts	✓	✓	✗

Managing users and access rights in the Manage Users and Groups panel

Use the Manage Users and Groups panel to set access rights and share-level access permissions for users and groups. This panel displays all the user and groups that are in the Microsoft Active Directory domain or LDAP Directory service that Unity is connected to; or all the local users and groups that you define, if the system is configured to use Unity authentication.

The options and settings that are available in the Manage Users and Groups panel vary depending on whether Unity is connected to a Microsoft Active Directory domain or LDAP Directory service, or whether the system is using Unity authentication.

This section includes these topics:

Opening the Manage Users and Groups panel	74
Viewing a user's or group's access rights	79
Viewing a user's or group's file system permissions	79
Viewing a user's group memberships	80
Viewing a group's members	81

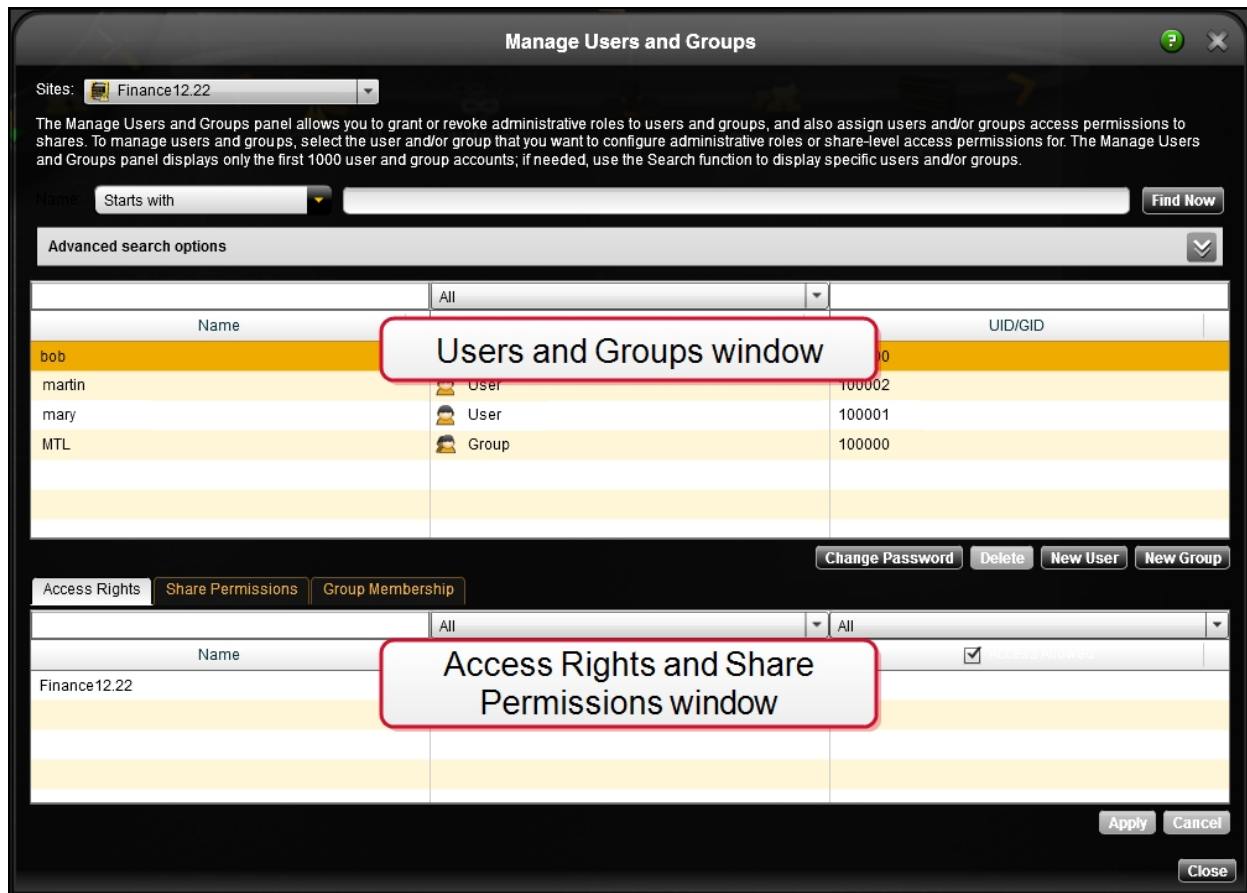
Opening the Manage Users and Groups panel

This task describes how to access the Manage Users and Groups panel.

► **To access the Manage Users and Groups panel:**

1. In the Unity toolbar, click **Security and Permissions**.
2. Select the **Manage Users** option. The Manage Users and Groups panel displays.

Figure 4-1: Manage Users and Groups panel



The Manage Users and Groups panel is divided into two sections:

- [Users and Groups window](#) below
- [Access Rights, CIFS Permissions, and Group Membership window](#) on page 78

The Manage Users and Groups panel allows you to view and set a user's access right and share permissions; refer to these topics:

- [Viewing a user's or group's access rights](#) on page 79
- [Viewing a user's or group's file system permissions](#) on page 79
- [Viewing a user's group memberships](#) on page 80
- [Viewing a group's members](#) on page 81

Users and Groups window

The Users and Group window, at the top of the Manage Users and Groups panel, lists all the user and groups that are in the Microsoft Active Directory domain or LDAP Directory service that Unity is connected to; or, if the system is configured to use Unity authentication, all the users and groups that you define on the system. When you select a user or a group in the Users and Group window, the Manage Users and Groups panel displays the user's or group's access rights, share permissions, and group membership (for users) or group members (for groups) in the Access Rights and Permissions window on the bottom half of the Manage Users and Groups panel.

If Unity is integrated with Microsoft Windows Active Directory domain or an LDAP Directory service, the Users and Group window displays the **Domain** drop-down list. In a multiple domain environment, the **Domain** drop-down list contains all the domains on the network; you can then select the corresponding domain server (s) that you want to view users and/or groups from in the Manage Users and Groups panel.

Note The Manage Users and Groups panel does not maintain sort and search settings when you exit the panel.

▶ **To use the Find function to display specific users and/or groups:**

1. Select the **Starts with** option from the pick list next to the **Name** text box.
2. For example, to display the user *Bob*: type **BO** (or **bo**) in the **Name** text box.
3. Click the **Find Now** button. Unity displays all users and/or groups with user and/or group names that start with the letters **b** and **o** in the **Search results** grid (on the bottom-left of the panel).

You can also use the advanced search function and set more specific search criteria. For example, you can search for only users or groups; or, you can search for users, groups, or users and/or groups in a specific Organizational Unit (OU).

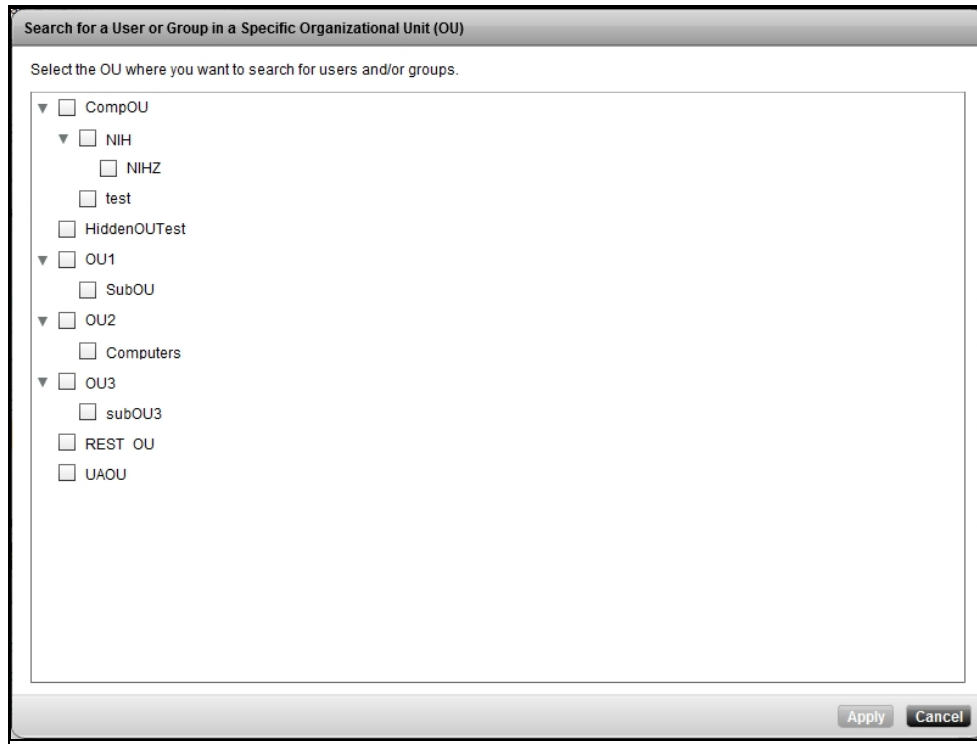
▶ **To use the advanced search function:**

1. Click the arrow to the right of **Advanced Search options** to display and configure advanced options.



2. Select either the **Users** or **Groups** option to search for only user accounts or group accounts, respectively.

- Click the button next to the **Organizational Unit (OU)** text box to display a list of OUs in the domain; a pop-up opens displaying available OUs.



- Select the OU that you want to search for users and/or groups in, and then click the Apply button to continue.
- Once you finish configuring advanced search options, click the **Find Now** button; Nexsan Unity displays all users and/or groups that match your search criteria in the search results grid (on the bottom-left of the panel).

You can then search for specific users or groups in the Users and Group window by entering a user or group name in the text box above the **Name** column heading. The Manage Users and Groups panel automatically filters the list as you type.

You can also filter the list of users and groups to display only users, or only groups: From the drop-down list above the **Type** column heading, select either **User** or **Group**; the default setting is **All**.



- ▶ **To sort the list in descending order:**
 - Click the sort pointer until the arrow points down.
- ▶ **To sort the list in ascending order:**
 - Click the sort pointer until the arrow points up.

Tip You can also sort the list according to type—*User* or *Group*—by clicking the sort pointer in the **Type** grid heading.

Access Rights, CIFS Permissions, and Group Membership window

The Access Rights, CIFS Permissions, and Group Membership window, at the bottom of the Manage Users and Groups panel, displays user access rights, permissions, and group membership information; it contains three tabs:

Note To display all three tabs in the Access Rights and Permissions window, select a user or group in the Users and Group window at the top of the Manage Users and Groups panel.

Access Rights tab

This tab displays sites—both local and remote (if configured)—and all storage pools available on the site(s). When you select a user or group in the list at the top of the Manage Users and Groups panel, a check mark is displayed in the **Access Allowed** column for each corresponding node in the **Access Level** column to which the selected user or group has access.

You can search for specific nodes in the list, or filter the list, by entering a site or storage pool name in the text box above the **Name** column heading. The Manage Users and Groups panel automatically filters the list as you type.

You can filter the list of nodes by access level—Site or Storage Pool: From the drop-down list above the **Access Level** column heading, select either **Site** or **Storage Pool**; the default setting is **All**. You can also filter the **Access Allowed** column by **Allowed** or **Denied**; again, the default setting is **All**.

You can sort the grid alphabetically in either ascending or descending order by clicking the sort pointer in the **Name** column heading.



You can also sort by **Access Level** or **Access Allowed**; or a combination of **Name**, **Access Level**, and **Access Allowed**, in any particular sort order that you want: 1, 2, and 3.

For example, to sort by **Name** first, and **Access Level** second:

1. Click the sort pointer in the **Name** column heading until **1** is displayed (with the arrow pointing either up for ascending order, or down for descending order).
2. Click the sort pointer in the **Access Level** column heading until **2** is displayed (with the arrow pointing either up for ascending order, or down for descending order).

CIFS Permissions tab

This tab displays the site(s)—both local and remote (if configured)—all storage pools available on each site, and their corresponding file systems. When you select a user or group in the list at the top of the Manage Users and Groups panel, the tab displays the permissions that the selected user or group is granted to each file system: **Read**, **Write**, or **Full**.

You can search for specific file systems in the list, or filter the list, by entering a file system name in the text box above the **file system** column heading. The Manage Users and Groups panel automatically filters the list as you type.

You can filter the list of file system that are displayed in the grid by a specific site or storage pool. For example, from the drop-down list above the **Site** or **Storage Pool** column headings, select the site or storage pool that you want to display file system for; the default display setting for both sites and storage pools is **All**. You can also filter the list of file system by **Read**, **Write**, or **Full** access by selecting the relevant display option from the corresponding drop-down lists.

You can sort the grid in the CIFS Permissions tab alphabetically by **Site**, **Storage Pool**, **file system**, **Read**, **Write**, and **Full** access permissions; the same sort procedures described for the **Access Rights** tab apply.

Note For detailed information about file system-level access permissions and how to assign permissions to users and groups, see [File Systems](#) on page 121.

Group Membership tab

When you select a user in the list at the top of the Manage Users and Groups panel, the Group Membership tab displays the groups that the selected user belongs to. When you select a group, the Group Membership tab displays the group members—both users and groups—of the selected group. You cannot make any changes to the contents of this tab if Unity is connected to a Microsoft Active Directory domain or LDAP Directory service. However, if Unity is configured to use Unity authentication, the Group Membership tab includes controls and options for managing groups (see [Managing users and groups with Nexsan Unity](#) on page 90).

Viewing a user's or group's access rights

This section describes how to view a user's or group's site- and storage pool-level access rights in the Manage Users and Groups panel.

Note For information on modifying a user's or group's access rights, see [Setting access rights](#) on page 82.

► **To view a user's or group's access rights:**

1. For multi-site environments: open the **Sites** drop-down list and select the site where the user or group that you want to view access rights for exists.
2. From the **Domain** drop-down list, in the Users and Group window at the top of the Manage Users and Groups panel, select the domain server(s) where the user or group that you want to view access rights for exists.

Note The panel displays the **Domain** drop-down list if Unity is integrated with a Microsoft Windows Active Directory domain or an LDAP Directory service. In a multiple domain environment, the **Domain** drop-down list contains all the domains on the network.

3. In the **Name** text box, type the name of the user or group that you want to give file system-level access permissions to exists, and then, click the **Find Now** button to display the specified user or group. If needed, you can use the **Find Now** function to display specific users and/or groups. For example, to display the user *Bob*:
 - a. Select the **Starts with** option from the pick list next to the Name text box.
 - b. Type **BO** (or **bo**) in the **Name** text box.
 - c. Click the **Find Now** button. Unity displays all users and/or groups with user and/or group names that start with the letters **b** and **o** in the **Search results** grid (on the bottom-left of the panel).

You can also use the **Advanced Search** function and set more specific search criteria; for more information, see [Users and Groups window](#) on page 75.

4. In the Access Rights and Permissions window, on the bottom half of the Manage Users and Groups panel, select the **Access Rights** tab.

The **Access Rights** tab displays the user's or group's access rights to sites—both local and remote (if configured)—and all storage pools available on the site(s).

Viewing a user's or group's file system permissions

This section describes how to view a user's or group's file system permissions in the Manage Users and Groups panel.

► **To view a user's or group's file system permissions:**

1. For multi-site environments: open the **Sites** drop-down list and select the site where the user or group that you want to view file system permissions for exists.
2. From the **Domain** drop-down list, in the Users and Group window at the top of the Manage Users and Groups panel, select the domain server(s) where the user or group that you want to view file system permissions for exists.

Note The panel displays the **Domain** drop-down list if Unity is integrated with a Microsoft Windows Active Directory domain or an LDAP Directory service. In a multiple domain environment, the **Domain** drop-down list contains all the domains on the network.

3. In the **Name** text box, type the name of the user or group that you want to give file system-level access permissions to exists, and then, click the **Find Now** button to display the specified user or group. If needed, you can use the **Find Now** function to display specific users and/or groups. For example, to display the user *Bob*:
 - a. Select the **Starts with** option from the pick list next to the Name text box.
 - b. Type **BO** (or **bo**) in the **Name** text box.
 - c. Click the **Find Now** button. Unity displays all users and/or groups with user and/or group names that start with the letters **b** and **o** in the **Search results** grid (on the bottom-left of the panel).

You can also use the **Advanced Search** function and set more specific search criteria; for more information, see [Users and Groups window](#) on page 75.

4. In the Access Rights and Permissions window, on the bottom half of the Manage Users and Groups panel, select the **Access Rights** tab.

The **Access Rights** tab displays all the file system on the site(s) and whether or not the selected user or group is granted access.

Viewing a user's group memberships

This section describes how to view the list of groups that a particular user belongs to in the Manage Users and Groups panel.

► **To view the groups that a user belongs to:**

1. For multi-site environments: open the **Sites** drop-down list and select the site where the user that you want to view group memberships for exists.
2. From the **Domain** drop-down list, in the Users and Group window at the top of the Manage Users and Groups panel, select the domain server(s) where the user that you want to view group membership for exists.

Note The panel displays the **Domain** drop-down list if Unity is integrated with a Microsoft Windows Active Directory domain or an LDAP Directory service. In a multiple domain environment, the **Domain** drop-down list contains all the domains on the network.

3. In the **Name** text box, type the name of the user or group that you want to give share-level access permissions to exists, and then, click the **Find Now** button to display the specified user or group. If needed, you can use the **Find Now** function to display specific users and/or groups. For example, to display the user *Bob*:
 - a. Select the **Starts with** option from the pick list next to the Name text box.
 - b. Type **BO** (or **bo**) in the **Name** text box.
 - c. Click the **Find Now** button. Unity displays all users and/or groups with user and/or group names that start with the letters **b** and **o** in the **Search results** grid (on the bottom-left of the panel).

You can also use the **Advanced Search** function and set more specific search criteria; for more information, see [Users and Groups window](#) on page 75.

4. In the Access Rights and Permissions window, on the bottom half of the Manage Users and Groups panel, select the **Group Membership** tab.

The **Group Membership** tab displays the groups that the selected user belongs to.

Viewing a group's members

This section describes how to view a group's members in the Manage Users and Groups panel.

► **To view a group's members:**

1. For multi-site environments: open the **Sites** drop-down list and select the site where the group that you want to view members for exists.
2. From the **Domain** drop-down list, in the Users and Group window at the top of the Manage Users and Groups panel, select the domain server(s) where the group that you want to view members for exists.

Note The panel displays the **Domain** drop-down list if Unity is integrated with a Microsoft Windows Active Directory domain or an LDAP Directory service. In a multiple domain environment, the **Domain** drop-down list contains all the domains on the network.

3. In the **Name** text box, type the name of the user or group that you want to give file system -level access permissions to exists, and then, click the **Find Now** button to display the specified user or group. If needed, you can use the **Find Now** function to display specific users and/or groups. For example, to display the user *Bob*:
 - a. Select the **Starts with** option from the pick list next to the Name text box.
 - b. Type **BO** (or **bo**) in the **Name** text box.
 - c. Click the **Find Now** button. Unity displays all users and/or groups with user and/or group names that start with the letters **b** and **o** in the **Search results** grid (on the bottom-left of the panel).

You can also use the **Advanced Search** function and set more specific search criteria; for more information, see [Users and Groups window](#) on page 75.

4. In the Access Rights and Permissions window, on the bottom half of the Manage Users and Groups panel, select the **Group Membership** tab.

The **Group Membership** tab displays the group members—both users and groups—of the selected group.

Setting access rights

This section describes how to give users and/or groups Site or Pool Administrator access to Unity.

This section includes these topics:

Giving Site Administrator access	82
Revoking Site Administrator access	84
Giving Pool Administrator access	85
Revoking Pool Administrator access	88

Giving Site Administrator access

Site Administrators have site-level access to Unity, including the ability to change network settings for the site, create, delete, and manage storage pools and shares, configure data replication, and so on (refer to [Nexsan Unity roles and access rights](#) on page 67 for the full list of access rights).

You assign the Site Administrator role to users and/or groups during the initial setup of Unity. After the site is set up, you can assign the Site Administrator role to additional users or groups; however, you must be logged on as the Unity Administrator (**nxadmin**) to perform this operation.

Note You must be logged on as the Unity Administrator (**nxadmin**) to give or revoke Site Administrator access.

► To give a user or group Site Administrator access from the toolbar:

1. [Open the Manage Users and Groups panel](#).
2. For multi-site environments: when the Manage Users and Groups panel displays, open the **Sites** drop-down list and select the site where the user or group that you want to give Site Administrator access to exists.

From the **Domain** drop-down list, select the domain server(s) where the user or group that you want to give Site Administrator access to exists.

Note The panel displays the **Domain** drop-down list if Unity is integrated with a Microsoft Windows Active Directory domain or an LDAP Directory service. In a multiple domain environment, the **Domain** drop-down list contains all the domains on the network.

3. In the **Name** text box, type the name of the user or group that you want to give file system-level access permissions to exists, and then, click the **Find Now** button to display the specified user or group.

If needed, you can use the **Find Now** function to display specific users and/or groups. For example, to display the user *Bob*:

- a. Select the **Starts with** option from the pick list next to the Name text box.
- b. Type **BO** (or **bo**) in the **Name** text box.
- c. Click the **Find Now** button. Unity displays all users and/or groups with user and/or group names that start with the letters **b** and **o** in the **Search results** grid (on the bottom-left of the panel).

You can also use the **Advanced Search** function and set more specific search criteria; for more information, see [Users and Groups window](#) on page 75.

4. On the bottom half of the Manage Users and Groups panel, select the **Access Rights** tab.
5. In the grid, select the site to which you want to add a Site Administrator.
6. When the site is highlighted in the grid, select its corresponding check box in the **Access Allowed**

column to give the user or group access to the site.

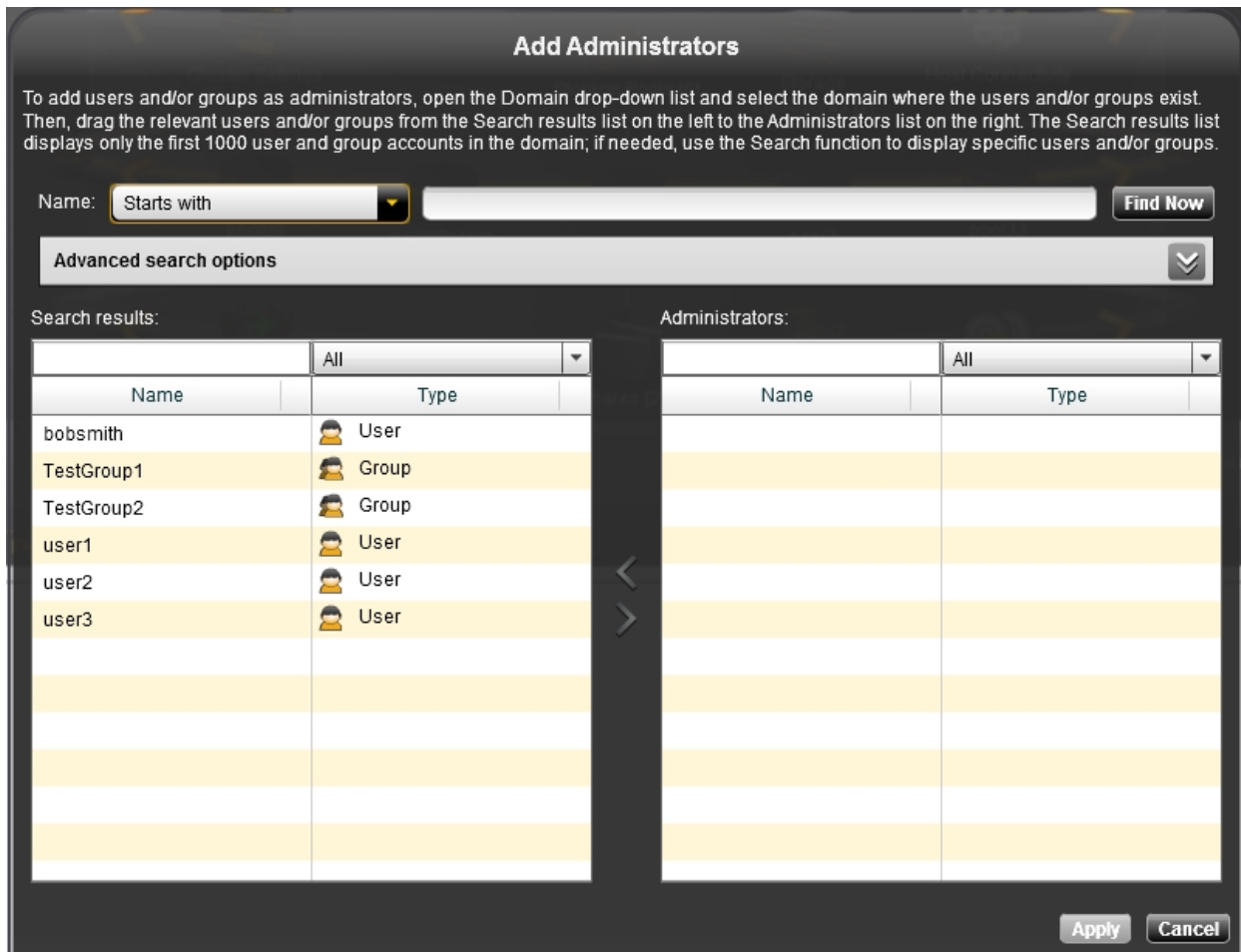
- Click **Apply** to save your settings.

► **To give users or groups Site Administrator access from the tree:**

Tip This method allows you to give Site Administrator access for multiple users and/or groups in a single operation.

- Click the Site node to display its child nodes.
- Expand the Site node's Properties panel.
- Select the **Administrators** tab.
- Select **Add Administrator**. The Add Administrators panel displays.

Figure 4-2: Add Administrators panel



- From the **Domain** drop-down list, select the domain server(s) where the user or group that you want to give Site Administrator access to exists.

Note The panel displays the **Domain** drop-down list if Unity is integrated with a Microsoft Windows Active Directory domain or an LDAP Directory service. In a multiple domain environment, the **Domain** drop-down list contains all the domains on the network.

6. In the **Name** text box, type the name of the user or group that you want to give share-level access permissions to exists, and then, click the **Find Now** button to display the specified user or group.
If needed, you can use the **Find Now** function to display specific users and/or groups. For example, to display the user *Bob*:
 - a. Select the **Starts with** option from the pick list next to the Name text box.
 - b. Type **BO** (or **bo**) in the **Name** text box.
 - c. Click the **Find Now** button. Unity displays all users and/or groups with user and/or group names that start with the letters **b** and **o** in the **Search results** grid (on the bottom-left of the panel).

You can also use the **Advanced Search** function and set more specific search criteria; for more information, see [Users and Groups window](#) on page 75.

7. In the **Search results** list, select the user or group that you want to add as a Site Administrator.
Hold down SHIFT or CTRL and click the left mouse button to select multiple entries in the **Search results** list.
You can also search for specific users or groups, or filter the list, by entering a user or group name in the **Filter/Search** box located above the **Search results** list.
8. Drag the selected user(s) to the **Administrators** list, or click the *right* arrow to move the selection.
Note The **Administrators** list displays the users and groups that already have Site Administrator access to the system.
9. Click **Apply**.

Revoking Site Administrator access

This section describes how to revoke a user's or group's Site Administrator access to Unity.

► **To revoke a user's or group's Site Administrator access from the toolbar:**

1. [Open the Manage Users and Groups panel](#).
2. For multi-site environments: when the Manage Users and Groups panel displays, open the **Sites** drop-down list and select the site where the user or group that you want to revoke Site Administrator access from exists.
3. From the **Domain** drop-down list, in the Users and Group window at the top of the Manage Users and Groups panel, select the domain server(s) where the user or group that you want to revoke Site Administrator access from exists.

Note The panel displays the **Domain** drop-down list if Unity is integrated with a Microsoft Windows Active Directory domain or an LDAP Directory service. In a multiple domain environment, the **Domain** drop-down list contains all the domains on the network.

4. In the **Name** text box, type the name of the user or group that you want to give share-level access permissions to exists, and then, click the **Find Now** button to display the specified user or group.

If needed, you can use the **Find Now** function to display specific users and/or groups. For example, to display the user *Bob*:

- a. Select the **Starts with** option from the pick list next to the Name text box.
- b. Type **BO** (or **bo**) in the **Name** text box.
- c. Click the **Find Now** button. Unity displays all users and/or groups with user and/or group names that start with the letters **b** and **o** in the **Search results** grid (on the bottom-left of the panel).

You can also use the **Advanced Search** function and set more specific search criteria; for more information, see [Users and Groups window](#) on page 75.

5. On the bottom half of the Manage Users and Groups panel, select the **Access Rights** tab.
6. In the grid, select the site that you want to revoke the selected user's or group's access to.
7. When the site is highlighted in the grid, clear its corresponding check box in the **Access Allowed** column to revoke the user's or group's access to the site.
8. Click **Apply** to save your settings.

▶ **To revoke a user's or group's Site Administrator access from the tree:**

Tip This method allows you to revoke Site Administrator access for multiple users and/or groups in a single operation.

1. Click the Site node to display its child nodes.
2. Expand the Site node's Properties panel.
3. Select the **Administrators** tab.
4. On the Properties panel, select the user(s) and/or group(s) that you want to revoke Site Administrator access from.
Hold down SHIFT or CTRL and click the left mouse button to select multiple users and/or groups.
5. Click the **Remove** button. Unity prompts you to confirm removal.
6. Click **Yes** to confirm. Unity revokes Site Administrator access from the selected user(s) and/or group(s).

Giving Pool Administrator access

Pool Administrators have pool-level access to Unity, including the ability to create, delete, and manage shares, perform data replications, configure snapshots, and so on (refer to [Nexsan Unity roles and access rights](#) on page 67 for the full list of access rights).

You assign users and/or groups as Pool Administrators to a storage pool after you create the pool.

Note By default, Site Administrators are granted Pool Administrator access to all storage pools on the system.

▶ **To give a user or group Pool Administrator access from the toolbar:**

1. [Open the Manage Users and Groups panel](#).
2. For multi-site environments: when the Manage Users and Groups panel displays, open the **Sites** drop-down list and select the site where the user or group that you want to give Pool Administrator access to exists.

3. From the **Domain** drop-down list, in the Users and Group window at the top of the Manage Users and Groups panel, select the domain server(s) where the user or group that you want to give Pool Administrator access to exists.

Note The panel displays the **Domain** drop-down list if Unity is integrated with a Microsoft Windows Active Directory domain or an LDAP Directory service. In a multiple domain environment, the **Domain** drop-down list contains all the domains on the network.

4. In the **Name** text box, type the name of the user or group that you want to give file system-level access permissions to exists, and then, click the **Find Now** button to display the specified user or group.

If needed, you can use the **Find Now** function to display specific users and/or groups. For example, to display the user *Bob*:

- a. Select the **Starts with** option from the pick list next to the Name text box.
- b. Type **BO** (or **bo**) in the **Name** text box.
- c. Click the **Find Now** button. Unity displays all users and/or groups with user and/or group names that start with the letters **b** and **o** in the **Search results** grid (on the bottom-left of the panel).

You can also use the **Advanced Search** function and set more specific search criteria; for more information, see [Users and Groups window](#) on page 75.

5. On the bottom half of the Manage Users and Groups panel, select the **Access Rights** tab.
6. In the grid, select the storage pool that you want to give the selected user or group Pool Administrator access to.
7. When the storage pool is highlighted in the grid, select the corresponding check box in the **Access Allowed** column to give the user or group access to the storage pool.
8. Click **Apply** to save your settings.

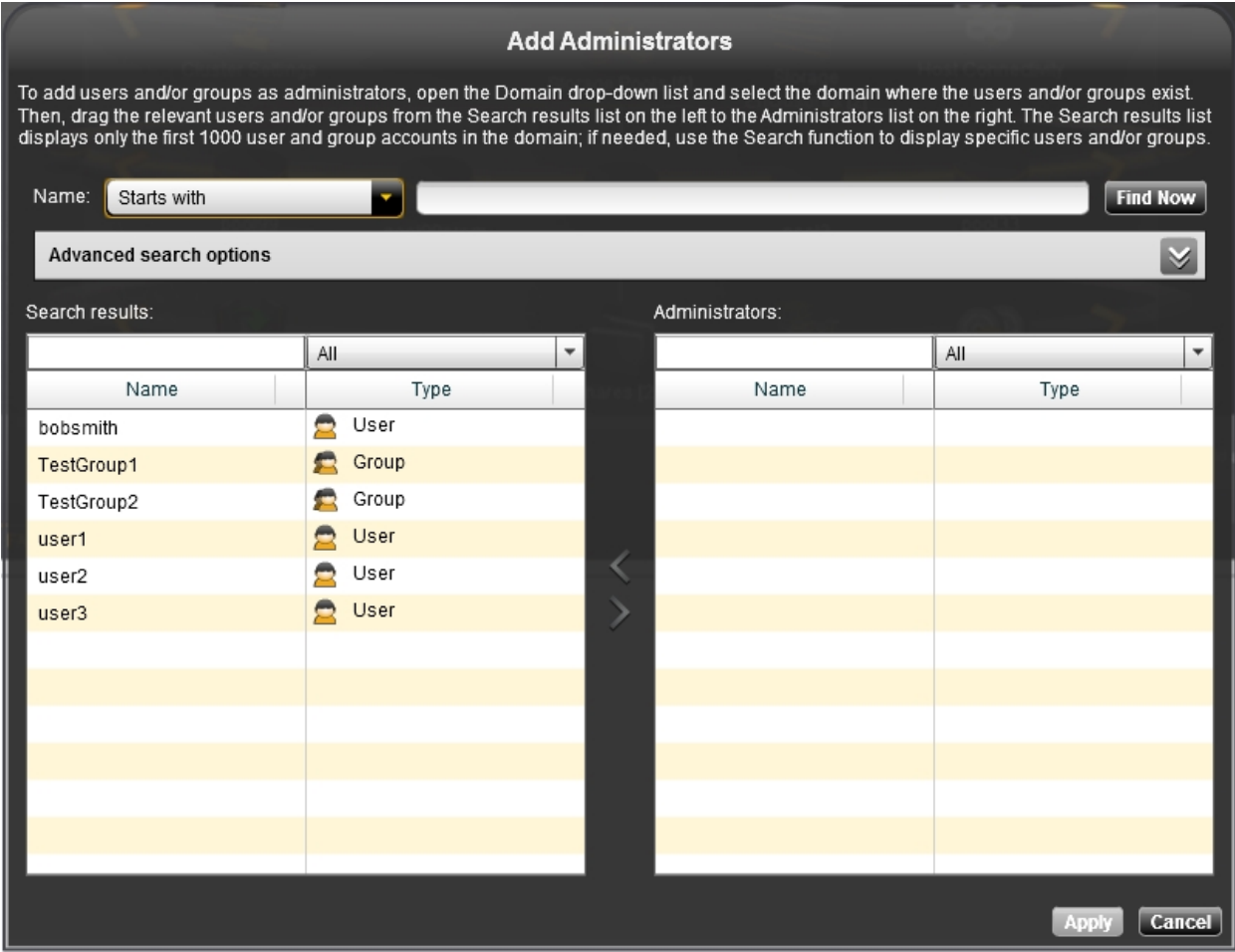
► **To give users and/or groups Pool Administrator access from the tree:**

Tip This method allows you to give Pool Administrator access to multiple users and/or groups in a single operation.

1. Click the Site node to display its child nodes.
2. Click the **Storage Pools** node.
3. Select the node belonging to the storage pool that you want to give a user or group Pool Administrator access to.
4. Expand the storage pool's Properties panel.
5. Select the **Administrators** tab.

6. Click **Add Administrator**. The Add Administrators panel displays.

Figure 4-3: Add Administrators panel—pool



7. From the **Domain** drop-down list, select the domain server(s) where the user or group that you want to give Pool Administrator access to exists.

Note The panel displays the **Domain** drop-down list if Unity is integrated with a Microsoft Windows Active Directory domain or an LDAP Directory service. In a multiple domain environment, the **Domain** drop-down list contains all the domains on the network.

You can give Pool Administrator access to users and groups from different domains, if needed.

8. In the **Name** text box, type the name of the user or group that you want to give file system-level access permissions to exists, and then, click the **Find Now** button to display the specified user or group.
If needed, you can use the **Find Now** function to display specific users and/or groups. For example, to display the user *Bob*:
 - a. Select the **Starts with** option from the pick list next to the Name text box.
 - b. Type **BO** (or **bo**) in the **Name** text box.
 - c. Click the **Find Now** button. Unity displays all users and/or groups with user and/or group names that start with the letters **b** and **o** in the **Search results** grid (on the bottom-left of the panel).
You can also use the **Advanced Search** function and set more specific search criteria; for more information, see [Users and Groups window](#) on page 75.
9. In the **Search results** list, select the user or group that you want to add as a Site Administrator.
Hold down SHIFT or CTRL and click the left mouse button to select multiple entries in the **Search results** list.
You can also search for specific users or groups, or filter the list, by entering a user or group name in the **Filter/Search** box located above the **Search results** list.
10. Drag the selected user(s) to the **Administrators** list. Or, click the *right* arrow to move the selection.
Note The **Administrators** list displays the users and groups that already have Pool Administrator access to the selected storage pool; this includes all Site Administrators on the system.
11. Click **Apply** to save your settings.

Revoking Pool Administrator access

This section describes how to revoke a user's or group's Pool Administrator access.

► **To revoke a user's or group's Pool Administrator access from the toolbar:**

1. [Open the Manage Users and Groups panel.](#)
2. For multi-site environments: when the Manage Users and Groups panel displays, open the **Sites** drop-down list and select the site where the user or group that you want to revoke Pool Administrator access from exists.
3. From the **Domain** drop-down list, in the Users and Group window at the top of the Manage Users and Groups panel, select the domain server(s) where the user or group that you want to revoke Pool Administrator access from exists.

Note The panel displays the **Domain** drop-down list if Unity is integrated with a Microsoft Windows Active Directory domain or an LDAP Directory service. In a multiple domain environment, the **Domain** drop-down list contains all the domains on the network.

4. In the **Name** text box, type the name of the user or group that you want to give file system-level access permissions to exists, and then, click the **Find Now** button to display the specified user or group.

If needed, you can use the **Find Now** function to display specific users and/or groups. For example, to display the user *Bob*:

- a. Select the **Starts with** option from the pick list next to the Name text box.
- b. Type **BO** (or **bo**) in the **Name** text box.
- c. Click the **Find Now** button. Unity displays all users and/or groups with user and/or group names that start with the letters **b** and **o** in the **Search results** grid (on the bottom-left of the panel).

You can also use the **Advanced Search** function and set more specific search criteria; for more information, see [Users and Groups window](#) on page 75.

5. On the bottom half of the Manage Users and Groups panel, select the **Access Rights** tab.
6. In the grid, select the storage pool that you want to revoke the selected user's or group's Pool Administrator access from.
7. When the storage pool is highlighted in the grid, clear its corresponding check box in the **Access Allowed** column to revoke the user's or group's access to the storage pool.
8. Click **Apply** to save your settings.

► **To revoke a user's or group's Pool Administrator access from the tree:**

1. Click the Site node to display its child nodes.
2. Click the **Storage Pools** node to display its child nodes.
3. Click the node belonging to the storage pool from which you want to revoke a user's or group's Pool Administrator access.
4. Expand the storage pool's Properties panel.
5. Select the **Administrators** tab.
6. Select **Remove**. Unity prompts you to confirm removal.
7. Click **Yes** to confirm. Unity revokes the selected user's or group's Pool Administrator access from the storage pool.

Managing users and groups with Nexsan Unity

When Unity is configured to use Unity authentication, you must add users, and optionally, groups, to the system. You can then give an Unity administrative role—Site Administrator or Pool Administrator—to a user or group that you add to the system, as well as give each user or group access permissions to shares on the system.

To add users or groups to the system, you use the Manage Users and Groups panel.

Note When you use Unity authentication, the process for giving a user or group Site or Pool Administrator access to the system is the same as when Unity is connected to a Microsoft Active Directory domain or an LDAP Directory service; for more information, see [Setting access rights](#) on page 82.

This section includes these topics:

Adding a user account	90
Adding a group	91
Adding a user to a group	92
Removing a user from a group	93
Deleting a user or a group	94
Changing a user's password	94
Changing the nxadmin password	95

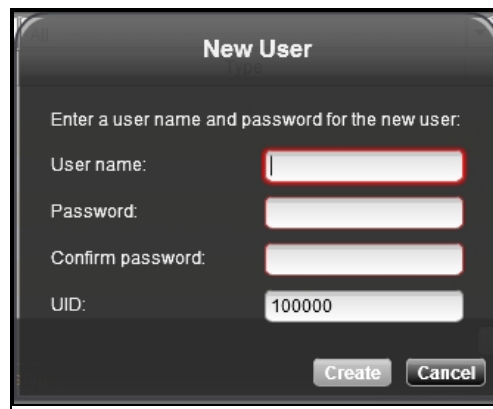
Adding a user account

This section describes how to add a [user account](#) to the system when using Unity authentication.

► **To add a user account:**

1. [Open the Manage Users and Groups panel](#).
2. For multi-site environments: when the Manage Users and Groups panel displays, open the **Sites** drop-down list, and select the site where you want to add a user account.
3. Click the **New User** button. This displays the New User dialog box.

Figure 4-4: New User dialog box



4. Enter the user's name in the **User name** field.

The user name can contain up to 16 characters and it must be unique to the system. It can contain any combination of upper-case or lower-case characters except these special characters:

" / \ [] : ; | = , + * ? < >

A user name cannot consist solely of periods (.) and spaces. Be consistent in the way you enter user names because Unity presents lists of user and group accounts in alphabetic order. It is a good idea to establish a standard for user names, such as a shortened combination of the first and last names; for example, *PeteMar* for Peter Marquis.

Note User names are case-sensitive. When logging on to Unity, the user are required to enter the user name using the same combination of lower- and upper-case letters that you entered when creating the account.

5. Enter a password in the **Password** field.

The user password must be at least 6 characters long, up to a maximum of 256 characters. The password must contain at least one lower-case letter, one upper-case letter, and at least one numeric or one special character, such as: ! @ # \$ % ^ & *

As an example, this is a valid password:

ITUnow\$

But this is **not** a valid password:

ITUnow

Note If the user forgets the password, it cannot be recovered. However, the password can be reset; see [Changing a user's password](#) on page 94.

6. Repeat the password in the **Confirm password** field.
7. Provide a user identifier in the **UID** field.

You cannot use these UID numbers because they are reserved:

- 0 to 101
- 60001
- 60002
- 65534
- 90000 to 90050

If one of these IDs is already assigned to a user on your network, please contact Nexsan Technical Support to request that they free up the reserved ID.

8. Click **Create**. The new user appears in the list of users and groups.

Adding a group

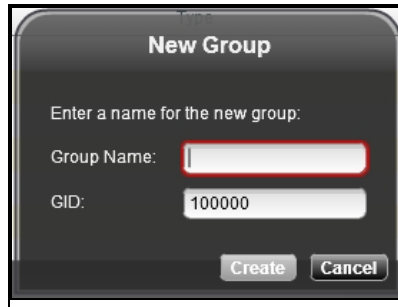
This section describes how to add a [group](#) to the system when using Unity authentication.

▶ To add a group:

1. [Open the Manage Users and Groups panel](#).
2. For multi-site environments: when the Manage Users and Groups panel displays, open the **Sites** drop-down list, and select the site where you want to add a group account.

3. Click the **New Group** button. This displays the New Group dialog box.

Figure 4-5: New Group dialog box



4. Enter a name for the group in the **Group Name** field.

The group name can contain up to 16 characters and it must be unique to the system. It can contain any combination of upper-case or lower-case characters except these special characters:

“ / \ [] : ; | = , + * ? < >

A group name cannot consist solely of periods (.) and spaces. Be consistent in the way you enter group names because Unity presents lists of user and group accounts in alphabetic order.

5. Provide a group identifier in the **GID** field.

You cannot use these GID numbers because they are reserved:

- 0 to 101
- 60001
- 60002
- 65534
- 90000 to 90050
- 99999

If one of these IDs is already assigned to a user on your network, please contact Nexsan Technical Support to request that they free up the reserved ID.

6. Click **Create**. The new group appears in the list of users and groups.

Adding a user to a group

If you want to add a [user](#) to a [group](#) with Site Administrator access to the system, you must be logged on as the Unity Administrator (**nxadmin**).

▶ **To add a user to a group:**

1. [Open the Manage Users and Groups panel](#).
2. For multi-site environments: when the Manage Users and Groups panel displays, open the **Sites** drop-down list, and select the site where you want to add a user account.

3. Perform one of the following actions:

To...	Do this
use the user's Group Memberships tab	<ol style="list-style-type: none"> In the Name text box, type the name of the user that you want to add to a group, and then, click the Find button to display the specified user or group. In the Group Membership tab, open the groups drop-down list and select the group that you want to add the user to. On the bottom half of the Manage Users and Groups panel, select the Group Membership tab. The Group Membership tab displays the groups that the user belongs to. Click the Grant Membership button to add the user to the group.
use the group's Group Members tab	<ol style="list-style-type: none"> In the Name text box, type the name of the group that you want to add a user to, and then, click the Find button to display the specified group. On the bottom half of the Manage Users and Groups panel, select the Group Members tab. The Group Members tab displays the users that are members of the group. In the Group Members tab, select the user that you want to add to the group from the users list. Click the Add User button to add the user to the group.

4. Click **Apply** to save your settings.

Removing a user from a group

This section describes how to remove a user from a group when using Unity authentication.

Note If you want to remove a user from a group with Site Administrator access to the system, you must be logged on as the Unity Administrator (**nxadmin**).

► **To remove a user from a group using the group's Group Members tab:**

- [Open the Manage Users and Groups panel.](#)
- For multi-site environments: when the Manage Users and Groups panel displays, open the **Sites** drop-down list, and select the site where you want to remove a user from a group.

- Perform one of these actions:

To...	Do this
use the group's Group Members tab	<ol style="list-style-type: none"> In the Name text box, type the name of the group that you want to remove a user from, and click the Find button to display the specified group. On the bottom half of the Manage Users and Groups panel, select the Group Members tab. The Group Members tab displays the users that are members of the selected group. In the list of users, select the user that you want to remove from the group. Click the Remove Selected User button to remove the user from the group.
use the group's Group Memberships tab	<ol style="list-style-type: none"> In the Name text box, type the name of the group that you want to remove a user from, and click the Find button to display the specified group. On the bottom half of the Manage Users and Groups panel, select the Group Memberships tab. The Group Memberships tab displays the groups that the user is a member of. Click the Revoke Membership button to remove the user from the group. In the list of groups, select the group that you want to remove the user from.

- Click **Apply** to save your settings.

Deleting a user or a group

This section describes how to delete a user or a group when using Unity authentication.

► **To delete a user or a group:**

- [Open the Manage Users and Groups panel.](#)
- For multi-site environments: when the Manage Users and Groups panel displays, open the **Sites** drop-down list, and select the site where you want to remove a user from a group.
- In the **Name** text box, type the name of the group that you want to remove a user from, and then, click the **Find** button to display the specified group.
- Click the **Delete** button to remove the user or group from the system. Unity prompts you to confirm deletion.
- Click **Yes** to confirm.

Changing a user's password

This section describes how to change a user's password when using Unity authentication.

Note Any user currently logged on the system, including the Nexsan Unity Administrator (**nxadmin**), can change their account password by selecting the **Change My Password** option from the Manage Users menu in the Nexsan Unity toolbar.

► **To change a user's password:**

- [Open the Manage Users and Groups panel.](#)
- For multi-site environments: when the Manage Users and Groups panel displays, open the **Sites** drop-down list, and select the site where you want to remove a user from a group.

- In the **Name** text box, type the name of the group that you want to remove a user from, and then, click the **Find** button to display the specified group.
- Click the **Change Password** button. The Change Password dialog box opens.

Figure 4-6: Changing a user's password

- Type the new password in the **New password** field.
The user password must be at least 6 characters long, up to a maximum of 256 characters. The password must contain at least one lower-case letter, one upper-case letter, and at least one numeric or one special character, such as: ! @ # \$ % ^ & *

As an example, this is a valid password:

ITUnow\$

But this is **not** a valid password:

ITUnow

Note If the user forgets the password, it cannot be recovered. However, the password can be reset; see [Changing a user's password](#) on the previous page.

- Repeat the password in the **Confirm password** field.
- Click **Save** to set the new password for the user account and close the Change Password dialog box.

Changing the nxadmin password

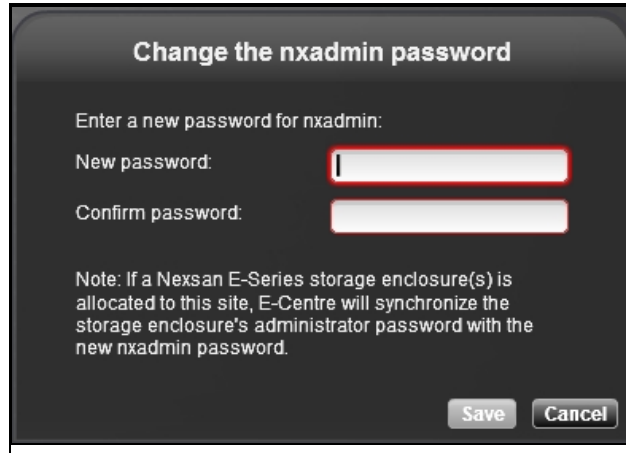
This section describes how to change the Administrator (nxadmin) account's password.

Note You must be logged on the system as Unity's Administrator (**nxadmin**) to perform these steps.

► **To change the nxadmin password:**

1. In the Nexsan Unity toolbar, click **Security and Permissions**.
2. Select the **Change My Password** option. The Change the nxadmin password dialog box opens.

Figure 4-7: Changing the nxadmin password



3. Type a password in the **Password** field.

The nxadmin password must contain a minimum of 6 characters and a maximum of 16 characters. It must contain one upper-case letter, one lower-case letter, AND one numeric character OR one of these special characters:

! \$ % & ' () * + , - . < > [] ^ _ ` { | } ~

For example, this is a valid password:

ITUnow\$

But this is not a valid password:

ITUnow

Note If Unity has a Nexsan storage system connected to it, Unity also automatically changes the Administrator password for the storage system, since that password is synchronized with the Unity Administrator (**nxadmin**).

4. Repeat the password in the **Confirm password** field.
5. Click **Save** to set the new password and close the Change Password dialog box.

Chapter 5

Storage Pools

A storage pool is a user-defined virtual grouping of volumes available on the Unity. Storage pools allow you to organize your storage into logical groups; expose file systems as shares to Windows-based (CIFS) and/or UNIX/Linux-based (NFS) clients on the network; and replicate all the data in the pool, or just a subset of it, for disaster recovery.

Unity provides several tools for managing storage pools on Unity.

Creating a storage pool	98
Scrubbing a storage pool	105
Adding volumes to a storage pool to expand capacity	107
Adding volumes to a replicated storage pool	109
Replacing a volume in a storage pool	110
Storage Pool Properties Panel	112
Modifying the snapshot auto-deletion setting for a storage pool	112
Enabling data compression on the storage pool	113
Enabling the Access Time mode on a storage pool	114
Viewing space usage information for storage pools	115
Setting space usage notification thresholds for a storage pool	115
Moving a storage pool	116
Viewing and clearing storage pool errors	118
Deleting a storage pool	120

Creating a storage pool

The first steps in getting started with managing your storage using Unity is creating a storage pool on Unity, and then exposing all or part of the pool as a share to CIFS and/or NFS clients, or as a block device (LUN) to iSCSI initiators on the network.

Unity includes wizard-based configuration tools to help you create a storage pool, and then set up shares and LUNs within that pool.

This section includes these topics:

Before you begin	98
Mixing volumes with different RAID levels	98
Adding a storage pool	100

Before you begin

If your Unity deployment is set up to use the Unity authentication, you may want to consider adding additional user accounts to the system that you can then assign as Pool Administrators to the storage pool. You may also want to add user accounts for file system-level access; you can then configure the relevant access permissions when you create file systems. For more information, see [Setting access rights](#) on page 82.

▶ **How to allocate storage on your Unity:**

- Take into account the number of file systems and/or LUNs that you need per storage pool, and divide the disk space in the storage pool accordingly. When allocating disk space, keep in mind that metadata and snapshots also consume storage.
- Consider future capacity requirements, particularly when allocating space usage to file systems and LUNs.
- You are not required to allocate all available volumes to the storage pool when you initially create the pool. However, keep in mind that any unallocated volumes remain unused on the system until you allocate them to the storage pool.
- Consider how you intend to expose file systems on the system: using [CIFS sharing](#) (to Windows-based systems), [NFS sharing](#) (to UNIX/Linux-based systems), or using both [CIFS and NFS](#) sharing.
- Consider the users and groups that will access the file systems, as well as the file systems-level access permissions that you need to give each user and/or group.
- If your deployment includes Unity Data Replication package, make sure the remote Unity that you intend to use as your replication site has adequate storage capacity to match the capacity on the primary site.
- If your deployment includes the Data Replication and/or Snapshots features, make sure there is enough storage capacity for both replicated data and scheduled snapshots of your data.
- If your deployment includes Nexsan storage enclosures attached externally to your Unity, make sure the system(s) is properly connected to Unity and that it is powered on.

Mixing volumes with different RAID levels

If you have multiple storage systems connected, Unity gives you the flexibility to configure different RAID levels on each storage system, depending on your requirements. However, you cannot mix volumes from different RAID levels to create a storage pool, as this can negatively impact performance; specifically, the storage pool inherits the performance of the less efficient or slower RAID level.

For example, if you have two Unity Storage System connected, you can set RAID 5 on the storage system that you will use mostly for read data, and RAID 10 on the second system, where you intend to store data

from mission critical applications (in particular, database applications). RAID 5 is the most cost effective option for both performance and redundancy, and it is well-suited for read-oriented applications; RAID 10, on the other hand, is a more expensive option since it requires more drives, but it offers excellent performance and redundancy for mission critical data. If you mix volumes from both these RAID levels to create a storage pool, the pool will inherit the performance of RAID 5, and only some of the redundancy of RAID 10.

This table highlights restrictions for mixing volumes.

Table 5-1: Storage systems and volume combinations

Storage system(s)	Volume mixing supported
Nexsan E5100 Storage (internal storage)	Not applicable
Nexsan E5100 Storage (internal storage) and NST5100X Unity Storage Expansion	Yes, if the RAID configuration is the same on both enclosures
US224X Unity Storage Expansion (connected via SAS)	Yes, if multiple Unity Storage Expansions are connected to Unity (in a daisy-chain configuration) and if the RAID configuration is the same on all enclosures
Nexsan E18, Nexsan E48, or Nexsan E60 storage system (connected via SAS or Fibre Channel)	Yes, if multiple systems are connected to Unity and if the RAID configuration is the same on all enclosures

Property settings order of precedence

When setting storage pool and dataset properties, Unity sets this order of precedence:

1. **Local:** The property setting is set locally at the storage pool or dataset level.
2. **Received:** The property setting is received from replication; the replicated storage pool automatically gets the same property settings as the primary pool. The dataset also gets the same property settings as the primary dataset, with some exceptions.
3. **Inherited:** The property setting is inherited from the parent at creation time. Datasets inherit the same property settings as the storage pool they belong to. Shares also inherit the same property settings as the parent file system.

Since a setting made locally takes precedence over inheritance, any changes made at the dataset level override the setting made at the storage pool level after creation. Similarly, any changes made at the storage pool level do not get inherited to existing datasets. Only new datasets created after the change will inherit the property settings of the storage pool.

This table summarizes the property settings that storage pools and datasets both have in common and their order of precedence. Property settings that are specific to shares and LUNs are not listed in this table.

Note L stands for Local, R for Received and I for Inherited.

Table 5-2: Order of precedence for new and updated pools and datasets

Property setting	Storage pool	Datasets	
		New	Existing
Access time, Data compression, and Auto-deletion	If...	Then...	
At pool creation time	Enabled (L) Disabled (L)	Enabled (I) Disabled (I)	N/A
Changes made at storage pool level	Enabled to Disabled (L) Disabled to Enabled (L)	Disabled (I) ¹ Enabled (I)	Enabled (I) ² Disabled (I)
Changes made at dataset level	Enabled (L) Disabled (L)	N/A - setting not available at dataset creation time	Enabled to Disabled (L) Disabled to Enabled (L)

Table 5-3: Order of precedence for replication

Property setting	Storage pool		Datasets	
	Primary	Remote	Primary	Remote
Access time	If...	Then...	If...	Then...
At replication time	Enabled (L) Disabled (L)	Enabled (R) Disabled (R)	Enabled (I or L) Disabled (I or L)	Disabled (L) Disabled (L)
Data compression	If...	Then...	If...	Then...
At replication time	Enabled Disabled	Enabled (R) Disabled (R)	Enabled (I or L) Disabled (I or L) Both ³	Enabled (R) Disabled (R) Disabled (L)
Auto-deletion of snapshots	If...	Then...	If...	Then...
At replication time	Enabled Disabled	Enabled (R) Disabled (R)	Enabled (I or L) Disabled (I or L)	Enabled (R) Disabled (R)

Adding a storage pool

Unity provides the Storage Pool Setup Wizard to guide you through the process of creating a storage pool.

¹Inherited from storage pool update

²Inherited from storage pool creation

³If you enable and then disable data compression (or vice-versa) for a dataset before replication, data compression is always disabled at the remote site.

► **To start the Storage Pool Setup Wizard:**

1. Under the site node, click the **Storage Pools** node to select it.
2. Perform one of these actions:

To...	Do this
use the Storage Pool's context menu	<ol style="list-style-type: none"> a. Click the context menu button on the Storage pool node. b. When the node context menu opens, click Add a Storage Pool.
use the Storage Pool's Properties panel	<ol style="list-style-type: none"> a. Click the Properties tab at the bottom of the screen to expand the Properties panel. b. Click Adda Storage Pool. button on the Properties panel.

The Storage Pool Setup Wizard starts. The wizard includes 4 steps that you must complete in the order presented to successfully create a storage pool.

This section includes these steps:

[Step 1: Adding volumes to the storage pool](#) below

[Step 2: Allocating FASTier cache devices to the storage pool](#) on page 103

[Step 3: Verifying settings](#) on page 104

[Step 4: Viewing configuration results](#) on page 105

Note [Step 2: Allocating FASTier cache devices to the storage pool](#) on page 103 is only displayed if Unity is configured with FASTier cache devices. If not, there are only 3 steps in the Storage Pool Setup Wizard. For more information about FASTier cache devices, please contact your Nexsan reseller or Nexsan Support Representative.

Step 1: Adding volumes to the storage pool

In *Step 1* of the Storage Pool Setup Wizard, you add volumes to the storage pool and specify a name for the pool. The panel for step 1 displays the site where Unity adds the new storage pool, as well as the storage systems that are connected to Unity.

► **To add volumes to the storage pool:**

1. In the devices/volumes list on the right side of the panel, expand each device (if there are multiple devices allocated to this site) to display their volumes; to expand a device and display its volumes, click the arrow button preceding the device name.

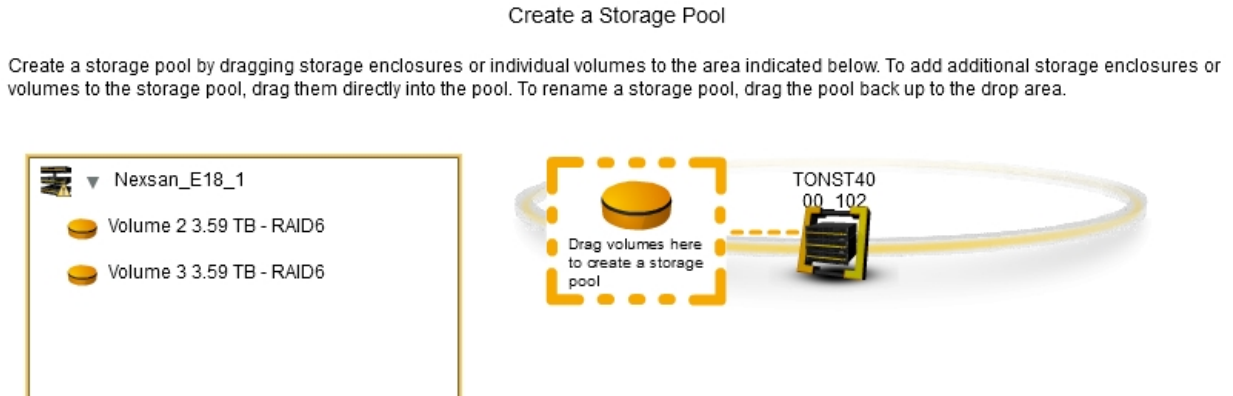
2. Select the volumes that you want to add to the pool.

To select multiple entries in the list, hold down SHIFT or CTRL and click the left mouse button.

To add all underlying volumes of a device to the storage pool, select the device.

Depending on the RAID configuration, you may not be able to combine volumes from different storage systems to create the storage pool; for more information, see.

Figure 5-1: Storage Pool Setup Wizard, step 1: add volumes to the storage pool



3. Drag your selection to the drop area indicated on the panel. As soon you drop the volumes in the drop area, the Storage Pool Setup Wizard prompts you to specify a name for the new pool and assign the pool to a Pool Resource Group (either Pool Resource Group 1 or 2).

Figure 5-2: Storage Pool Setup Wizard, step 1: specify a pool name



4. Type a name for the storage pool.

The name must start with an (upper-case or lower-case) alphabetic or numeric character; and, with the exception of the hyphen (-), and period (.), the name can only contain alphanumeric characters, without spaces.

These characters are NOT allowed:

" / \ _ [] : ; | = , + * ? < >

These names are reserved by the system: *mirror*, *spare*, and *log*; as are names that begin with this pattern: *c[0-9]*.

5. From the **Resource Group** drop-down, select the Pool Resource Group that you want to assign the storage pool to. Pool Resource Groups act as the virtual access point for the data (shares and/or LUNs) in storage pools. Specifically, end users and client systems on the network access their data in the storage pools using the corresponding Pool Resource Group's virtual IP address. Each Pool Resource Group is hosted on one of the two controller nodes in the cluster.

6. Once you type the name for the storage pool and assign it to a Pool Resource Group, click **OK**. The new pool appears under the site node in the Storage Pool Setup Wizard, with the volumes that you added to the storage pool appearing on a revolving bar directly below the pool.
7. Verify the new storage pool and your volume selections; if you are satisfied with your selections, click the right arrow on the panel to continue to [Step 2: Allocating FASTier cache devices to the storage pool](#) below.

Notes:

- You can rename the storage pool or change the Pool Resource Group it's assigned to by dragging the pool back up to the drop area; the Storage Pool Setup Wizard prompts you for a new name and Pool Resource Group to assign the storage pool to.
- You can add additional volumes and/or devices to the storage pool by dragging them directly into the pool.
- You can delete the new storage pool by dragging all its volumes back to the list of devices/volumes on the right side of the panel.

Step 2: Allocating FASTier cache devices to the storage pool

Step 2 is only displayed if Unity has FASTier cache devices installed. The wizard displays the total number of FASTier read, write, and read/write SSD cache devices available on Unity.

► General guidelines for assigning FASTier cache devices:


- You assign a read/write cache device as either read cache OR write cache.
- The Unity only uses read cache devices once the RAM cache on the system is full. Read cache devices are filled only as files are read. This means that the Unity uses read caching only on the second file access.
- Write-only cache devices aggregate smaller writes in one large write. They are particularly useful for many small, synchronous writes. Asynchronous writes will see no improvement.

Figure 5-3: Storage Pool Setup Wizard, step 2: allocate FASTier cache devices

Configure FASTier Cache: test

Assign Nexsan FASTier cache devices to the storage pool. Nexsan's FASTier SSD cache devices enhance the performance of the NST appliance by caching data during read or write operations on the system.

FASTier Devices

There is 1 FASTier device. 

1 FASTier Read	Use	<input style="width: 30px; text-align: center;" type="text" value="1"/>	▲▼	FASTier device(s) for read
0 FASTier Write				
0 FASTier Read or Write	Use	<input style="width: 30px; text-align: center;" type="text" value="0"/>	▲▼	FASTier device(s) for write

Summary

Read Devices Assigned: 0 FASTier Read

Write Devices Assigned: 0 FASTier Write, 0 FASTier Read or Write

► **To configure and allocate FASTier cache devices to the storage pool:**

1. Specify the number of read cache devices that you want to allocate to the storage pool by typing or selecting a value in the **Use FASTier device(s) for read** box .
2. For the Unity 5000, specify the number of write cache devices that you want to allocate to the storage pool by typing or selecting a value in the **Use FASTier device(s) for write** box .

For example, on an Unity with 2 FASTier read cache devices and 2 FASTier read/write cache devices:

- You can allocate all 4 cache devices as read cache, OR
- You can allocate 3 cache devices as read cache, and 1 cache device as write cache, OR
- You can allocate 2 cache devices as read cache, and 2 cache device as write cache.

As you select the number of read and write cache devices to allocate to the storage pool, the Summary section on the wizard panel automatically updates to display how your selections impact cache assignment on the system.

By default, FASTier write cache is assigned automatically on the Unity 4000.

By default, FASTier write cache is assigned automatically on the Unity 6000.

3. When you finish allocating FASTier cache devices to the storage pool, click the right arrow on the wizard panel to continue to [Step 3: Verifying settings](#) below.

Step 3: Verifying settings

Step 3 of the Storage Pool Setup Wizard summarizes the settings you selected for your pool and initiates the pool creation process when you click **Start**. Review the summary carefully before applying configuration settings.

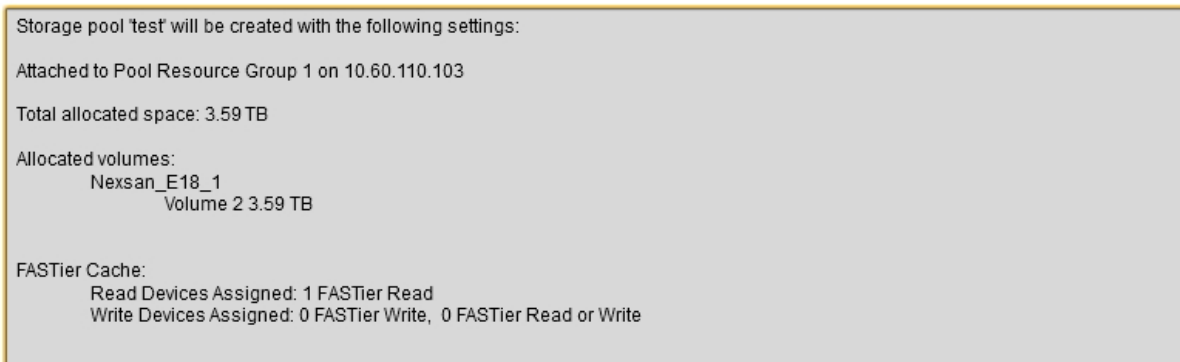
► **To change a configuration setting:**

- Click the back arrow to navigate back to the corresponding configuration step.
Or
- Click the corresponding step identifier at the top of the Storage Pool Setup Wizard panel. For example, if you want to rename the pool, click **Step 1**.

Figure 5-4: Storage Pool Setup Wizard, step 3: verifying settings

Verify Settings

Please verify your configuration settings. If you want to change a setting, click the back arrow to navigate to the relevant configuration panel. Or, click the step identifier at the top of the wizard panel to go back to a specific step.



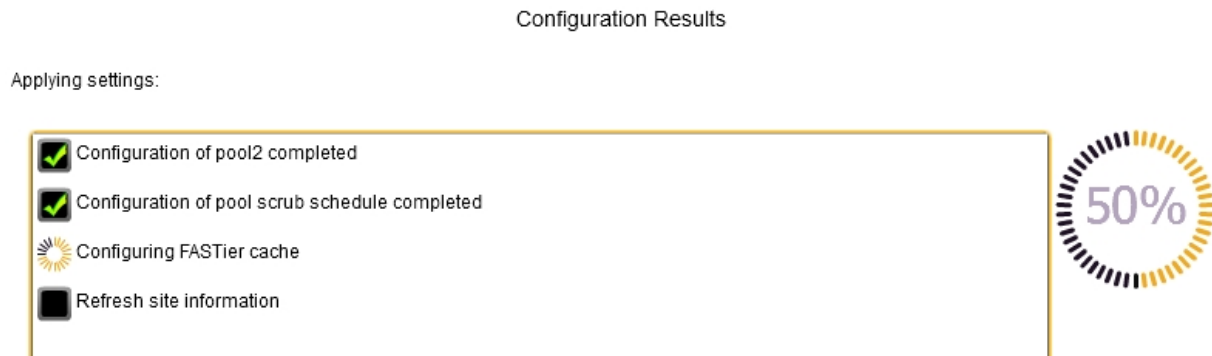
If you are satisfied with the settings, click the **Start** button at the bottom of the panel. The Storage Pool Setup Wizard automatically proceeds to [Step 4: Viewing configuration results](#) below, where you can view progress as Nexsan Unity creates the new storage pool and applies your configuration settings. If you configured data replication for the storage pool, Nexsan Unity also creates a replica of the storage pool on the remote Unity.

Step 4: Viewing configuration results

Step 4 of the Storage Pool Setup Wizard displays progress as Unity creates the new pool.

The Storage Pool Setup Wizard displays error events that the system encounters during the pool creation process. You can view more details about an error event by expanding the corresponding entry.

Figure 5-5: Storage Pool Setup Wizard, step 4: viewing progress



► To view more details for an error event:

- Click the plus (+) sign corresponding to the error event.

Unity's informs you when it successfully creates the storage pool, and prompts you to add a file system or LUN to the pool.

Figure 5-6: Add a share or LUN prompt



Choose one of these options:

- Click the **Add a file system** button to add a file system to the storage pool. This launches the file system Setup Wizard—see [Adding a file system using the Setup Wizard](#) on page 123.
- Click the **Add a LUN** button to add a LUN (block device) to the storage pool. This launches the LUN Setup Wizard—see [Adding a LUN](#) on page 216.
- Click **No** if you do not want to add a file system or a LUN. This closes the Storage Pool Setup Wizard.

Scrubbing a storage pool

Unity provides a pool scrubbing mechanism that checks the meta data that comprise the volumes in a storage pool on the Unity, for read or write errors.

Unity's pool scrubbing mechanism scans a storage pool to identify data integrity problems. It sequentially reads all the data on the hard disks, as well as the data's corresponding parity information, and rebuilds parity wherever needed. Performing routine scrubbing on a storage pool prevents parity errors and data corruption.

However, keep in mind that a pool scrub operation can consume significant system resources—depending on the amount of data to be processed. We recommend that you schedule pool scrub operations during off-peak business hours to prevent performance degradation on the system.

Unity allows you to manually initiate a pool scrub operation, or schedule automatic pool scrubbing.

This section these topics:

- [Performing a manual pool scrub below](#)
- [Modifying the scrub schedule for a storage pool below](#)

Performing a manual pool scrub

Tip You can also initiate a manual pool scrub on a storage pool's replica on the remote Unity; for more information, see the *Nexsan Unity Snapshots and Replication Guide*.

▶ **To manually initiate a pool scrub operation for a storage pool:**

1. If you are managing multiple sites (multi-site management of remote systems): in Unity's tree view, click the **Site** node where the storage pool that you want to scrub exists.
2. Click the **Storage Pools** node to display its child nodes.
3. Click the node representing the storage pool that you want to scrub.
4. Expand the storage pool node's Properties panel.
5. Click the **Scrub** button.

Tip You can also initiate a pool scrub operation by opening the storage pool node's context menu and selecting **Scrub**.

Unity starts the pool scrub operation. The progress of the scrub operation is displayed in the Tasks in progress panel.

If needed, you can stop the pool scrub operation by selecting the relevant task in the Tasks in progress panel, and clicking the **Stop Selected** button. In most cases, a pool scrub operation should continue to completion. Stop a scrub operation at your own discretion if system performance is impacted by the operation.

Modifying the scrub schedule for a storage pool

By default, when you add a storage pool to the site, Unity enables scheduled pool [scrubbing](#).

The default schedule for pool scrubbing is set to every 4 weeks, on Saturday, at 12 AM. The default schedule assumes that 12 AM on Saturdays is an off-peak business hour—which, typically, is the ideal time during which to perform pool scrub operations. If you change the default schedule, we recommend that you schedule scrub operations during off-peak business hours to prevent performance degradation.

Note If a storage pool is replicated, you can also configure a scrub schedule for the storage pool's replica on the remote site; see the *Nexsan Unity Snapshots and Replication Guide*.

▶ **To set or modify the scrub schedule for a storage pool:**

1. If you are managing multiple sites (multi-site management of remote systems): in Unity's tree view, click the **Site** node where the storage pool for which you want to set a scrub schedule exists.
2. Click the **Storage Pools** node.
3. Click the node representing the storage pool that you want to set a scrub schedule for.

4. Expand the storage pool node's Properties panel.
5. Select the **Scrub Schedule** tab.

Figure 5-7: Storage Pool's properties panel—Scrub Schedule tab

The screenshot shows the 'Scrub schedule' tab in the Unity interface. It features a tabbed header with 'Pool Properties', 'Scrub schedule', 'iSCSI Targets', and 'System Notifications'. Under the 'Scrub schedule' tab, there is a checked checkbox for 'Enable scrub Scheduling'. Below this, the 'Start date' is set to '2014/05/12' with a calendar icon, and the time is '12:00 AM'. The 'Recur every' field is set to '4' with a dropdown menu currently showing 'Week(s)'. The 'On:' section has radio buttons for days of the week, with 'Saturday' selected. At the bottom, a status message reads: 'This storage pool was last scrubbed on 2014/06/14 12:00:21 AM'.

6. Select the **Enable scrub Scheduling** option.
7. Modify the scrub schedule for the storage pool:
 - a. Modify the start date for the schedule by clicking the **Start date** field and selecting a date from the calendar.
 - b. Modify the time when you want Unity to perform pool scrub operations on the storage pool. The default time is 12 AM.
 - c. Select a new recurrence pattern for the schedule by typing a value in the **Recur every** field.
 - d. Select the recurrence type from the drop-down list: **Minutes(s)**, **Hour(s)**, **Day(s)**, **Week(s)**, or **Month(s)**.
8. When you finish modifying the scrub schedule for the storage pool, click **Apply** to save the new schedule.

Unity scrubs the storage pool according to the schedule you specify. Similar to a manual pool scrub operation, the progress of a scheduled scrub operation is displayed in the Tasks in progress panel.

If needed, you can stop a scheduled pool scrub operation by selecting the relevant task in the Tasks in progress panel, and clicking the **Stop Selected** button. In most cases, a pool scrub operation should continue to completion. Stop a scrub operation at your own discretion if system performance is impacted by the operation.

Adding volumes to a storage pool to expand capacity

You can add volumes to a storage pool to expand its capacity—if there are available volumes on the system.

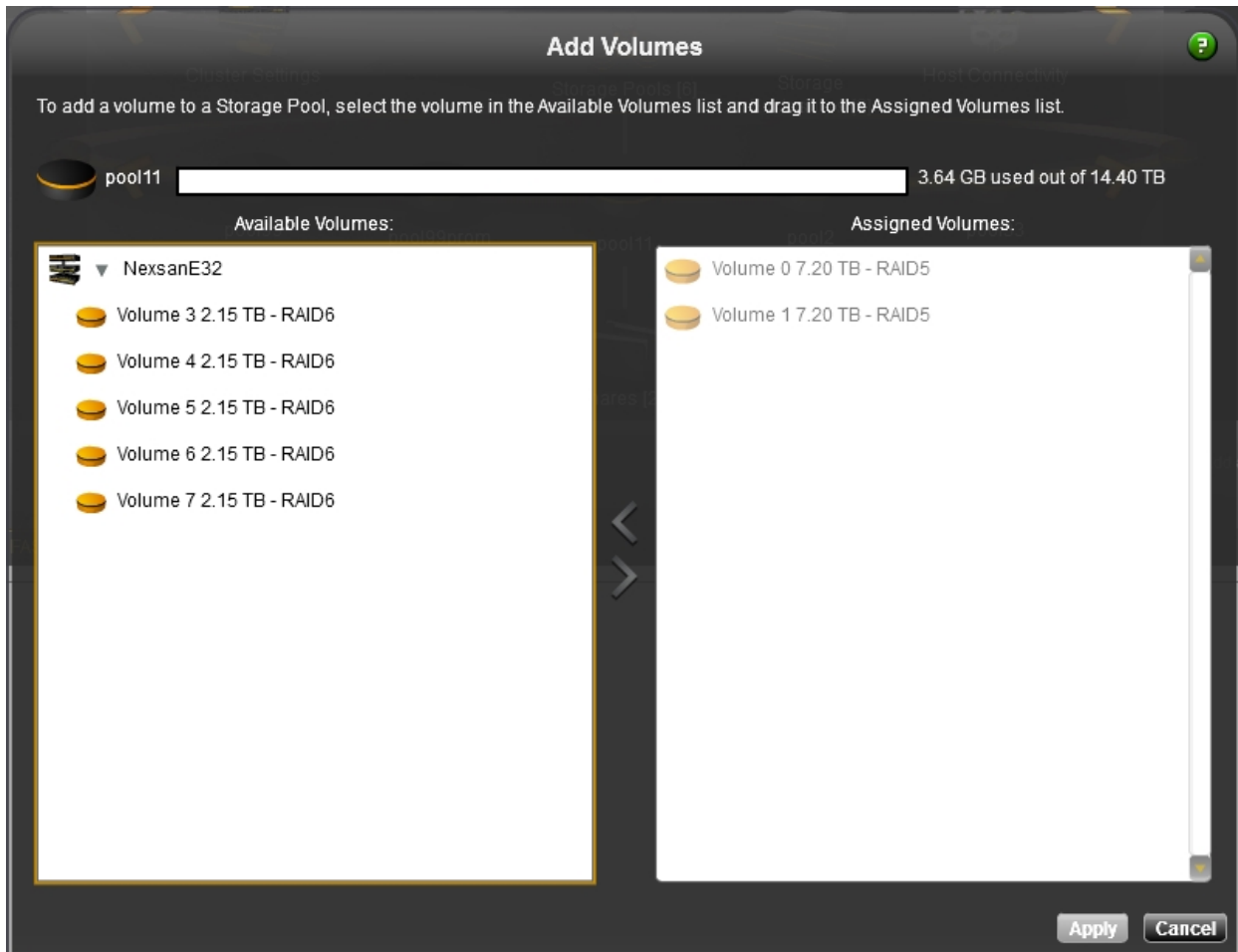
Note The process for adding volumes to a storage pool that is replicated to a remote Unity differs from the process for adding volumes to a non-replicated pool; for more information, see [Adding volumes to a replicated storage pool](#) on page 109.

► To add volumes to a storage pool:

1. If you are managing multiple sites (multi-site management of remote systems): in Unity's tree view, click the Site node where the storage pool that you want to add volumes to exists.
2. Click the **Storage Pools** node to display its child nodes.
3. Click the node representing the storage pool that you want to add volumes to.

- Expand the storage pool's Properties panel.
- Click the **Add a Volume** button. This opens the Add Volumes panel.

Note You can also open the Add Volumes panel by opening the storage poolnode's context menu and selecting **Add**.



5

The Add Volumes panel displays available volumes on all storage system(s) connected to Unity. For performance considerations, we highly recommend that you only add volume(s) with the same RAID level as the existing volume(s) in the storage pool; see [Mixing volumes with different RAID levels on page 98](#).

- In the **Available Volumes:** list on the Add Volumes panel, expand a storage system to display its available volumes.
- Select the volume that you want to add to the storage pool, and drag the volume to the **Assigned Volumes:** list.

Hold down SHIFT or CTRL and click the left mouse button to select multiple volumes. You can also select a storage system to add all its underlying volumes.

- Click **Apply** when you finish allocating volumes. Unity adds the volumes to the storage pool.

Adding volumes to a replicated storage pool

The Add Volume Wizard guides you through the process for adding volumes to a storage pool that is replicated to a remote site.

To learn about data replication and to enable replication for a storage pool, refer to the *Nexsan Unity Snapshots and Replication Guide*.

► To start the Add Volumes Wizard:

1. Under the site node where you want to add volumes to a storage pool, click the **Storage Pools** node.
2. Click the node representing the storage pool to which you want to add volumes.
3. Expand the storage pool's Properties panel.
4. Click **Add**.

Note You can also open the Add Volumes panel by opening the storage pool node's context menu and selecting **Add**.

The Add Volumes Wizard starts. The wizard includes 4 steps that you must complete in the order presented to successfully add volumes to the storage pool and its replica on the remote Unity.

This section includes these steps:

Step 1: adding volumes to the primary storage pool	109
Step 2: adding volumes to the storage pool's replica	109
Step 3: Verifying settings	110
Step 4: Viewing progress	110

Step 1: adding volumes to the primary storage pool

Step 1 displays available volumes on all storage enclosure(s) connected to Unity. We highly recommend that you only add volume(s) with the same RAID level as the existing volume(s) in the storage pool; see [Mixing volumes with different RAID levels on page 98](#).

► To add volumes to the source storage pool:

1. In the **Available Volumes:** list, expand a storage system to display its available volumes.
2. Select the volume that you want to add to the storage pool, and drag the volume to the **Assigned Volumes:** list.
Hold down SHIFT or CTRL and click the left mouse button to select multiple volumes. You can also select a storage system to add all its underlying volumes.
3. When you finish allocating new volumes to the storage pool, click the forward arrow on the panel to continue to [Step 2: adding volumes to the storage pool's replica below](#).

Step 2: adding volumes to the storage pool's replica

In *step 2* of the Add Volumes Wizard, you allocate new volumes to the storage pool's replica on the remote site. For synchronous replication, you must match volumes one-to-one on both sites.

Note This step is optional for asynchronous replication. You can add volumes to the replica at a later time, if needed; see [Adding volumes to a storage pool to expand capacity on page 107](#).

Step 2 displays available volumes on all storage enclosure(s) connected to the remote Unity. We highly recommend that you only add volume(s) with the same RAID level as the existing volume(s) in the replicated storage pool; see [Mixing volumes with different RAID levels on page 98](#).

There are two ways to add volumes to the replica:

► **To manually allocate volumes on the remote site:**

1. In the **Storage on Remote System** list box on the left-hand side of the panel, highlight the corresponding storage system on the remote site—where the volume(s) that you want to allocate to the replica of the storage pool exists—by selecting the storage system in the list.
2. Expand the storage system to display its available volumes, by clicking the arrow preceding the device name.
3. Drag the volume(s) that you want to allocate to the replica of the storage pool to the **Remote Volumes** list box.
4. When you finish allocating new volumes to the storage pool's replica, click **Add a Volume** on the panel to continue to *step 3*.

► **To allow Unity to suggest volume allocation:**

1. Click the **Suggest Allocation** button below the **Storage on Remote System** list box.
Unity automatically allocates volumes to the replica of the storage pool, based on the size of the volume—or, if the storage pool has multiple volumes allocated to it, based on the total combined size of the volumes—that you allocated to the source, or primary, storage pool.
2. Click the right arrow on the panel to continue to [Step 3: Verifying settings](#) below.

Step 3: Verifying settings

Step 3 of the Add Volumes Wizard summarizes your configuration settings and adds the volumes you selected to the primary storage pool, as well as to the storage pool's replica on the remote site, when you click **Start**.

Review the summary carefully before proceeding.

► **To change a configuration setting:**

- Click the back arrow to navigate back to the corresponding configuration step.
Or
- Click the step identifier at the top of the Add Volumes Wizard panel to go back to a specific step. For example, if you want to change volume allocation for the storage pool's replica, click **Step 2**.

If you are satisfied with the configuration settings, click the **Start** button at the bottom of the panel. The Add Volumes Wizard automatically moves forward to [Step 4: Viewing progress](#) below.

Step 4: Viewing progress

Step 4 of the Add Volumes Wizard displays progress while it adds the volumes you selected to the primary storage pool and to the storage pool's replica on the remote site.

The Add Volumes Wizard displays any error events that the system encounters during the configuration process. You can view more details about an error event by expanding the corresponding entry.

► **To view more details for an error event:**

Click the plus (+) sign corresponding to the error event.

Replacing a volume in a storage pool

If a physical disk drive(s) associated with a volume in a storage pool fails, you can replace the volume with another volume from the corresponding storage enclosure, or with a volume on another storage enclosure.

This feature is only available for storage pools that you create with volumes from a Nexsan E-Series storage enclosure.

► **To replace a volume:**

1. If you are managing multiple sites (multi-site management of remote systems): in Unity's tree view, click the Site node where the storage pool that you want to replace a volume on exists.
2. Click the **Storage Pools** node to display its child nodes.
3. Click the node representing the storage pool where you want to replace a volume.
4. Expand the storage pool's Properties panel.
5. Click the **Volumes** tab.
6. Select the volume to be replaced from the list.
7. Click the **Replace** button. This opens the Replace Volume panel.

Note You can also open the Replace Volume panel by opening the storage pool node's context menu and selecting **Replace Volume**.

Tip Likewise, you can open the Replace Volume panel by selecting the desired E-Series storage enclosure under the **Storage Enclosures** node, and then selecting the volume under the **Volumes** tab. This can be useful if you do not remember to which storage pool the volume is associated.

The Replace Volume panel displays available volumes on all storage system(s) connected to Unity. For performance considerations, we highly recommend that the replacement volume(s) you select has the same RAID level as the volume(s) you are replacing; see [Mixing volumes with different RAID levels on page 98](#).

8. In the **Available Volumes:** list on the Replace Volume panel, expand a storage system to display its available volumes.
9. Select the volume that you want to allocate as the replacement volume, and drag the volume to the **Replacement Volume:** box. If the volume is a suitable replacement—in terms of disk space capacity—a check mark displays.
10. Click **Apply**.
11. A Replacing Volume popup window appears briefly.

This process triggers a resilvering operation while Unity copies the data from the original volume to its replacement. The resilvering operation can take some time to complete, depending on the amount of data to copy.

During the resilvering operation, a warning condition trickles down through Unity's tree view indicating that the corresponding storage pool is in a degraded state: a yellow warning icon (exclamation mark) is superimposed over the relevant node to indicate the warning condition. You can ignore this warning condition; Unity clears the warning once the resilvering operation completes. For more information about error and warning conditions related to storage pools and their underlying volumes, see [Viewing and clearing storage pool errors on page 118](#).

Storage Pool Properties Panel

From this panel, you can perform the following tasks:

- [Adding volumes to a storage pool to expand capacity on page 107](#)
- [Deleting a storage pool on page 120](#)
- [Moving a storage pool on page 116](#)
- [Performing a manual pool scrub on page 106](#)

If this is a replicated pool, you can perform the following tasks:

- [Performing a failover of a storage pool on page 453](#)
- [Adding volumes to a replicated storage pool on page 109](#)

Pool Properties tab

- [Modifying the snapshot auto-deletion setting for a storage pool below](#)
- [Enabling the Access Time mode on a storage pool on page 114](#)
- [Enabling data compression on the storage pool on the facing page](#)

Scrub Schedule tab

- [Modifying the scrub schedule for a storage pool on page 106](#)

System Notifications tab

- [Setting space usage notification thresholds for a storage pool on page 115](#)

Volumes tab

- Allows you to view volumes currently used in this storage pool, the amount of space used, and the associated storage enclosure.

Administrators tab

- [Giving Pool Administrator access on page 85](#)
- [Revoking Pool Administrator access on page 88](#)

VSS Client tab

- [Enabling the Microsoft VSS client for LUNs on page 263](#)

Modifying the snapshot auto-deletion setting for a storage pool

The snapshot auto-deletion mechanism lets you specify a global setting for Unity to automatically start deleting snapshots for datasets (file systems and iSCSI LUNs) that have the snapshot auto-deletion function enabled. The global setting that you specify for snapshot auto-deletion is a disk space consumption threshold for a storage pool, using a percentage value.

The default is 80%. TheUnity deletes snapshots—starting with the oldest automatic snapshot on the system—until used disk space capacity in the storage pool falls below the 80% threshold.

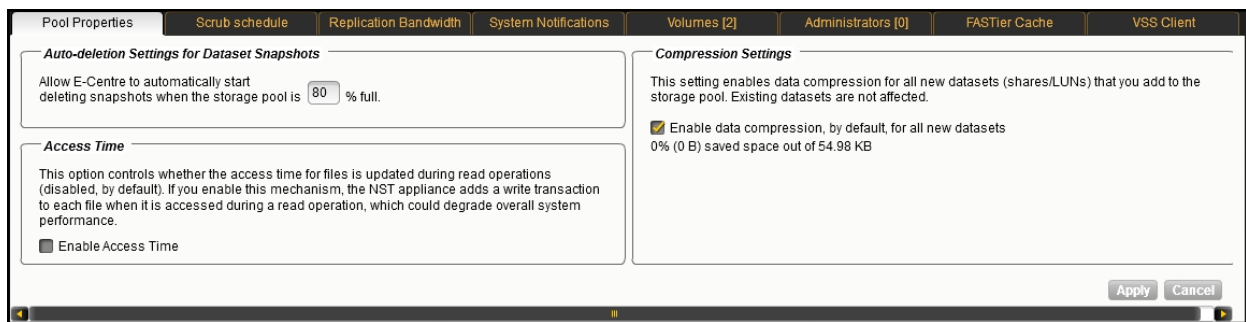
Unity **ONLY** deletes snapshots for datasets (shares and iSCSI LUNs) that have the snapshot auto-deletion function enabled.

Note Snapshot auto-deletion settings are configured from the primary storage pool only. If the storage pool is replicated, the snapshots will also be automatically deleted from its replica using the same threshold, during a subsequent replication session.

► **To set or modify the snapshot auto-deletion setting for a storage pool:**

1. If you are managing multiple sites (multi-site management of remote systems): in Unity's tree view, click the Site node where the storage pool for which you want to set a scrub schedule exists.
2. Click the **Storage Pools** node.
3. Click the node representing the storage pool for which you want to modify the snapshot auto-deletion setting.
4. Expand the storage pool node's Properties panel.
5. Select the **Pool Settings** tab.
6. In the **Auto-deletion Settings for Dataset Snapshots** section, type a disk space consumption threshold value for the storage pool.

Figure 5-8: Storage Pool's properties panel—Pool Properties tab



7. When you finish modifying the snapshot auto-deletion setting for a storage pool, click **Apply**.

Enabling data compression on the storage pool

You can enable compression at the pool level on Unity. Any new dataset (shares or LUNs) created in that pool will inherit the pool settings, thus will also have compression enabled. Existing datasets are not affected. If you wish to enable or disable compression on a specific share or LUN; see [Enabling/disabling data compression on a LUN](#) on page 230 or [Enabling/disabling data compression on a file system](#) on page 141.

Compression allows for better performance of the storage pool since the files to read/write are much smaller. However, it will also increase CPU usage. Compression can be enabled/disabled at any time. Disabling data compression affects all new data written to the storage pool; existing data remain compressed.

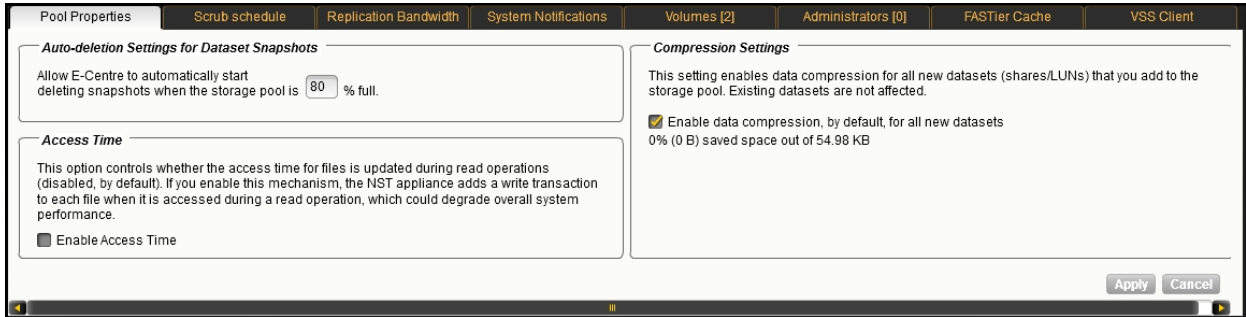
Note When you set up replication for storage pools that have the compression setting enabled, pools on the remote site inherit the compression settings. However, shares and LUNs belonging to the remote pool remain with data compression disabled.

► **To enable compression for a storage pool:**

1. Click the Site node.
2. Click the **Storage Pools** node.

3. Click the storage pool for which you want to enable data compression.
4. Expand the storage pool's Properties panel.
5. Select the **Pool Properties** tab.

Figure 5-9: Storage Pool's properties panel—Pool Properties tab



6. Select the **Enable data compression** option.
7. Click **Apply**.

Enabling the Access Time mode on a storage pool

The Access Time mode controls whether the access time for files is updated when they are read. By default, the Access Time mode is disabled; this avoids producing write traffic when reading files and results in significant performance gain.

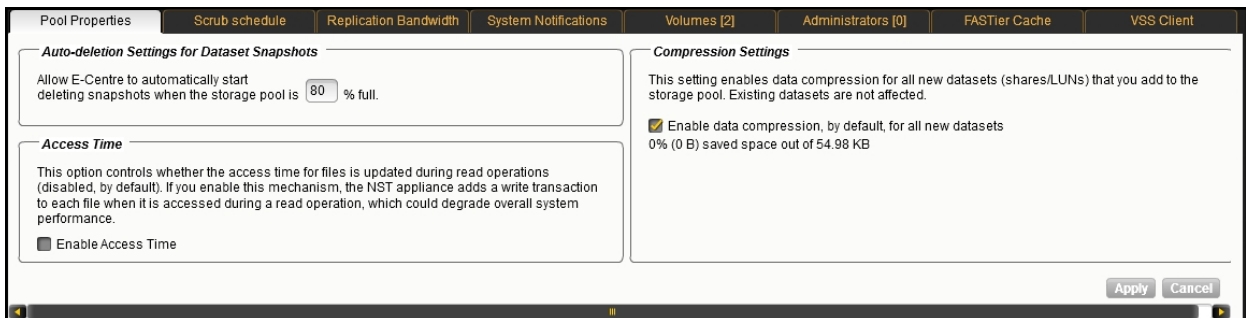
The Access Time mode can be set at the share level or pool level. This value can be modified at any time. To enable it for a specific share, see [Enabling the Access Time mode on a file system](#) on page 142.

Note When you enable the Access Time mode at the pool level, only new shares added to the pool after the change will inherit the setting. Existing shares remain unchanged. Replicated pools will inherit the pool settings; however, replicated shares always keep the Access Time mode disabled.

▶ To enable the Access Time mode for a pool:

1. In Unity's tree view, click the Site node.
2. Click the **Storage Pools** node.
3. Click the storage pool for which you want to enable the Access Time mode.
4. Expand the storage pool's Properties panel.
5. Select the **Pool Properties** tab.

Figure 5-10: Storage Pool's properties panel—Pool Properties tab



6. Select the **Enable Access Time** option.
7. Click the **Apply** button.

Viewing space usage information for storage pools

Unity gives you a detailed overview of each storage pool's used and available disk space.

► To access the Storage Pools node's Properties panel:

1. In Unity's tree view, click the Site node.
2. Click the **Storage Pools** node.
3. Expand the Storage Pools node's Properties panel. The **Storage Pools** tab displays a grid that lists all pools created for the site.

Figure 5-11: Storage pools node's properties panel—Storage Pools tab

Name	Health	Total	Available	User Data	Snapshots	Reserved	System	Compression Savings	FASTier Read	FASTier Write
FinancePool2015	OK	421.24 MB	418.57 MB	77.73 KB	0 B	0 B	2.59 MB	0% (0 B)	0	0

Tip Double-click a storage pool in the grid to open the pool's properties panel and display its child nodes.

► Columns related to space usage:

- **Capacity:** The total allocated space from volumes added to the storage pool.
- **Available:** The amount of space that is available for writing data or for reserving space. Space that is reserved but not used is not counted.
- **User Data:** The amount of user data that is currently written to the storage pool, excluding snapshots.
- **Snapshots:** The amount of space consumed by snapshots, including reservation added for snapshots.
- **Reserved:** The amount of reservation for all user-created datasets, including both used and unused space.
- **System:** The amount of space reserved for all system-created datasets.

► Related topics:

[Setting space usage notification thresholds for a storage pool](#) below

[Adding volumes to a storage pool to expand capacity](#) on page 107

Setting space usage notification thresholds for a storage pool

Unity allows you to set space usage thresholds for storage pools to trigger email notifications if space consumption in the storage pool reaches or exceeds a threshold that you set for the pool:

- **Critical:** an email notification is triggered when the space consumption in the storage pool reaches the value that you set for this threshold. An email notification is triggered again when space consumption exceeds this threshold. The default critical threshold is set to 95% of the total available disk space in the storage pool; this means that when disk space consumption in the storage pool reaches or exceeds 95% of the pool's total capacity, space usage in the pool is considered to be in critical state.

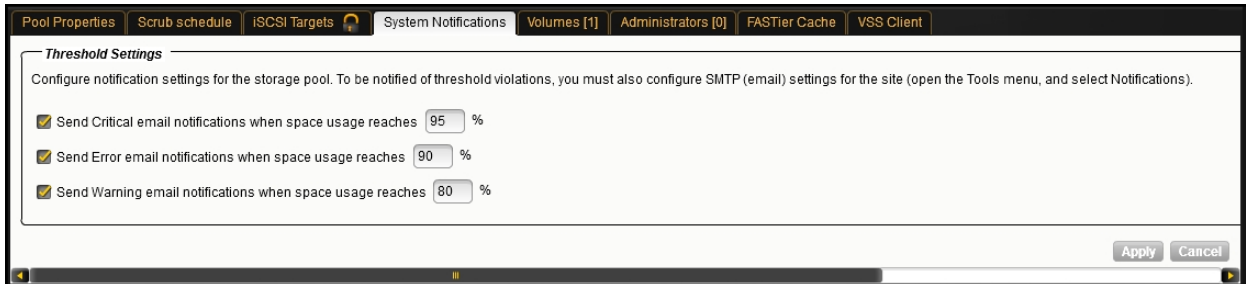
- **Error:** an email notification is triggered when the space consumption in the storage pool reaches the value that you set for this threshold. An email notification is triggered again when space consumption exceeds this threshold. The default error threshold is set to 90% of the total available disk space in the storage pool; this means that when disk space consumption in the storage pool reaches or exceeds 90% of the pool's total capacity, space usage in the pool is considered to be in error state.
- **Warning:** an email notification is triggered when the space consumption in the storage pool reaches the value that you set for this threshold. An email notification is triggered again when space consumption exceeds this threshold. The default warning threshold is set to 80% of the total available disk space in the storage pool; this means that when disk space consumption in the storage pool reaches or exceeds 80% of the pool's total capacity, space usage in the pool is considered to be in warning state.

Note In order for Unity to send email notifications when space consumption reaches or exceeds a threshold that you set for the storage pool, you must first configure SMTP settings and system notification settings for the site; for more information, see [Event logging and notification](#) on page 517.

► **To set or modify space usage notification thresholds for a storage pool:**

1. Click the Site node where the storage pool that you want to set space usage thresholds for exists.
2. Click the **Storage Pools** node.
3. Click the node representing the storage pool that you want to set space usage thresholds for.
4. Expand the storage pool node's Properties panel
5. Select the **System Notification Settings** tab.

Figure 5-12: Storage Pool's properties panel—System Notifications tab



6. Enable the threshold setting that you want to receive email notifications for by selecting the corresponding option, and then set a percentage value for the threshold. For example:
To receive an email notification when space consumption reaches or exceeds **critical** level:
 - a. Select the **Send critical notification when space usage reaches** option.
 - b. Type a threshold percentage value in the text box.

Notes:

- By default, all threshold settings are enabled. To disable a threshold setting, clear its check box.
- Space usage thresholds settings that you set at the storage pool-level become the default space usage threshold settings for new shares that you add to the storage pool.

7. Click **Apply** to set the new threshold settings for the storage pool.

Moving a storage pool

You can move a storage pool from the Pool Resource Group to which the storage pool is currently assigned to the other Pool Resource Group.



CAUTION: This process may result in data loss. You should only move a storage pool if you need to rebalance the I/O load on the system, since this changes the virtual end point through which end users and client systems access data sets (shares and/or LUNs) in the storage pool. When you move a storage pool from one Pool Resource Group to the other, the data sets in the storage pool are no longer accessible through the virtual IP address of the Pool Resource Group that the storage pool was previously assigned to.

You will need to manually update all share and LUN mappings on client systems to reflect the virtual IP address of the Pool Resource Group that you move the storage pool to; for more information, see [Example of data access in a typical Unity cluster implementation](#) on page 300.

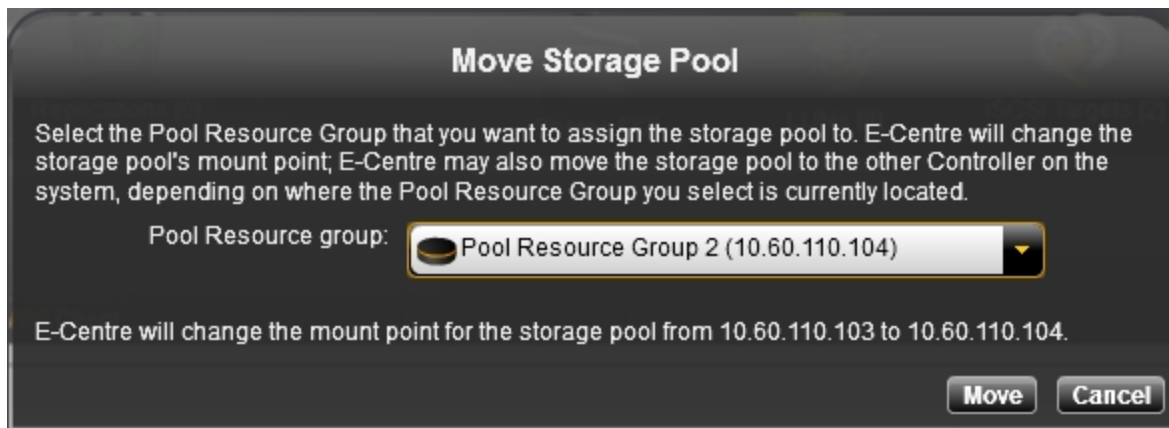
Before proceeding, make sure that client systems with an active connection to any shares or LUNs in the storage pool that you want to move are disconnected; also make sure to quiesce any applications with an active connection to Unity.

You can move a storage pool from the pool's properties panel or from the controller's node.

► **To move a storage pool using the pool's properties panel:**

1. In Unity's tree view, click the Site node.
2. Click the **Storage Pools** node.
3. Click the Storage pool that you want to move.
4. Click the **Move Storage Pool** button on the pool's Properties panel, or select the **Move Storage Pool** option from the pool node's context menu.
5. The Move Storage Pool dialog box appears. Unity selects the other Pool Resource Group node automatically. Click the **Move** button.

Figure 5-13: Move Storage Pool dialog box



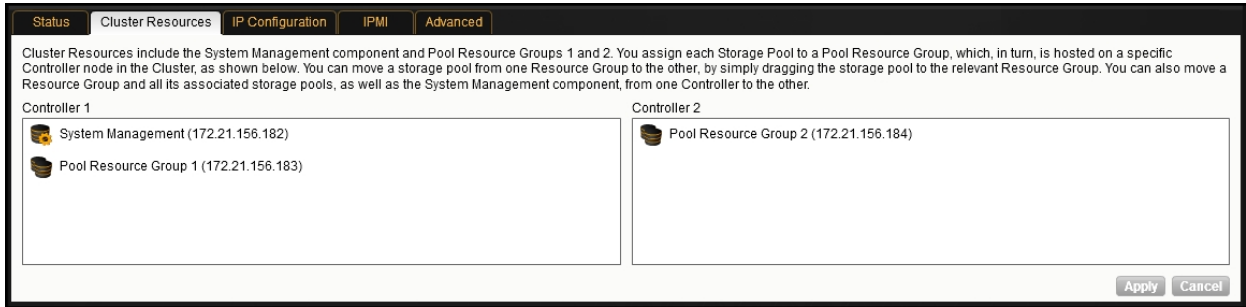
6. When prompted to confirm the action, click **Yes**. Unity informs you when the process completes.

► **To move a storage pool using the Cluster settings properties panel:**

1. If you are managing multiple sites: in Unity's tree view, click the Site node representing the clustered Unity that you want to perform a manual switchover on.
2. Click the **Cluster Settings** node.
3. Expand the Cluster Properties panel, by clicking the **Properties** tab.

4. Select the **Cluster Resources** tab to see a visual representation of where each resource in the cluster is currently hosted: Controller 1 or Controller 2. In addition, the **Cluster Resources** tab indicates the Pool Resource Group that each storage pool on the systems is currently assigned to.

Figure 5-14: Cluster Settings properties panel—Cluster Resources tab



5. Select the storage pool that you want to move to by clicking it in the corresponding Controller box, and then drag the storage pool to the Pool Resource Group that you want to move the storage pool to.
6. If needed, move additional storage pools.
7. Click the **Apply** button.
8. When prompted to confirm the action, click **Yes**. Unity informs you when the process completes.

Viewing and clearing storage pool errors

Unity displays the health status of storage pools and their underlying volumes using error or warning indicators in Unity's tree view. These indicators are superimposed over node icons to help you identify where the error condition originates. You can then drill down Unity's tree view to see more details about the error, including suggestions or instructions for resolving the error condition; and, if applicable, you can clear the error condition once you take the necessary corrective measures.

For example, if Unity detects that one of the disks associated with a storage pool's volume has failed, Unity may display this error condition in the tree view when you mouse-over the corresponding storage pool.

Figure 5-15: Storage Pool error


Error message: One or more devices has experienced an error resulting in data corruption. Applications may be affected. To clear the error state, go to the Storage Pools node and click the Details button in its Properties panel.

When you rest the cursor over a storage pool or volume node with an error or warning condition, Unity displays more details about the error.

This table lists possible error conditions related to storage pools and their underlying volumes, and the corresponding error or warning indicator that Unity displays in the tree view.

Table 5-4: Storage pool error conditions

Error condition indicator	Error condition
	FAULTED: this error condition indicates that one or more disks associated with the corresponding storage pool's volume(s) has failed. The storage pool

Error condition indicator	Error condition
	<p>continues functioning, but in a degraded state.</p> <p>UNAVAILABLE: this error condition indicates that one or more disks associated with the corresponding storage pool's volume(s) are faulted in response to persistent errors. There are insufficient replicas for the storage pool to continue functioning.</p> <p>OFFLINE: this error condition indicates that the storage pool is offline; this may be due to the storage system where the pool exists being turned off, or disconnected from Unity.</p>
	<p>DEGRADED: this error condition indicates that a resilvering operation is currently underway on the storage pool. Unity triggers a resilvering operation when:</p> <ul style="list-style-type: none"> ● you replace a disk drive associated with a volume; ● a disk drive fails and a hot spare is brought online to replace the failed drive; ● you replace a volume with a new volume. <p>During the resilvering operation, Unity copies the data from one disk to another, or from one volume to another.</p> <p>The storage pool continues functioning, but in a degraded state. This error condition is cleared once the resilvering operation completes.</p> <p>If Unity triggers a resilvering operation due to a hot spare being brought online, the status of the corresponding storage pool changes to FAULTED after the resilvering operation completes; this is to indicate that one or more disks associated with the corresponding storage pool's volume(s) has failed.</p>

Note Not all error conditions can be cleared: for example, if a storage pool is in the UNAVAILABLE, OFFLINE, or DEGRADED state (due to a resilvering operation), clearing the error condition has no effect.

► **To view an error or warning related to a storage pool and clear the error state:**

1. If you are managing multiple sites (multi-site management of remote systems): in Unity's tree view, click the Site node where the storage pool that you want to view errors for exists.
2. Click the Storage Pools node to display its child nodes.
3. Click the node representing the storage pool that you want to view errors for.
4. Expand the storage pool node's Properties panel
5. Click the **Status Details** button. This opens the Pool State Details popup.
6. The Pool State Details popup provides details about the error or warning condition. If applicable, the Pool State Details popup provides suggestions or instructions for resolving the error condition. For example, if a disk associated with the corresponding storage pool's volume(s) has failed, the Pool State Details popup instructs you to replace the failed drive and then clear the error condition; in most cases, the Pool State Details popup also indicates the bay number where the disk drive is located in the Unity chassis.

7. Once you take the necessary corrective measure to resolve the error condition—for example, you replace the failed disk drive on Unity—select the **Attempt to clear error state** option to clear the error condition.
8. Click the **OK** button.

Deleting a storage pool

This section explains how to delete a storage pool on Unity.



CAUTION: Deleting a storage pool also deletes all shares and their underlying data in the storage pool, including snapshots of the data. If the storage pool is replicated, Unity will ask you if you want to also delete the storage pool's replica on the remote site, or if you want to promote the storage pool's replica to primary pool.

► **To delete a storage pool:**

1. In Unity's tree view, click the Site node to display its child nodes.
2. Click the **Storage Pools** node.
3. Perform one of these actions:

To...	Do this
Use the storage pool's node context menu	<ol style="list-style-type: none"> a. Select the node representing the storage pool that you want to delete. b. Click the context menu button to open the node context menu. c. When the node context menu opens, select Delete Pool.
Use the Storage Pools node's Properties panel	<ol style="list-style-type: none"> a. Expand the Storage Pool node's Properties panel. The Storage Pool node's Properties panel displays all the storage pools on the system. b. In the grid, select the storage pool that you want to delete from the system. c. Click the Delete Pool button.
Use the storage pool's Properties panel	<ol style="list-style-type: none"> a. Select the node representing the storage pool that you want to delete. b. Expand the storage pool's Properties panel. c. Click the Delete Pool button.

4. Unity prompts you to confirm the action. Type **Yes** in the text box.
5. Click **Yes** to delete the storage pool.

Chapter 6

File Systems

A file system is added to a storage pool on the Unity, and then exposed to Windows and UNIX/Linux-based systems on the network using one of these [sharing methods](#):

- [CIFS sharing](#) allows you to expose a share to Windows-based systems using the Common Internet File System (CIFS) protocol.
- [NFS sharing](#) allows you to expose a share to UNIX/Linux-based systems using the Network File System (NFS) protocol.
- [FTP sharing](#) allows you to expose a share to Windows- or UNIX/Linux-based systems using the File Transfer Protocol. This sharing method is only visible when using Unity authentication. FTP support must be enabled at the site level beforehand; see [Enabling FTP support on page 405](#).
- [CIFS and/or NFS and/or FTP sharing](#) allows you to expose a share to Windows and UNIX/Linux-based systems over all protocols (in mixed environments).

CIFS and/or NFS and/or FTP sharing allow you to expose a share to Windows and UNIX/Linux-based systems over all protocols (in mixed environments).

Note FTP access is available only when a Unity Storage System is using local authentication.

This section includes these topics:

Overview of data management functions on file systems	122
Before you begin	122
Adding a file system using the Setup Wizard	123
Modifying file system properties	134
Viewing space usage information for file systems	149
Deleting a file system	149
Managing home directories	151
Managing shares	168
Viewing mount point information for file systems	186
Managing access permissions to shares	186
Managing snapshots for file systems	194
Nexsan Unity n-Way Sync	207

Overview of data management functions on file systems

Unity includes several data management functions that protect the data in your shares from unauthorized access and also ensure continuous availability of the data.

This section provides a quick overview of the data management functions that are available in Unity:

- **Data security using access permissions:** Permissions define the type of access granted to a user or group for a file system that you add to a storage pool, and subsequently expose to Windows (CIFS) or UNIX/Linux (NFS) clients of Unity. You can give users and/or groups either Read, Write, or Full access permissions to a share on the system, or you can allow all users and groups on the network to anonymously access a file system. For more information about access permissions, see [Managing access permissions to shares](#) on page 186.
- **Space usage configuration and capacity planning:** Unity allows you to configure space usage reservations and/or quotas for each file system. When you set a space usage reservation for a file system, Unity reserves the specified amount of disk space in the storage pool for the file system. A usage quota allows Unity to dynamically expand a file system's storage capacity when the file system runs out of disk space; you can set a fixed quota limit to prevent the file system's storage capacity from increasing beyond a certain size, or you can set the quota to unlimited to allow the file system's storage capacity to grow in relation to the storage pool's available disk capacity. For more information about configuring space usage for a file system, see [Accessing an NFS file system from UNIX/Linux](#) on page 177.
- **Disaster recovery with Data Replication:** Unity allows you to replicate the data contained in each file system to a remote Unity site, including setting replication schedules. You can use the Data Replication feature to replicate all the file system in a storage pool or select only a subset of file system to replicate. If the primary site goes down (for routine maintenance or a natural disaster), Unity allows you to failover your entire site, or just a storage pool and its associated file systems, to the replicated site.
- **Data protection using Snapshots:** Unity allows you to take point-in-time snapshots of the data contained in each file system, including scheduled automatic snapshots. This allows you to maintain a set of previous versions of all files in a file system. You can then browse or traverse the contents of a snapshot just as you would its corresponding file system—except the snapshot is read-only—and restore individual files and/or folders as needed. You can also roll back the data in a file system to a specific point-in-time snapshot. For more information about the Snapshots feature, see .
- **Data backups with NDMP support:** Unity allows you to configure Unity as a Network Data Management Protocol (NDMP) host to participate in remotely-coordinated automatic backups.

Before you begin

Planning the content, size, and distribution of file systems on Unity can improve performance, manageability, and overall ease-of-use of the system.

You should carefully choose the contents of a file system to avoid two common pitfalls: having too many file systems of a very specific nature; or having very few file systems of a general nature. For example, file systems for general use are easier to set up in the beginning, but can cause problems later. A better approach is to create separate file systems with a specific purpose or group of users in mind.

However, creating too many file systems also has its drawbacks. For example, it is much more efficient to create a *home* file system rather than creating separate file systems for each user's home directory; for more information, see [Managing home directories](#) on page 151.

In general, by keeping the number of file systems and other resources low, the performance of Unity is optimized.

Before you add file systems to a storage pool on Unity, review these guidelines:

- Take into account the number of file systems that you need per storage pool, and divide the disk space in the storage pool accordingly. When allocating disk space, keep in mind that file system metadata and snapshots also consume storage.
- Consider future capacity requirements, particularly when allocating space usage to file system.
- Consider how you intend to expose file systems: either CIFS sharing, NFS sharing, FTP sharing (Nexsan Unity authentication only), or CIFS and/or NFS and/or FTP sharing.
- Consider the users and groups that will access the file systems as well as the share-level access permissions that you need to give each user and group.

Adding a file system using the Setup Wizard

Unity provides the File System Setup Wizard to guide you through the process of creating a file system.

► To start the File System Setup Wizard:

1. Under the site node, click the Storage Pools node to select it and display its child nodes.
2. Click the storage pool to select it and display its child nodes.
3. Click the **File Systems** node to select it.
4. Perform one of these actions:

To...	Do this
use the File System context menu	<ol style="list-style-type: none"> a. Click the context menu button on the File Systems node to open the node context menu. b. When the node context menu opens, click Add.
use the File System Properties panel	<ol style="list-style-type: none"> a. Click the Properties tab at the bottom of the screen to expand the File System Properties panel. b. Click the Add a File System button on the File System Properties panel.

► To start the File System Setup Wizard:

1. Under the site node, click the Storage Pools node to select it and display its child nodes.
2. Click the storage pool to select it and display its child nodes.

3. Click the **File Systems** node to select it.
4. Perform one of these actions:

To...	Do this
use the File System context menu	<ol style="list-style-type: none"> a. Click the context menu button on the File Systems node to open the node context menu. b. When the node context menu opens, click Add.
use the File System Properties panel	<ol style="list-style-type: none"> a. Click the Properties tab at the bottom of the screen to expand the File System Properties panel. b. Click the Add a File System button on the File System Properties panel.

The File System Setup Wizard starts. The wizard includes the following steps that you must complete in the order presented to successfully create a file system.

This section includes these steps:

[Step 1: Creating a file system and configuring space usage below](#)

[Step 2: Configuring the access method on page 126](#)

[Step 3: Enabling data replication and configuring snapshot scheduling on page 127](#)

[Step 4: Configuring your archive settings on page 129](#)

[Step 5: Verifying settings on page 131](#)

[Step 6: Viewing configuration results on page 132](#)

Note [Step 3: Enabling data replication and configuring snapshot scheduling on page 127](#) is only displayed if your Unity deployment includes Unity's Data Protection feature. For more information about Snapshots and Data Replication, please contact your Nexsan reseller or Nexsan Support Representative.

Step 1: Creating a file system and configuring space usage

Step 1 of the File System Setup Wizard prompts you to specify a name for the file system, enable Collaboration Features and linking, and configure space usage settings for the file system. You can change space usage settings for the file system once the file system is created and added to the storage pool.

► **To create a file system:**

1. Enter a name for the file system in the **File System Name** field.

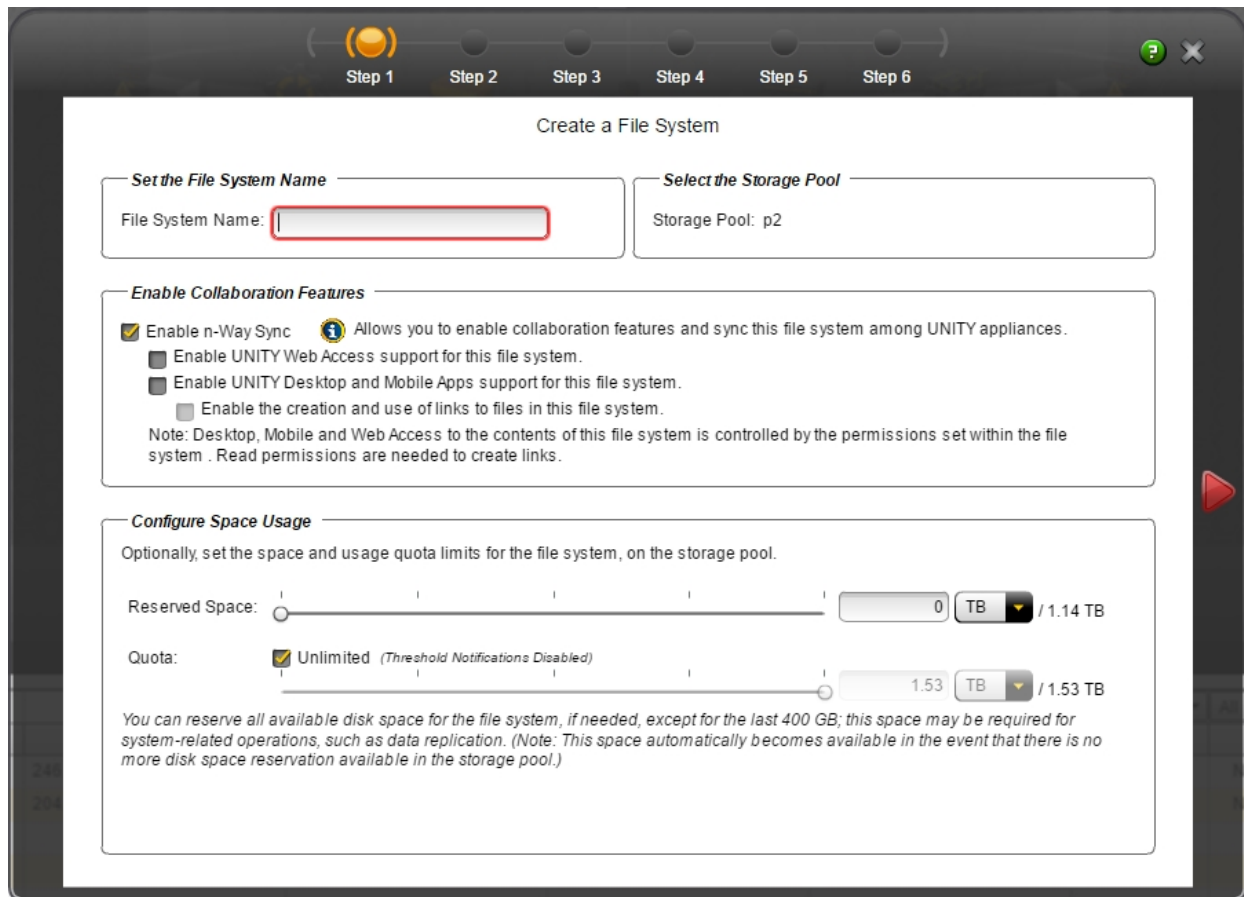
The name must start with an (upper-case or lower-case) alphabetic or numeric character; and, with the exception of the hyphen (-), and period (.), the name can only contain alphanumeric characters, without spaces.

These characters are NOT allowed:

" / \ [] : ; | = , + * ? < >

2. Specify the **Reserved space**.
3. Specify the **Quota**.
4. Click the right arrow on the wizard panel to continue.

Note Web, desktop, and mobile access can be independently disabled at any time.



Reserved space

You can reserve a set amount of disk space in the storage pool for the exclusive use of the file system. Unity automatically allocates the specified amount of disk space in the storage pool to the file system. If you add another file system to the storage pool, the space available to the new file system is the difference of the total disk space in the storage pool minus any reservations that you set for other file systems on the system.

For example, in a storage pool with 2 file systems and 10 TB of available disk space, if a reservation of 6 TB is allocated to one file system, then the second file system has 4 TB of disk space available to it.

To reserve space for the file system in the storage pool, move the slider left or right to set the desired amount. You can also type a value in the box to the right of the slider. To increase reserved space when you are using a limited quota, you must first increase the quota.

Quota

A usage quota allows Unity to dynamically expand a file system's storage capacity when the file system runs out of disk space. You can set a fixed quota limit to prevent the file system's storage capacity from increasing beyond a certain size, or you can set the quota to *Unlimited* to allow the file system's storage capacity to grow in relation to the storage pool's available disk capacity.

To limit the quota for the file system, clear the **Unlimited** check box, and then move the **Quota** slider left or right to decrease or increase the quota limit. You can also type a value in the box to the right of the slider.

Note The quota limit cannot be less than the reserved space, nor can it exceed the total available space in the pool.

Table 6-1: Distribution of disk space to file systems when setting reservations and quotas for file systems

Total available space in storage pool: 10 TB			
Space usage settings	File System 1	File System 2	File System 3
Reservation	5 TB	2 TB	Not specified
Quota	Unlimited	3 TB	Not specified
Total available space	8 TB <i>2 TB reserved for File System 2. Since the quota is set to Unlimited, the total available space increases as new storage is allocated to the pool.</i>	3 TB <i>Total available space cannot exceed set quota limit.</i>	3 TB <i>7 TB reserved for File System 1 and File System 2</i>

Figure 6-1: File System Setup Wizard, Step 1: Setting the file system name and space usage

Step 2: Configuring the access method

Step 2 of the File System Setup Wizard prompts you to select the **Access Method** for the file system.

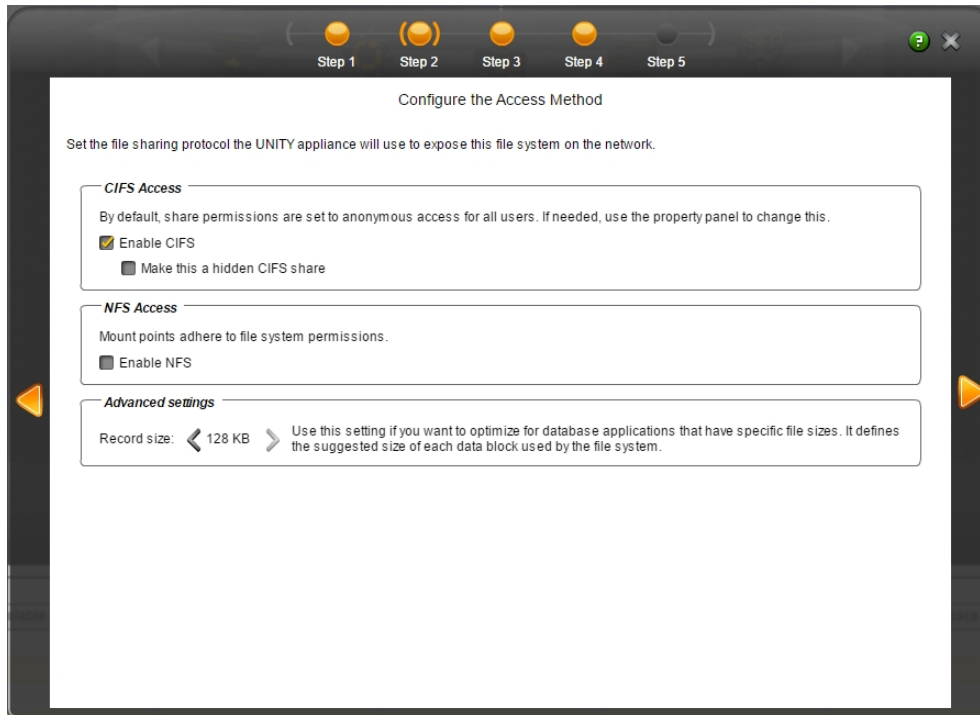
Notes:

- **WARNING:** To control Mobile or Web access to the file system, you must set Windows or Linux file system permissions. CIFS share permission settings do NOT apply to Mobile, Web, NFS, or FTP access.



CAUTION: To prevent a user from inadvertently deleting a folder you must manually remove that ability by modifying the advanced permission settings on each folder. By default, file system permissions are set to anonymous access for all users. This means that by default all users have the ability to create and delete top level folders, which in turn will cause that folder to be deleted on all other systems.

- A file system that you expose using the CIFS sharing method can also be accessed by UNIX/Linux-based systems using a CIFS client implementation for UNIX (such as, *Samba*).
- A file system that you expose using the NFS sharing method can also be accessed by Windows-based systems using an NFS client implementation for Windows (available in *Microsoft Services for UNIX*)
- You cannot expose a file system to Windows-based systems over the CIFS protocol if Unity is connected to an LDAP Directory service; the CIFS sharing option is not available in LDAP Directory service implementations.
- If you configured LDAP Directory service as the user authentication mode for Unity: exposing a file system over the CIFS protocol in an LDAP environment is only supported with anonymous read and/or anonymous read/write access enabled for the share.
- A file system that you expose using the FTP sharing method can be accessed by UNIX/Linux-based and Windows-based systems using the FTP protocol. FTP sharing is only supported for Nexsan Unity authentication. It must be enabled at the site level beforehand; see "Enabling FTP support" ([page 405](#)).
- If the file system will be accessed over IIS, do not enable case-sensitivity for the share.



► **To configure the sharing method:**

1. To select a share method, perform one of these actions:

- To expose the file system to Windows-based systems over the CIFS protocol, select the **Enable CIFS** option. This option is selected by default if Unity is joined to a Microsoft Active Directory domain.
- To make the file system a hidden CIFS share, Select the **CIFS** option, and then select the **Make this a hidden CIFS share** option.

When you configure a file system as a hidden CIFS share, the file system is not visible to Windows-based clients on the network; Windows-based clients interpret a hidden share as an administrative file system on the network, and prevent its display when you browse file systems on Unity.

To access a hidden (CIFS) share on Unity from a Windows-based client, you must specify the share's full path on Unity, including the \$ character appended to the end of the share's name; for example:

```
\\<Pool Resource Group Virtual IP>\<Storage Pool>\<FileSystemName>$
```

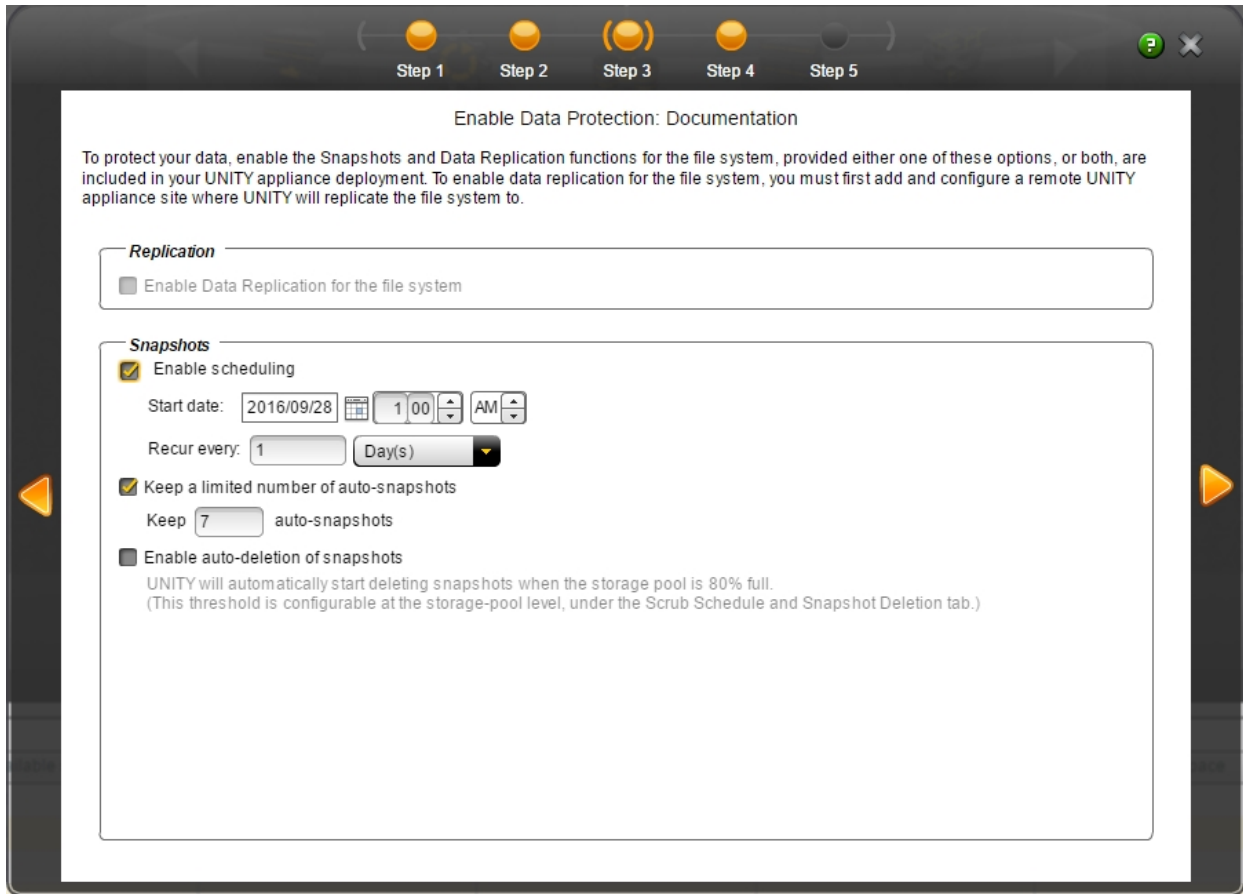
Where <FileSystemName> is the name of the hidden (CIFS) share on Unity.

- To expose the file system to UNIX/Linux-based systems over the NFS protocol, select the **Enable NFS** option. This option is selected by default if Unity is connected to an LDAP Directory service, or if the system is configured to use Unity authentication.
- To expose the file system to both Windows and UNIX/Linux-based systems, select both the **CIFS** and **NFS** options for a mixed-mode operation.
- To expose the file system over the FTP protocol, select the **FTP** option. This option is only available when using local authentication.

Step 3: Enabling data replication and configuring snapshot scheduling

This step is only displayed if your Unity includes the Snapshots or Data Replication feature, or both features.

Notes: Data Replication is not possible if n-Way Sync is enabled. If you do not want to enable snapshot scheduling, click the right arrow on the wizard panel to continue.



6

▶ **To configure snapshot scheduling for the file system:**

1. Select the **Enable scheduling** option to enable snapshots scheduling.
2. Adjust the snapshots schedule according to your preference. The default schedule for snapshots is once a day at 1 AM, with the start date set to the current date on Unity. This means that Unity will take an automatic snapshot of the file system at 1 AM every day starting on the current date.
 - a. Specify the start date for the schedule by clicking the **Start date** field and selecting a date from the calendar.
 - b. Specify the time when you want Unity to take snapshots. The default time is 1 AM.
 - c. Specify a recurrence pattern for the schedule by typing a value in the **Recur every** field; then, select the recurrence type from the drop-down list: **Minutes(s)**, **Hour(s)**, **Day(s)**, **Week(s)**, or **Month(s)**.
 - For example, if you want Unity to take a snapshot every two hours, type **2** in the **Recur every** field and select **Hour(s)** from the recurrence type drop-down list.
 - If you select **Week(s)** from the recurrence type drop-down list, you must then select the day or days of the week that you want Unity to take automatic snapshots on.
 - If you select **Month(s)**, you must then select the month or months of the year, as well as the calendar dates that you want Unity to take automatic snapshots on.

3. Configure auto-deletion settings for the file system:
 - a. Select the **Enable scheduling** option to enable snapshots scheduling (if not already enabled); this enables the options under **Auto-deletion Settings**.
 - b. Select the **Keep a limited number of auto-snapshots** option (selected by default) if you want Unity to only keep the specified number of automatic snapshots on the system—the default is 7 snapshots. This means that, after 7 snapshots, when Unity takes the 8th scheduled automatic snapshot of the share, it automatically delete the oldest automatic snapshot on the system. Unity does not delete manual snapshots when you enable this option; only scheduled automatic snapshots are processed. Change the default value if needed.
 - c. Select the **Enable the auto-deletion of snapshots** option if you want Unity to automatically delete automatic scheduled snapshots when the storage pool is 80% full. Unity deletes snapshots—starting with the oldest automatic snapshot on the system—until used disk space capacity in the storage pool falls below the 80% threshold. Unity does not delete manual snapshots when you enable this option; only scheduled automatic snapshots are processed.

Note The snapshot auto-deletion threshold is configurable at the storage pool-level.

Note The snapshot auto-deletion function can only be set on the primary dataset. When a snapshot is deleted on the primary dataset, its replica will be deleted during a subsequent replication session.

4. Click the right arrow on the wizard panel to continue.

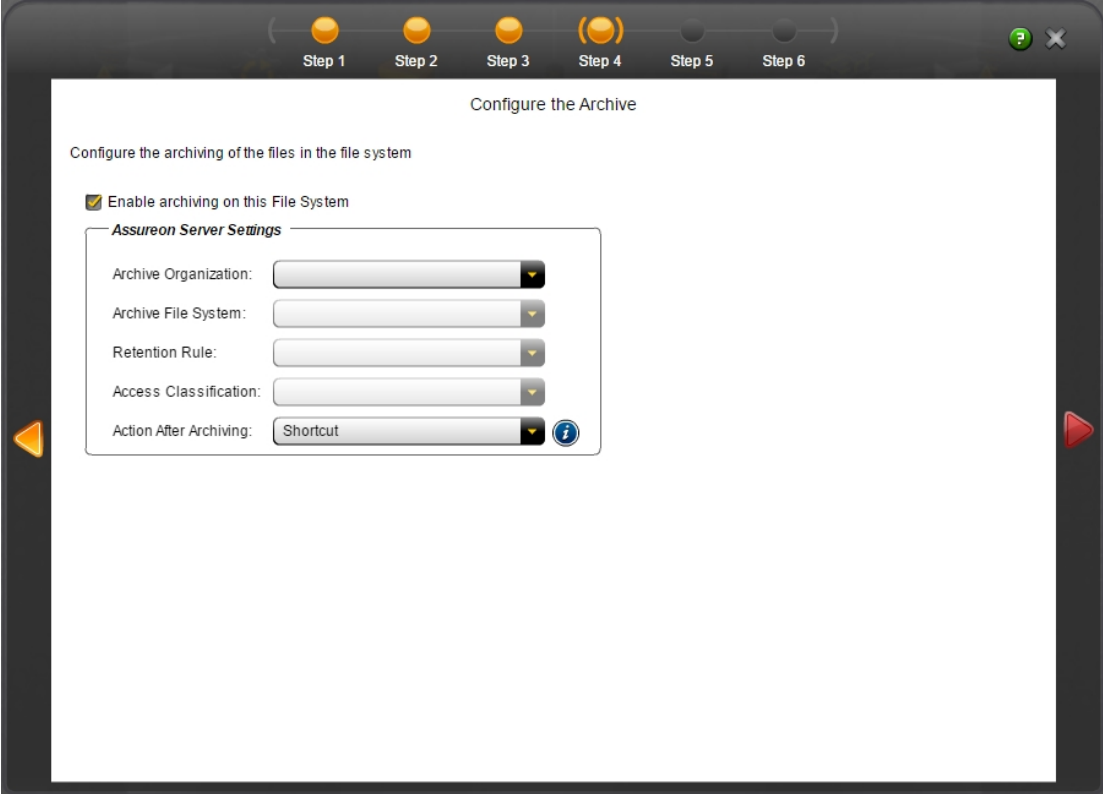
Note If you enable snapshots scheduling, and you set the current date (or today's date) as the start date for the schedule, Unity takes an automatic snapshot of the file system immediately after you set the schedule. Thereafter, Unity takes an automatic snapshot of the file system according to the schedule you specify. For more information about the Snapshots feature, see .

Step 4: Configuring your archive settings

Step 4 of the File System Setup Wizard prompts you to select the **Assureon Archive Settings** for the file system.

This step only appears if you have Active Archive on this Unity. Active Archive allows you to set data retention policies to automatically offload stale data and release primary storage. This allows you to increase the performance of your primary storage without increasing it's primary size.

Archiving allows you to retain data, using Nexsan's Assureon archiving capabilities.



6

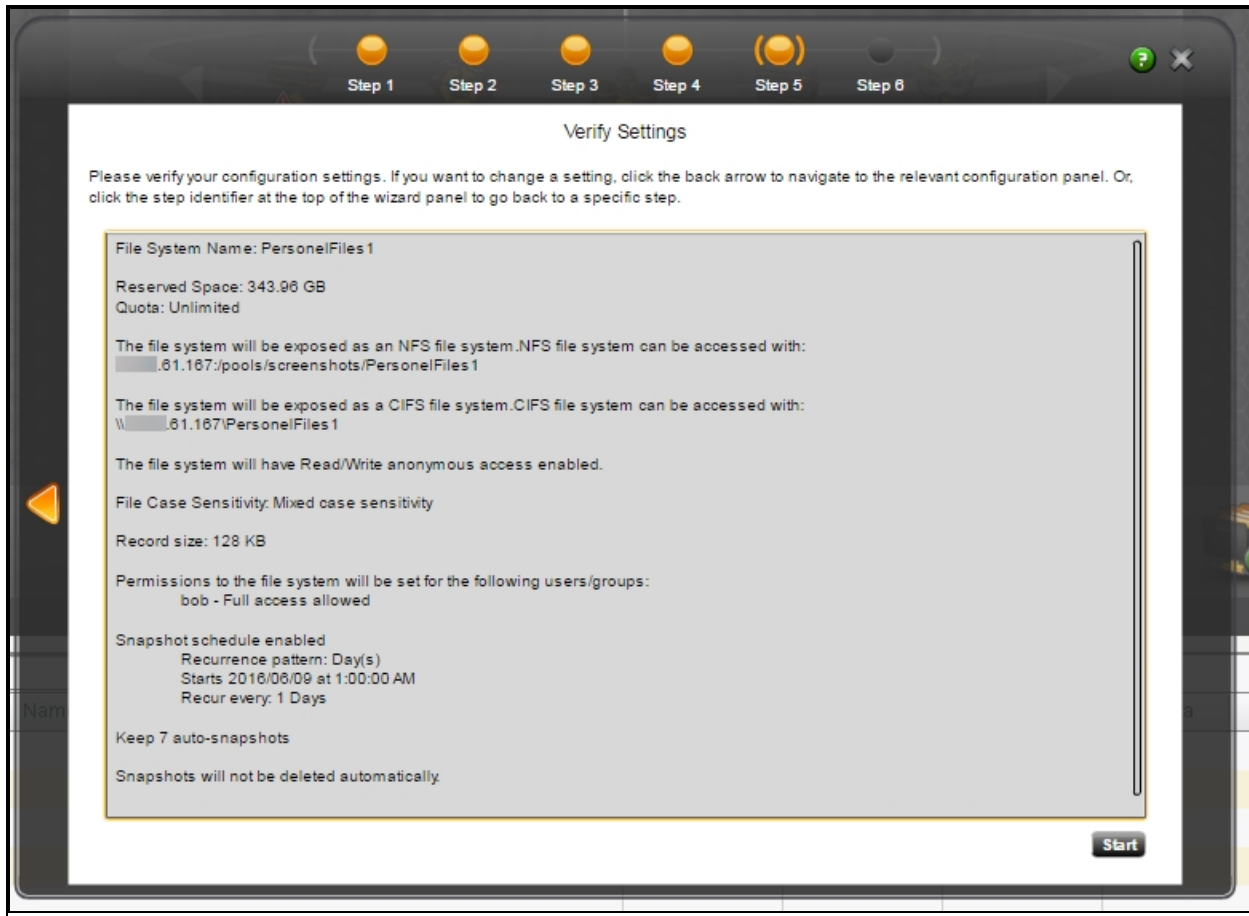
▶ **To configure Active Archive settings:**

1. Select the **Enable archiving on the file system** checkbox.
2. Configure the Assureon Archive Server that is to be used for archiving purposes. These are the settings on Assureon Archive Server to which data from your file system will be archived. The options that appear here are defined on the Assureon Server.
 - **Archive Organization:** Select the Assureon organization to be used for archiving. An organization is a group of one or more file systems which share retention rules, access classifications and reports.
 - **Archive File System:** Select the file system in the Archive Organization to be used for archiving. A file system consists of a database, storage location (the stores), manifest and audit files as well as replication options. Think of it as a self-contained archive that shares properties with the other file systems within an organization.
 - **Retention Rule:** Select the retention rule to be used for data archived from this file system. Retention rules specify how long a file is kept under management. For example, 180 days.
 - **Access Classification:** Select the access classification to be used for data archived from this file system. When a file is placed under Assureon management, it is stored using classification and sub classification information. Classifications allow you to control access to files. They also provide an intuitive way to search, audit, and dispose of files.
 - **Action After Archiving:** Define what is to happen to files once they have been archived. For example, create a shortcut to the files, leave them as they are, or remove them from the file system. Note that files will not be converted to shortcuts, or removed if n-Way Sync or asynchronous replication is enabled.

Note If enabled on the Assureon Archive Server, Schedule Archiving allows for a complete archive of this file system, initiated manually or scheduled on the Assureon Server. This does not affect Real-Time archiving.

Step 5: Verifying settings

Step 5 of the File System Setup Wizard summarizes the settings you selected for your file system and creates the file system in the storage pool when you click **Start**. Review the summary carefully before applying the configuration settings.



6

► **To change a configuration setting:**

- Click the back arrow to navigate back to the corresponding configuration step.
- Or
- Click the corresponding step identifier at the top of the File System Setup Wizard panel. For example, if you want to rename the share, click **Step 1**.

If you are satisfied with the settings, click the **Start** button at the bottom of the panel.

Step 6: Viewing configuration results

Step 6 of the File System Setup Wizard displays progress as Unity creates the new file system.

The File System Setup Wizard displays error events that the system encounters during the file system creation process. You can view more details about an error event by expanding the corresponding entry.

► **To view more details for an error event:**

- Click the plus (+) sign corresponding to the error event.

Unity informs you when it successfully creates the file system. It also asks you if you want to create another file system in the storage pool.

Choose one of these actions:

- Click **Yes** if you want to create a new file system ; the File System Setup Wizard scrolls back to [Step 1: Creating a file system and configuring space usage](#) on page 124 and resets all configuration settings to

their defaults.

- Click **No** if you do not want to create a file system. This closes the File System Setup Wizard.

The new file system appears in the Unity tree view under the File System node. You can now access the file system from a Windows-based (CIFS) system and/or mount the share on a UNIX/Linux-based (NFS) system, depending on the sharing method you selected.

Modifying file system properties

This section describes how to modify properties for a file system once you add the file system to a storage pool.

This section includes these topics:

Disabling data sharing for a file system.....	135
Modifying a file system's sharing method.....	136
Modifying a file system's space usage settings.....	137
Modifying a file system's record size.....	138
Setting space usage notification thresholds for file systems.....	139
Enabling/disabling data compression on a file system.....	141
Enabling the Access Time mode on a file system.....	142
Setting up IP restrictions.....	143
Managing home directories.....	151

Renaming a file system

If the file system is replicated, Unity also renames the file system's replica on the remote site.



CAUTION: If you rename a file system, client systems on the network will be disconnected from the file system; this could result in data loss. Before renaming a file system, make sure that client systems with an active connection to the file system disconnect any mapped drive(s) to the file system; also make sure to quiesce any applications with an active connection to the file system.

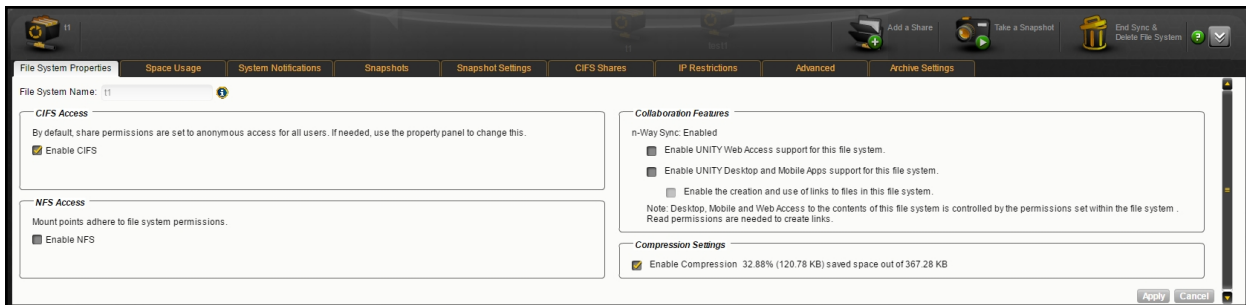
In addition, if the file system that you rename is mapped to Windows-based client computers, or if the file system is mounted on UNIX/Linux-based client computers on the network, you will need to recreate the mappings and/or mount points using the file system's new name.

File systems that have n-Way Sync enabled cannot be renamed.

► **To rename a file system:**

1. In Unity's tree view, click the Site node to display its child nodes.
2. Click the **Storage Pools** node.
3. Click the storage pool that contains the file system whose name you want to modify.
4. Click the **File Systems** node.
5. Select the corresponding file system.
6. Expand the file system's Properties panel.

Figure 6-2: File System's properties panel—File System Properties tab



- In the **File System Properties** tab, enter a new name for the file system in the **File System Name** field. The name must start with an (upper-case or lower-case) alphabetic or numeric character; and, with the exception of the hyphen (-), and period (.), the name can only contain alphanumeric characters, without spaces.

These characters are NOT allowed:

“ / \ [] : ; | = , + * ? < >

- Click the **Apply** button to change the file system’s name.
- Click **OK** at the warning message.

Disabling data sharing for a file system

If needed, you can disable data sharing for a file system, which makes the file system inaccessible over the network.

This section describes how to disable data sharing for a file system.



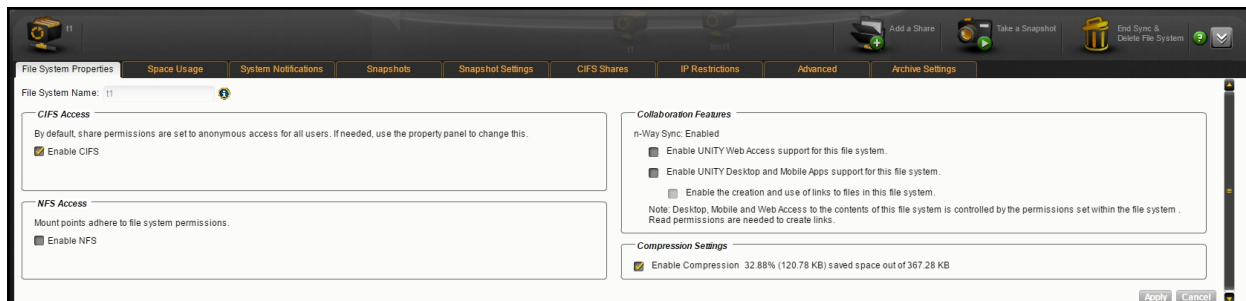
CAUTION: It is important to note that when you disable data sharing for a file system, client systems or applications on the network that access the file system will lose their connection to the file system; this could result in data loss. Before disabling data sharing, make sure that client systems with an active connection to the file system disconnect any mapped drive(s) to the file system; also make sure to quiesce any applications with an active connection to the file system.

Note Disabling data sharing for a file system does not affect shares that reside within the file system; any share that exists in a file system on which you disable data sharing remains accessible over the network until you manually unshare it; for more information, see [Disabling data sharing for a share](#) on page 183.

► To disable data sharing for a file system:

- In Unity’s tree view, click the Site node to display its child nodes.
- Click the **Storage Pools** node.
- Click the storage pool that contains the file system for which you want to disable data sharing.
- Click the **File Systems** node.
- Select the file system for which you want to disable data sharing.
- Expand the file system node’s Properties panel.

Figure 6-3: File System’s properties panel—File System Properties tab



- In the **File System Properties** tab, clear all selected sharing options.
- Click the **Apply** button. The file system will no longer be accessible over the network.

Modifying a file system's sharing method

Changing the [sharing method](#) for a file system affects file systems that reside below the root file system; that is, the sharing method for a file system changes when you change the sharing method for its parent file system.

- A file system that you expose using the CIFS sharing method can also be accessed by UNIX/Linux-based systems using a CIFS client implementation for UNIX (such as, *Samba*).
- A file system that you expose using the NFS sharing method can also be accessed by Windows-based systems using an NFS client implementation for Windows (available in *Microsoft Services for UNIX*)
- You cannot expose a file system to Windows-based systems over the CIFS protocol if Unity is connected to an LDAP Directory service.
- A file system that you expose using the FTP sharing method can be accessed by UNIX/Linux-based and Windows-based systems using the FTP protocol. FTP sharing is only supported for Nexsan Unity authentication. It must be enabled at the site level beforehand; see [Enabling FTP support](#) on page 405.



CAUTION: Changing the sharing method affects user access to the file system. More specifically, if any Windows-based systems on your network have a network drive mapped to the share and you disable CIFS sharing, the Windows-based systems will lose connection to the mapped file system.

Similarly, if any UNIX/Linux-based systems have the file system mounted and you disable NFS sharing, the file system will become unmounted. To avoid any loss of data as a result of changing a file system's sharing method, make sure that client systems with an active connection to the file system disconnect any mapped drive(s) to file system share before you change a file system's sharing method; also make sure to quiesce any applications with an active connection to the file system.

▶ Hidden CIFS share

Unity allows you to configure a file system as a hidden CIFS share. A hidden CIFS share is not visible to Windows-based clients on the network; Windows-based clients interpret a hidden share as an administrative share on the network, and prevent its display when you browse file systems on Unity. This mechanism allows you to further restrict access to a file system.

To access a hidden (CIFS) share on Unity from a Windows-based client, you must specify the file system's full path on Unity, including the \$ character appended to the end of the share's name; for example:

```
\\<Pool Resource Group Virtual IP>\<Storage Pool>\\<FileSystemName>$
```

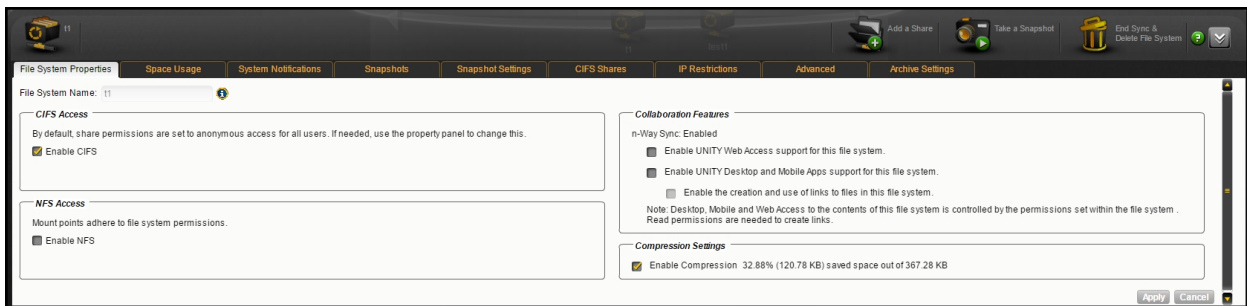
Where <File SystemName> is the name of the hidden (CIFS) share on Unity.

▶ To modify a file system's sharing method:

1. In Unity's tree view, click the Site node.
2. Click the **Storage Pools** node.
3. Click the storage pool that contains the file system for which you want to change the sharing method.
4. Click the **File Systems** node.
5. Select the file system for which you want to change the sharing method.
6. Expand the file system's Properties panel.

- In the **File System Properties** tab, modify the sharing method for the file system by clearing or selecting the relevant options.

Figure 6-4: File System's properties panel—File System Properties tab



- Click the **Apply** button.

Modifying a file system's space usage settings

Reserved space

You can reserve a set amount of disk space in the storage pool for the exclusive use of the file system. Unity automatically allocates the specified amount of disk space in the storage pool to the file system. If you add another file system to the storage pool, the space available to the new file system is the difference of the total disk space in the storage pool minus any reservations that you set for other file systems on the system.

For example, in a storage pool with 2 file systems and 10 TB of available disk space, if a reservation of 6 TB is allocated to one file system, then the second file system has 4 TB of disk space available to it.

To reserve space for the file system in the storage pool, move the slider left or right to set the desired amount. You can also type a value in the box to the right of the slider. To increase reserved space when you are using a limited quota, you must first increase the quota.

Quota

A usage quota allows Unity to dynamically expand a file system's storage capacity when the file system runs out of disk space. You can set a fixed quota limit to prevent the file system's storage capacity from increasing beyond a certain size, or you can set the quota to *Unlimited* to allow the file system's storage capacity to grow in relation to the storage pool's available disk capacity.

To limit the quota for the file system, clear the **Unlimited** check box, and then move the **Quota** slider left or right to decrease or increase the quota limit. You can also type a value in the box to the right of the slider.

Note The quota limit cannot be less than the reserved space, nor can it exceed the total available space in the pool.

Table 6-2: Distribution of disk space to file systems when setting reservations and quotas for file systems

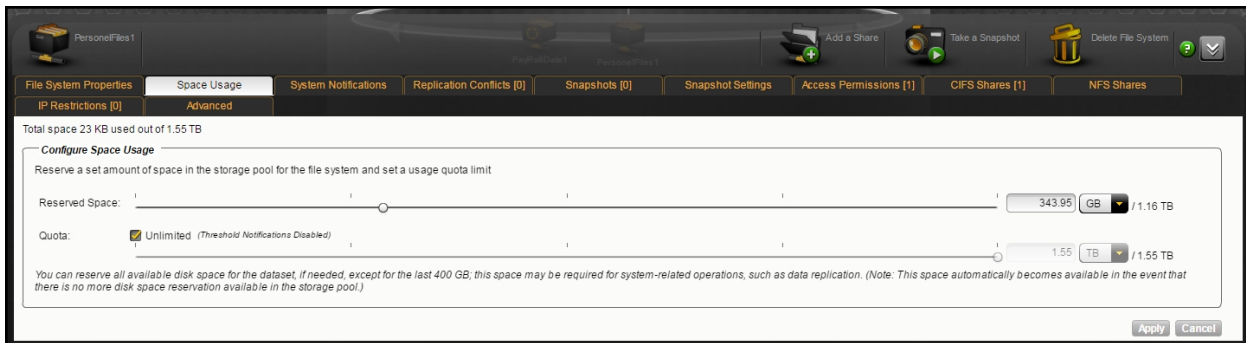
	Total available space in storage pool: 10 TB		
Space usage settings	File System 1	File System 2	File System 3
Reservation	5 TB	2 TB	Not specified
Quota	Unlimited	3 TB	Not specified
Total available space	8 TB <i>2 TB reserved for File</i>	3 TB <i>Total available space</i>	3 TB <i>7 TB reserved for File</i>

Total available space in storage pool: 10 TB			
Space usage settings	File System 1	File System 2	File System 3
	System 2. Since the quota is set to Unlimited, the total available space increases as new storage is allocated to the pool.	cannot exceed set quota limit.	System 1 and File System 2

► **To modify a file system’s space usage settings:**

1. In Unity’s tree view, click the Site node to display its child nodes.
2. Click the **Storage Pools** node.
3. Click the storage pool containing the file system that you want to modify space usage settings for; this displays its child nodes.
4. Click the **File Systems** node.
5. Select the share whose space usage settings you want to modify.
6. Expand the file system’s Properties panel.

Figure 6-5: File System’s properties panel—Space Usage tab



7. Select the **Space Usage** tab.
8. Modify space usage settings for the file system by selecting or changing one of the available options.
9. Click the **Apply** button to save your changes.

Modifying a file system's record size

A file system's record size is somewhat dynamic and Unity can write in smaller blocks for applications requiring a different record size. It is not recommended to change the default record size of file systems except in very specific circumstances where the application is database-driven and the database record size is precisely known. File systems have a default record size of 128 KB, which is the maximum size.

Note On the Unity 2000, the minimum values of the share record size differ for higher capacity drives:

- For the Unity 2000C (16 drives):
 - For drives < 4 TB: The minimum record size will be 32 KB.
 - For drives >= 4 TB and < 6 TB: The minimum record size will be 64 KB.

- For drives ≥ 6 TB: The minimum record size will be 128 KB.

Note A 1 TB drive is typically 109 bytes and not 230 bytes.

- For the Unity 2000P (24 drives), the minimum record size will be 8 KB.

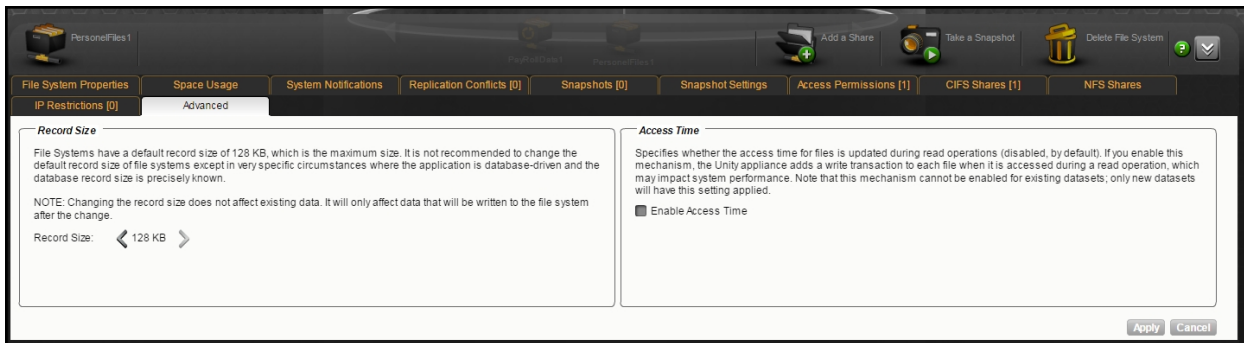
For the recommended record size according to the application used, see [Step 2: Configuring the access method](#) on page 126.

Note Changing the record size does not affect existing data. It will only affect data that will be written to the file system after the change.

► **To modify the record size of a file system:**

1. In Unity's tree view, click the Site node to display its child nodes.
2. Click the **Storage Pools** node.
3. Click the storage pool that contains the file system for which you want to change the sharing method.
4. Click the **File Systems** node.
5. Select the file system for which you want to change the record size.
6. Expand the file system's Properties panel.
7. Select the **Advanced** tab.

Figure 6-6: File System's properties panel—Advanced tab



8. Modify the record size by entering a number or using the arrows.
9. Click the **Apply** button.

Setting space usage notification thresholds for file systems

Unity allows you to set space usage thresholds for file systems to trigger email notifications if space consumption in the file system reaches or exceeds a threshold that you set for the file system. You can only set space usage thresholds for a file system when you enable a space usage quota for the file system; for more information, see [Modifying a file system's space usage settings](#) on page 137.

Unity sends an email notification when the space consumption in a file system reaches the value that you set for a particular threshold. An email notification is triggered again when space consumption exceeds the threshold. In order for Unity to send email notifications when space consumption reaches or exceeds a threshold that you set for the file system, you must first configure SMTP settings and system notification settings for the site; for more information, see [Event logging and notification](#) on page 517.

Unity lets you set these space usage thresholds for a file system:

- **Critical:** the default critical threshold for a file system is set to the same value that you configured for the storage pool where the file system resides: if the storage pool's critical threshold is set to 95%, the default

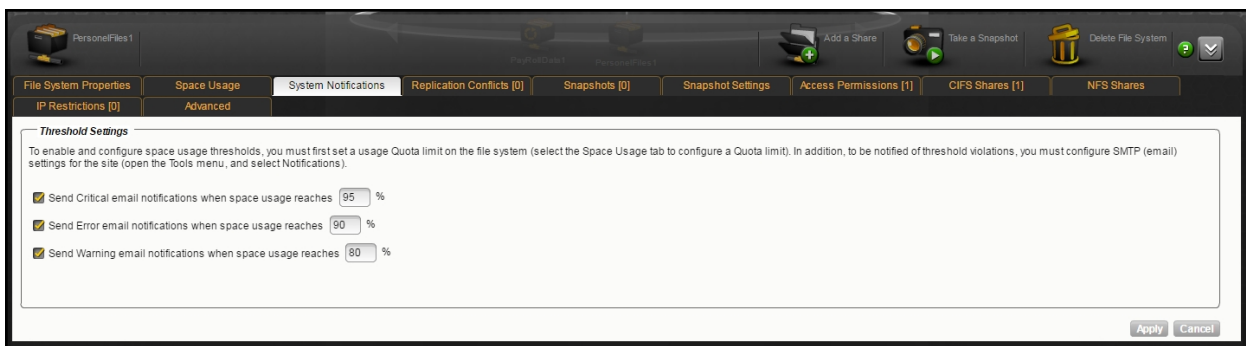
critical threshold for any new file system that you add to the storage pool is also set to 95%. The space usage calculation for the critical threshold takes the quota limit that you set for the file system into account; for example, if the critical threshold is set to 95% for the file system, space usage in the file system is considered to be in critical state when disk space consumption reaches or exceeds 95% of the quota limit that you set for the file system.

- **Error:** the default error threshold for a file system is set to the same value that you configured for the storage pool where the file system resides: if the storage pool's error threshold is set to 90%, the default error threshold for any new file system that you add to the storage pool is also set to 90%. The space usage calculation for the error threshold takes the quota limit that you set for the file system into account; for example, if the error threshold is set to 90% for the file system, space usage in the file system is considered to be in error state when disk space consumption reaches or exceeds 90% of the quota limit that you set for the file system.
- **Warning:** the default warning threshold for a file system is set to the same value that you configured for the storage pool where the file system resides: if the storage pool's warning threshold is set to 80%, the default warning threshold for any new file system that you add to the storage pool is also set to 80%. The space usage calculation for the warning threshold takes the quota limit that you set for the file system into account; for example, if the warning threshold is set to 80% for the file system, space usage in the file system is considered to be in warning state when disk space consumption reaches or exceeds 80% of the quota limit that you set for the file system.

▶ **To set or modify space usage notification thresholds for a file system:**

1. If you are managing multiple sites (multi-site management of remote Unities): in Nexsan Unity's™ tree view, click the Site node where the file system that you want to set space usage thresholds for exists.
2. Click the **Storage Pools** node to display its child nodes.
3. Click the node representing the storage pool where the file system that you want to set space usage thresholds for exists.
4. Click the **File Systems** node.
5. Click the node representing the file system for which you want to set space usage thresholds.
6. Expand the file system node's Properties panel
7. Select the **System Notifications** tab.

Figure 6-7: File System's properties panel—System Notifications tab



8. Enable the threshold setting that you want to receive email notifications for by selecting the corresponding option, and then set a percentage value for the threshold. For example:
To receive an email notification when space consumption reaches or exceeds **critical** level:
 - a. Select the **Send critical notification when space usage reaches** option.
 - b. Type a threshold percentage value in the text box.
 By default, all threshold settings are enabled. To disable a threshold setting, clear its check box.
9. Click **Apply** to set the new threshold settings for the file system.

Enabling/disabling data compression on a file system

You can enable/disable compression at the file system level. This setting takes precedence over the settings defined at the storage pool level. If you enabled data compression at the pool level before creating this file system, the file system already has data compression enabled—see [Enabling data compression on the storage pool on page 113](#). If you choose to disable data compression on the file system, only that file system will be affected.

Compression allows for better performance of the file system since the files to read/write are much smaller. However, it will also increase CPU usage. Compression can be enabled/disabled at any time.

Notes:

- When you set up replication for file systems that have the compression setting enabled, file systems on the remote site inherit the compression settings.
- Enabling or disabling data compression does not affect existing data. It will only affect data that will be written to the file system after the change.



CAUTION: If you turn on data compression for a file system, and then you turn it off, before you set up replication for the file system, part of the data is compressed and the other part is not. Since the file system has not been replicated yet, the compression settings are not inherited and data compression is off at the remote site.

If you set a space quota on the file system and that quota is almost full, the file system on the remote site will not have enough space to accommodate data coming from the primary file system.

As a result, replication will fail.

Perform one of these actions before replication:

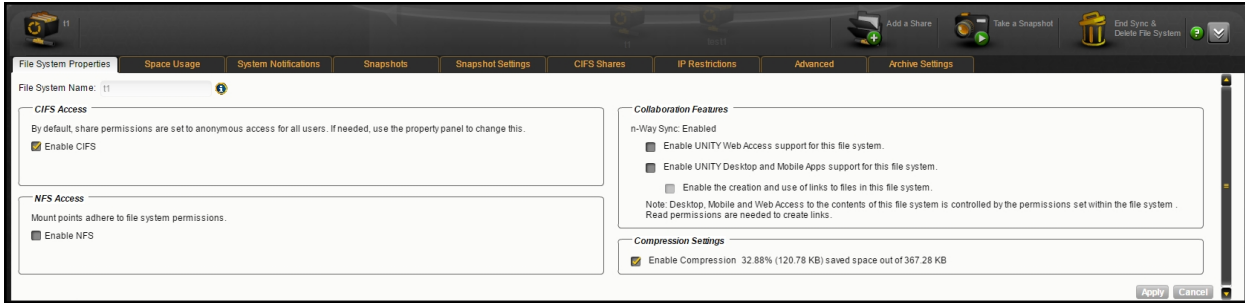
- Increase the quota to match the actual space used by data on the file system.
- Set the quota to *Unlimited*.
- Enable data compression on both sites.

► **To enable data compression on a file system:**

1. In Unity's tree view, click the Site node to display its child nodes.
2. Click the **Storage Pools** node.
3. Click the storage pool to which the file system belongs.
4. Click the **File Systems** node.
5. Select the file system for which you want to enable data compression.
6. Expand the file system's Properties panel.

7. Select the **File System Properties** tab

Figure 6-8: File System’s properties panel—File System Properties tab



8. Select the **Enable Compression** option.

9. Click **Apply**.

Enabling the Access Time mode on a file system

The Access Time mode controls whether the access time for files is updated when they are read. By default, the Access Time mode is disabled, including for replicated file systems. This avoids producing write traffic when reading files and results in significant performance gains.

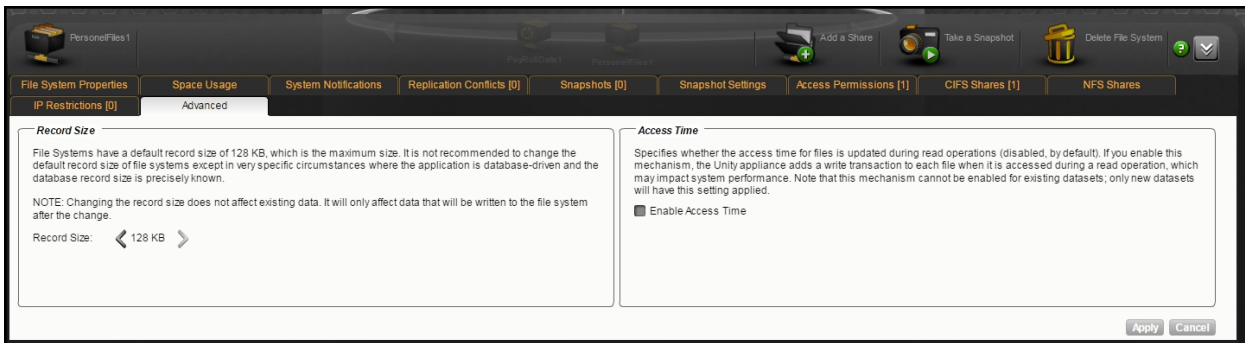
The Access Time mode can be set at the file system level or pool level. This value can be modified at any time. To enable it for the pool, see [Enabling the Access Time mode on a storage pool](#) on page 114.

Note When you enable the Access Time mode at the pool level, only new file systems added to the pool after the change will inherit the setting. Existing file systems remain unchanged. Replicated file systems do not inherit this setting, so the Access Time mode is always disabled.

► **To enable the Access Time mode for a file system:**

1. In Unity’s tree view, click the Site node.
2. Click the **Storage Pools** node.
3. Click the storage pool that contains the file system for which you want to enable the Access Time mode.
4. Click the **File Systems** node.
5. Select the file system for which you want to enable the Access Time mode.
6. Expand the file system’s Properties panel.
7. Select the **Advanced** tab.

Figure 6-9: File System’s properties panel—Advanced tab



8. Select the **Enable Access Time** option.
9. Click the **Apply** button to save your changes.

Setting up IP restrictions

Unity allows you to restrict access to CIFS and NFS shares based on a client system's IP address. To set up IP restrictions using the `nxadmin` CLI; see the *nxadmin Command-line Interface Reference Guide*. With this mechanism, you can give a client system, or a group of client systems on a specific subnet, one of these access levels to a file system:

- **Read-write access (rw)**: only a client system with an IP address corresponding to the list, or range, of IP addresses that you add to the Read-write access list for the file system is granted both Read and Write access to the file system. Any client system with an IP address that does not correspond to an entry in the Read-write access list is prevented from accessing the file system.
- **Read-only access (ro)**: only a client system with an IP address corresponding to the list, or range, of IP addresses that you add to the Read-only access list for the file system are granted Read-only access to the file system. Any client system with an IP address that does not correspond to an entry in the Read-only access list is prevented from accessing the file system.
- **No access (none)**: any client system with an IP address corresponding to the list, or range, of IP addresses that you add to the No access list for the file system is prevented from accessing the file system.

► NFS shares:

NFS shares, by default, have their Read-write flag set to `enabled`. You can configure separate access restrictions for each share on Unity. In addition, you can configure different access levels for the same share based on the IP address. To see what access gets priority according to your settings, see [Share IP permission precedence](#) on page 145.

You can also set the `no_root_squash` property to allow NFS clients on the network to access files on an NFS share on Unity with `root` privileges.

► CIFS shares:

For CIFS shares, the Read/Write flag set to `all` (or `rw = *` in the `nxadmin` CLI) is implied. However, when you set an IP restriction to a share (Read/Write = No Access, or `rw = none` in the `nxadmin` CLI), you must ALSO set it to `all` so that all OTHER IP addresses (clients) can access that share. The same applies for hosts; if you set an IP restriction based on a network prefix, no other IP addresses in that range will be able to access the share unless you set it to All. For CIFS, "Read/Write = All" is implied only if no other IP restrictions are set, and required if any other restrictions are set.

Notes:

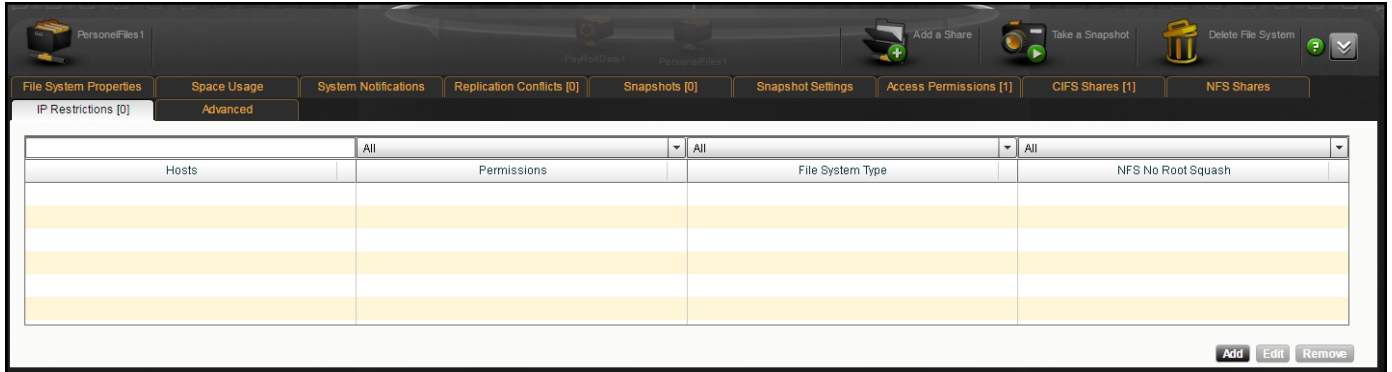
- **IP-based restrictions on a share are additive to share-level user access permissions:** When you enable IP-based access for a share to specific client systems on the network, it does NOT grant user access to the share. This mechanism is provided to explicitly deny access to any client system with an IP address that does not correspond to an entry in the Read-write or Read-only access lists that you configure for the share.
- User access permissions on the share can override IP-based permissions, depending on the precedence given by CIFS or NFS rules; for examples, see [Share IP permission precedence](#) on page 145.

► To set up IP restrictions for shares:

1. In Unity's tree view, click the Site node.
2. Click the **Storage Pools** node.

3. Select the pool where the share is hosted.
4. Click the **File System** node.
5. Expand the file system's Properties panel.
6. Select the share.
7. Select the **IP Restrictions** tab

Figure 6-10: Share's properties panel—IP Restrictions tab



8. Click **Add**.

Figure 6-11: Configure IP Restrictions dialog box



9. Select the client system(s) for which to configure the IP restriction:
 - **All** means all systems connected to Unity.
 - **Host IP** applies to a specific host. Enter the host IP address.
 - **Network prefix** and **Netmask** apply to multiple hosts. Enter the network prefix and netmask.

10. From the **Protocol** drop-down list, select **CIFS/NFS** if a share has both CIFS and NFS sharing enabled for it, or **CIFS**, or **NFS**.
Note FTP support is not supported for IP restrictions.
11. From the **Permissions** drop-down list, select one of the access levels (**Read/Write**, **Read only**, or **No access**).
12. (Optionally) You can select the **Enable No Root Squash** option if this share uses NFS; it will allow NFS clients to access files on this share with `root` privileges.
13. Click **Apply**.
14. Repeat these steps for other client systems, as required.

Share IP permission precedence

The order of precedence depends on the type of share. Permissions on NFS shares are not treated the same way as the ones on CIFS shares.

Note The `no root squash` permission is independent of the other permissions and provides access to the NFS shares with `root` privileges.

Table 6-3: Order of permission precedence for shares

When a share permission is set to...	Precedence on NFS is...	Precedence on CIFS is...
None	None Read/Write Read/Write for all shares Read-Only Read-Only for all shares None for all shares	None Read/Write Read/Write for all shares Read-Only Read-Only for all shares None for all shares
Read/Write	Read/Write Read/Write for all shares Read-Only Read-Only for all shares None for all shares	Read/Write Read/Write for all shares Read-Only for all shares None for all shares
Read-Only	Read-Only Read/Write for all shares Read-Only for all shares None for all shares	Read-Only Read/Write Read/Write for all shares Read-Only for all shares None for all shares
Read/Write for all shares	Read/Write for all shares Read-Only for all shares None for all shares	

When a share permission is set to...	Precedence on NFS is...	Precedence on CIFS is...
None for all shares		None for all shares Read/Write for all shares Read-Only for all shares

This table provides examples for NFS shares and describes how permission precedence is assigned when access to shares is based on IP restrictions and user access permissions.

Table 6-4: IP Permission order of precedence for NFS shares

If you give...	Precedence is...
Read/Write access and Read-Only access to the same IP address.	Read/Write for the IP address
Read-Only access to user Bob and Read/Write access to an IP address.	Read-Only for Bob
Read/Write access to user Bob and Read-Only access to an IP address.	Read-Only for Bob
Read-Only access to an IP address and Read/Write access to a subnet.	Read/Write for the subnet Read/Write=@xxx.xx.1 Read-Only=@xxx.xx.14.30 local
Read/Write access to an IP address and Read-only access to a subnet.	Read/Write for the IP address Read/Write=@xxx.xx.14.30 Read-Only=@xxx.xx.14 local
Read/Write access to an IP address and None access to a subnet.	None
Read/Write access to all and Read-Only access to an IP address.	Read-Only for the IP address
Read-Only access to all and Read/Write access to an IP address.	Read/Write for the IP address Read-Only=@xxx.xx.14.30 Read/Write=* local

Archive settings

Archiving allows you to retain data, using Nexsan's Assureon archiving capabilities.

► **To view Archive settings for a file system:**

1. In Unity's tree view, click the Site node.
2. Click the **Storage Pools** node.
3. Click the storage pool that contains the file system for which you want to enable the Access Time mode.

4. Click the **File Systems** node.
5. Select the file system for which you want to enable the Access Time mode.
6. Expand the file system's Properties panel.
7. Select the **Archive Settings** tab.

► **To configure Active Archive settings:**

1. Select the **Enable archiving on the file system** checkbox.
2. Configure the Assureon Archive Server that is to be used for archiving purposes. These are the settings on Assureon Archive Server to which data from your file system will be archived. The options that appear here are defined on the Assureon Server.
 - **Archive Organization:** Select the Assureon organization to be used for archiving. An organization is a group of one or more file systems which share retention rules, access classifications and reports.
 - **Archive File System:** Select the file system in the Archive Organization to be used for archiving. A file system consists of a database, storage location (the stores), manifest and audit files as well as replication options. Think of it as a self-contained archive that shares properties with the other file systems within an organization.
 - **Retention Rule:** Select the retention rule to be used for data archived from this file system. Retention rules specify how long a file is kept under management. For example, 180 days.
 - **Access Classification:** Select the access classification to be used for data archived from this file system. When a file is placed under Assureon management, it is stored using classification and sub classification information. Classifications allow you to control access to files. They also provide an intuitive way to search, audit, and dispose of files.
 - **Action After Archiving:** Define what is to happen to files once they have been archived. For example, create a shortcut to the files, leave them as they are, or remove them from the file system. Note that files will not be converted to shortcuts, or removed if n-Way Sync or asynchronous replication is enabled.

Note If enabled on the Assureon Archive Server, Schedule Archiving allows for a complete archive of this file system, initiated manually or scheduled on the Assureon Server. This does not affect Real-Time archiving.

The Archive Settings tab also displays statistical information on the number of files that have been archived from this file system over the previous 24 hours.

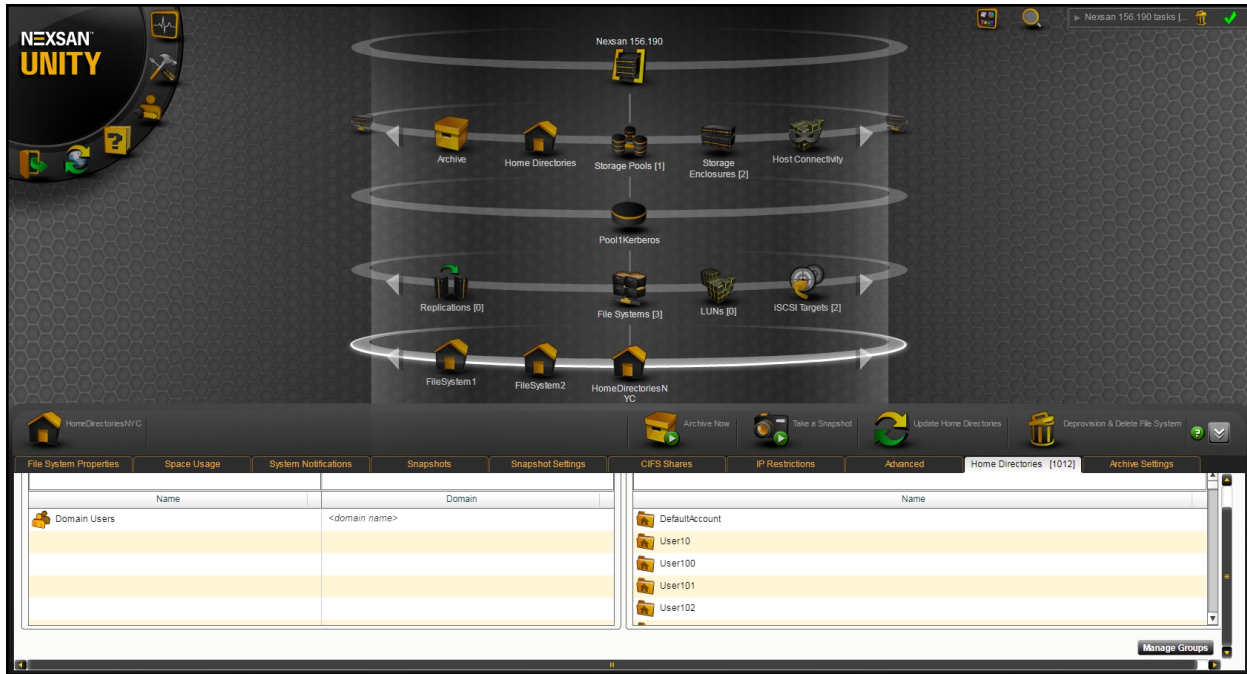
Managing home directories

Use this topic for information about the working with the file system-level **Home Directories** tab.





► **To open the file system for a home directories:**

1. In the Unity tree, click the **Site** node to display its child nodes.
2. Select the **Storage Pools** node.
3. Select the **File Systems** node.
4. Select the **Home Directories** node.
5. Click the **Home Directories** tab.

Figure 6-12: The File Systems Home Directories tab



6

To...	Click...
Run Active Archive	The Archive Now icon  (appears only if you have Assureon Active Archive). See Using Active Archive on page 343
Take a snapshot of the data	The Take a Snapshot icon  . See also Using the File Systems properties panel on page 194
Update Home Directories	The Update Home Directories icon  . Unity performs a background update every 5 minutes, but you can force an update at any time using the Update Home Directories button.
Delete a file system for home directories	The Delete and Deprovision File System icon  to open a popup where you can delete all data in Unity for the file system created for this home directory, including all user-specific home folders and their contents. All snapshots of the data if they exist as well as replicated data on remote Unity Systems will be deleted.
Manage Home Directories group assignments	The Manage Groups button at the bottom of the panel to open a popup where you can assign groups that will have home directories. See Managing group assignments on page 165

Viewing space usage information for file systems

Unity gives you a detailed overview of each file system's used and available disk space. To modify space usage settings, see [Modifying a file system's space usage settings](#) on page 137.

► To access the file system node Properties panel:

1. In Unity's tree view, click the Site node.
2. Click the **Storage Pools** node.
3. Click the storage pool containing the file systems for which you want to view space usage information.
4. Expand the file system node's Properties panel. The **File Systems** tab displays a grid that lists all the shares in a storage pool.

Figure 6-13: File Systems node's properties panel—File Systems tab

Name	Available s...	User Data	Snapshots	Quota	Reserved S...	n-Way Sync...	Compression
PayRollData1	1.22 TB	25 kB	0 B			true	7.4% (2 kB)
PersonnelFiles1	343.95 GB	23 kB	0 B	343.95 GB	343.95 GB	false	0% (0 B)

Tip Double-click a file system in the grid to automatically open the share's properties panel and display its child nodes.

► To sort the list:

- Click the sort pointer in the **Name** column heading until the arrow points down for descending order, or until the arrow points up for ascending order.

► File Systems tab columns related to space usage:

- **Available space:** The amount of space left on the file system. Depending on reservation settings, this space might be shared between multiple datasets in the storage pool.
- **User Data:** The amount of space currently consumed by user data, excluding snapshots.
- **Snapshots:** The amount of space used by snapshots
- **Quota:** The current setting for quota. When the quota is set to *Unlimited*, nothing is displayed in the column.
- **Reserved space:** The current setting for reservation. If there is none, nothing is displayed in the column.
- **Compression:** Displays the percentage of compressed data and its equivalent in units (megabytes or terabytes).

Deleting a file system

This section describes how to delete a file system from a storage pool.



CAUTION: When you delete a file system from a storage pool, you also permanently remove all the data contained in the file system, including snapshots of the data. If the file system is replicated to a remote Nexsan Unity site, the replicated file system, including all the data in the replicated file system is permanently removed as well.

▶ **To delete a file system:**

1. In Nexsan Unity's tree view, click the Site node to display its child nodes.
2. Click the **Storage Pools** node.
3. Click the storage pool from which you want to delete a file system.
4. Click the **File Systems** node to display its child nodes.
5. Click the context menu button to open the node context menu.
6. Click **End Sync and Delete File Transfer**.
7. Type **Delete** in the text box.
8. Click the **Yes** button.

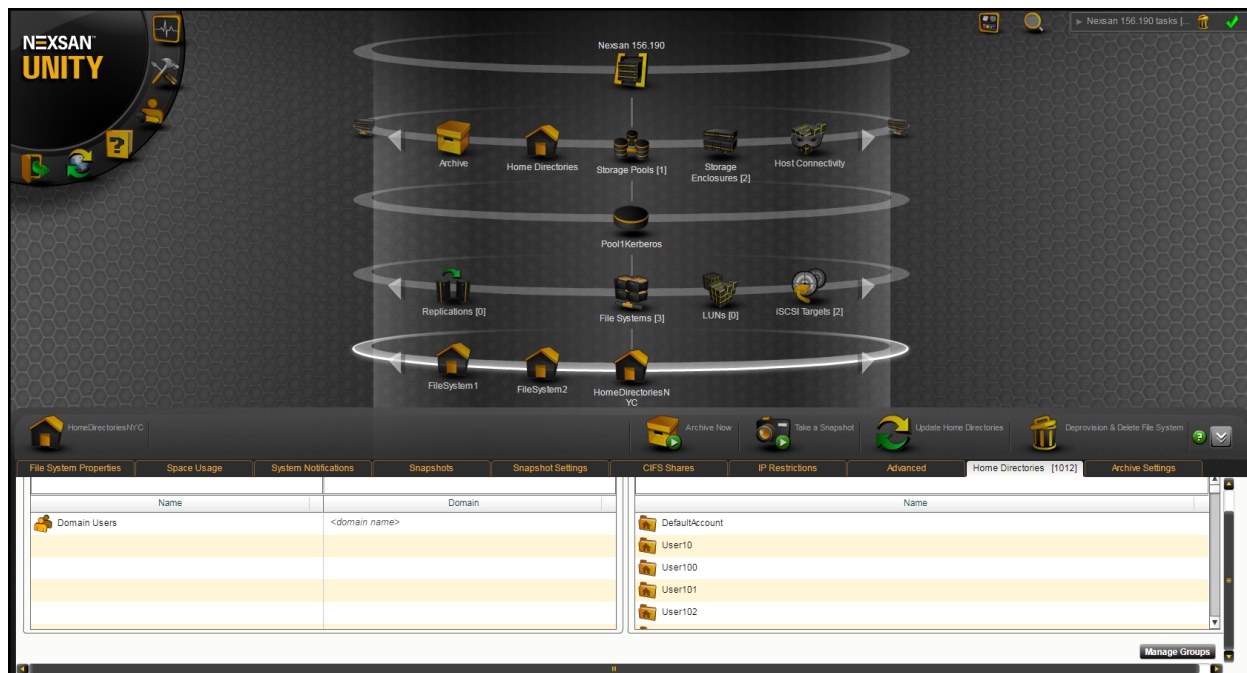
Managing home directories




Use this topic for information about the working with the file system-level **Home Directories** tab.


► **To open the file system for a home directories:**

1. In the Unity tree, click the **Site** node to display its child nodes.
2. Select the **Storage Pools** node.
3. Select the **File Systems** node.
4. Select the **Home Directories** node.
5. Click the **Home Directories** tab.

Figure 6-14: The File Systems Home Directories tab



To...	Click...
Run Active Archive	The Archive Now icon  (appears only if you have Assureon Active Archive). See Using Active Archive on page 343
Take a snapshot of the data	The Take a Snapshot icon  . See also Using the File Systems properties panel on page 194
Update Home Directories	The Update Home Directories icon  . Unity performs a background update every 5 minutes, but you can force an update at any time using the Update Home Directories button.

To...	Click...
Delete a file system for home directories	The Delete and Deprovision File System icon  to open a popup where you can delete all data in Unity for the file system created for this home directory, including all user-specific home folders and their contents. All snapshots of the data if they exist as well as replicated data on remote Unity Systems will be deleted.
Manage Home Directories group assignments	The Manage Groups button at the bottom of the panel to open a popup where you can assign groups that will have home directories. See Managing group assignments on page 165

Creating file systems for home directories

Use the **Create a File System for Home Directories** wizard to set up a file system and home directories for groups of users and to assign users as administrators.

Prerequisites

The home directories feature requires that Unity be configured to use Microsoft Active Directory for user authentication. In the Unity tree view, under the **Unity Systems node**, select the **User Authentication** tab from the properties panel.

For general guidelines about file system management, see [Before you begin on page 122](#)

[Step 1: Setting the name, storage pool, and space settings on the facing page](#)

[Step 2: Assigning user groups on page 156](#)

[Step 3: Assigning administrators on page 158](#)

[Step 4: Selecting an access protocol on page 159](#)

[Step 5: Enabling data protection on page 160](#)

[Step 6: Configuring your archive settings on page 161](#)

Step 1: Setting the name, storage pool, and space settings

In this step, set the name and storage pool assignment, and space usage for the file system that will contain the home directories.

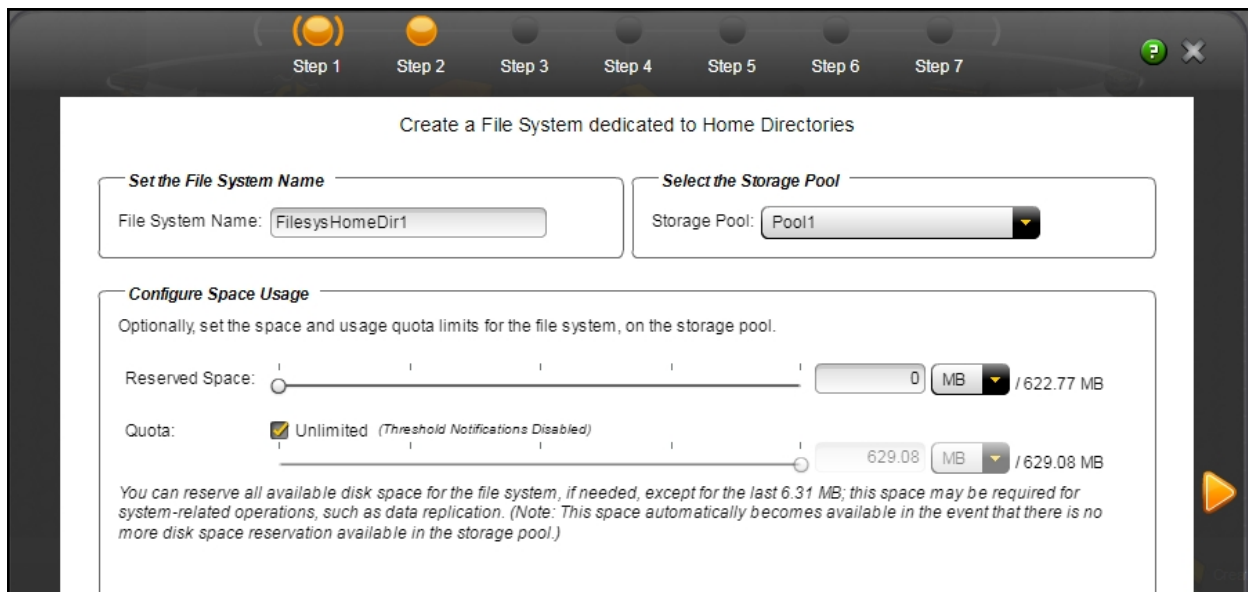
Prerequisites

- Unity Systems that will include home directories must be configured to use Microsoft Active Directory, because the home folders and administration will be stored or used on CIFS-based or NFS-based systems. For details, see [Step 4: Selecting an access protocol on page 159](#). To set up AD authentication, in the **Unity Systems panel**, select **Summary > User Authentication**.

▶ To set the home directory name and storage pool:

1. Under the site node, click the **Home Directories** node.
2. Log in with the required Active Directory credentials. A login popup displays if you have not already logged in to Active Directory.
3. Click **Create Home Directories**. The wizard opens.


Figure 6-15: Setting the name, storage pool, and space usage



4. Enter a **File System Name**.
5. Select a **Storage Pool** to assign the file system for home directories to.

6. For **Space Configuration**, you can specify:

Setting	Description
<p>Reserved Space</p>	<p><i>You can reserve a set amount of disk space in the storage pool for the exclusive use of the file system. (Read more ...)</i></p> <p>If you add another file system to the storage pool, the space available to the new file system is the difference of the total disk space in the storage pool minus any reservations set aside for other Unity file systems. For example, in a storage pool with two file systems and 10 TB of available disk space, if a reservation of 6 TB is allocated to one file system, then the second file system has 4 TB of available disk space.</p> <p>▶ To reserve space for the file system in the storage pool:</p> <ul style="list-style-type: none"> ● Move the slider left or right to set the desired amount of reserved space, <p>Or</p> <ul style="list-style-type: none"> ● Enter a value in the box to the right of the slider. <p>Note To increase reserved space when you are using a limited quota, you must first increase the quota.</p>
<p>Quota</p>	<p><i>A usage quota allows Unity to dynamically expand a file system’s storage capacity. (Read more ...)</i></p> <p>You can reserve all available disk space for the file system, if needed, except for the last 6.31 MB, which may be required for system-related operations, such as data replication. Note: This space automatically becomes available in the event that there is no more disk space reservation available in the storage pool.)</p> <p>▶ To set an unlimited quota:</p> <ul style="list-style-type: none"> ● Enable the Unlimited quota checkbox. <p>▶ To specify a quota:</p> <ol style="list-style-type: none"> 1. Uncheck the Unlimited quota checkbox. 2. Do one of the following: <ul style="list-style-type: none"> Move the Quota slider left or right to decrease or increase the quota limit, <p>Or</p> <ul style="list-style-type: none"> Enter a value in the box to the right of the slider.
<p>Record Size</p>	<p><i>Use this setting if you want to optimize for database applications that have specific file sizes. It defines the suggested size of each data block used by the File System. (Read more ...)</i></p> <p>File system record size is dynamic and Unity can write in smaller blocks for applications requiring a different record size. It is not recommended to change the default file systems record size except where the application is database-driven and</p>

Setting	Description
	<p>the database record size is precisely known.</p> <p>File systems have a default record size of 128 KB, which is the maximum size.</p>
<p>Data Compression</p>	<p> CAUTION: If you turn on data compression for a file system, and then you turn it off before you set up replication for the file system, part of the data is compressed and the other part is not. Since the file system has not been replicated yet, the compression settings are not inherited and data compression is off at the remote site.</p> <p>If you set a space quota on the file system and that quota is almost full, the file system on the remote site will not have enough space to accommodate data coming from the primary file system.</p> <p>As a result, replication will fail.</p> <p>Perform one of these actions before replication:</p> <ul style="list-style-type: none"> ● Increase the quota to match the actual space used by data on the file system. ● Set the quota to <i>Unlimited</i>. ● Enable data compression on both sites. <p>You can enable/disable compression at the file system level.</p> <p>Compression allows for better performance of the File Systems or LUNs, since the files to read/write are much smaller. However, it will also increase CPU usage. Compression can be enabled or disabled at any time.</p> <p>This setting takes precedence over the settings defined at the storage pool level. If you enabled data compression at the pool level before creating this file system, the file system already has data compression enabled—see Enabling data compression on the storage pool on page 113. If you choose to disable data compression on the file system, only that file system will be affected.</p> <p>Compression allows for better performance of the file system since the files to read/write are much smaller. However, it will also increase CPU usage. Compression can be enabled/disabled at any time.</p> <p>Notes:</p> <ul style="list-style-type: none"> ● When you set up replication for file systems that have the compression setting enabled, file systems on the remote site inherit the compression settings. ● Enabling or disabling data compression does not affect existing data. It will only affect data that will be written to the file system after the change.

Note [Step 4: Selecting an access protocol](#) on page 159 is only displayed if your Unity deployment includes Unity's Data Protection feature. For more information about Snapshots and Data Replication, please contact your Nexsan reseller or Nexsan Support Representative.

7. Click the **Next** arrow to proceed.

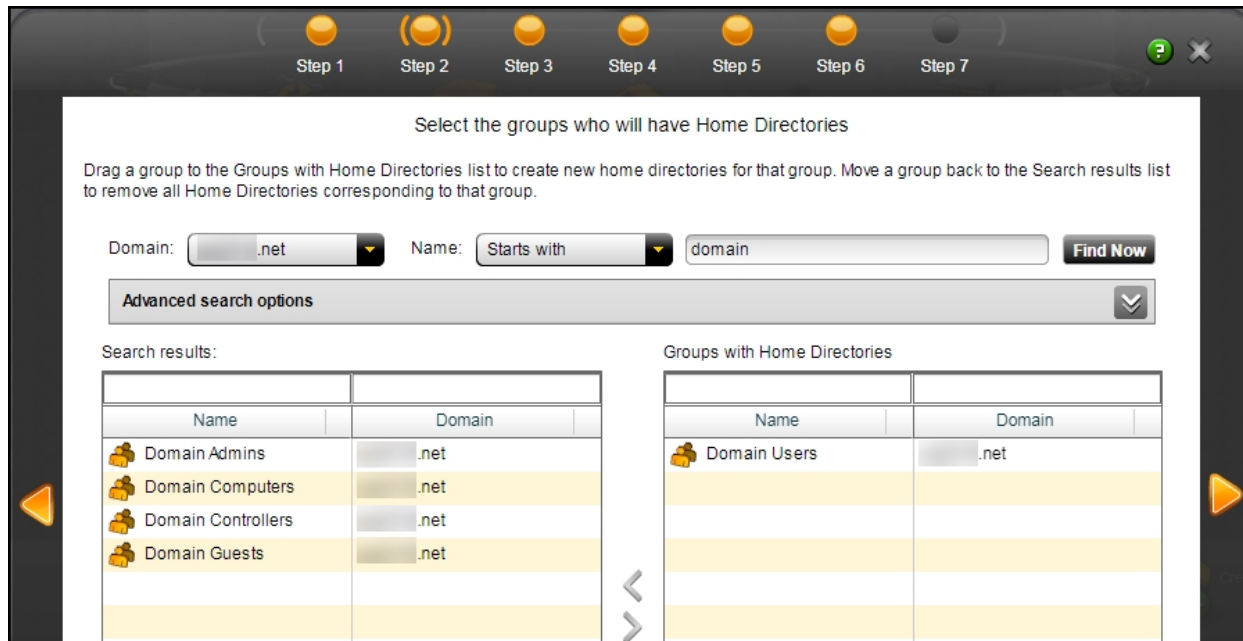
Step 2: Assigning user groups

In this step, assign the group or groups you need to create home directories for.

Prerequisites

- User groups must first be set up using Microsoft Active Directory in Windows.

Figure 6-16: Assigning user groups

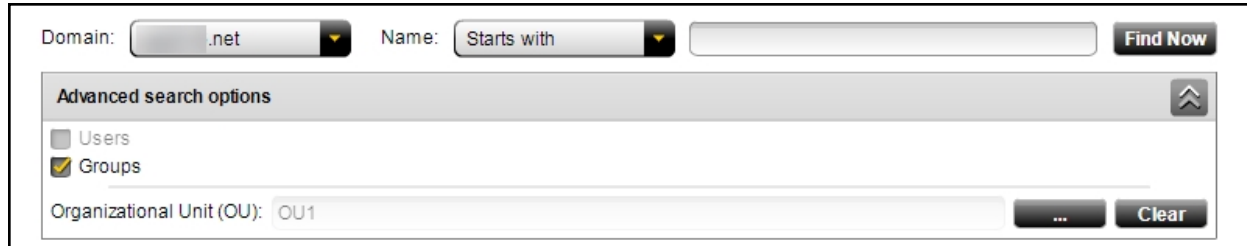


▶ To assign groups you want to create home directories for:

1. Click to select a group from the **Search results**.
2. Click the right arrow to add the group to the **Groups with Home Directories**.
You can click the left arrow to **remove** the group assignment from the **Groups with Home Directories** list.
3. Click the **Next** arrow to proceed.

Note Optionally, you can narrow the search using any of the following:

- In the **Domain** box, select an alternate domain.
- In the **Name** box, select between **Starts with**, **Ends with**, or **Is exactly**.
- Click the down arrow to display **Advanced Search Options**, and include organizational units in the criteria, if applicable. See [Users and Groups window](#) on page 75



The screenshot shows a search interface with the following elements:

- Domain:** A dropdown menu currently set to ".net".
- Name:** A dropdown menu currently set to "Starts with", followed by an empty text input field.
- Find Now:** A button to execute the search.
- Advanced search options:** A section with a collapse arrow (upward-pointing triangle) in the top right corner.
- Users:** A checkbox that is currently unchecked.
- Groups:** A checkbox that is currently checked.
- Organizational Unit (OU):** A text input field containing "OU1", followed by a browse button (three dots) and a "Clear" button.

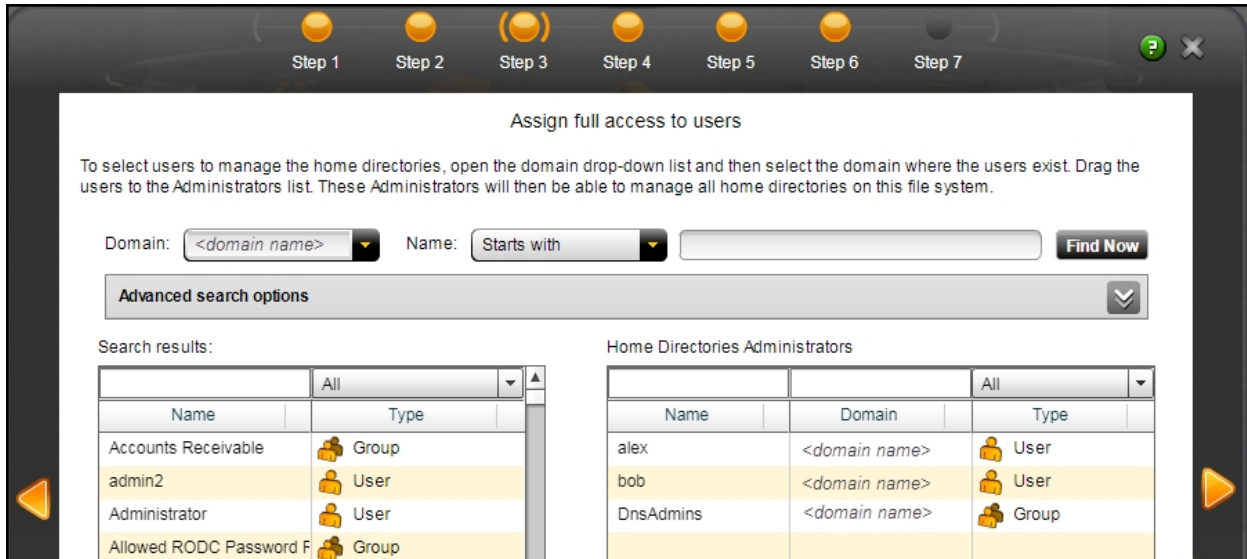
Step 3: Assigning administrators

In this step, assign administrators to manage the new home directories.

Prerequisites

- The users you assign as administrators must first be set up using Microsoft Active Directory in Windows. Any user can be assigned as an administrator.

Figure 6-17: Assigning administrators

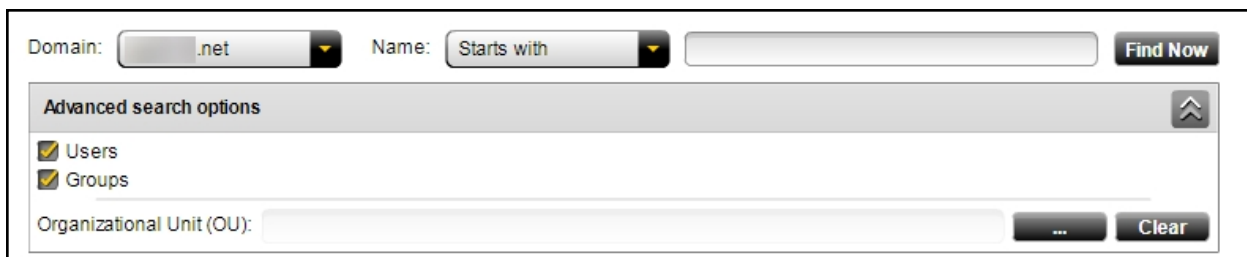


► **To assign administrators to manage home directories:**

1. Click to select users or group from the **Search results**.
2. Click the right arrow to add the users or groups to the **Home Directories Administrators** list.
You can click the left arrow to **remove** the assignment from the list.
3. Click the **Next** arrow to proceed.

Note Optionally, you can narrow the search using any of the following:

- In the **Domain** box, select an alternate domain.
- In the **Name** box, select between **Starts with**, **Ends with**, or **Is exactly**.
- Click the down arrow to display **Advanced Search Options**, and include or exclude users, groups, or organizational units, if applicable, from the criteria. See [Users and Groups window](#) on page 75

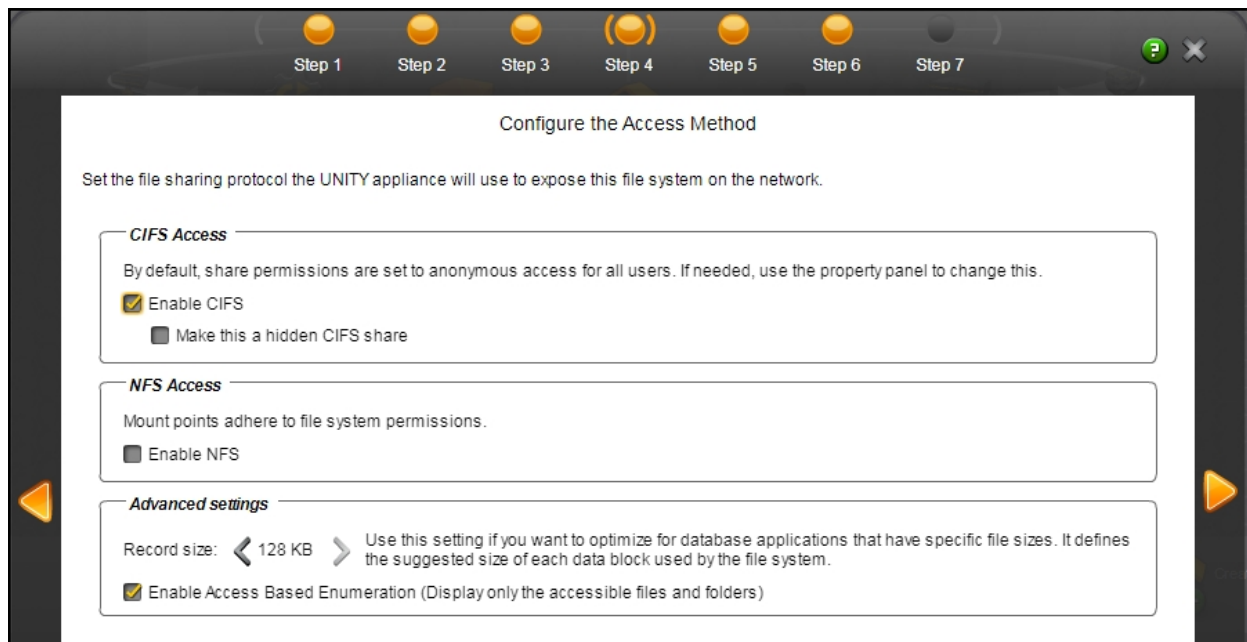


Step 4: Selecting an access protocol

Now select the **Access Protocol** for the file system used for the home directories.

- A file system that you expose using the CIFS sharing method can also be accessed by UNIX/Linux-based systems using a CIFS client implementation for UNIX (such as, *Samba*).
- A file system that you expose using the NFS sharing method can also be accessed by Windows-based systems using an NFS client implementation for Windows (available in *Microsoft Services for UNIX*)
- You cannot expose a file system to Windows-based systems over the CIFS protocol if Unity is connected to an LDAP Directory service; the CIFS sharing option is not available in LDAP Directory service implementations.
- If you configured LDAP Directory service as the user authentication mode for Unity: exposing a file system over the CIFS protocol in an LDAP environment is only supported with anonymous read and/or anonymous read/write access enabled for the share.
- If the file system will be accessed over IIS, do not enable case-sensitivity for the share.

Figure 6-18: Selecting an access protocol



► To configure the access protocol for the new home directories:

1. Choose any of the following:

CIFS Access (default)

To expose the file system to Windows-based systems over the CIFS (SMB) protocol, select the **Enable CIFS** option. This option is selected by default if Unity is joined to a Microsoft Active Directory domain.

NFS Access

To expose the file system to UNIX/Linux-based systems over the NFS protocol, select the **Enable NFS** option. This option is selected by default if Unity is connected to an LDAP Directory service, or it the system is configured to use Unity authentication.

Access Based Enumeration

Restricts exposure of folders and files in a CIFS file system based on user access privileges. When this option is enabled for a CIFS file system, any user that accesses the file system sees only the files and folders to which they have access. This mechanism is only available for CIFS file systems. This option is selected by default.

2. Click the **Next** arrow to proceed.

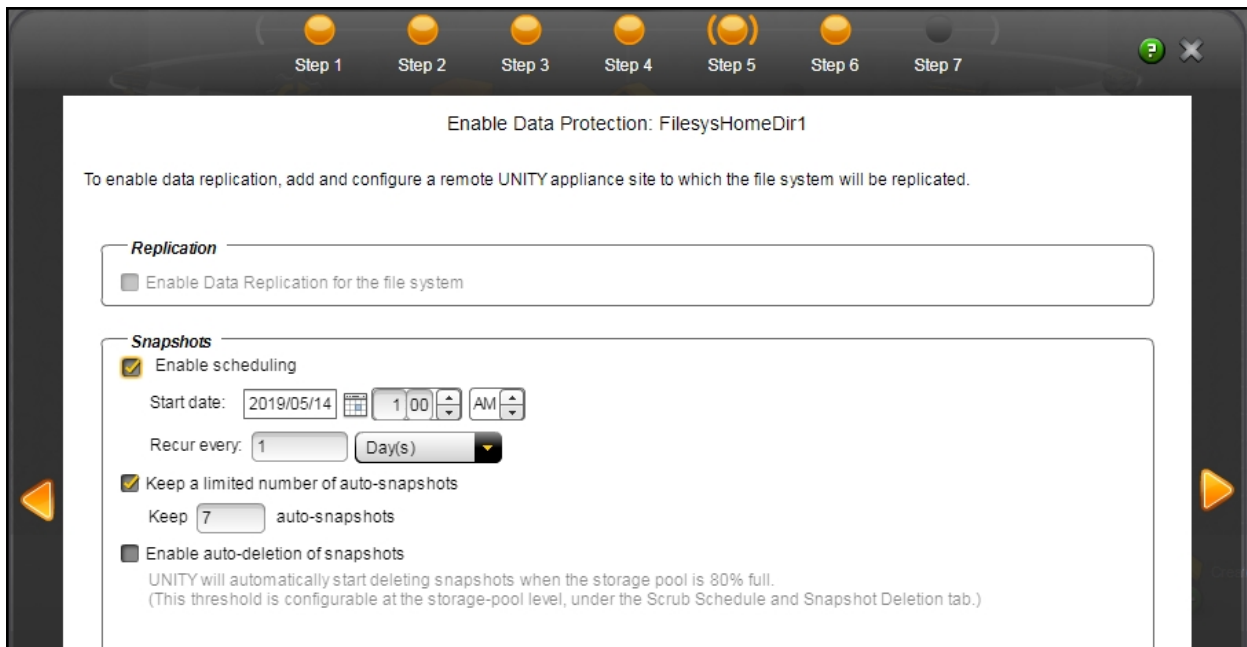
Step 5: Enabling data protection

Now you need to enable:

- Replication
- Snapshots scheduling

Note To enable replication for a file system, you need a second Unity Storage System that you can connect the current system to. See [Data replication](#) on page 419

Figure 6-19: Enabling data protection



► **To enable data protection for file system for home directories:**

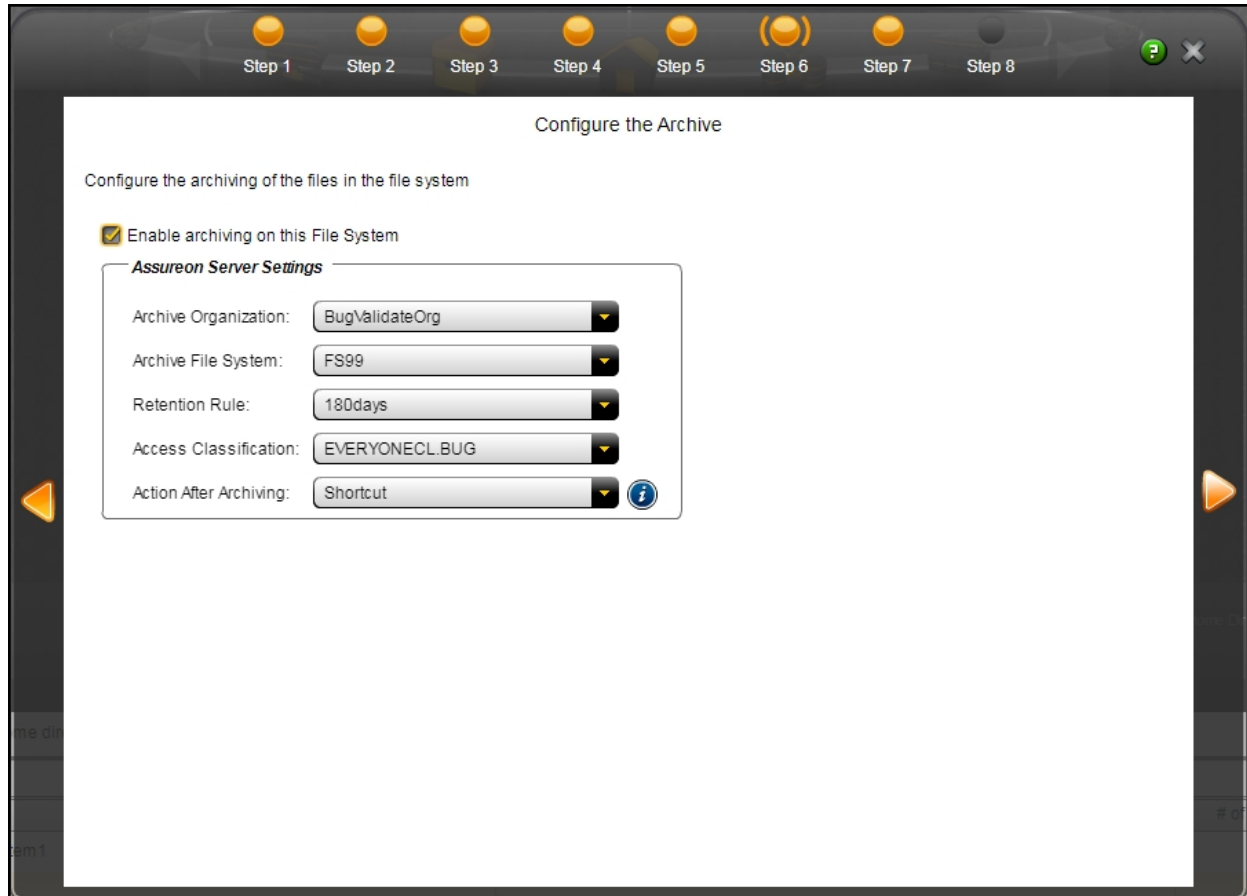
1. If your Unity System is connected to a remote Unity System and has replication set up, select **Enable Replication**.
2. Optionally, select **Enable snapshot scheduling**. By default, automatic snapshots are enabled every day at midnight and a limit of seven snapshots are maintained.
3. Adjust the schedule for auto-snapshots to be taken, according to your requirements. You can change the number, frequency and time of day.
4. Specify the maximum number of auto-snapshots to be retained.
5. Enable auto deletion of snapshots if you want Unity to delete snapshots when the storage pool is 80% full. The threshold is configured on the **Storage Pool Advanced Settings** page.
6. Click the **Next** button.

Step 6: Configuring your archive settings

Step 6 of the Home Directories wizard prompts you to select the **Assureon Archive Settings** for the file system.

This step only appears if you have Active Archive on this Unity. Active Archive allows you to set data retention policies to automatically offload stale data and release primary storage. This allows you to increase the performance of your primary storage without increasing its primary size.

Archiving allows you to retain data, using Nexsan's Assureon archiving capabilities.



► **To configure Active Archive settings:**

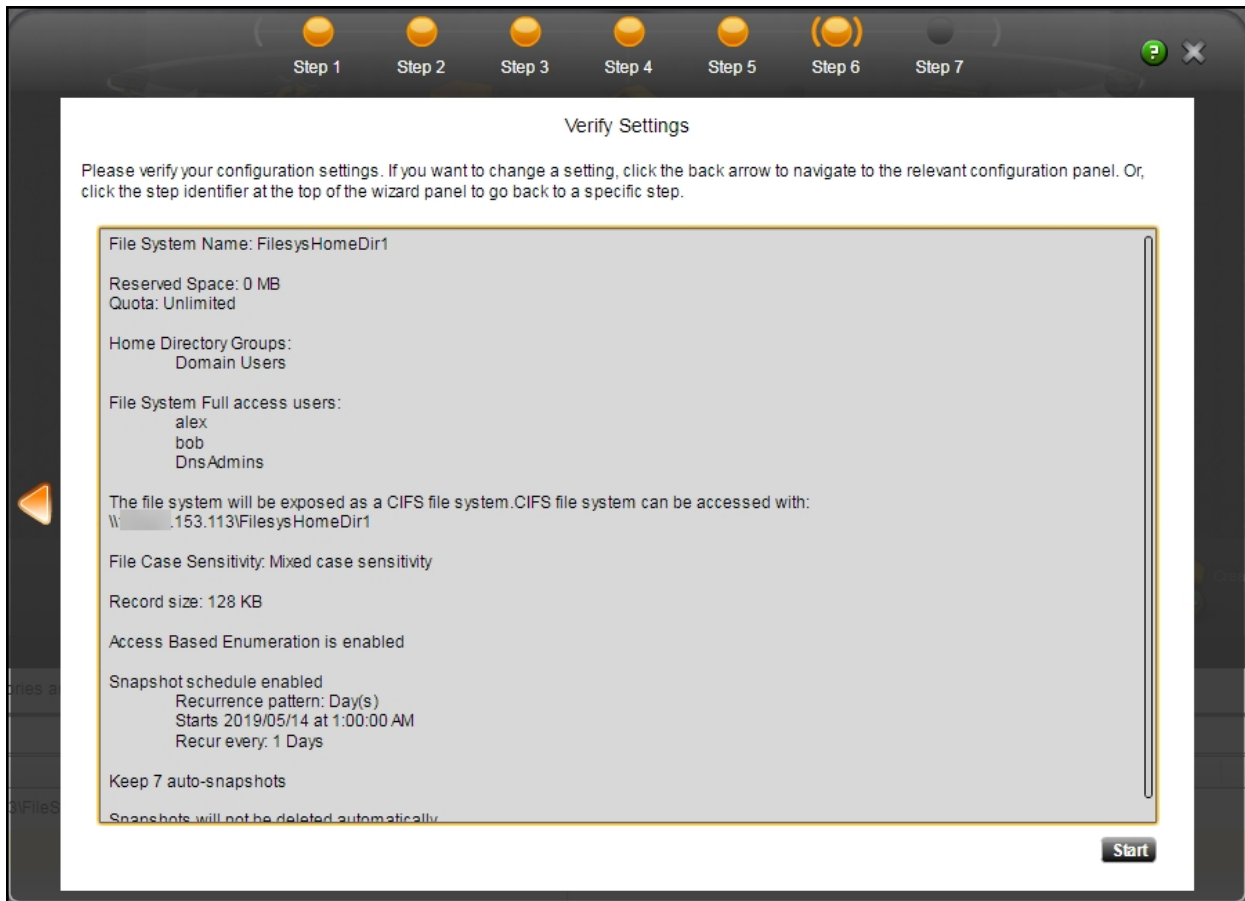
1. Select the **Enable archiving on the file system** checkbox.
2. Configure the Assureon Archive Server that is to be used for archiving purposes. These are the settings on Assureon Archive Server to which data from your file system will be archived. The options that appear here are defined on the Assureon Server.
 - **Archive Organization:** Select the Assureon organization to be used for archiving. An organization is a group of one or more file systems which share retention rules, access classifications and reports.
 - **Archive File System:** Select the file system in the Archive Organization to be used for archiving. A file system consists of a database, storage location (the stores), manifest and audit files as well as replication options. Think of it as a self-contained archive that shares properties with the other file systems within an organization.
 - **Retention Rule:** Select the retention rule to be used for data archived from this file system. Retention rules specify how long a file is kept under management. For example, 180 days.
 - **Access Classification:** Select the access classification to be used for data archived from this file system. When a file is placed under Assureon management, it is stored using classification and sub classification information. Classifications allow you to control access to files. They also provide an intuitive way to search, audit, and dispose of files.
 - **Action After Archiving:** Define what is to happen to files once they have been archived. For example, create a shortcut to the files, leave them as they are, or remove them from the file system. Note that files will not be converted to shortcuts, or removed if n-Way Sync or asynchronous replication is enabled.

Note If enabled on the Assureon Archive Server, Schedule Archiving allows for a complete archive of this file system, initiated manually or scheduled on the Assureon Server. This does not affect Real-Time archiving.

Verifying settings

In this step, the wizard displays the file system for home directories settings for review.

Figure 6-20: Verifying settings



► To review your settings:

1. Review the summary of the settings shown on screen.
2. To revise any of your settings:
Click the **Back** arrow to go back.

OR

Click any of the step numbers at the top of the panel to jump to that section of the wizard.

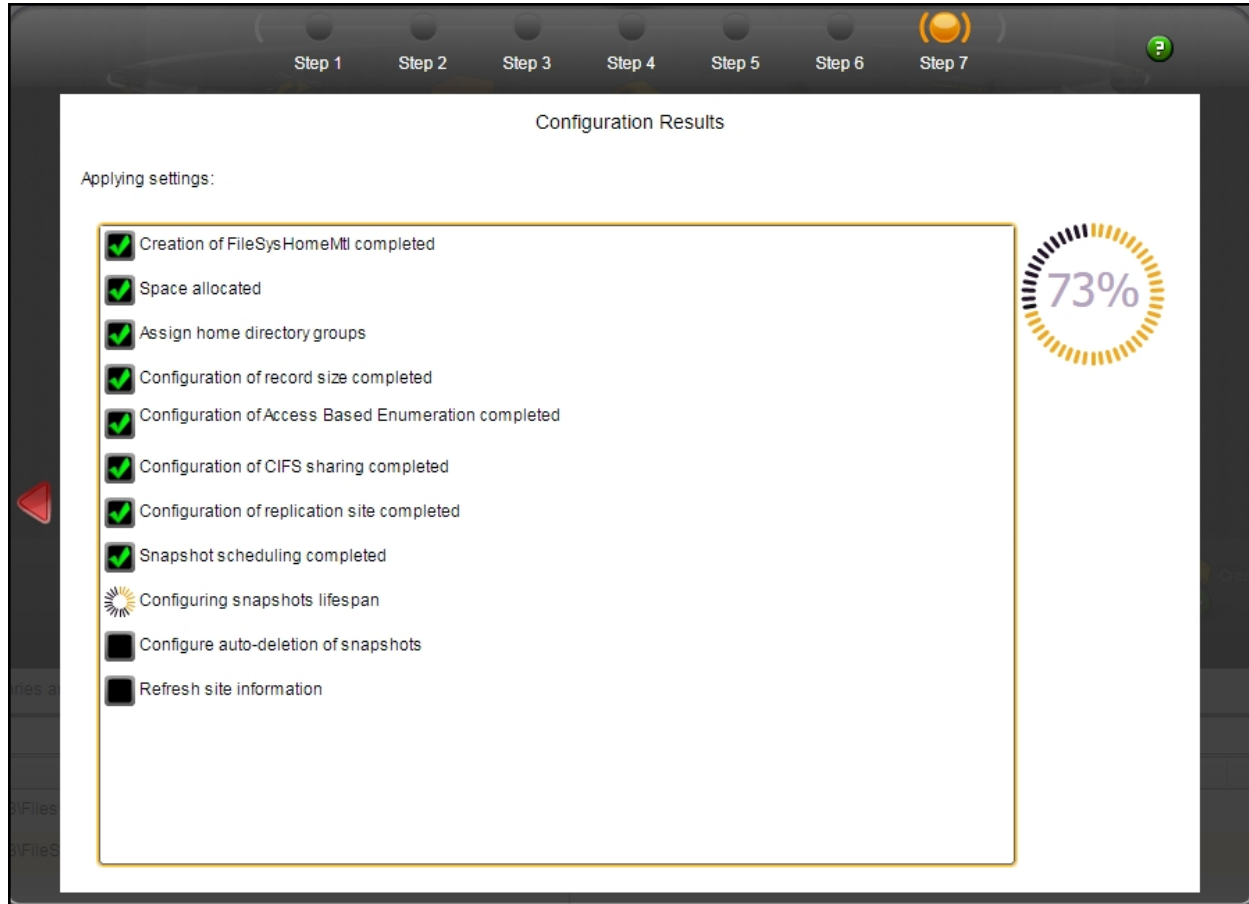
3. When you are ready to proceed, click **Start**.

The wizard displays file system creation progress as it applies your settings.

Viewing results

In this step, the wizard displays progress and results as Unity creates the new file system for home directories.

Figure 6-21: Viewing configuration results



The wizard displays error events that the system encounters during the creation process. You can view more details about an error event by expanding the corresponding entry.

► **To view more details for an error event:**

- Click the plus (+) sign corresponding to the error event.

Unity informs you when it successfully creates the file system and home directories.

Managing group assignments

Use this procedure for details about managing group assignments for file systems for home directories.

Prerequisites

- To manage home directory group assignments, you need to know the composition of the Active Directory user groups and the available groups you're maintaining.

Figure 6-22: Home Directories > Manage Groups

Home Directories dedicated File Systems

File Systems on this UNITY that have been dedicated to home directories are displayed below.

Name	CIFS Mount Point	NFS Mount Point	# of Groups	# of Directories
FSHomeDirs	\\ .156.233\FSHomeDirs	N/A	2	1013

1 File System(s) dedicated to Home Directories on this system.

Manage Groups List Directories Deprovision & Delete

► To modify the groups in a file system for home directories:

- In the Unity tree, click the **Site** node to display its child nodes.
- Select the **Home Directories** node.
- In the properties panel, select a file system for home directories.
- Click the **Manage Groups** button at the bottom of the window (see image) to open a popup window, where you can assign groups that will have home directories.

5. Select a group or groups and use the arrows to add or remove them from the file system. The domain you use when you set up the file system for home directories determines the available groups.
6. Click the **Apply** button.
7. If you want to view the changes immediately, click the **Update Home Directories** button. Unity performs a background update every 5 minutes, but you can force an update at any time using the Update Home Directories button.

Performing file system-level tasks for home directories



Use this topic for information about file system-level features available for home directories.

► **To open a file system for home directories:**

1. In the Unity tree, click the **Site** node to display its child nodes.
2. Select the **Storage Pools** node.
3. Select the **File Systems** node.
4. Select the **Home Directories** node.

Figure 6-23: File Systems panel

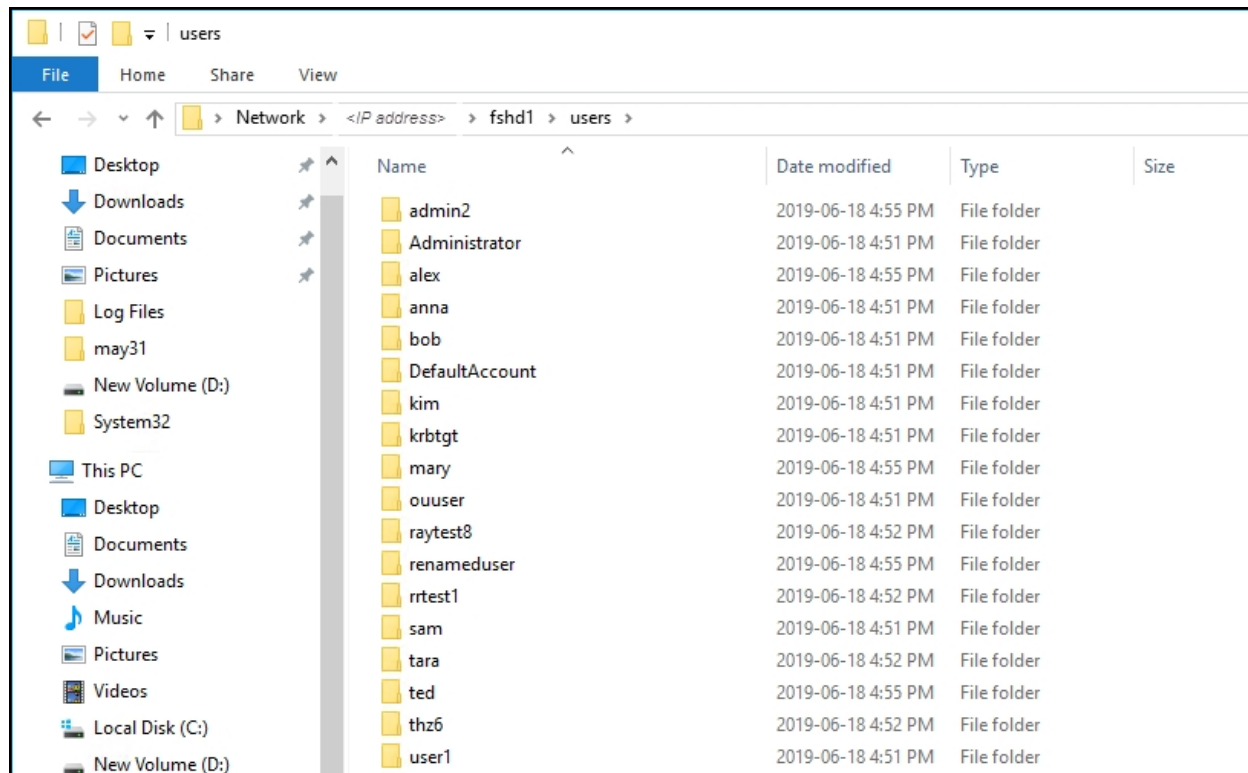


To...	Click...
Delete a file system for home directories	The Delete and Deprovision File System icon  to open a popup where you can delete all data in Unity for the file system created for this home directory, including all user-specific home folders and their contents. All snapshots of the data if they exist as well as replicated data on remote Unity Systems will be deleted.
Update Home Directories	The Update Home Directories icon  . Unity performs a background update every 5 minutes, but you can force an update at any time using the Update Home Directories button.

Example file system for home directories

Here is an example of a file system set up for home directories in Windows:

Figure 6-24: Viewing a file system for home directories in Windows



The folder path that Unity creates is `\\<Unity System IP address><Unity file system>\users\<dedicated folder for each user >`

For instructions about how to connect to a Unity file system, see [Accessing a CIFS share from Windows](#) on page 173.

Managing shares

Unity allows you to add shares to file system on Unity. A share is a shared network folder that resides inside a parent file system. Unity exposes a share to Windows and UNIX/Linux-based clients on the network as a separate network resource over the CIFS protocol—completely independent of the parent file system in which it resides.

► **Space usage settings, snapshots, and Data Replication for shares:**

A share inherits space usage settings from the parent file system, and as such, all disk space consumed by files in a share affect the overall disk space consumption of its parent file system.

In addition, Unity automatically takes snapshots of the data in shares, and also replicates shares to the corresponding remote Unity—provided you enable and configure Snapshots and Data Replication on the parent share.

This section includes these topics:

Adding a share.....	168
Disabling data sharing for a share.....	183
Renaming a share.....	184

Adding a share

Unity provides the Share Setup Wizard to guide you through the process of adding a share.

► **To start the Share Setup Wizard:**

1. Under the site node, click the **Storage Pools** node to display its child nodes.
2. Click the storage pool containing the file system to which you want to add a share.
3. Click the **File Systems** node.
4. Click the **File System** to which you want to add a share.
5. Expand the share's Properties panel.
6. Click **Add a Share**.

Note You can also open the wizard by opening the Share node's context menu and selecting **Add Share**.

The Share Setup Wizard guides you through the process of adding a share.

This section includes these steps:

Step 1: Setting the share's name.....	168
Step 2: Assigning access permissions to the share.....	170
Step 3: Verifying settings.....	171
Step 4: Viewing configuration results.....	172

Step 1: Setting the share's name

Step 1 of the Share Setup Wizard prompts you to specify a name for the share, and if needed, configure the share as a hidden CIFS share.

When you configure a share as a hidden CIFS share, the share is not visible to Windows-based clients on the network; Windows-based clients interpret a hidden share as an administrative share on the network, and prevent its display when you browse shares on Unity. This mechanism allows you to further restrict access to a share, if needed.

To access a hidden CIFS share on Unity from a Windows-based client, you must specify the share's full path on Unity, including the \$ character appended to the end of the share's name; for example:

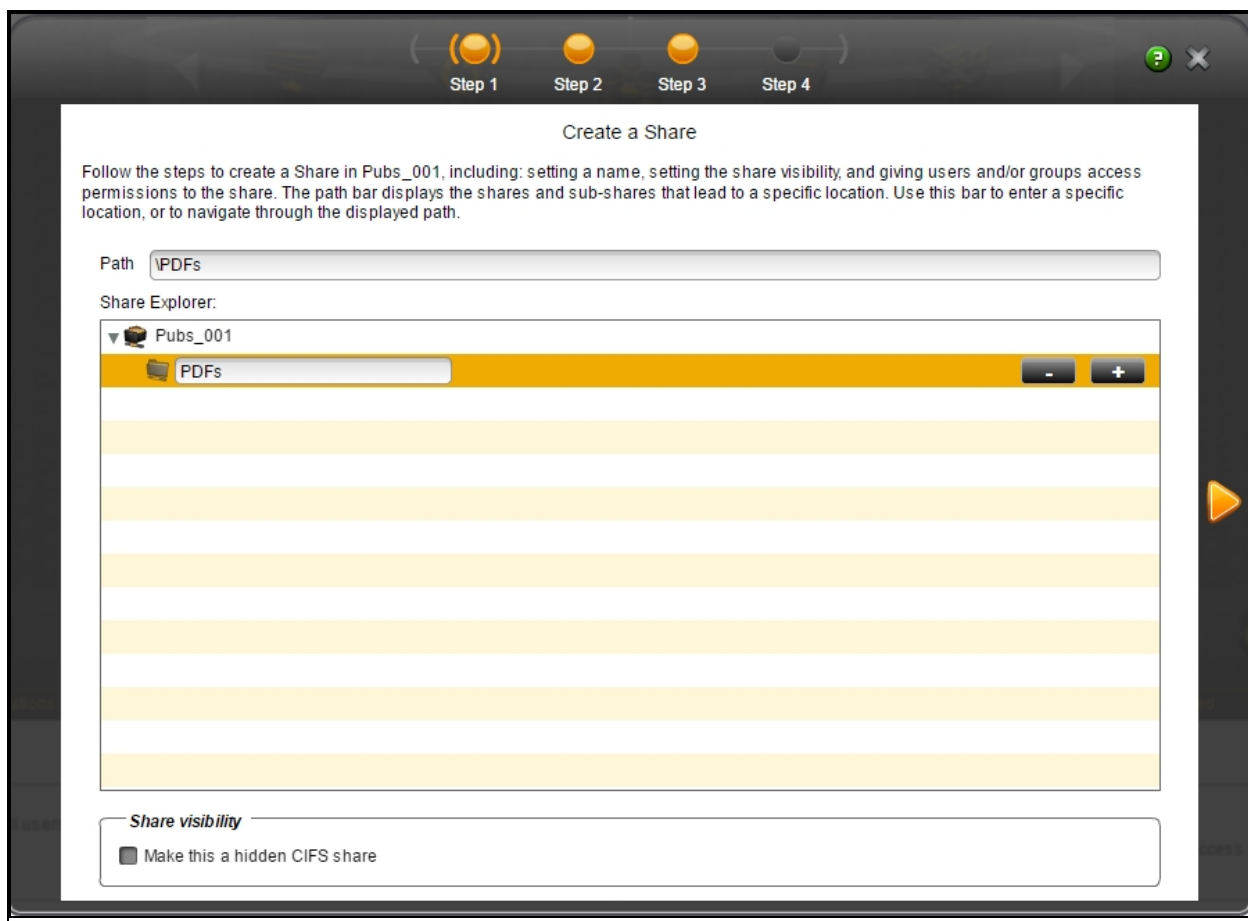
```
\\<ShareName>$
```

Where <ShareName> is the name of the hidden CIFS share on Unity.

Notes:

- Unity currently does not support exposing a share over the NFS protocol. When you add a share to an NFS share, Unity automatically exposes the share over the CIFS protocol. This also applies when you add a share to a share that has no sharing method specified (data sharing is disabled): Unity exposes the share over the CIFS protocol.
- You can configure a share as a hidden CIFS share even if you set the sharing method for its parent share to NFS sharing.

Figure 6-25: Share Setup Wizard, Step 1: Setting the share's name



► To create a share:

1. Type a name for the share in the open text field.

The name must start with an (upper-case or lower-case) alphabetic or numeric character; and, with the exception of the hyphen (-), and period (.), the name can only contain alphanumeric characters, without spaces.

These characters are NOT allowed:

“ / \ [] : ; | = , + * ? < >

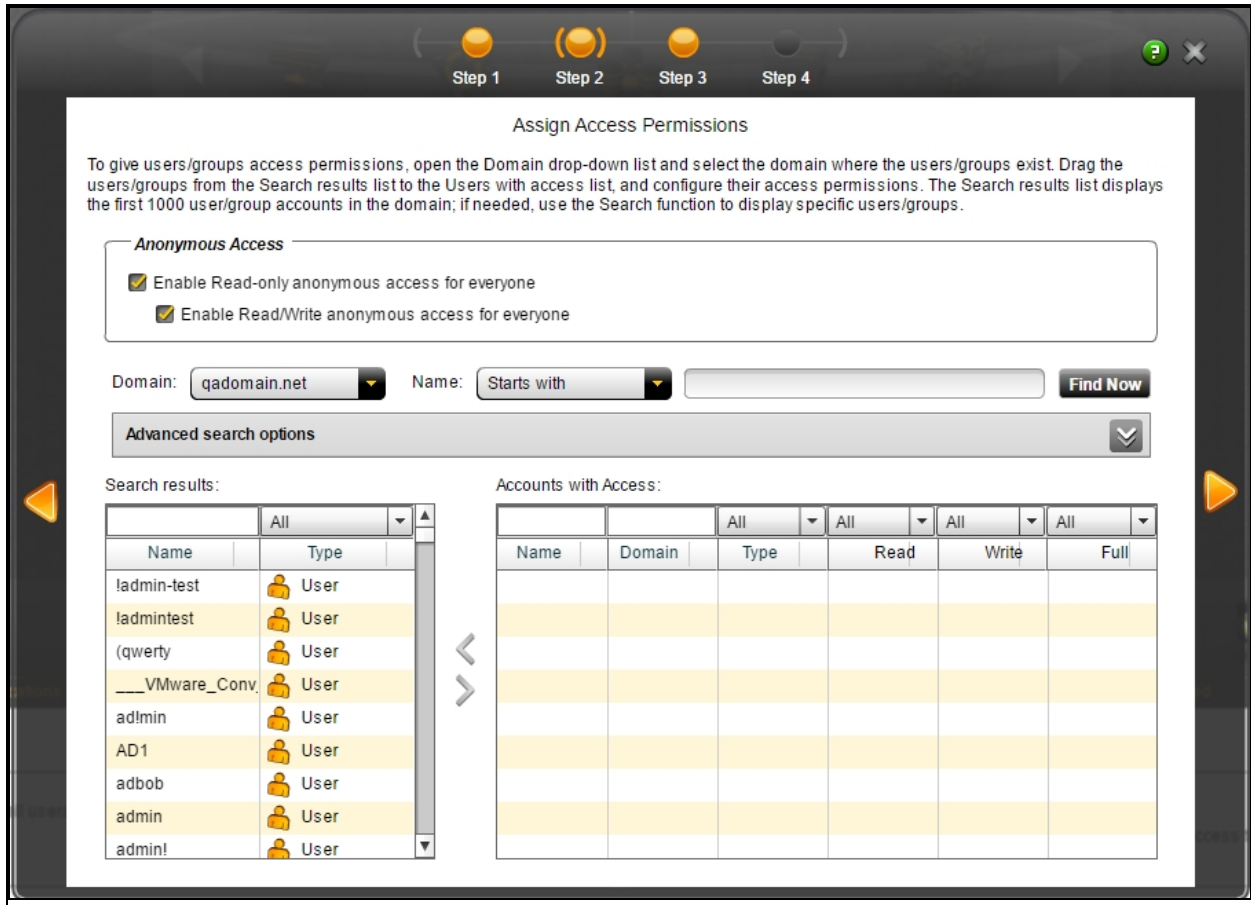
Note You can also manually enter a new location for the share, using the Path Bar. Or, you can use the Share Explorer to navigate to the new location for the share. Click the plus sign (+) to create additional locations within the file path.

2. (Optionally) Select the **Make this a hidden CIFS share** option.
3. Click the forward arrow on the panel to continue to [Step 2: Assigning access permissions to the share below](#).

Step 2: Assigning access permissions to the share

Step 2 of the Share Setup Wizard prompts you to select the user(s) and/or group(s) that will access the share, and configure their access permissions. You can search for specific users and/or groups in the Microsoft Active Directory domain or LDAP Directory service that Unity is connected to; or, if the system is configured to use Nexsan Unity authentication, users and/or groups that you defined on the system.

Notes: By default Read/Write access is granted to everyone. To assign Read/Write access to ONLY a specific user or group you must disable this setting.



▶ To configure access permissions for a share:

1. From the **Domain** drop-down list, select the domain server(s) where the users or groups that you want to give access permissions to exist.

Note The panel displays the **Domain** drop-down list if Unity is integrated with a Microsoft Windows Active Directory domain or an LDAP Directory service. In a multiple domain environment, the **Domain** drop-down list contains all the domains on the network.

You can give users and groups from different domains access to the share, if needed.

2. In the **Name** text box, type the name of the user or group that you want to give share-level access permissions to exists, and then, click the **Find** button to display the specified user or group.

If needed, you can use the **Find Now** function to display specific users and/or groups. For example, to display the user *Bob*:

- a. Select the **Starts with** option from the pick list next to the Name text box.
- b. Type **BO** (or **bo**) in the **Name** text box.
- c. Click the **Find Now** button. Unity displays all users and/or groups with user and/or group names that start with the letters **b** and **o** in the **Search results** grid (on the bottom-left of the panel).

You can also use the **Advanced Search** function and set more specific search criteria; for more information, see [Users and Groups window](#) on page 75.

3. In the **Search results** grid, select the user or group that you want to give access permissions to by highlighting the relevant user or group in the grid.

Hold down SHIFT or CTRL and click the left mouse button to highlight multiple entries in the grid.

You can also search for specific users or groups in the grid, or filter the list of users or groups, by entering a user or group name in the text box located above the **Name** column.

4. Drag your selection to the **Accounts with Access** list on the right-hand side of the panel.
5. Next, for each user and/or group that you add to the Accounts with Access list, select the relevant check box in the **Read**, **Write**, or **Full** column corresponding to the level of access that you want to give to the user and/or group. For example, if you want to give the selected user or group Full access to the share, select the **Full** check box; the **Read** and **Write** check boxes are automatically selected as well.

If you want to give all users and groups Read, Write, or Full access to the share, select the corresponding top-level check box in the Read, Write, or Full column heading.

6. Once you finish configuring user access to the share, click the forward arrow on the panel to continue to [Step 3: Verifying settings](#) below.

Note You can modify the **Permissions** list for the share—for example, remove permissions or change permissions for users—once you finish adding the share.

Step 3: Verifying settings

Step 3 of the Share Setup Wizard summarizes the settings you selected for your share and creates the share when you click **Start**. Review the summary carefully before applying the configuration settings.

► **To change a configuration setting:**

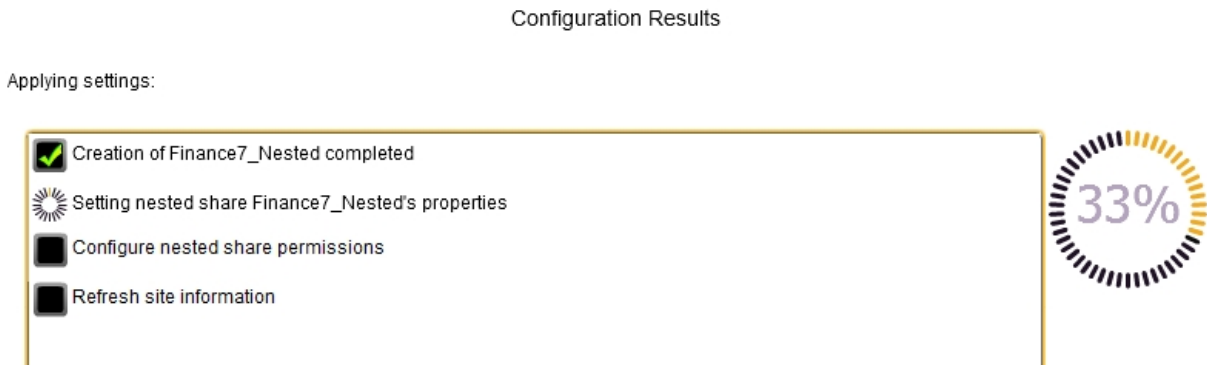
- Click the back arrow to navigate back to the corresponding configuration step.
Or
- Click the corresponding step identifier at the top of the Share Setup Wizard panel. For example, if you want to rename the share, click **Step 1**.

If you are satisfied with the configuration settings, click the **Start** button at the bottom of the panel. The Share Setup Wizard automatically proceeds to [Step 4: Viewing configuration results](#) on the next page.

Step 4: Viewing configuration results

Step 4 of the Share Setup Wizard displays progress as Nexsan Unity creates the new share.

Figure 6-26: Share Setup Wizard, Step 4: Viewing configuration results



The Share Setup Wizard displays error events that the system encounters during the share creation process. You can view more details about an error event by expanding the corresponding entry.

▶ **To view more details for an error event:**

- Click the plus (+) sign corresponding to the error event.

Unity informs you when it successfully creates the share. It also asks you if you want to create another share:

- Clicking **Yes** takes you back to Step 1 and resets all configuration settings to their defaults.
- Clicking **No** closes the Share Setup Wizard.

You can now access the share from a Windows-based (CIFS) system in the same way that you access a CIFS share; see [Accessing a CIFS share from Windows](#) on the facing page.

Accessing shares

This section explains how to access a share on Unity from Windows and UNIX/Linux based systems.

Table 6-5: Supported accessibility methods

CIFS sharing	NFS sharing	FTP Sharing	CIFS and/or NFS and/or FTP sharing
The share can be accessed from:			
<ul style="list-style-type: none"> Windows-based systems using CIFS 	<ul style="list-style-type: none"> Windows-based systems using an NFS version 3¹ client 	<ul style="list-style-type: none"> Windows-based systems using FTP 	<ul style="list-style-type: none"> Windows-based systems using CIFS and/or FTP
<ul style="list-style-type: none"> UNIX/Linux-based systems using a CIFS client 	<ul style="list-style-type: none"> UNIX/Linux-based systems using NFS version 3 and/or NFS version 4 	<ul style="list-style-type: none"> UNIX/Linux-based systems using FTP 	<ul style="list-style-type: none"> UNIX/Linux-based systems using a CIFS client and/or FTP
		<p>Note FTP sharing is only supported for local authentication.</p>	<ul style="list-style-type: none"> Windows-based systems using an NFS version 3 client and/or FTP
			<ul style="list-style-type: none"> UNIX/Linux-based systems using NFS version 3 and/or NFS version 4 and/or FTP

This section includes these topics:

Accessing a CIFS share from Windows.....	173
Accessing an NFS file system from UNIX/Linux.....	177
Using an NFS version 3 (NFSv3) client to access an NFS share with Microsoft Active Directory.....	178
Using an NFS version 4 (NFSv4) client to access an NFS share.....	179

Accessing a CIFS share from Windows

You access a CIFS share on Unity from Windows in the same way that you access a network share; and like a network share, you can map a CIFS share on Unity to a drive letter on your local Windows machine. You need the IP address or DNS (host) name of Unity where the CIFS share that you want to access is located, as well as the share's name.

Note To access a share, your user account must be granted access permissions to the share in Unity (or it must be a member of a group that is granted access); see [Viewing mount point information for file systems](#) on page 186.

¹If you want to access a share from Windows-based systems using the NFS protocol, you must enable the Read-only anonymous access option for the share.

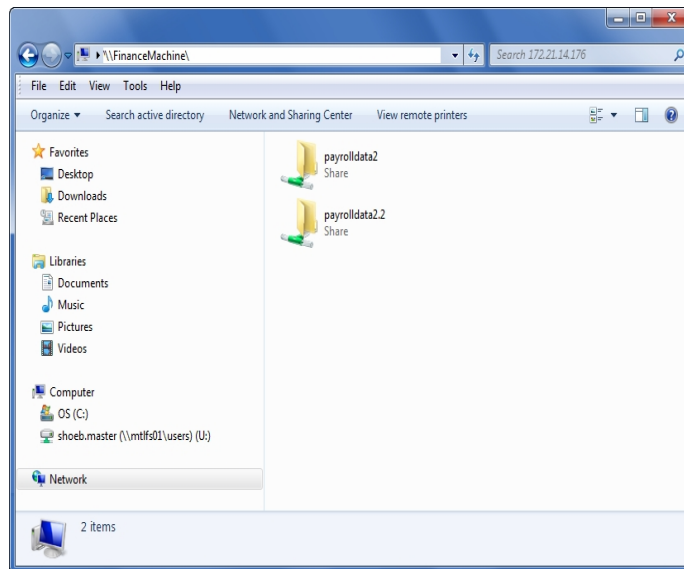
► **To access a CIFS share from Windows:**

1. Open Windows Explorer.
2. In the Windows Explorer address bar, type the virtual IP address of the Pool Resource Group on Unity where the CIFS share that you want to access is located. For example, if the share is in a storage pool assigned to Pool Resource Group 1, with the virtual IP address xxx.xx.12.25, type:

\\xxx.xx.12.25\

Tip You can also access a share directly on Unity by adding the share's name in the address path; for example: \\xxx.xx.12.25\payrolldata2.

3. Press Enter. This displays all the CIFS shares on Unity.



4. Double-click the share that you want to access. You may be prompted for a user name and password to access the share, if:
 - The share is not configured for Read-only or Read/Write anonymous access, and if the share you are attempting to access is on an Unity in a different domain.
 - The share is not configured for anonymous access, and the user that you are currently logged on with to the local Windows system does not have access permissions to the share.
 - Unity is configured to use Unity authentication. With Unity authentication, user accounts are created and stored locally on Unity, and since there is no authentication through a domain controller or LDAP Directory service, you are required to enter valid logon credentials when accessing a share on the system; see [User authentication modes](#) on page 66.

Note To access a share, your user account must be granted access permissions to the share in Unity (or it must be a member of a group that is granted access); for more information, see [Managing access permissions to shares](#) on page 186.



5. If applicable, enter a valid user name and password and click **OK** to access the share. Windows displays the contents of the share.

Note Windows caches the credentials that are collected during an interactive domain logon to let you authenticate to a network or a network resource one time. Thereafter, you are granted access to all authorized network resources without providing credentials again. This also applies to shares on Unity; you are not prompted for a user name or password when you next attempt to access a share on Unity that Windows has already cached credentials for. Windows clears cached credentials when you log off or reboot the Windows system.

Mapping a CIFS share to a drive letter

If needed, you can also map a CIFS share to a drive letter on a Windows-based system.

► Before you begin:

If you did not grant access permissions to the share during its creation, you must follow the steps mentioned in [Giving share-level access permissions to a user or group](#) on page 189.

► **To map a CIFS share to a drive letter on a Windows-based system:**

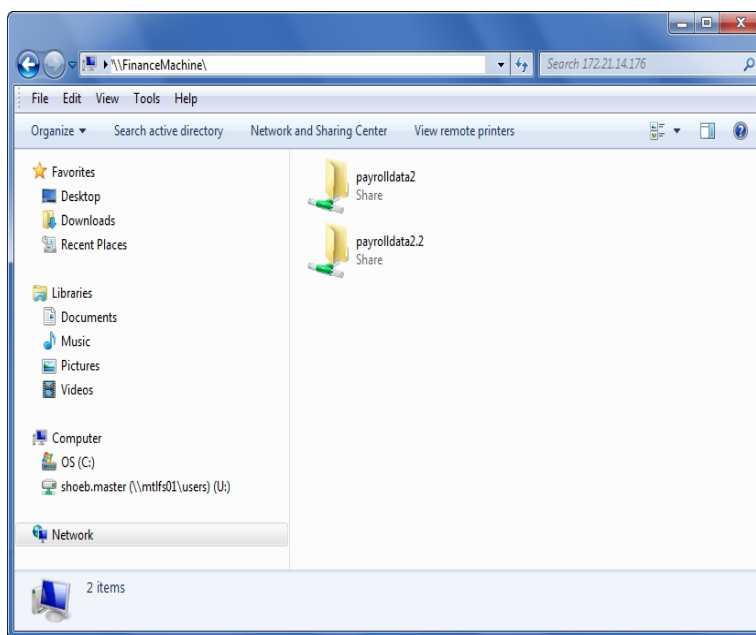
1. Open Windows Explorer.
2. In the Windows Explorer address bar, type the virtual IP address of the Pool Resource Group on Unity where the CIFS share that you want to access is located. For example, if the share is in a storage pool assigned to Pool Resource Group 1, with the virtual IP address xxx.xx.12.25, type:

\\xxx.xx.12.25\

Tip You can also access a share directly on Unity by adding the share's name in the address path; for example: \\xxx.xx.12.25\payrolldata2.

3. Press the Enter key. This displays all the CIFS shares on Unity.

Figure 6-27: Mapping a CIFS share to a drive letter on a Windows-based system



4. Right-click the share that you want to access and select the **Map network drive** option.

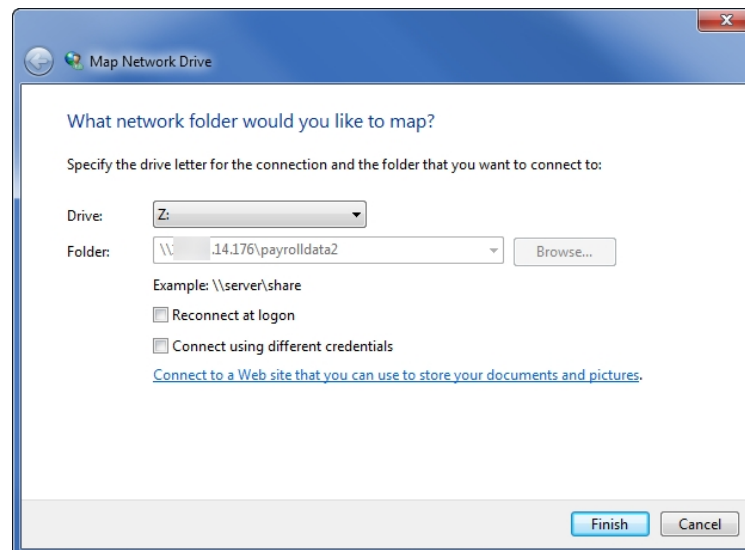
- You may be prompted for a user name and password to access the share. Enter a valid user name and password and click **OK**.

Figure 6-28: Specify a user name and password to map the CIFS share



- Windows prompts you to select the drive letter to map to. From the **Drive** drop-down list, select the drive letter that you want to map the share to.

Figure 6-29: Map network drive



- Click **Finish**.

Accessing an NFS file system from UNIX/Linux

To access an NFS file system on Unity from UNIX/Linux, you must first create a mount point for the file system on the UNIX/Linux-based system (from where you want to access the file system), and then mount the file system that you want to access to the mount point, over the NFS protocol. A mount point is a folder on the UNIX/Linux-based system in which an external file system is mounted; the file system's contents are dropped into that folder.

► **To access an NFS file system from UNIX/Linux:**

1. On the UNIX/Linux system where you want to access the NFS file system, logon as root:

```
# su root
```

2. Create the folder (or mount point) where you want to mount the NFS file system; for example, type:

```
# mkdir /mnt/payrolldata/
```

3. Mount the NFS file system to the /mnt/payrolldata/ mount point; for example, type:

```
# mount 177.22.16.111:/pools/FinancePool/PayRollData2 /mnt/payrolldata/
```

Substitute `177.22.16.111` with the virtual IP address of the Pool Resource Group on Unity where the file system is located; substitute `FinancePool` with the name of the storage pool where the NFS file system that you want to mount exists; and substitute `PayRollData2` with the actual NFS file system name; for more information, see [Viewing mount point information for file systems](#) on page 186.

The `mount` command drops the contents of the `PayRollData2` file system into the `/mnt/payrolldata` mount point.

Note When mounting an NFS file system, Storage Pool names and NFS file system names are case-sensitive. You must type the storage pool and file system names as they appear in Nexsan Unity, using the same lower- and upper-case letters, where appropriate.

4. To view the contents of the NFS file system that you mounted in the `/mnt/payrolldata` mount point in **Step 3**, you must logon as a user that is granted access permissions to the file system (or a user that is a member of a group that is granted access). For example, the user `bob` has Full access to the `PayRollData2` file system; to logon as `bob`, type:

```
# su bob
```

5. You can now access the contents of the `PayRollData2` file system in the `/mnt/payrolldata` mount point by simply accessing the mount point folder; for example, type:

```
#cd /mnt/payrolldata
```

6. Use the `ls` command to view the contents of the `/mnt/payrolldata` mount point; for example, type:

```
# ls -a
```

Using an NFS version 3 (NFSv3) client to access an NFS share with Microsoft Active Directory

Unity's `nxadmin` command line interface (CLI) includes the `useradd`, `groupadd`, and `idmap` combination of commands that allow you to enable Microsoft Active Directory users and/or groups to connect to and authenticate with an NFS share on Unity through an NFS version 3 (NFSv3) UNIX/Linux client machine.

To achieve this, you use the **useradd** and **groupadd** commands to add corresponding user and group accounts, respectively, to Unity, with the same UNIX UID (for user accounts) and UNIX GID (for group accounts) assigned to the users and groups in the Microsoft Active Directory domain—see the **useradd** and **groupadd** commands in the *Nexsan Unity nxadmin CLI Reference Manual*.

Then, you map the user or group accounts that you add to Unity to their corresponding user or group account names in the Microsoft Active Directory domain—see the **nstusermaps** command in the *Nexsan Unity nxadmin CLI Reference Manual*.

Note NFSv3 uses UID/GID based permissions mapping. This means users must have the same UID/GID on both the client and Unity.

► **Requirements:**

- Make sure the Active Directory user/group accounts have UNIX UIDs/GIDs configured for them on the Microsoft Active Directory server.
- On Unity, add corresponding user or group accounts with the same UID (for user accounts) or GID (for group accounts) associated with the user or group in the Microsoft Active Directory domain.
- Map the user or group accounts that you add to Unity to their corresponding user or group account names in the Microsoft Active Directory domain.

Using an NFS version 4 (NFSv4) client to access an NFS share

To access or mount an NFS share from an NFS version 4 (NFSv4) client, you must perform some additional configuration steps, both on Unity where the NFS share exists and on the NFSv4 client computers where you intend to mount the NFS share.

Note NFSv4 uses name-based permissions mapping. This means users must have the same name on both the client and Unity. It also requires an NFSv4 Domain to be set. This must be identical on both Unity and the client.

► **On Unity where the NFS share exists, you must:**

1. specify a domain name to enable user/group mapping between Unity and your NFSv4 clients;
2. define NFS settings, such as the maximum number of client connections;
3. use the nxadmin command line interface (CLI) to add user and/or group accounts, respectively, on Unity with account names that correspond to user and/or group accounts on the NFSv4 client computers where you intend to mount the NFS share.

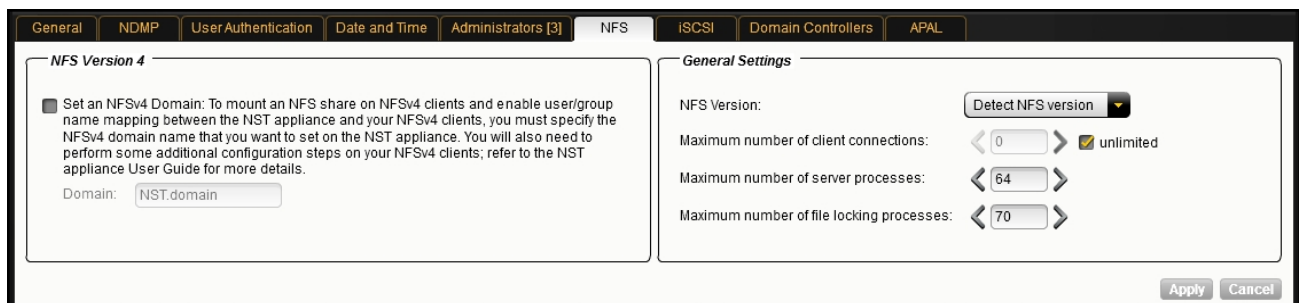
► **On the NFSv4 client computers where you intend to mount the NFS share, you must:**

1. add the NFSv4 domain name you specified on Unity to the `/etc/idmapd.conf` file;
2. stop and then restart the idmap (Identity Mapping) service;
3. make sure this service starts on system boot up: `chkconfig rpcidmapd on`;
4. mount the NFS share.

► **To configure NFSv4 support:**

1. In Nexsan Unity's tree view, click the Site node corresponding to Unity where the NFS share exists; this displays its child nodes.
2. Expand the Site node's Properties panel.
3. Select the **NFS** tab.

Figure 6-30: Site node's properties panel—NFS tab



4. Specify a domain name to enable user mapping between Unity and your NFSv4 clients:
 - a. Select the check box to enable the domain.
 - b. In the **Domain** text box, type a domain name for NFSv4 support. You will be required to specify this domain name on all NFSv4 client systems where you intend to mount the NFS share. You can use the default domain name, **NST.domain**, or specify a new name; the domain name must contain a period (.).
5. On the **General Settings** panel, define these settings:
 - a. In the **NFS Version** drop-down list, select the global NFS version control:
 - **Detect NFS version:** By default, Unity supports both NFSv3 and NFSv4. Choose this option if your environment is composed of mixed client versions. Unity will detect the version and use the same as the client automatically.
 - **NFSv3 only:** Choose this option for Unity to only use NFSv3.
 - b. Enter the maximum number of **client connections** in the corresponding field. Enter a value between **2** and **32** or select the **unlimited** option.
 - c. Enter the maximum number of **server processes** in the corresponding field. This setting allows you to tune NFS for better performance. When a request is made for an NFS service, the Services for UNIX NFS server generates a thread to handle the request. Each thread can process one NFS request. A large pool of threads can allow a server to handle more NFS requests in parallel.

To determine the number of threads to make available, use the following formula:

$$16 + (4 \textit{ processors})$$

where *processors* is the number of additional processors on the NFS server. Enter a value between 1 and 256.
 - d. Enter the maximum number of **file locking processes** in the corresponding field. This setting defines the number of threads that can be used for NFS file locking. Enter a value between 0 and 256.
6. Click **Apply** to save your settings.

7. Use the `nxadmin` command line interface (CLI) to add user and/or group accounts to Unity with account names that correspond to user and/or group accounts on the NFSv4 client computers where you intend to mount the NFS share:
 - a. Access the `nxadmin` CLI on Unity.
 - b. Log on as `nxadmin`.
 - c. In the NestOS Admin Menu, type **4 (Run a Command)**.
 - d. Press the **Enter** key.
 - e. At the `command:` prompt, type the `useradd` command using this syntax to add a user:
`useradd -u <uid> <user name>`
You cannot use these UID numbers because they are reserved:
 - 0 to 101
 - 60001
 - 60002
 - 65534
 - 90000 to 90050If one of these IDs is already assigned to a user on your network, please contact Nexsan Technical Support to request that they free up the reserved ID.
 - f. Press the **Enter** key.
 - g. At the `command:` prompt, type the `groupadd` command using this syntax to add a group:
`groupadd -u <gid> <group name>`
You cannot use these GID numbers because they are reserved:
 - 0 to 101
 - 60001
 - 60002
 - 65534
 - 90000 to 90050
 - 99999If one of these IDs is already assigned to a user on your network, please contact Nexsan Technical Support to request that they free up the reserved ID.
 - h. Press the **Enter** key.

8. Assign the local user and/or group accounts (that you created in the previous step) access permissions to the NFS share. You perform this step in the nxamin Command Line Interface (CLI) using the `shareacl` command:
 - a. Type the `shareacl` command to display its command reference and options. As an example, to assign the user `bobsummers` Full access permissions to the NFS share `PayRollData1` in storage pool `FinancePool1`, type:


```
shareacl -c append -p FinancePool1 -s PayRollData1 -u bobsummers -a full_set -d allow
```

 - To assign Read-only access permissions, replace `-a full_set` with `-a read_set`; or, to assign Read/Write access permissions, replace `-a full_set` with `-a write_set`.
 - To deny access, replace `-d allow` with `-d deny`.
9. Open the `/etc/idmapd.conf` file and change the value for the Domain parameter to correspond to the NFSv4 domain name you specified in Step 1; for example:


```
Domain = NST.domain
```
10. Stop and start the `idmap` (Identity Mapping) service; for example:


```
service rpcidmapd stop
service rpcidmapd start
```
11. Make sure this service starts on boot up:

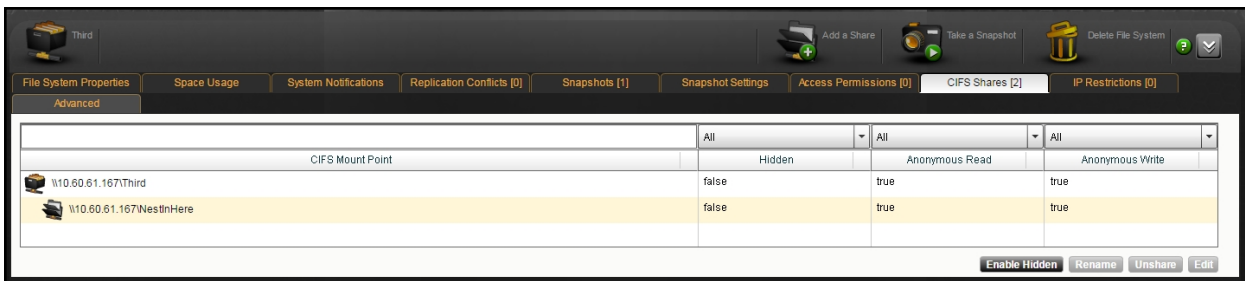

```
chkconfig rpcidmapd on
```
12. Mount the NFS share. See [Accessing an NFS file system from UNIX/Linux](#) on page 177.

Moving a share

This section describes how to move a share.

- ▶ **To move a share:**
 1. In the Unity tree, click the Site node to display its child nodes.
 2. Click the corresponding **Storage Pools** node.
 3. Select the node corresponding to the storage pool where the share exists.
 4. Click the **File Systems** node.
 5. Click the file system where the share that you want to modify resides.
 6. Expand the share's Properties panel.
 7. Select the **File Systems** tab.

Figure 6-31: File System's properties panel—File Systems tab



8. Select the share that you want to move by highlighting it in the grid and click **Move**.
You can search for a specific share in the grid, or filter the list, by entering a share name in the text box located above the **Path** column.
9. Manually enter a new location for the share in the path bar, or use the **Share Explorer** to navigate to the new location. Click the plus sign (+) to create additional locations within the file path.
10. Click **Move**.

Disabling data sharing for a share

If needed, you can disable data sharing for a share, which makes the share inaccessible over the network.

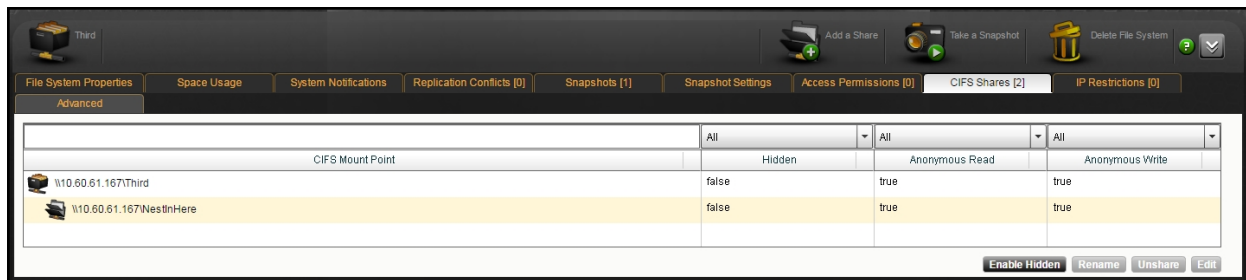


CAUTION: When you disable data sharing for a share, client systems or applications that access the share will lose their connection to the share; this could result in data loss. Before disabling data sharing, make sure that client systems with an active connection to the share disconnect any mapped drive(s) to the share; also make sure to quiesce any applications with an active connection to the share.

► To disable data sharing for a share:

1. In the Unity tree, click the **Site** node to display its child nodes.
2. Click the **Storage Pools** node.
3. Select the node corresponding to the storage pool where the share exists.
4. Click the **File Systems** node.
5. Click the file system where the share that you want to disable data sharing for resides.
6. Expand the share's Properties panel.
7. Select the **Shares** tab.

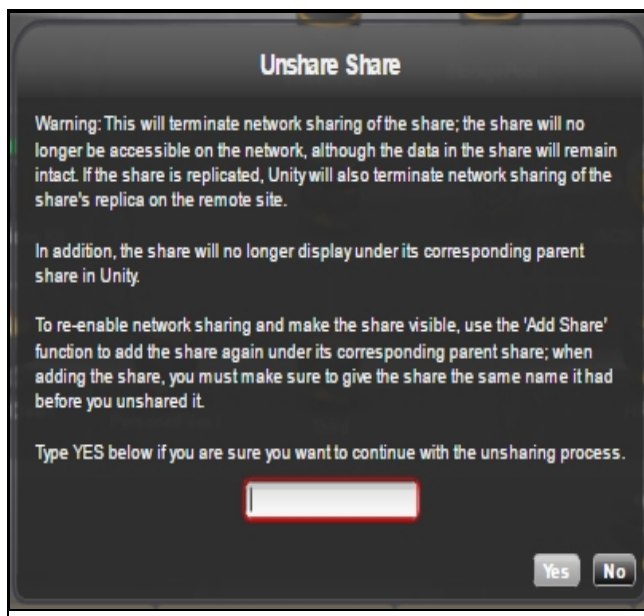
Figure 6-32: File System's properties panel—Shares tab



8. Select the share that you want to disable data sharing for by highlighting it in the grid.
9. You can search for a specific share in the grid, or filter the list, by entering a share name in the text box located above the **CIFS Mount Point** column.
10. Once you have highlighted the share that you want to disable data sharing for, click the **Unshare** button at the bottom of the Share Properties panel.

11. Unity prompts you to confirm the action. Type **Yes** in the text box provided to disable data sharing for the share.

Figure 6-33: share: confirm disable data sharing



12. Click the **Yes** button.

Renaming a share

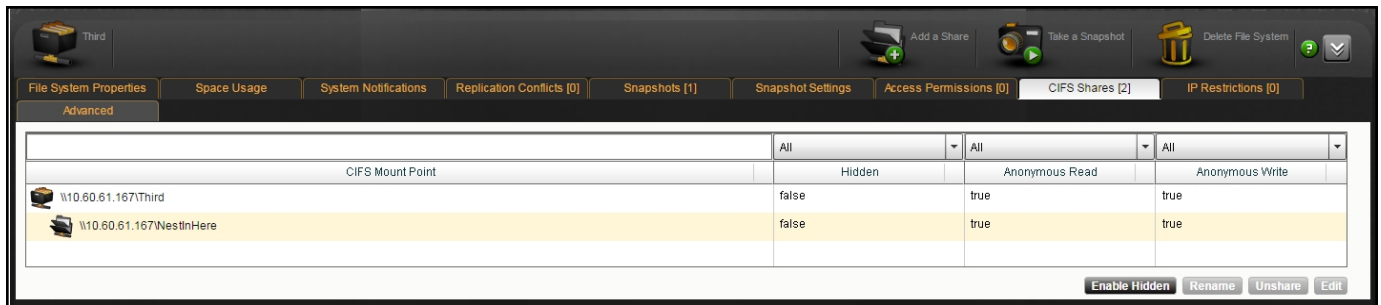
If you rename a share, client systems on the network that have a network drive mapped to the share will lose their connection to the share; this could result in data loss. Before renaming a share, make sure that client systems with an active connection to the share disconnect any mapped drive(s) to the share; also make sure to quiesce any applications with an active connection to the share.

► **To rename a share:**

1. In the Unity tree, click the **Site** node to display its child nodes.
2. Click the **Storage Pools** node.
3. Select the node corresponding to the storage pool where the share exists.
4. Click the **File Systems** node.
5. Click the share where the share that you want to modify resides.
6. Expand the share's Properties panel.

7. Select the **Shares** tab.

Figure 6-34: File System's properties panel—Shares tab

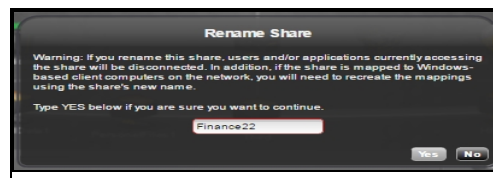


8. Select the share that you want to rename by highlighting it in the grid.
You can search for a specific share in the grid, or filter the list, by entering a share name in the text box located above the **Share name** column.
9. Once you highlight the share that you want to rename, click the **Rename** button.
10. Unity prompts you to specify a new name for the share. Type a new name for the share.
The name must start with an (upper-case or lower-case) alphabetic or numeric character; and, with the exception of the hyphen (-), and period (.), the name can only contain alphanumeric characters, without spaces.

These characters are NOT allowed:

" / \ [] : ; | = , + * ? < >

Figure 6-35: Share: specify new name



11. Click **OK**.
12. Click **OK** at the warning message.

Unity changes the share's name. If the share is replicated, Unity also renames the share's replica on the remote Unity.

Viewing mount point information for file systems

Once you add a file system to Unity, Nexsan Unity displays the mount point(s) for the file system in the file system's Properties panel, under the **CIFS File Systems** and **NFS File Systems** tabs. The mount point identifies the (network) path to use to access a file system from a Windows-based (CIFS) system, or mount a file system on a UNIX/Linux-based (NFS) system, or the FTP URL link—depending on the sharing method you selected when creating the file system.

The mount point displays the virtual IP address of the Pool Resource Group to which the storage pool, where you added the file system, is assigned. You **MUST** use the Pool Resource Group's virtual IP address to access the file system.

For example:

- If you add a CIFS file system, `PayRollData2`, to a storage pool on Pool Resource Group 1, with the virtual IP address `xxx.xx.12.25`, the mount point for the file system is represented as:
`\\xxx.xx.12.25\PayRollData2`
- If you add an NFS file system, `PayRollNFS1`, to the `FinancePool1` on Pool Resource Group 1, with the virtual IP address `xxx.xx.12.25`, the mount point for the file system is represented as:
`xxx.xx.12.25:/pools/FinancePool/PayRollNFS1`
- If you expose a file system over FTP, `FinanceFileSystem`, with the virtual IP address `xxx.xx.156.183`, the FTP URL is represented as:
`ftp://xxx.xx.156.183/FinanceFileSystem`

Note FTP sharing is only supported for Unity authentication.

Note The syntax for NFS mount points is case sensitive: when mounting an NFS file system, make sure to specify the exact letter case of the storage pool's name and the NFS file system's name in the mount command syntax.

▶ To view a file system's mount points:

1. In Unity's tree view, click the Site node.
2. Click the **Storage Pools** node.
3. Click the storage pool containing the file system for which you want to view mount point information.
4. Click the **file system** node.
5. Click the file system for which you want to view mount point information.
6. Expand the shares Properties panel.
7. Select the **CIFS FileSystems** tab or the **NFS FileSystems** tab.

Managing access permissions to shares

When you add a share, Unity lets you to set access permissions to the share for individual users and/or groups in the Microsoft Active Directory domain or LDAP Directory service that Unity is connected to; or, if the system is configured to use Unity authentication, for individual users and groups that you define on the system.

Access permissions protect your data from unauthorized access by letting you define the type of access granted to a user or group for a share that you create in Unity, and subsequently expose to Windows (CIFS) or UNIX/Linux-based (NFS) system of Unity. For example, if you grant the Finance group Read/Write

permissions to a CIFS share named PayrollData, only members of the Finance group can perform Read and Write operations on the contents of the PayrollData share from their Windows systems.

File system permissions are set on the file systems themselves.

This section includes these topics:

Understanding access permissions in Nexsan Unity.....	187
Giving share-level access permissions to a user or group.....	189
Modifying share-level access permissions.....	192
Revoking file system-level access permissions.....	193

Understanding access permissions in Nexsan Unity

When you set permissions, you specify the level of access that a user or a group has to a specific share that you create in Unity. For example, you can let one user or group view the contents of a share (Read access), let another user or group make changes to files in the share (Read/Write or Full access), and prevent all other users and/or groups from accessing the share. You can also allow all users and groups in your Microsoft Windows Active Directory domain or LDAP Directory service to *anonymously* browse the contents of a share (Read-only anonymous access; or, let all users and groups *anonymously* perform Read/Write operations on the contents of a share (Read/Write anonymous access); for more information about anonymous access, see [Read-only and Read/Write anonymous access](#) below.

Unity applies share-level permissions cumulatively. For example, if you give Jack Read-only access to the PayRollData share, and then you give the Finance group—of which Jack is a member—Write access to the PayRollData share, Jack will automatically have Read/Write access to the PayRollData share.

Additionally, user access permissions are applied on all files and folders in the share. For example, if you give the user *bob* Full access to a share in Unity, *bob* is automatically granted Full access to all files and folders in the share; similarly, if you revoke *bob's* access to a share, *bob's* access to all files and folders in the share is revoked as well.

Unity supports these permission settings on shares:

- Read
- Write
- Full

Read-only and Read/Write anonymous access

Unity supports both Read-only and Read/Write anonymous access to shares. For example, if you have a share that contains generic policies and forms, like blank expense reports, you may want all users on your network to access the share—in which case, you can set the share's sharing method to Read-only anonymous access or Read/Write anonymous access.

Notes: By default Read/Write access is granted to everyone. To assign Read/Write access to ONLY a specific user or group you must disable this setting.

Read-only anonymous access gives all users on the network Read access to the data contained in a share, including the ability to display and traverse folders and read the contents of files.

Read/Write anonymous access gives all users on the network Write access to the data contained in a share, including the ability to delete and create folders and files and change the contents of files.

From the perspective of a Window-based (CIFS) system, the *Everyone* account on the system has either Read-only or Read/Write access to the share, depending on the anonymous setting you specify for the share in Unity. And on a UNIX/Linux-based (NFS) system, the *guest* account has either Read-only or Read/Write access to the share.

Windows and UNIX Access Control Lists (ACLs)

Unity supports both UNIX/Linux and Windows NTFS-style ACL (Access Control List) access privileges on shares; for example:

- If you enable NFS sharing for a share: Unity supports traditional UNIX-style ACL attributes (such as, rwx) for owner, group owner, and other.
- If you enable CIFS sharing for a share: Unity supports the semantics of Windows NTFS ACLs, including configuration, enforcement, and inheritance models.



CAUTION: If you run the `chmod` command on an NFS share, all Windows ACLs are cleared.

This table shows how Unity maps permissions that you set for shares to ACL access privileges in Windows (CIFS sharing) and UNIX/Linux (NFS sharing) environments.

Table 6-6: Permission mappings

Permissions in Nexsan Unity	Windows ACLs (CIFS sharing)	NFS version 4 ACLs (NFS sharing)	NFS version 3 ACLs (NFS sharing)
Read	Read and execute List folder contents Read	Read Data (r) Execute (x) Read Attributes (a) Read Extended Attributes (R)	Read Data (r) Execute (x)
Read/Write	Modify Read and execute List folder contents Read Write	Read Data (r) Write Data (w) Execute (x) Delete (d) Delete Child (D) Read Attributes (a) Write Attributes (A) Read Extended Attributes (R) Write Extended (W) Read ACL (c)	Read Data (r) Write Data (w) Execute (x)
Full	Full Control Modify Read and execute List folder contents	Read Data (r) Write Data (w) Execute (x) Delete (d)	Read Data (r) Write Data (w) Execute (x)

Permissions in Nexsan Unity	Windows ACLs (CIFS sharing)	NFS version 4 ACLs (NFS sharing)	NFS version 3 ACLs (NFS sharing)
	Read Write	Delete Child (D) Read Attributes (a) Write Attributes (A) Read Extended Attributes (R) Write Extended (W) Read ACL (c) Write ACL (C) Change Owner (o)	

Giving share-level access permissions to a user or group

This section describes how to give a user and/or group access permissions to a share.

Note You must have, at least, one storage pool and one share defined on the system to perform this operation.

► **To give share-level access permissions to a user or group from the toolbar:**



CAUTION: If you give a user access permissions to a share, the new permission settings are applied on all files and folders in the share. For example, if you give the user *bob* Read, Read/Write, or Full access to a share, *bob* is automatically granted Read, Read/Write, or Full access to all files and folders in the share.

1. Open the Manage Users and Groups panel, as described in [Opening the Manage Users and Groups panel](#) on page 74.
2. For multi-site environments: open the **Sites** drop-down list and select the site where the user or group that you want to give share-level access permissions to exists.
3. From the **Domain** drop-down list, in the Users and Group window at the top of the Manage Users and Groups panel, select the domain server(s) where the user or group that you want to give share-level access permissions to exists.

Note The panel displays the **Domain** drop-down list if Unity is integrated with a Microsoft Windows Active Directory domain or an LDAP Directory service. In a multiple domain environment, the **Domain** drop-down list contains all the domains on the network.

4. In the **Name** text box, type the name of the user or group that you want to give share-level access permissions to exists, and then, click the Find button to display the specified user or group.

If needed, you can use the **Find Now** function to display specific users and/or groups. For example, to display the user *Bob*:

- a. Select the **Starts with** option from the pick list next to the Name text box.
- b. Type **BO** (or **bo**) in the **Name** text box.
- c. Click the **Find Now** button. Unity displays all users and/or groups with user and/or group names that start with the letters **b** and **o** in the **Search results** grid (on the bottom-left of the panel).

You can also use the **Advanced Search** function and set more specific search criteria; for more information, see [Users and Groups window](#) on page 75.

5. On the bottom half of the Manage Users and Groups panel, select the **File System Permissions** tab.
6. In the grid, select the share that you want to give the user or group access permissions to.
7. When the share is highlighted in the grid, select the relevant check box in the **Read**, **Read/Write**, or **Full** column that corresponds to the level of access that you want to give the user or group to the share.
 - If you select the **Read** check box, the user or group is granted only Read-level access permissions to the share.
 - If you select **Read/Write**, the user or group is granted Read and Write access permissions to the share, and the **Read** check box is automatically selected as well.
 - If you select the **Full** check box, the user or group is granted Full access permissions to the share, and both the **Read** and **Read/Write** check boxes are also automatically selected.
8. Click **Apply** to save your settings.

Repeat these steps to give the user or group access permissions to more shares on the system.

▶ **To give share-level access permissions to a user or group from Nexsan Unity's tree:**

Tip This method allows you to give multiple users or groups access permissions to a share in a single operation.



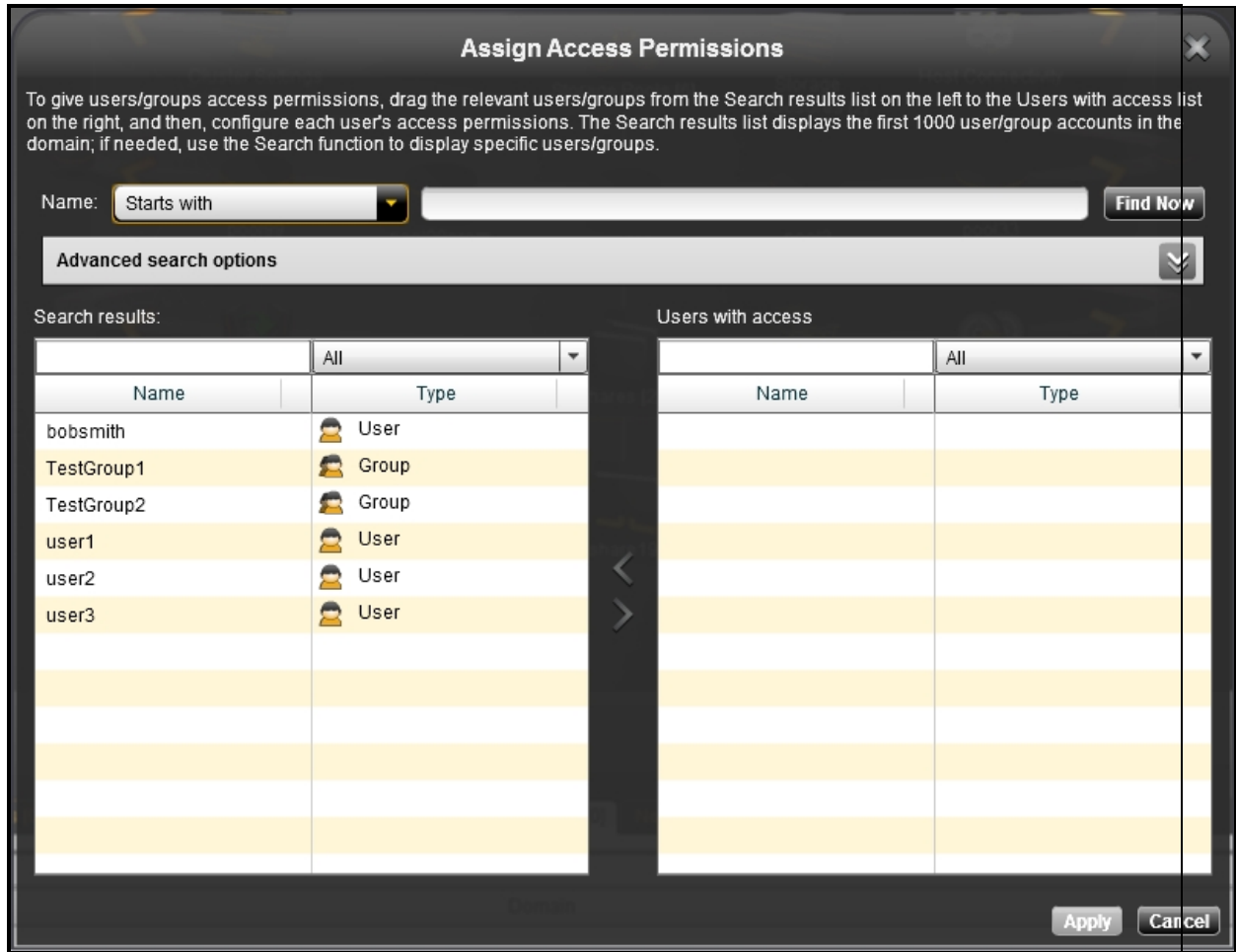
CAUTION: When giving share-level access permissions to a user(s) or group(s) from the tree view, the user(s) or group(s) are granted Read-only access permissions to the share. To give the user(s) or group(s) Read/Write or Full access permissions to the share, you must change the user's or group's access permissions; see [Modifying share-level access permissions](#) on page 192.

1. In the tree, click the Site node to display its child nodes.
2. Click the **Storage Pools** node.
3. Select the node belonging to the storage pool where the share exists.
4. Click the **file system** node.
5. Select the file system that you want to give the user or group access permissions to.
6. Expand the file system's Properties panel.
7. Click the **CIFS File Systems** tab.
8. Click the **Edit File System Permissions** button.

9. From the **Domain** drop-down list, select the domain server(s) where the user or group that you want to give share-level access permissions to exists.

Note The panel displays the **Domain** drop-down list if Unity is integrated with a Microsoft Windows Active Directory domain or an LDAP Directory service. In a multiple domain environment, the **Domain** drop-down list contains all the domains on the network.

Figure 6-36: Assign Access Permissions panel



10. In the **Name** text box, type the name of the user or group that you want to give share-level access permissions to exists, and then, click the **Find** button to display the specified user or group. If needed, you can use the **Find Now** function to display specific users and/or groups. For example, to display the user *Bob*:
- Select the **Starts with** option from the pick list next to the Name text box.
 - Type **BO** (or **bo**) in the **Name** text box.
 - Click the **Find Now** button. Unity displays all users and/or groups with user and/or group names that start with the letters **b** and **o** in the **Search results** grid (on the bottom-left of the panel).

You can also use the **Advanced Search** function and set more specific search criteria; for more information, see [Users and Groups window](#) on page 75.

11. In the **Search results** list, select the user or group that you want to give share-level access permissions to.

Hold down SHIFT or CTRL and click the left mouse button to select multiple entries in the list.

You can also search for specific users or groups, or filter the list, by entering a user or group name in the **Filter/Search** box located above the **Search results** list.

12. Drag the selected user(s) or group(s) to the **Users with access** list, or click the *right* arrow to move the selection.

Note The **Users with access** list displays the users and groups that already have access permissions to the share.

13. Click **Apply** to save your settings and close the **Assign Access Permissions** panel.

Modifying share-level access permissions

This section describes how to modify a user's or group's share-level access permissions.



CAUTION: If you modify a user's access permissions to a share, the new permission settings are applied on all files and folders in the share. For example, if the user *bob* initially has Read access to a share, and then you give *bob* Full access permissions to the share, *bob* is automatically granted Full access to all files and folders in the share.

Note You must have, at least, one storage pool and one share defined on the system to perform this operation.

▶ **To modify a user's or group's share-level access permissions from the toolbar:**

1. Open the Manage Users and Groups panel, as described in [Managing users and access rights in the Manage Users and Groups panel](#) on page 74.
2. For multi-site environments: open the **Sites** drop-down list and select the site where the user or group that you want to modify share-level access permissions for exists.
3. From the **Domain** drop-down list, in the Users and Group window at the top of the Manage Users and Groups panel, select the domain server(s) where the user or group whose share-level access permissions you want to modify exists.

Note The panel displays the **Domain** drop-down list if Unity is integrated with a Microsoft Windows Active Directory domain or an LDAP Directory service. In a multiple domain environment, the **Domain** drop-down list contains all the domains on the network.

4. In the **Name** text box, type the name of the user or group that you want to give share-level access permissions to exists, and then, click the **Find** button to display the specified user or group.

If needed, you can use the **Find Now** function to display specific users and/or groups. For example, to display the user *Bob*:

- a. Select the **Starts with** option from the pick list next to the Name text box.
- b. Type **BO** (or **bo**) in the **Name** text box.
- c. Click the **Find Now** button. Unity displays all users and/or groups with user and/or group names that start with the letters **b** and **o** in the **Search results** grid (on the bottom-left of the panel).

You can also use the **Advanced Search** function and set more specific search criteria; for more information, see [Users and Groups window](#) on page 75.

5. On the bottom half of the Manage Users and Groups panel, select the **File System Permissions** tab.

6. In the grid, select the share that you want to modify or revoke access permissions to (for the selected user or group).
7. When the share is highlighted in the grid, select the corresponding check box in the **Read**, **Write**, or **Full** column to modify the user's or group's access permissions to the share.
For example, if the user or group only has Read access to the share, and you want to give the user Full access permissions, select the **Full** check box; the **Read** and **Write** check boxes are automatically selected as well.
8. Click **Apply** to save your settings.

Repeat these steps to modify the user's or group's access permissions to other shares on the system.

Revoking file system-level access permissions

This section describes how to revoke a user's or group's file system-level access permissions.



CAUTION: If you revoke a user's access permissions to a file system, the new permission settings are applied on all files and folders in the file system. For example, if you revoke the user *bob*'s access permissions to a file system, *bob* is automatically denied access to all files and folders in the file system.

Note You must have, at least, one storage pool and one file system defined on the system to perform this operation.

► **To revoke a user's or group's file system-level access permissions from the toolbar:**

1. Open the Manage Users and Groups panel, as described in [Managing users and access rights in the Manage Users and Groups panel on page 74](#).
2. For multi-site environments: open the **Sites** drop-down list and select the site where the user or group that you want to revoke file system-level access permissions from exists.
3. From the **Domain** drop-down list, in the Users and Group window at the top of the Manage Users and Groups panel, select the domain server(s) where the user or group that you want to revoke file system-level access permissions from exists.

Note The panel displays the **Domain** drop-down list if Unity is integrated with a Microsoft Windows Active Directory domain or an LDAP Directory service. In a multiple domain environment, the **Domain** drop-down list contains all the domains on the network.

4. In the **Name** text box, type the name of the user or group that you want to revoke file system-level access permissions to, and then click the **Find** button to display the specified user or group.

If needed, you can use the **Find Now** function to display specific users and/or groups. For example, to display the user *Bob*:

- a. Select the **Starts with** option from the pick list next to the Name text box.
- b. Type **BO** (or **bo**) in the **Name** text box.
- c. Click the **Find Now** button. Unity displays all users and/or groups with user and/or group names that start with the letters **b** and **o** in the **Search results** grid (on the bottom-left of the panel).

You can also use the **Advanced Search** function and set more specific search criteria; for more information, see [Users and Groups window on page 75](#).

5. On the bottom half of the Manage Users and Groups panel, select the **CIFS Permissions** tab.
6. In the grid, select the relevant file system.

7. When the file system is highlighted in the grid, clear the **Read** check box to revoke the selected user's or group's access permissions to the share. If the **Write** and/or **Full** check boxes are selected, Unity automatically clears them as well.
8. Click **Apply** to save your settings.

Managing snapshots for file systems

Unity provides continuous data protection with the Snapshots feature, which allows you to capture, store, and access point-in-time copies of the data in Unity file systems.

Using the File Systems properties panel

The File Systems Properties panel lists all the snapshots for the corresponding File System; it also provides options and settings for configuring the snapshots schedule, taking manual snapshots, enabling and disabling snapshot browsing, and deleting snapshots.

▶ **To access a share's Snapshots:**

1. In Unity's tree view, click the Site node to display its child nodes.
2. Click the **Storage Pools** node.
3. Click the Storage Pool containing the File System for which you want to manage Snapshots.
4. Click its **File System** node.
5. Click the File System for which you want to manage Snapshots.

The File System Properties panel includes two tabs for snapshots:

- [Snapshots tab](#) below
- [Snapshot Settings tab](#) on page 197

Snapshots tab

The **Snapshots** tab displays a grid that lists all the snapshots recorded for the corresponding file system.

Figure 6-37: File System's properties panel—Snapshots tab

Browsing status	Name	Date	Time	Size	Type
	auto_2014-06-11-103304	2014/06/11	10:33:00 AM	0 B	Automatic
	auto_2014-06-12-010002	2014/06/12	1:00:00 AM	0 B	Automatic
	auto_2014-06-13-010003	2014/06/13	1:00:00 AM	0 B	Automatic

The grid shows this information for each snapshot:

- **Browsing status:** this column indicates whether or not browsing is enabled for the snapshot; it displays one of these icons:



Browsing is enabled



Browsing is disabled

- **Name:** this column displays the snapshot's name; the name displayed in this column varies depending on whether the snapshot is a scheduled (automatic) snapshot or a manual snapshot:
 - For a scheduled (automatic) snapshot, the snapshot name is prefixed with `auto_` and includes the date and time the snapshot is recorded; for example: Unity assigns this name for a scheduled snapshot recorded on June 15, 2011 at 1:01 AM: `auto_2011-06-15-010100`.
 - For a manual snapshot, the name can be a value that you define when taking the snapshot, or if you use the default snapshots naming convention, the name is prefixed with `manual_` and includes the date and time the manual snapshot is recorded; for example: if you take a manual snapshot on June 15, 2011 at 1:01 PM and you use the default snapshots naming convention, Unity assigns this name to the snapshot: `manual_2011-06-15-130101`.
- **Date:** this column displays the date the snapshot is recorded.
- **Time:** this column displays the time the snapshot is recorded.

Note Unity converts the date and time to local format; that is, the date and time on the system where Unity is currently running.
- **Size:** this column displays the size of the snapshot. When a snapshot is recorded it initially consumes no disk space; however, as data within the snapshot's parent share changes—for example, new data is added or existing data is updated—Unity updates the snapshot size accordingly.
- **Type:** this column indicates whether the snapshot is an **Automatic** (scheduled) or **Manual** snapshot.

Sorting the list of snapshots

You can sort the list of snapshots displayed in the grid in either ascending or descending (alphabetical) order by clicking the sort pointer in the **Name** column heading.



▶ To sort the list in descending order:

- Click the sort pointer until the arrow points down.

▶ To sort the list in ascending order:

- Click the sort pointer until the arrow points up.


You can also sort by **Browsing status**, **Date**, **Time**, **Size**, and **Type**; or a combination of **Name**, **Browsing status**, **Date**, **Time**, **Size**, and **Type**, in any particular sort order that you want: 1, 2, and 3.

For example, to sort by **Date** first, and **Name** second:

1. Click the sort pointer in the **Date** column heading until **1** is displayed (with the arrow pointing either up for ascending order, or down for descending order).
2. Click the sort pointer in the **Name** column heading until **2** is displayed (with the arrow pointing either up for ascending order, or down for descending order).

Filtering snapshots in the grid

You can filter the snapshots displayed in the grid by **Browsing status**, **Name**, **Date**, **Time**, **Size**, and **Type**, and you can also filter the snapshots to only display snapshots recorded within a specific time period.

To...	Do this
only display snapshots recorded within a specific time period	<ol style="list-style-type: none"> Click the From date field above the snapshots grid, and select a starting date for the time period that you want to display snapshots from.  Click the To date field, and select an end date for the time period.
only display snapshots with a specific Browsing status	<ol style="list-style-type: none"> Open the drop-down list above the Browsing status column heading in the grid. Select the browsing status (Browsing enabled or Browsing disabled) that you want to display snapshots for in the grid. The default filter setting is All.
only display snapshots of a specific type	<ol style="list-style-type: none"> Open the drop-down list above the Type column heading in the grid. Select the type (Manual or Automatic) that you want to display snapshots for in the grid. The default filter setting is All.
filter snapshots further	<p>Combine filter settings. For example, if you only want to display snapshots that have Browsing enabled, of type Automatic, and which were recorded between May 15, 2015 and May 18, 2015, set these filter settings in the grid:</p> <ol style="list-style-type: none"> Click the From date field above the snapshots grid, and select May 15 in the calendar. Click the To date field, and select May 18 in the calendar. Unity filters the grid to only display snapshots recorded within the specified time period. Open the drop-down list above the Browsing status column heading in the grid and select Browsing enabled. Unity filters the grid to only display snapshots that you enabled browsing for. Open the drop-down list above the Type column heading in the grid and select Automatic. Unity filters the grid again to only display scheduled (automatic) snapshots.

Note To reset filter settings in the grid, click another node in Unity’s tree view and then return to the Snapshots Properties panel by clicking the corresponding Snapshots node. All filter options in the grid revert to their default settings.

Searching for a specific snapshot in the grid

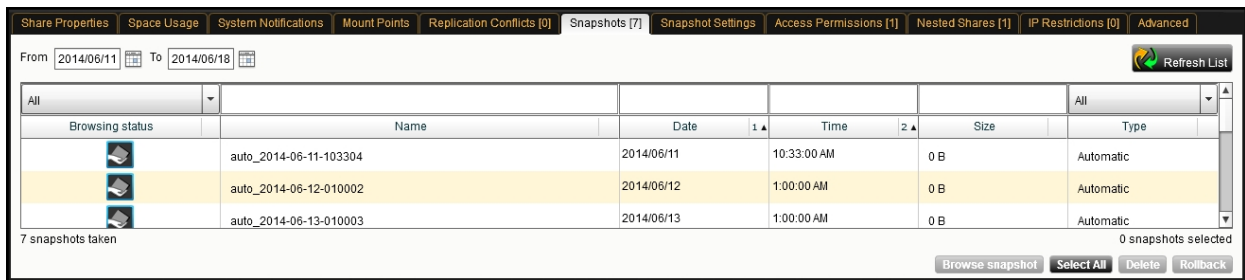
You can search for a specific snapshot in the grid by **Name**, **Date**, **Time**, or **Size**, simply by entering a search string in the text boxes above the corresponding column headings.

► **To search for a specific snapshot in the grid:**

- Enter a search string in the text boxes above the **Name**, **Date**, **Time**, or **Size** column headings.

For example, if you want to search for all snapshots that are 0 B in size, simply enter 0 in the text box above the **Size** column heading.

Figure 6-38: File System's properties panel—Snapshots tab



Unity displays all snapshots matching your search criteria.

Snapshot Settings tab

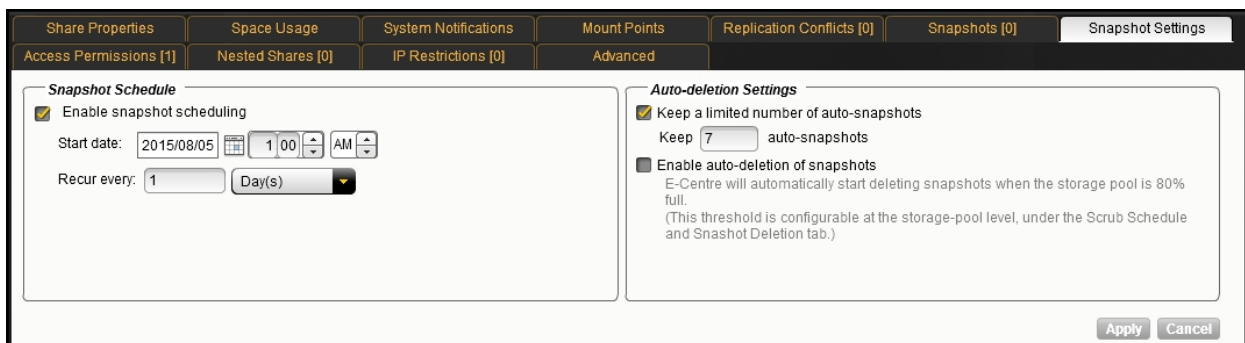
The Snapshot **Settings** tab provides options for configuring a snapshots schedule and for specifying auto-deletion settings for snapshots.

When you set a snapshots schedule, Unity automatically takes periodic snapshots of the file system according to the schedule you define; for more information, see [Setting a schedule for automatic file system snapshots](#) below.

Note There can only be one snapshot schedule per file system.

Auto-deletion settings allow you to specify the maximum number of snapshots that you want Unity to keep on the system for the corresponding file system. These settings only apply to scheduled (automatic) snapshots. For more information, see [Configuring auto-deletion settings for file system snapshots](#) on page 204.

Figure 6-39: File System's properties panel—Snapshot Settings tab



Setting a schedule for automatic file system snapshots

This section describes how to take automatic snapshots. For instructions to take manual snapshots, see [Taking a manual LUN snapshot](#) on page 253.

When you set a snapshots schedule, Unity automatically takes periodic snapshots of the file system according to the schedule you define. Typically, you set a snapshots schedule when you initially create the file system. You can then modify or disable the schedule in the Snapshots Properties panel.

Note There can only be one snapshot schedule per share.

► To set or modify a schedule for automatic snapshots:

1. In Unity's tree view, click the Site node to display its child nodes.
2. Click the **Storage Pools** node.
3. Click the storage pool containing the file system for which you want to set a snapshots schedule.

4. Click its **File System** node.
5. Click the file system for which you want to set a snapshots schedule.
6. Expand the share's Properties panel.
7. Click the **Snapshot Settings** tab and configure the snapshots schedule for the file system:
 - a. Select the **Enable snapshot scheduling** option. This option is selected by default. Clearing the check box disables snapshot scheduling.
 - b. Adjust the snapshots schedule according to your preference. The default setting is once a day at 1 AM, with the start date set to the current date on Unity.
 - Specify the start date for the schedule by clicking the **Start date** field and selecting a date from the calendar.
 - Specify a recurrence pattern for the schedule by typing a value in the **Recur every** field.
 - Select the recurrence type from the drop-down list: **Minutes(s)**, **Hour(s)**, **Day(s)**, **Week(s)**, or **Month(s)**.
 - c. Click the **Apply** button to save your settings. If you select today's date as the start date for the schedule, Unity takes an automatic snapshot of the file system immediately after you set the schedule. Thereafter, Unity takes an automatic snapshot of the file system according to the schedule you specify.

Note By default, Unity refreshes site information every 5 minutes; as a result, a scheduled snapshot that Unity records may not be immediately visible in the snapshots grid. You can manually refresh the list of snapshots displayed in the grid by clicking the **Refresh List** button.

Taking a manual file system snapshot

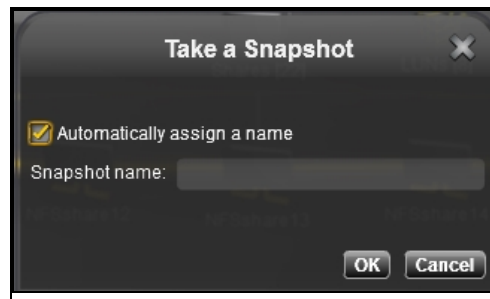
You can take manual snapshots of a file system at any time, even if you have scheduled (automatic) snapshots enabled. This mechanism allows you record a copy of the contents of a file system at any point in time.

▶ **To take a manual snapshot:**

1. In Unity's tree view, click the Site node to display its child nodes.
2. Click the Storage Pools node.
3. Click the storage pool containing the file system for which you want to set a snapshots schedule.
4. Click its **File System** node.
5. Click the file system for which you want to set a snapshots schedule.
6. Expand the file system's context menu.

- Click the **Take a Snapshot** button. Unity displays the Take a Snapshot dialog box.

Note You can also open this dialog box by opening the File System node 's context menu and selecting **Take a Snapshot**.



To...	Do this
specify a name for the manual snapshot	<ol style="list-style-type: none"> Clear the Automatically assign a name option (selected by default) and type a name for the snapshot in the Snapshot name field. The name must start with an (upper-case or lower-case) alphabetic or numeric character; and, with the exception of the hyphen (-), and period (.), the name can only contain alphanumeric characters, without spaces. These characters are NOT allowed: " / \ [] : ; = , + * ? < > Click the OK button to set the name and close the dialog box.
let Unity automatically assign a name to the manual snapshot	<ol style="list-style-type: none"> Make sure the Automatically assign a name option is selected (default selection). Click the OK button to close the Take a Snapshot dialog box. <p>The snapshot is assigned a default name that is prefixed with <code>manual_</code> and includes the date and time the manual snapshot is recorded.</p> <p>For example: if you take a manual snapshot on May 15, 2013 at 1:01PM, Unity assigns this name to the snapshot: <code>manual_2013-06-15-130101</code></p>

Browsing a file system snapshot

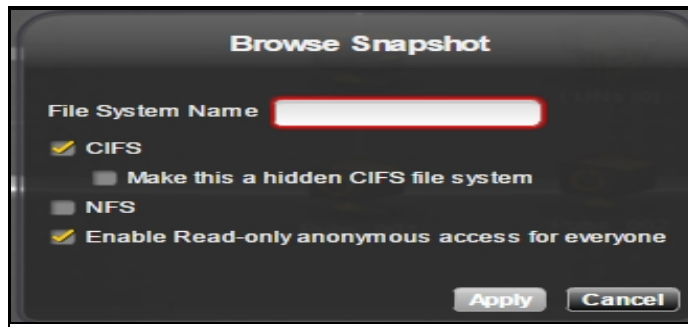
Setting [browsing for a snapshot](#) allows you to access the snapshot from a Windows-based (CIFS) system and/or a UNIX/Linux-based (NFS) system and browse its contents—in the same way that you access a file system. A snapshot that you browse is a read-only copy of its parent file system and its contents mirror the parent file system's contents at the time the snapshot is recorded.

► **To set browsing for a snapshot:**

- In Unity's tree view, click the Site node to display its child nodes.
- Click the **Storage Pools** node.
- Click the storage pool containing the parent file system of the snapshot for which you want to set browsing.
- Click its **File System** node.

5. Click the file system containing the snapshot for which you want to set browsing.
6. Expand the file system's properties panel.
7. Select the **Snapshots** tab. The Snapshots tab displays a grid that lists all the snapshots—both automatic (scheduled) and manual snapshots—that exist on the system for the file system.
8. Highlight the snapshot that you want to set browsing for by selecting the snapshot in the grid.
9. Click the **Browse snapshot** button. Unity displays the Browse Snapshot dialog box where you specify the name that you and your users will use to access the snapshot, as well as the sharing method.

Figure 6-40: Browse Snapshot dialog box—File Systems



10. Specify a browsing name for the snapshot and set its sharing method:

- a. In the
- File System Name**
- field, type a browsing name for the snapshot.

The name must start with an (upper-case or lower-case) alphabetic or numeric character; and, with the exception of the hyphen (-), and period (.), the name can only contain alphanumeric characters, without spaces.

These characters are NOT allowed:

" / \ [] : ; | = , + * ? < >

- b. Select the sharing method that you want to use to expose the snapshot to client computers on the network:

To...	Do this
expose the snapshot to Windows-based systems over the CIFS protocol	Select the CIFS option.
expose the snapshot to UNIX/Linux-based systems over the NFS protocol	Select the NFS option.
expose the snapshot to both Windows and UNIX/Linux-based systems (mixed-mode operation)	Select both the CIFS and NFS options.
gives all users on the network Read access to the snapshot, including the ability to display and traverse folders and read the contents of files in the snapshot	Select the Enable Read-only anonymous access for everyone option.

Note To enable the Read-only anonymous access options, you must first select either the CIFS sharing, NFS sharing, or both the CIFS and NFS sharing options.

- c. Click
- Apply**
- to save your settings and close the Browse Snapshot dialog box.

Once Unity completes this process, the **Browsing status** column in the snapshots grid displays the browsing enabled icon for the snapshot. If you mouse over the browsing enabled icon, Unity displays a ToolTip identifying the browsing name that you set for the snapshot.

Note When you select a snapshot that has browsing enabled in the snapshots grid, the **Browse snapshot** button changes to **Stop browsing**.

Stopping file system snapshot browsing

► **To disable browsing for a snapshot:**

1. In Unity's tree view, click the Site node.
2. Click the **Storage Pools** node.
3. Click the storage pool containing the parent file system of the snapshot for which you want to disable browsing.
4. Click its **File System** node.
5. Click the file system containing the snapshot for which you want to disable browsing.
6. Expand the file system's Properties panel.

7. Select the **Snapshots** tab. The Snapshots tab displays a grid that lists all the snapshots—both automatic (scheduled) and manual snapshots—that exist on the system for the file system.
8. Highlight the snapshot that you want to disable browsing for by selecting the snapshot in the grid.
9. Click the **Stop browsing** button.

Note The **Stop browsing** button is only displayed if you select a snapshot in the grid that has browsing enabled.

Once Unity disables browsing for the snapshot, the **Browsing status** column in the snapshots grid displays the browsing disabled icon for the snapshot.

Rolling back the data in a share to a snapshot

The rollback function reverts a file system's contents to what they were at the time the snapshot was taken, including all file- and folder-level permission settings and access-level attributes. This function also automatically deletes all snapshots that are newer than the snapshot that you roll back to, including all manual snapshots of the file system and snapshots that have browsing enabled.



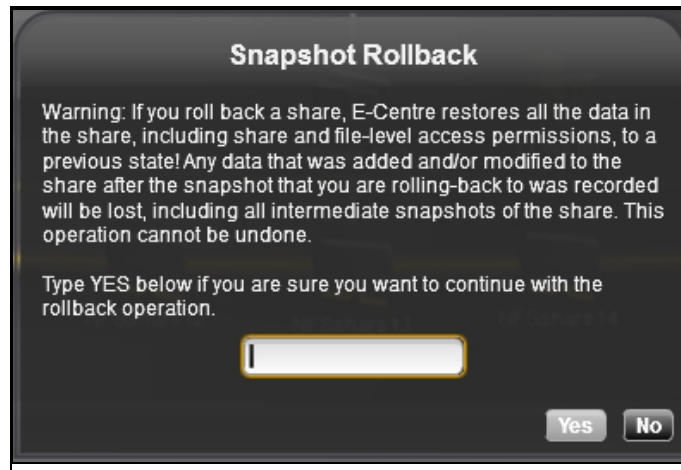
CAUTION: Unity rolls back all the data in the file system to the contents of the snapshot. This includes all file- and folder-level permission settings and file system-level access attributes as they were when the snapshot was recorded. Additionally, Unity deletes all snapshots that are newer than the snapshot that you roll back to, including all manual snapshots of the file system and snapshots that have browsing enabled.

▶ **To roll back the data to a point-in-time snapshot:**

1. In Unity's tree view, click the Site node to display its child nodes.
2. Click the **Storage Pools** node.
3. Click the storage pool containing the file system that you want to roll back.
4. When the storage pool's child nodes are displayed, click its **File System** node.
5. Click the file system containing the snapshot that you want to roll back to.
6. Expand the file system's Properties panel.
7. Select the **Snapshots** tab to display a grid that lists all the snapshots—both automatic (scheduled) and manual snapshots—that exist on the system for the share.
8. Highlight the snapshot that you want to roll back to by selecting the snapshot in the grid.

9. Click the **Rollback** button. Unity displays a confirmation dialog box.

Figure 6-41: Snapshot Rollback Confirmation dialog box



10. Type **Yes** in the text box.
11. Click the **Yes** button.

Using the Windows Volume Shadow Copy service to roll back the data in a share

If Unity is joined to a Microsoft Active Directory domain, Unity automatically exposes all the snapshots for each share on Unity to Microsoft Windows (CIFS) clients that access the shares—provided the Microsoft Windows client computers support Microsoft Volume Shadow Copy (or VSS).

You can then use Microsoft VSS on the Windows client computers to restore previous versions of files and folders from a snapshot of a share, or roll back a share to a specific point-in-time snapshot.



CAUTION: The restore operation cannot be undone.

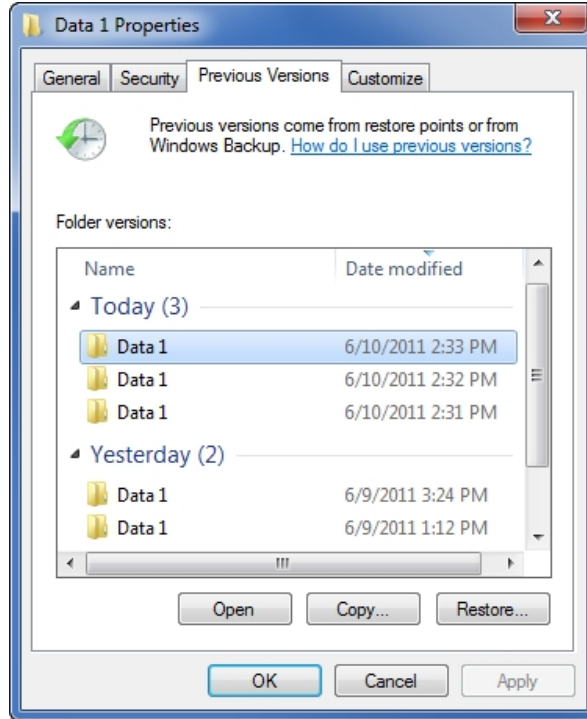
► **To use Microsoft VSS on a Windows client computer to roll back the data in a share:**

1. In Unity:
 - a. Make sure the share has CIFS sharing enabled.
 - b. Make sure the share has manual or automatic (scheduled) snapshots recorded; see [Setting a schedule for automatic file system snapshots](#) on page 197.
2. Access the share from a Windows-based (CIFS) system.

3. On the Windows-based (CIFS) system: right-click the file or folder that you want to restore to a previous version or snapshot, and then click **Restore previous versions**. (Or, if you want to roll back all the contents of the share to a snapshot, right-click the share and then click **Restore previous versions**.)

Microsoft Windows displays a list of available previous versions or snapshots of the file, folder, or share.

Figure 6-42: Microsoft VSS, Restore previous version of file, folder, or share



4. Before restoring a previous version of a file, folder, or share, select the previous version in the list, and click **Open** to view it to make sure it's the version you want to roll back to.
5. To roll back to a previous version, select the previous version in the list, and click **Restore**.

Similar to the roll back function in Unity, Microsoft VSS rolls back all the data in the share to the contents of the snapshot you select—this includes all file- and folder-level permission settings and share-level access attributes. However, unlike Unity's roll back function, Microsoft VSS does not delete any new files or folders that were added to the share since the snapshot that you select as your restore point was recorded: the restore function only rolls back files and folders that exist in both the share and the snapshot that you are rolling back to.

Configuring auto-deletion settings for file system snapshots

Auto-deletion settings allow you to specify the maximum number of snapshots that you want Unity to keep on the system for the corresponding file system. For example, to keep only 7 snapshots on the system for the file system, set the auto-deletion setting to 7; Unity automatically deletes the first, or oldest snapshot on the system when it records the next scheduled (or eighth) snapshot.

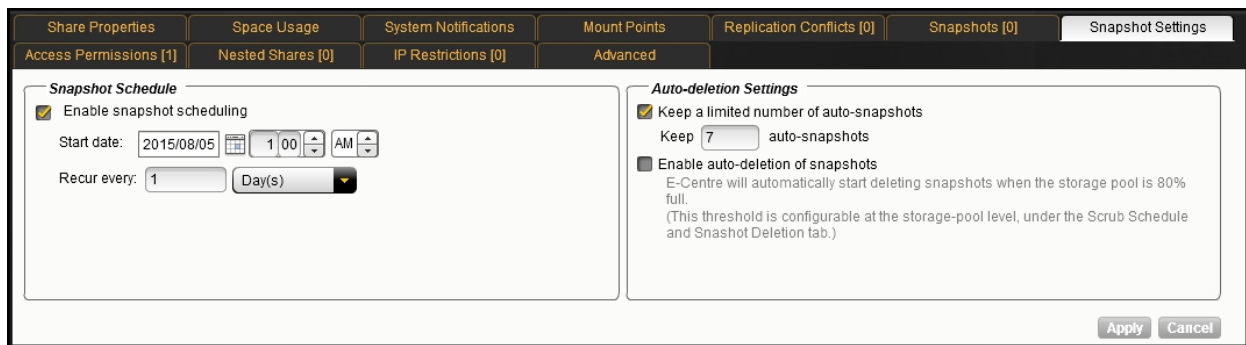
You can also enable automatic deletion of snapshots when space usage in the storage pool reaches 80% of its total capacity. Auto-deletion settings only apply to scheduled (automatic) snapshots; Unity does not automatically delete manual snapshots. The snapshot auto-deletion threshold is configurable at the storage pool-level; see [Modifying the snapshot auto-deletion setting for a storage pool](#) on page 112.

Note Snapshot auto-deletion settings are configured from the primary file system only. If the file system is replicated, the snapshots will also be automatically deleted from its replica using the same threshold, during a subsequent replication session.

► **To set auto-deletion settings for snapshots:**

1. In Unity's tree view, click the Site node to display its child nodes.
2. Click the **Storage Pools** node.
3. Click the storage pool containing the file system for which you want to set auto-deletion settings.
4. Click its **File System** node.
5. Click the file system for which you want to set auto-deletion settings.
6. Expand the file system's Properties panel.
7. Select the **Snapshot Settings** tab.

Figure 6-43: File System's properties panel—Snapshot settings tab



8. Under **Auto-deletion Settings**, select the **Keep a limited number of auto-snapshots** option (default setting).
9. Type a value in the **Keep auto-snapshots** field. For example, if you want Unity to keep only 5 snapshots on the system, type 5 in the field.
10. Optionally, if you want Unity to automatically delete snapshots when the used space in the storage pool reaches 80% of its total capacity, select the **Enable auto-deletion of snapshots** option. When this option is enabled, Unity automatically deletes snapshots for the share—starting with the oldest snapshot—until used space in the storage pool drops below 80%.

Manually deleting file system snapshots

This section describe how to delete snapshots for a file system. You can delete both manual snapshots and automatic (scheduled) snapshots.

► **To manually delete snapshots for a file system:**

1. In Unity's tree view, click the Site node to display its child nodes.
2. Click the **Storage Pools** node.
3. Click the storage pool containing the file system from which you want to delete snapshots.
4. Click its **File System** node.
5. Click the file system from which you want to delete snapshots.
6. Expand the file system's Properties panel.

7. Select the **Snapshots** tab. The Snapshots tab displays a grid that lists all the snapshots—both automatic (scheduled) and manual snapshots—that exist on the system for the share.
8. Highlight the snapshot that you want to delete by selecting it in the grid. You can also select multiple snapshots: hold down SHIFT or CTRL and click the left mouse button; or, to select all the snapshots in the grid, click the **Select All** button.
9. Click the **Snapshot** button.
10. Unity prompts you to confirm deletion; click **Yes** to continue.

Nexsan Unity n-Way Sync

Overview

Nexsan Unity n-Way Sync allows you to synchronize file systems among two or more Nexsan Unitys on a real-time, ongoing basis. After setting up the first two appliances, you may add additional appliances to the n-Wayfile system in the same manner as the second.

Requirements

To use n-Way Sync, you must have the following:

- Active Directory (AD)
- Two or more Nexsan Unitys in the same AD domain and same Nexsan Central Services (CS) organization are required for actual sync to take place. Alternately, you may convert only one NST to Unity and enable n-Way Sync to access other features which rely on its file systems, such as mobile access.
- Internet connectivity

What is the CS organization?

A CS *organization* is an administrative entity to which you attach two or more Unitys for the purpose of using the n-Way Sync and related features, such as Nexsan Unity Mobile App. Unitys must be in the same CS organization to access each others' n-Way file systems. A CS organization allows the CS to know which Unity appliances are part of the same group.

You create CS organizations as one of the first steps during the setup of n-Way Sync. This then resides on CS servers and contain only the minimal metadata required to securely link your Unitys. Actual user data remains on your appliances only.

A Unity may belong to only one CS organization, and n-Way Sync between CS organizations is not supported.

Access Control

- Unity uses access control lists (ACLs) to control user permissions/access.
- To establish access, you must manually set the ACL for the root of the file system. Below root of the file system, n-Way Sync will replicate ACLs along with the files.
- **WARNING:** To control Mobile or Web access to the file system, you must set Windows or Linux file system permissions using a CIFS or NFS client. CIFS share permission settings do NOT apply to Mobile, Web, NFS, or FTP access.

Network considerations

In an institutional network environment, enhanced security measures may block Unity connection methods. At any applicable firewalls, be sure to whitelist the URLs and IP addresses listed here.

Server names:

- `stun.connecteddata.com`
- `stun-pool-1.connecteddata.com`
- `stun-pool-2.connecteddata.com`

- dws.connecteddata.com
- devicesoftware.connecteddata.com
- unity.nexsan.com
- links.nexsan.com

Relay IP addresses:

- 199.217.118.148
- 69.12.70.194
- 85.25.218.217
- 198.16.72.170

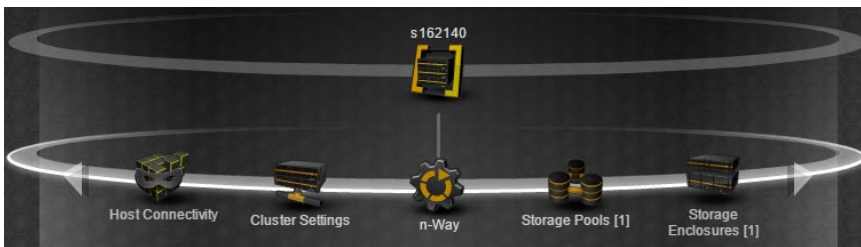
Additional notes:

- Relay is the least-preferred connection method, used only when Unitys can't negotiate a direct peer-to-peer connection. Relay redirects your encrypted packets without ever storing them. Relay uses an outbound connection to TCP port 80 or TCP port 23456.
- Unity (n-Way) makes use of UDP. Please be sure that you are not blocking UDP traffic.
- To establish initial connections between appliances, n-Way Sync must be able to connect to NexsanCentral Services (CS) servers. Thus at least minimal Internet connectivity is required during setup. A Unity on a fully isolated network would not be able to set up n-Way Sync but could sync once set up.

Preparing to create an n-Way file system

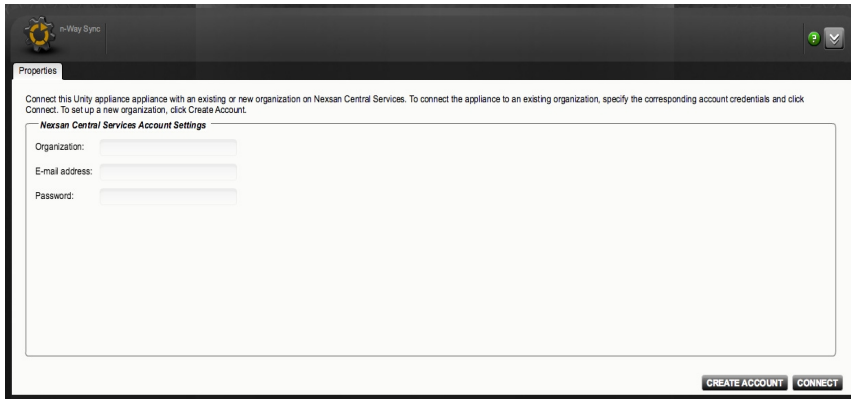
You will first create a source file system on one Unity. Then on a second (and any subsequent) Unity you will sync the file system from a list of available n-Way file systems.

1. At the admin page for the source Unity, click the **n-Way** button.



2. Click the **Properties** tab, then click the **Connect** button.

- To create your CS organization, click **Create Account** and follow the prompts.
Important: This is where you must use the dedicated email address that the customer reserved for this purpose.



Creating an n-Way File system

Once you have completed setting up your organization, you can add n-Way file systems that can sync between Unitys and mobile devices. To do this you will first create a source file system on one Unity. Then on a second (and any subsequent) Unity you will sync the file system from a list of available n-Way file systems.

WARNING: To control Mobile or Web access to the file system, you must set Windows or Linux file system permissions. CIFS share permission settings do NOT apply to Mobile, Web, NFS, or FTP access.

To start the n-Way File System Setup Wizard:

- Under the site node, click the **n-Way** node to select it.
- Perform one of these actions:

To...	Do this
use n-Way's context menu	<ol style="list-style-type: none"> Click the context menu button on the n-Way node. When the node context menu opens, click Create an n-Way file system
use n-Way's Properties panel	<ol style="list-style-type: none"> Click the Properties tab at the bottom of the screen to expand the Properties panel. Click click Create an n-Way file system button on the Properties panel.

This launches the [Create a File System](#) wizard. Continue creating the file system as you normally would.

Steps to sync an n-Way file system

Once you have created an n-Way file system on one Unity device you can sync it to another Unity device, also known as the destination Unity system. However note that once you set them up they will sync in both directions

1. Go to the admin page for the destination Unity, and click the **n-Way** button.
2. Click the **Properties** tab, and connect Unity to the same CS organization that you created during setup of the first Unity system.
3. Click the **n-Way File Systems** tab. Locate the n-Way file system that you just created at the first Unity. It should appear as Available. Select it and click the **Sync** button.
4. Complete the setup dialogs as desired, and continue.
5. To verify the folder's status, click the **Status** tab.
6. For a third or subsequent Unity, repeat these steps for that Unity.
7. Suggest a brief connectivity test: As a user, mount the n-Way file system from each Unity. Copy a different small file, such as a desktop picture, into the mounted file system of each Unity. Wait a minute for sync to occur, then check that all the files appear in the mounted file systems of all Unities that you configured.

Usage Notes

- **WARNING:** To control Mobile or Web access to the file system, you must set Windows or Linux file system permissions. CIFS share permission settings do NOT apply to Mobile, Web, NFS, or FTP access
- Unity models don't need to be the same size to use n-Way Sync.
- Files remain private and are not stored in the cloud.
- Clients connect via CIFS/NFS on LAN.
- WAN traffic between Unity appliances is encrypted via AES-256.
- n-Way Sync occurs at the whole-file level, not block level.
- n-Way-enabled file systems should not contain live databases targeted by users, because the sync is designed for unstructured data. However, it's OK to store a non-live, backup database on an n-Way file system.
- n-Way Sync does not support file locking.
- A given Unity storage pool may use n-Way Sync or asynchronous replication, not both.

Working with links

Nexsan Unity Desktop and the Nexsan Unity Mobile App give you the ability to easily create and share links to individual files stored on your Unity.

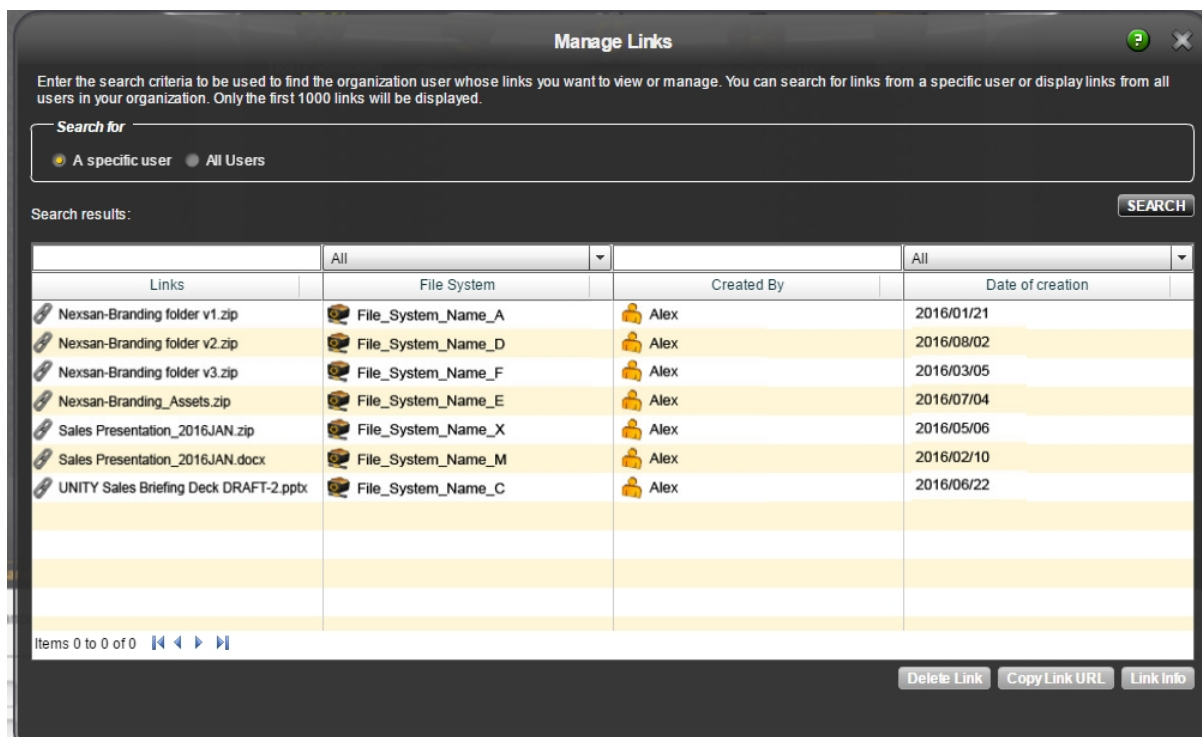
From Nexsan Unity, you can:

- View information on how many times a file has been linked to, and who has been viewing it.
- Copy a link URL, to send to another recipient
- Delete the link.

To manage links:

1. Under the site node, click the n-Way node to select it.
2. Perform one of these actions:

To...	Do this
use the n-Way's context menu	<ol style="list-style-type: none"> a. Click the context menu button on the n-Way node. b. When the node context menu opens, click Manage Links.
use the n-Way Properties panel	<ol style="list-style-type: none"> a. Click the Properties tab at the bottom of the screen to expand the Properties panel. b. Click Manage Links button on the Properties panel.



Viewing link access information

The **Manage Links** dialog can be used to view the number of times a link has been accessed, and who it has been accessed by.

To view link access information, use the following procedure:

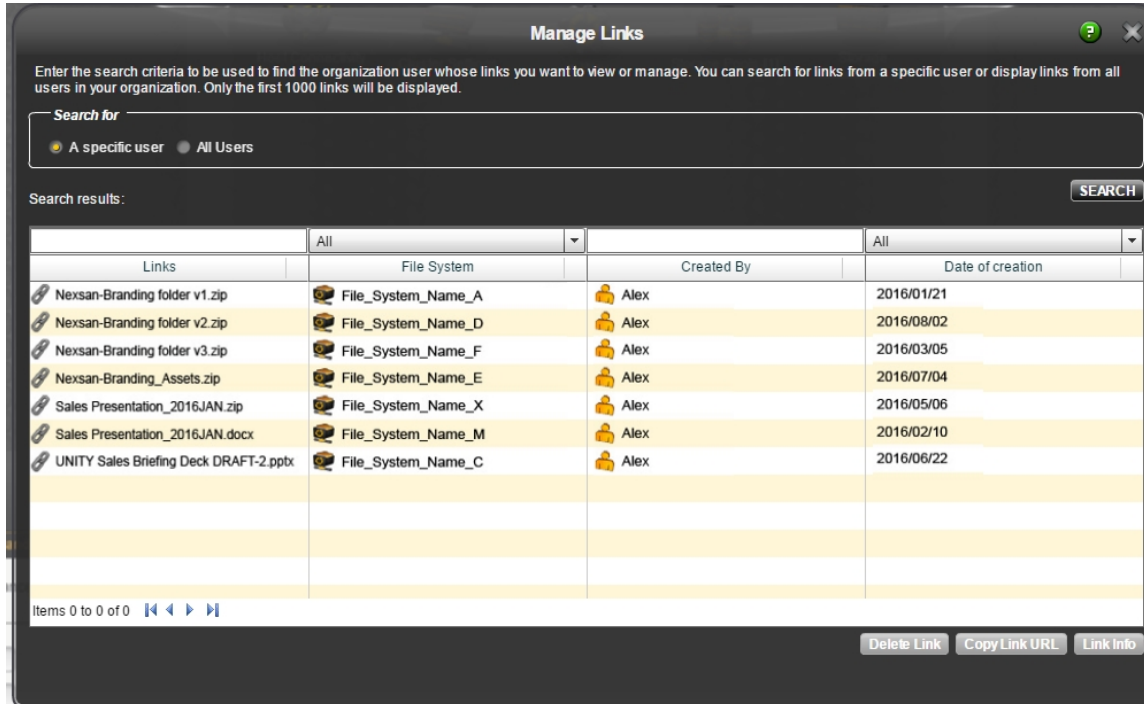
1. In the **Manage Links** dialog, search for a link, either by searching for a specific user, or by selecting **All Users**, which will display all available links.
2. Select the link that you want information on.
3. Click **Link Info**.

A list of the last 25 IP addresses to use the link, and the date that they used it, is displayed.

Finding Users

The **Manage Links** dialog can be used to see links from all users, or to see only links created by a specific user.

To see all links, simply select the **All Users** option, and then click **Search**.



To see links created by a specific user, select the **Specific User** option, and click **Search**. A new dialog appears, with a list of all users in your organization. To narrow your search, enter a full, or even partial name into the search dialog. Select the user whose links you want to see, and click **Show Links**.

Copying link URLs

Copying a URL link allows you to send it to others through email or secured chat. From there, the recipients of your link can access the files it references.

To copy a URL, use the following procedure:

1. In the **Manage Links** dialog, search for a link, either by searching for a specific user, or by selecting **All Users**, which will display all available links.
2. Select the link that you want information on.
3. Click **Copy URL**.

Your link can now be pasted into an email, or a secure chat, and can be sent to another user.

Chapter 7

LUNs

Unity supports block-level storage access using storage protocols (iSCSI). A storage protocol enables block level data transfer between requesting applications and [iSCSI target devices](#). The protocol allows client systems ([initiators](#)) to send SCSI commands (CDBs) to storage devices (targets) on a remote storage system, such as Unity. This allows organizations to consolidate storage into data center storage arrays while providing hosts (such as database and web servers) with the illusion of locally-attached disks.

A LUN is essentially a block of storage that you add to a storage pool on Unity, and then present to client systems (initiators) on the network through a target.

This section includes these topics:

Overview of data management functions on LUNs	214
Guidelines for adding and managing LUNs	214
Understanding disk space consumption	214
Adding a LUN	216
Modifying LUN properties	226
Viewing space usage information for LUNs	232
Setting up host connectivity	233
Adding an iSNS server	244
Managing snapshots for LUNs	245
iSCSI Functions	280
Deleting a LUN	291

Overview of data management functions on LUNs

Unity includes several data management functions that ensure continuous availability of the data in your LUNs.

- **Space usage configuration and Thin Provisioning:** Unity allows you to reserve a specific amount of disk space for each LUN that you add to the system, and also configure Thin Provisioning for each LUN—where disk space is allocated only when needed. With Thin Provisioning, you can flexibly allocate the disk space (on an iSCSI LUN) to the client system (initiator), in order to expand the storage capacity available to the client system at anytime. Thin provisioning allows efficient storage management since the system administrator need only monitor the storage capacity of one single server (Unity). Over-allocation is also allowed since the storage capacity of Unity can be expanded by allocating more storage to the system.
- **Disaster recovery with Data Replication:** Unity allows you to replicate the data contained in each LUN to a remote Unity site, including setting replication schedules. You can use the Data Replication feature to replicate all the LUNs in a storage pool or select only a subset of LUNs to replicate. If the primary site goes down (for routine maintenance or a natural disaster), Unity allows you to failover your entire site, or just a storage pool and its associated file systems and LUNs, to the replicated site. For more information about the Data Replication feature, the *Nexsan Unity Snapshots and Replication Guide*.
- **Data protection using Snapshots:** Unity allows you to take point-in-time snapshots of the data contained in each LUN, including scheduled automatic snapshots. This allows you to maintain a set of previous versions of all files in a LUN.
- **Data backups with NDMP support:** Unity allows you to configure Unity as a Network Data Management Protocol (NDMP) host to participate in remotely-coordinated automatic backups. For more information about NDMP backup support, see [Site-level tasks on page 347](#).

Guidelines for adding and managing LUNs

Before you add LUNs to a storage pool on Unity, review these guidelines:

- Determine which initiators will access the LUNs. In general, a target should only be accessed by a single client (iSCSI or Fibre Channel initiator) at a time; simultaneous access by multiple clients is not recommended as this may result in data corruption. However, if your network infrastructure uses clustering technologies, such as Microsoft Cluster Server (MSCS) software, simultaneous access by multiple initiators to a single LUN is supported.
- Determine the maximum number of LUNs for each storage pool. Planning the content, size, and distribution of LUNs can improve performance, manageability, and overall ease-of-use of the system. In general, by keeping the number of LUNs and other resources low, the performance of Unity is optimized.
- Take into account the number of LUNs that you need, and divide the disk space in the storage pool accordingly. When allocating disk space, keep in mind that LUN metadata and snapshots also consume storage.
- Consider future capacity requirements, particularly when allocating space usage to LUNs.
- Use a 1 Gbps Network or higher speed network: using a 1 Gbps Network, including 1Gbps NICs, Ethernet cables, and network switches, ensure optimal iSCSI performance.
- If you plan on using CHAP (Challenge Handshake Authentication Protocol) authentication, determine the CHAP credentials that each initiator will use.

Understanding disk space consumption

This section describes how space is used on disk when creating snapshots and replicating data. It also provides recommendations for setting up your replication, especially if you are using thick LUNs. As opposed

to thin-provisioned LUNs or file systems, thick LUNs use the same amount of space as their allocated disk size. In other words, the amount of reserved space is the same as the disk's physical capacity.

▶ **When creating snapshots:**

- Every snapshot uses space outside the LUN's or file system's reserved space.
- When the LUN/file system is almost full, the snapshot uses that same amount space, so it almost doubles the size of the LUN/file system.
- When creating multiple snapshots, any changes in data (deletions/additions/rewrites) in between snapshots will use additional space on thick LUNs, so the total amount of space may go over the LUN's size.

▶ **When creating replications:**

Unity takes two snapshots:

1. The baseline snapshot captures the data of last replication.
2. The incremental snapshot captures the new data added after the last replication.

The total amount of space used by the two snapshots will be equivalent or greater than the amount of data on thick LUNs.

▶ **Recommendations:**

- When your data is replicated on LUNs, use thin-provisioned LUNs.
Note If you already created thick LUNs, please contact Nexsan Technical Support to have them converted to thin LUNs.
- Make sure to have enough disk space on your storage pool because snapshots and replications will use additional space, as explained above.
- Turn data compression on.
- Use a shorter replication interval to save space and replication time.

This table compares the total space used by a thin-provisioned LUN and a thick LUN. Our example uses asynchronous replication on a LUN with a size of 2 TB. (File Systems use the same amount of disk space as thin-provisioned LUNs.)

Table 7-1: Used space comparison

#	Action	Data written	Data size	Baseline snapshot	Increment. snapshot	THIN LUN	THICK LUN
1	Create LUN	0	0	0	0	0	2 TB
2	Write 1 TB of data	1 TB	1 TB	0	0	1 TB	2 TB
3	Replicate LUN (the first snapshot is taken)	0	1 TB	1 TB	0	1 TB	3 TB
4	Write 100 GB of data (new blocks)	100 GB	1.1 TB	1 TB	0	1.1 TB	3 TB
5	Write 100 GB of data (existing blocks)	200 GB	1.1 TB	1 TB	0	1.2 TB	3 TB

#	Action	Data written	Data size	Baseline snapshot	Increm. snapshot	THIN LUN	THICK LUN
6	Replicate LUN:						
	a. A new, second snapshot is taken.	0	1.1 TB	1 TB	200 GB	1.2 TB	3.2 TB
	b. The first snapshot is deleted and the updates are merged.	0	1.1 TB	1.1 TB ¹	0	1.1 TB	3.1 TB ²
7	Delete 100 GB	0	1.0 TB	1.1 TB	0	1.1 TB	3.1 TB
8	Delete 100 GB	0	0.9 TB	1.1 TB	0	1.1 TB	3.1 TB
9	Write 1.1 TB of data (new blocks)	1.1 TB	2 TB	1.1 TB	0	2.2 TB	3.1 TB
10	Replicate LUN:						
	a. A new, third snapshot is taken.	0	2 TB	1.1 TB	1.1 TB	2.2 TB	4.2 TB
	b. The second snapshot is deleted and the updates are merged.	0	2 TB	2 TB	0	2.0 TB	4.0 TB
11	Write 400 GB of data (existing blocks)	400 GB	2 TB	2 TB	0	2.4 TB	4.0 TB
12	Replicate LUN:						
	a. A new, fourth snapshot is taken.	0	2 TB	2 TB	400 GB	2.4 TB	4.4 TB
	b. The third snapshot is deleted and the updates are merged.	0	2 TB	2 TB	0	2.0 TB	4.0 TB

Adding a LUN

This section describes the process for adding a LUN to a storage pool on Unity, including guidelines for LUN management, and steps for setting up CHAP (Challenge Handshake Authentication Protocol) authentication. You add a LUN to a storage pool using the LUN Setup Wizard; before starting the LUN Setup Wizard, review the guidelines provided in the subsequent sections.

► Before you begin:

- If you intend to use CHAP (Challenge Handshake Authentication Protocol) authentication, you must add CHAP users to the site; see [Configuring and managing CHAP authentication](#) on page 281.
- You can add one or more iSCSI targets to the storage pool(s) where you intend to add LUNs. You can create a separate target for each LUN or assign multiple LUNs to a single target; see [Adding an iSCSI target](#) on page 288.

The LUN Setup Wizard guides you through the process of adding a LUN to a storage pool.

¹ For the thick LUN, 1.1 TB is the value when existing blocks are **fully** reused.

² The same applies to the total used space.

► **To start the LUN Setup Wizard:**

1. Under the site node, click the **Storage Pools** node to select it and display its child nodes.
2. Click the storage pool to which you want to add a LUN.
3. Click the LUNs node to select it.
4. Perform one of these actions:
 - Expand the **Properties** tab for the LUNs node, and click **Add a LUN**.

Note [Enabling data replication and configuring snapshot scheduling on page 220](#) is only displayed if your Unity deployment includes the Snapshots feature, the Data Replication feature, or both features. To purchase the Snapshots or the Data Replication feature, please contact your Nexsan reseller or Nexsan Support Representative.

This section includes these steps:

[Setting the LUN name and block size below](#)

[Configure space usage settings for the LUN on the next page](#)

[Enabling data replication and configuring snapshot scheduling on page 220](#)

Setting the LUN name and block size

This step of the LUN Setup Wizard prompts you to specify a name for the new LUN, set the block size for the LUN, as well as define client-specific (initiators) settings.

Figure 7-1: LUN Setup Wizard, Step 1: Setting the LUN name and block size

Specify a Name

Specify the name that you want to assign to the LUN; you can also adjust the default blocksize for the LUN, if needed.

Set the LUN Name

LUN Name:

LUN Blocksize

Adjust the blocksize for the LUN, if needed. To ensure optimal I/O performance, set the LUN's blocksize to the same value as the typical I/O blocksize of the host application.

Keep in mind that you CANNOT modify the LUN's blocksize once the LUN is created.

Blocksize < 8 KB >

LUN Caching

Adjust the read caching for the LUN, if needed. For OLTP Log LUNs, disable read caching to increase performance. Examples would be Exchange Logs, Oracle OLTP Logs, or SQL Logs.

Disable read caching

► **To define the LUN:**

1. Type a name for the LUN in the **LUN Name** field.

The name must start with an (upper-case or lower-case) alphabetic; and, with the exception of the hyphen (-), and period (.), the name can only contain alphanumeric characters, without spaces.

These characters are NOT allowed:

" / \ [] : ; | = , + * ? < >

2. In the **LUN Blocksize** section, adjust the block size for the LUN, if needed.

Note On the Unity 2000, the default and minimum values of the LUN block size differ for higher capacity drives.

- For the Unity 2000C (16 drives): The default block size will be 128 KB.
 - For drives < 4 TB: The minimum block size will be 32 KB.
 - For drives >= 4 TB and < 6 TB: The minimum block size will be 64 KB.
 - For drives >= 6 TB: The minimum block size will be 128 KB.
- For the Unity 2000P (24 drives), the default block size for the LUN will be 32 KB. The minimum block size will be 8 KB.

Note A 1 TB drive is typically 109 bytes and not 230 bytes.

To ensure optimal I/O performance, set the LUN's block size to the same value as the typical I/O block size of the host application. Aligning the volume block size to the typical I/O block size from the application can significantly improve application performance.

Table 7-2: Recommended block size for the application used

Application / Data type	Recommended block size
Windows / Linux Boot	64 KB
Microsoft Exchange 2010 DB	32 KB
Microsoft Exchange 2010 Log	128 KB
Oracle OLTP	8 KB
SQL Server	64 KB
Video Streaming	128 KB

Notes:

- You CANNOT modify the LUN's block size once the LUN is created.
 - The maximum block size for Unity is 128 KB.
3. (Optionally) Disable read caching for the LUN. For database OLTP LUNs, we recommend to disable read caching to increase performance.
 4. Click the right arrow on the wizard panel to continue to [Configure space usage settings for the LUN below](#).

Configure space usage settings for the LUN

This step of the LUN Setup Wizard prompts you to specify space usage settings for the LUN.

This table illustrates how Unity distributes disk space to LUNs for a storage pool of 10 TB.

Table 7-3: Distribution of disk space to LUNs

	Total available space in storage pool: 10 TB	
Space usage settings	LUN 0 (Thin-provisioned)	LUN 1 (Thick-provisioned)
Reservation	4 TB	6 TB
Virtual volume size	20 TB	N/A
Physical capacity	4 TB	6 TB
Virtual volume size as seen by initiators	20 TB	6 TB

Figure 7-2: LUN Setup Wizard, Step 2: Configuring space settings for the LUN

Configure Space Usage Settings for the LUN


Use these settings to create a Thin- or Thick-provisioned LUN. Thin-provisioning allows you to flexibly allocate space to the LUN, without the need to immediately allocate physical storage. Thick-provisioning will allocate the specified amount of physical disk space to the LUN.

LUN Type:

Thin-provisioned LUN

Virtual Size GB / 16,384 GB
Maximum size: 16 TB

Reservation MB / 142.59 MB
(Optional)

 Once set, the virtual volume size CANNOT be decreased; however, you may increase the value as needed.

Thick-provisioned LUN

Size MB / 142.59 MB

► **To configure space usage for the LUN:**

1. To use a **Thin Provisioned LUN**, select the corresponding option, then perform the next two steps.
2. Specify a virtual volume size for the LUN. This determines the disk space that clients see when they connect to the LUN; see [Thin Provisioning](#) on page 573.

Select the relevant capacity unit from the drop-down list; and type a value in the box.

Notes:

- Once you set the virtual volume size for a LUN, you cannot decrease it; however, you can increase it at any time.
- The virtual volume size cannot be less than the reserved space.
- You cannot switch to Thick Provisioning after the LUN is created.

3. Select the relevant capacity unit from the drop-down list; and then type a value in the box.

When you reserve space for a LUN, Unity allocates the specified amount of disk space in the storage pool to the LUN. If you add another LUN to the storage pool, the space available to the new LUN is the difference of the total disk space in the storage pool minus any reservations that you set for other LUNs on the system.

For example, in a storage pool with 2 LUNs and 10 TB of available disk space, if a reservation of 6 TB is allocated to one LUN, then the second LUN has 4 TB of disk space available to it.

Note If you use Thick Provisioning for the LUN, you **MUST** reserve a fixed amount of disk space.

4. To use a **Thick-provisioned LUN**, select the corresponding option.

Select the relevant capacity unit from the drop-down list; and type a value in the box. Thick Provisioning will use the specified amount of physical disk space.

Notes:

- You cannot switch to Thin Provisioning after the LUN is created.
- Once you set the minimum volume size for a LUN, you cannot decrease it; however, you can increase it as needed.
- If you intend to use snapshots with a Thick-provisioned LUN, keep in mind that each snapshot consumes disk space equivalent to the total size of the snapshot, so please make sure to plan your space consumption requirements accordingly.

5. Click the right arrow on the wizard panel to continue to .

Enabling data replication and configuring snapshot scheduling

This step of the LUN Setup Wizard prompts you to enable data replication for the LUN, if data replication is configured for the storage pool, and also to configure the snapshots schedule and auto-deletion settings for snapshots.

Note We do not recommend enabling snapshots scheduling when using LUNs in a Hyper-V environment. You can take manual snapshots and rollback data to a snapshot

Note This step is only displayed if your Unity includes the Snapshots or Data Replication feature, or both features.

Figure 7-3: LUN Setup Wizard, Step 4: Enable data replication and configure snapshots

Enable Data Protection for the LUN: MTL_test

To protect your data, enable the Snapshots and Data Replication functions for the LUN, provided either one of these options, or both, are included in your E-Centre deployment. To enable data replication for the LUN, you must first add and configure a remote NST appliance site where E-Centre will replicate the LUN.

Replication

Enable Data Replication for the LUN

Snapshots

2014/04/17 AM

Day(s)

Keep a limited number of auto-snapshots

Keep auto-snapshots

Enable auto-deletion of snapshots

E-Centre will automatically start deleting snapshots when the storage pool is 80% full.
(This threshold is configurable at the storage-pool level, under the Scrub Schedule and Snapshot Deletion tab.)

▶ **To enable data replication for the LUN:**

1. Select the **Enable Data Replication for the file system** option. This option is disabled if you have not yet configured data replication for the storage pool. If you enable this option, Unity replicates the LUN to the remote site during the next scheduled data replication.
2. If you do not enable snapshot scheduling, click the right arrow on the wizard panel to continue to [Add the LUN to a new LUN Mask](#) on page 223.

▶ **To enable and configure snapshot scheduling for the LUN:**

Note There can only be one snapshot schedule per LUN.

1. Configure the snapshots schedule for the LUN:
 - a. Select the **Enable scheduling** option to enable snapshots scheduling. This option is selected by default. Clearing the check box disables snapshot scheduling.
 - b. Adjust the snapshots schedule according to your preference. The default schedule for snapshots is once a day at 1 AM, with the start date set to the current date on Unity. This means that Unity will take an automatic snapshot of the data in the LUN at 1 AM every day starting on the current date.
 - c. Specify the start date for the schedule by clicking the **Start date** field and selecting a date from the calendar.
 - d. Specify the time when you want Unity to take snapshots. The default time is 1 AM.

- e. Specify a recurrence pattern for the schedule by typing a value in the **Recur every** field; then, select the recurrence type from the drop-down list: **Minutes(s)**, **Hour(s)**, **Day(s)**, **Week(s)**, or **Month(s)**.
 - For example, if you want Unity to take a snapshot every two hours, type 2 in the **Recur every** field and select **Hour(s)** from the recurrence type drop-down list.
 - If you select **Week(s)** from the recurrence type drop-down list, you must then select the day or days of the week that you want Unity to take automatic snapshots on.
 - If you select **Month(s)**, you must then select the month or months of the year, as well as the calendar dates that you want Unity to take automatic snapshots on.
2. Configure snapshot auto-deletion settings for the LUN:
 - a. Select the **Enable scheduling** option to enable snapshots scheduling (if not already enabled); this enables the options under **Auto-deletion Settings**.
 - b. Select the **Keep a limited number of auto-snapshots** option (selected by default) if you want Unity to only keep the specified number of automatic snapshots on the system—the default is 7 snapshots. This means that, after 7 snapshots, when Unity takes the 8th scheduled automatic snapshot of the data in the LUN, it automatically deletes the oldest automatic snapshot on the system. Unity does not delete manual snapshots when you enable this option; only scheduled automatic snapshots are processed. Change the default value if needed.
 - c. Select the **Enable the auto-deletion of snapshots** option if you want Unity to automatically delete automatic scheduled snapshots for the LUN when the storage pool is 80% full. Unity deletes snapshots—starting with the oldest automatic snapshot on the system—until used disk space capacity in the storage pool falls below the 80% threshold. Unity does not delete manual snapshots when you enable this option; only scheduled automatic snapshots are processed.
3. Click the right arrow on the wizard panel to continue to [Add the LUN to a new LUN Mask](#) on the facing page.

Note If you enable snapshots scheduling, and you set the current date (or today's date) as the start date for the schedule, Unity takes an automatic snapshot of the data in the LUN immediately after you set the schedule. Thereafter, Unity takes an automatic snapshot of the data in the LUN according to the schedule you specify.

Selecting a Mask for the LUN

This step of the LUN Setup Wizard prompts you to select a LUN Mask. A LUN Mask allows you to make a LUN accessible to hosts through the selected Target(s). You can use an existing LUN Mask or create a new one. Unity has two types of LUN Masks, one for Fibre Channel and the other one for iSCSI for each storage pool.

Note If the system is replicated, you must also create a LUN Mask on the replicated site for the LUN to be accessible when a failover occurs.

Figure 7-4: LUN Setup Wizard, Step 4: Selecting a Mask for the LUN

Select a Mask

ALUN Mask allows you to make a LUN accessible to hosts through the selected Target(s). You can use an existing LUN Mask or create a new one. The NST appliance has one pre-defined LUN Mask for Fibre Channel and another one for iSCSI for each storage pool. If the system is replicated, you must also create a LUN Mask on the replicated site for the LUN to be accessible when a failover occurs.

- Use pre-defined Fibre Channel LUN Mask
- Use pre-defined iSCSI LUN Mask (testPool)
The default iSCSI LUN Mask contains all iSCSI targets and is accessible to all hosts.
- Use an existing LUN Mask
- Create a new LUN Mask
- None
If you select None, you will need to select or create a LUN Mask later to make the LUN accessible to hosts.

▶ **To assign the LUN to a Mask:**

1. Select one of these options:
 - **Use pre-defined Fibre Channel LUN Mask:** This mask includes the common, unique Fibre Channel target.
 - **Use pre-defined iSCSI LUN Mask:** This mask contains all iSCSI targets and is accessible to all hosts.
 - **Use an existing LUN Mask:** If you previously created one or more LUN Masks, they will display in the drop-down list.
 - **Create a new LUN Mask**
 - **None:** If you select this option, you will need to select or create a LUN Mask later to make the LUN accessible to hosts; see [Setting up host connectivity](#) on page 233.
2. Click the forward arrow. If you selected to create a new LUN Mask, the wizard will continue to [Add the LUN to a new LUN Mask](#) below.
If you selected an existing LUN Mask, the wizard will continue to [Verifying settings](#) on the next page.

Add the LUN to a new LUN Mask

This step of the LUN Setup Wizard prompts you to create a new LUN Mask if you selected that option in the previous step. The LUN mask that will allow you to make the LUN visible to a host using the target with which you associate the LUN.

When creating an iSCSI LUN, you specify the initiator(s) you want and assign one or more of the available iSCSI targets to the LUN. If you have not created iSCSI targets yet, you must skip this step because the wizard will not let you continue. After creating the LUN, you have the possibility to associate it to a target by following the steps in [Adding a LUN mask](#) on page 237. For steps to create an iSCSI target, see [Adding an iSCSI target](#) on page 288.

When creating a Fibre Channel LUN, you specify the initiator(s) you want and then assign the unique common Fibre Channel target to the LUN.

► **To add a LUN to a new mask:**

1. Select the **Add to a new LUN Mask** option.

Figure 7-5: LUN Setup Wizard, Step 5: Add the LUN to a new LUN Mask

Add the LUN to a New LUN Mask

This step allows you to create a LUN Mask to make the new LUN accessible to hosts through the selected target(s). Associate the LUN with one or more initiators by selecting an existing Initiator Group or creating a new one. An Initiator Group must contain either Fibre Channel or iSCSI initiators. An initiator cannot be selected in multiple groups. LUN IDs must be unique within the same LUN Mask.

The screenshot shows a configuration form with the following fields and values:

- Name:** FinanceMask
- Type:** Fibre Channel
- LUN ID:** 0
- Initiator Group:** Existing: fibreGroup1
- New Initiator Group:** (Unselected)
 - Name:** (Empty field)
 - Initiator:** (Empty field)
- Target:** Fibre Channel

2. Enter a meaningful name in the **Name** field.
3. From the **Type** drop-down list, select **iSCSI** or **Fibre Channel**. The **Target** selection gets automatically updated with the existing target associated with the storage pool.
4. Enter a LUN ID or let Unity assign the next available number. The LUN ID is a number used to identify a LUN—from 0 to 254. Each LUN associated to the same target and the same initiators must have a unique LUN ID. However, if you associate each LUN to a different target or to different initiators (even if they are part of the same target), there is no need for the LUN IDs to be different. For LUN masking, the LUN ID has to be unique within the same mask.
5. Select an Initiator Group. An initiator group must contain either Fibre Channel or iSCSI initiators. An initiator cannot be selected in multiple groups.

To create a new initiator group:

- a. Enter a name for the group.
- b. Enter the IQN number.

IQN format: `iqn.1999-05.com.microsoft:17bwmm1.nexasan.com`.

Tip To look for existing IQN numbers, see the iSCSI Target's properties panel—**Properties** tab. For targets that are connected but not defined on Unity, use the CLI command, `wwn`. This command will display all iSCSI targets connected to Unity.

6. Click the right arrow on the wizard panel to continue to [Verifying settings below](#).

Verifying settings

This step of the LUN Setup Wizard summarizes the settings you selected for your LUN. Review the summary carefully before applying the configuration settings.

► **To change a LUN configuration setting:**

- Click the back arrow to navigate back to the corresponding configuration step.
- Or
- Click the corresponding step identifier at the top of the LUN Setup Wizard panel. For example, if you want to rename the LUN, click **Step 1**.

Figure 7-6: LUN Setup Wizard, Step 6: Verify Settings

Verify Settings

Please verify your configuration settings. If you want to change a setting, click the back arrow to navigate to the relevant configuration panel. Or, click the step identifier at the top of the wizard panel to go back to a specific step.

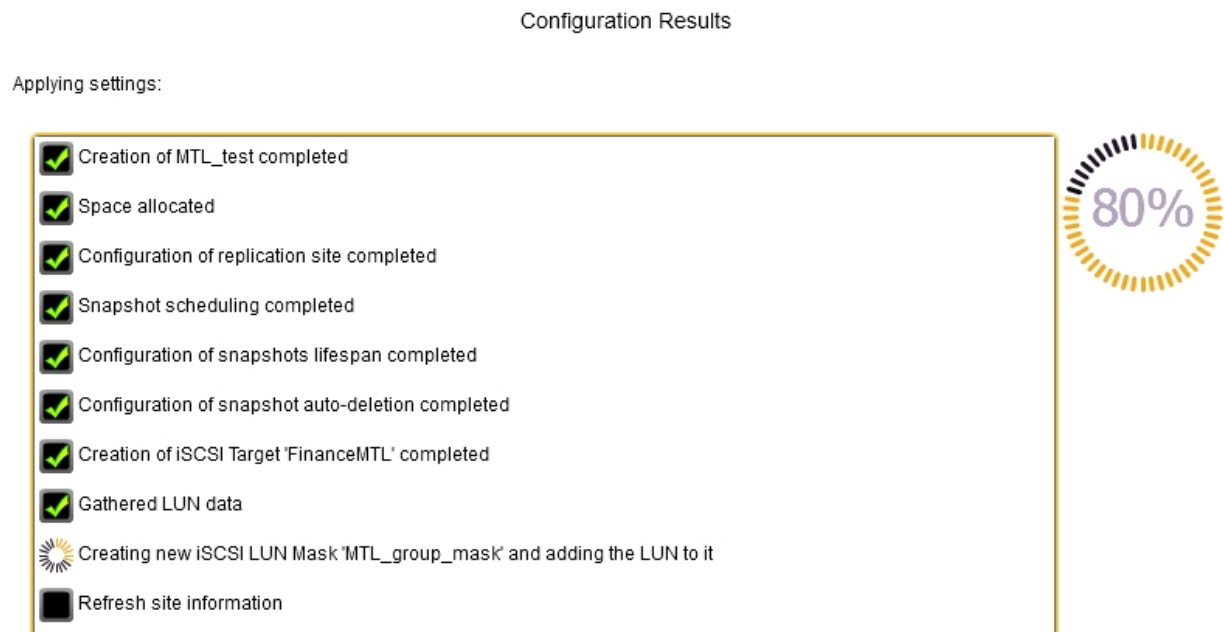


If you are satisfied with the configuration settings, click the **Start** button at the bottom of the panel. The LUN Setup Wizard automatically proceeds to [Viewing progress](#) below.

Viewing progress

Step 7 of the LUN Setup Wizard displays progress as Unity creates the new LUN.

Figure 7-7: LUN Setup Wizard, Step 7: Viewing configuration results



The LUN Setup Wizard displays error events that the system encounters during the LUN creation process. You can view more details about an error event by expanding the corresponding entry.

► **To view more details for an error event:**

- Click the plus (+) sign corresponding to the error event.

Unity informs you when it successfully creates the LUN. It also asks you if you want to create another LUN in the storage pool.

- Click **Yes** if you want to create a new LUN; the LUN Setup Wizard scrolls back to [Setting the LUN name and block size on page 217](#) and resets all configuration settings to their defaults.
- Click **No** if you do not want to create a LUN. This closes the LUN Setup Wizard.

Modifying LUN properties

This section describes how to modify properties for a LUN once you add the LUN to a storage pool.

You modify a LUN's properties in its Properties panel:

LUN Properties tab

- [Renaming a LUN on the facing page](#)
- [Enabling client-side space usage notifications for a LUN on page 228](#)
- [Enabling VMware VAAI hardware acceleration for a LUN on page 228](#)
- [Enabling/disabling data compression on a LUN on page 230](#)
- [Disabling Read caching on page 231](#)

Space Usage tab

- [Modifying LUN space settings on page 229](#)

VSS tab

- To view and configure VSS settings, see the *Nexsan Unity Snapshots and Replication Guide*.

Snapshots tab

- To manage snapshots, see the *Nexsan Unity Snapshots and Replication Guide*.

Snapshot Settings tab

- To view and configure snapshot settings, see the *Nexsan Unity Snapshots and Replication Guide*.

Renaming a LUN

If the LUN is replicated, Unity also renames the LUN's replica on the remote Unity.



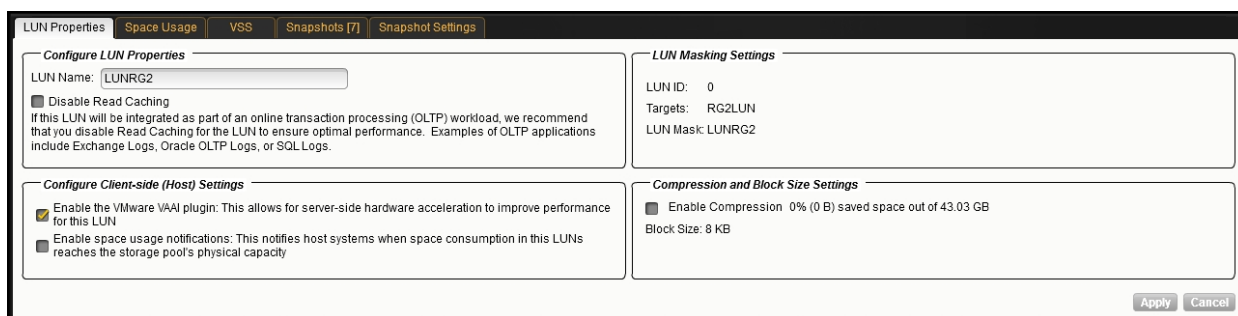
CAUTION: If you rename a LUN, client systems on the network will be disconnected from the LUN; this could result in data loss. Before renaming a LUN, make sure that active client systems disconnect from the LUN.

After renaming the LUN, you will need to update the host connection to the LUN using the new name.

► To rename a LUN:

1. In Unity's tree view, click the Site node.
2. Click the **Storage Pools** node.
3. Click the storage pool that contains the LUN whose name you want to modify.
4. Click the **LUNs** node.
5. Select the corresponding LUN.
6. Expand the LUN's Properties panel.

Figure 7-8: LUN's properties panel—LUN Properties tab



7. In the **Properties** tab, enter a new name for the LUN in the **LUN Name** field.

The name must start with an (upper-case or lower-case) alphabetic or numeric character; and, with the exception of the hyphen (-), and period (.), the name can only contain alphanumeric characters, without spaces.

These characters are NOT allowed:

" / \ [] : ; | = , + * ? < >

8. Click the **Apply** button to change the LUN's name.

Configuring client-side (host) settings for a LUN

Unity provides two configuration options that allow you to set client-specific (iSCSI or Fibre Channel initiators) settings for a LUN; these include:

1. [Enabling VMware VAAI hardware acceleration for a LUN](#) below
2. [Enabling client-side space usage notifications for a LUN](#) below

Enabling VMware VAAI hardware acceleration for a LUN

Unity includes a built-in [VAAI plugin](#) to provide hardware acceleration on Unity when integrated into a VMware ESX/ESXi environment. The VAAI plug-in controls both hardware acceleration and the UNMAP primitive for Thin Provisioned LUNs.

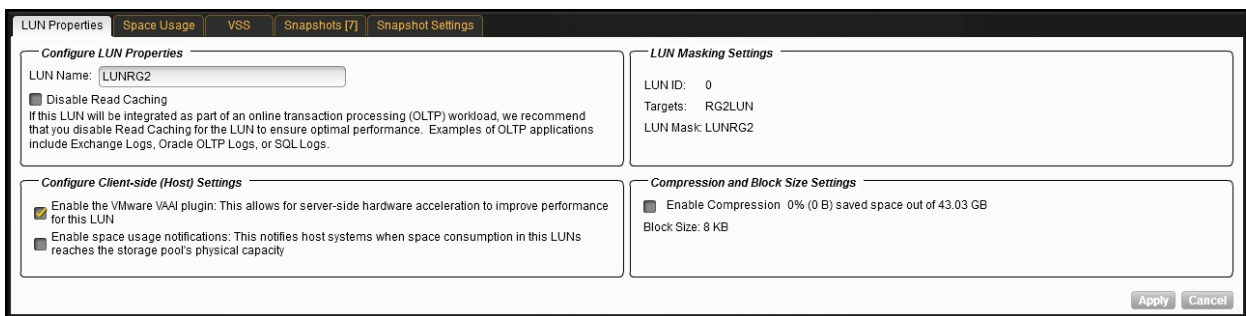
You must configure and enable VAAI hardware acceleration functionality on your VMware ESX/ESXi to support for the VAAI plug-in on Unity to work; for more information, please refer to the VMware documentation.

Note The VMware VAAI plug-in is always disabled by default when you create a LUN. You can enable the VAAI plug-in during LUN creation, if your VMware ESX/ESXi environment supports this feature. You can also disable or enable it at any time from the corresponding LUN's Properties panel.

► **To enable the VAAI plug-in for a LUN:**

1. In Unity's tree view, click the Site node.
2. Click the **Storage Pools** node.
3. Click the node corresponding to the storage pool where the LUN for which you want to enable the VAAI plug-in exists.
4. Click the **LUNs** node.
5. Click the node corresponding to the LUN that you want to enable the VAAI plug-in for.
6. Expand the LUN's Properties panel.
7. Select the **Properties** tab.

Figure 7-9: LUN's properties panel—LUN Properties tab



8. Check the **Enable the VMware VAAI plugin** option to enable the VAAI plug-in for the LUN.
9. Click the **Apply** button.

Enabling client-side space usage notifications for a LUN

Unity provides a notification mechanism that automatically notifies client systems (iSCSI initiators), connected to a LUN on Unity, when space consumption on the LUN reaches the storage pool's physical capacity.

When you enable this option for a LUN, Unity triggers space usage notifications based solely on the physical capacity of the storage pool where the LUN exists. Typically, the storage pool's physical capacity is less than the *virtual* capacity allocated to the LUN (the LUNs *virtual volume size*). As a result, to a client system, the LUN appears to have more space available to it than what the space usage notifications mechanism indicates. This mechanism notifies you when you need to expand the storage pool's physical capacity to keep up with the LUN's virtual capacity.

This client-side space usage notification mechanism is disabled, by default.

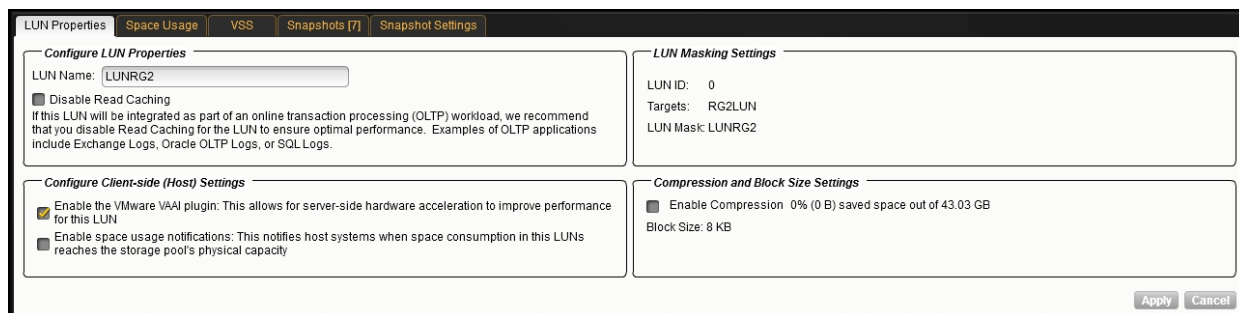
▶ **Before enabling this option, it is recommended that you:**

- remove the mask at the target level; see [Deleting a LUN mask](#) on page 242.
- disconnect the LUN at the client level.

▶ **To enable client-side space usage notifications for a LUN:**

1. In Unity's tree view, click the Site node.
2. Click the **Storage Pools** node.
3. Click the node corresponding to the storage pool where the LUN for which you want to enable client-side space usage notifications exists.
4. Click the **LUNs** node.
5. Click the node corresponding to the LUN for which you want to enable client-side space usage notifications.
6. Expand the LUN's Properties panel.
7. Select the **Properties** tab.

Figure 7-10: LUN's properties panel—LUN Properties tab



8. Click the **Space usage notifications** option to enable the client-side space usage notifications for the LUN.
9. Click the **Apply** button.

Modifying LUN space settings

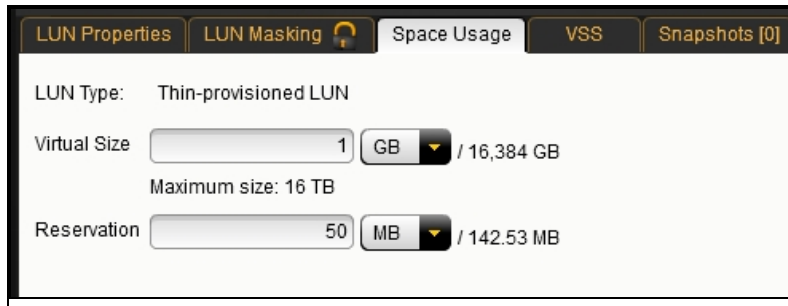
One set, the LUN size cannot be decreased, but you can add more space as needed. For information on how Unity distributes disk space to a LUN, see [Configure space usage settings for the LUN](#) on page 218.

▶ **To add more space to a LUN:**

1. In Unity's tree view, click the Site node to display its child nodes.
2. Click the **Storage Pools** node.

3. Click the node corresponding to the storage pool where the LUN for which you want to configure LUN masking exists.
4. Click the **LUNs** node.
5. Click the node corresponding to the LUN for which you want to modify space settings.
6. Expand the LUN's Properties panel.
7. Select the **Space Usage** tab.

Figure 7-11: LUN's properties panel—Space Usage tab



8. Perform one of these actions:

For a...	Do this
Thick-provisioned LUN	<ul style="list-style-type: none"> ● To change the volume size, select the relevant capacity unit from the drop-down list and type a value in the box. <p>You can increase the physical volume size but you cannot decrease it. However, make sure that the host operating system, where the LUN is mounted, supports online expansion of volumes before proceeding.</p>
Thin-provisioned LUN	<ul style="list-style-type: none"> ● To change the virtual size, select the relevant capacity unit from the drop-down list and type a value in the box. You can increase the virtual volume size but you cannot decrease it. ● To change the space reservation, select the relevant capacity unit from the drop-down list and type a value in the box. You can increase the reservation size but you cannot decrease it. <p>Note The virtual volume size cannot be less than the reserved space.</p>

9. Click **Apply** to save your changes.

Enabling/disabling data compression on a LUN

You can enable compression at the LUN level. This setting takes precedence over the settings defined at the pool level. If you enabled data compression at the pool level before creating this LUN, the LUN already has data compression enabled—see [Enabling data compression on the storage pool](#) on page 113. If you choose to disable data compression on the LUN, only that LUN will be affected.

Compression allows for better performance of the LUN since the files to read/write are much smaller. However, it will also increase CPU usage. Compression can be enabled/disabled at any time.

Notes:

- When you set up replication for LUNs that have the compression setting enabled, LUNs on the remote site inherit the compression settings.
- Enabling data compression does not affect existing data. It will only affect data that will be written to the LUN after the change.



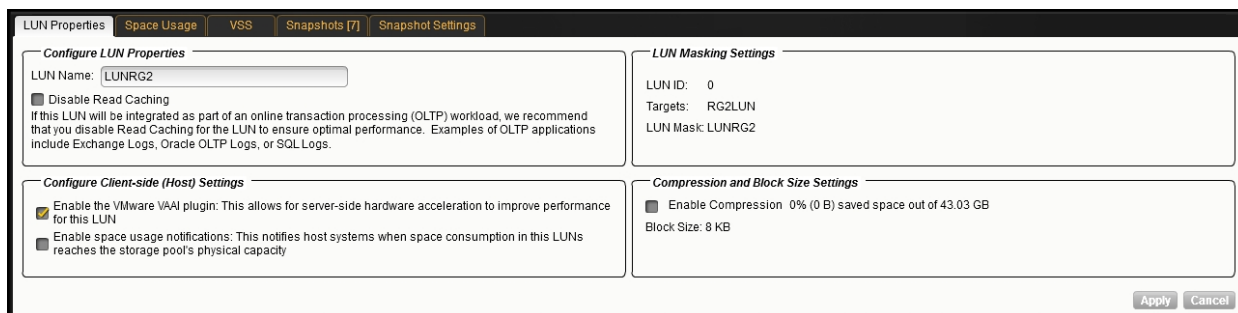
CAUTION: If you turn on data compression for a LUN, and then you turn it off before you set up replication for the LUN, part of the data will be decompressed and the other part will not. Since the LUN has not been replicated yet, the compression settings are not inherited and data compression is off at the remote site.

This means that data is taking less space on the primary LUN than it will on the replica. As a result, replication may fail if the LUN on the remote site does not have enough space. In this instance, it is recommended to enable data compression on both sites before replication.

► **To enable data compression on a LUN:**

1. In Unity's tree view, click the Site node.
2. Click the **Storage Pools** node.
3. Click the storage pool to which the LUN belongs.
4. Click the **LUNs** node.
5. Select the LUN for which you want to enable data compression.
6. Expand the LUN's Properties panel.
7. Select the **Properties** tab

Figure 7-12: LUN's properties panel—LUN Properties tab



8. Select the **Enable Compression** option.
9. Click **Apply**.

Disabling Read caching

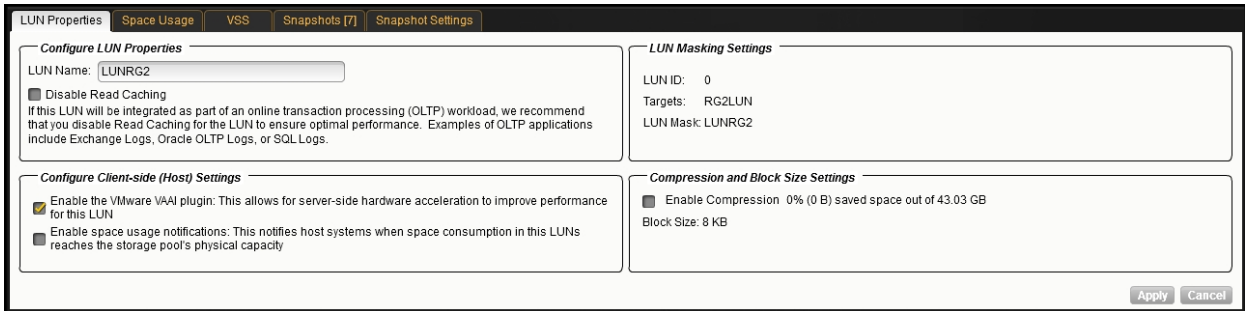
Unity uses [FASTier](#) Read cache devices when the RAM cache on the system is full. Read cached devices are filled as files as read (not written). For database OLTP LUNs, we recommend to disable read caching to increase performance.

When you create a LUN, FASTier Read caching is enabled by default. If you did not select the option to disable Read caching during LUN creation, you can disable it at any time afterwards using the LUN's properties panel.

► **To disable Read caching:**

1. In Unity's tree view, click the Site node.
2. Click the **Storage Pools** node.
3. Click the storage pool to which the LUN belongs.
4. Click the **LUNs** node.
5. Select the LUN for which you want to disable Read caching.
6. Expand the LUN's Properties panel.
7. Select the **LUN Properties** tab.

Figure 7-13: LUN's properties panel—LUN Properties tab



8. Select the **Disable read caching** option.
9. Click **Apply**.

Viewing space usage information for LUNs

Unity gives you a detailed overview of each LUN's used and available disk space. To modify space usage settings, see [Modifying LUN space settings](#) on page 229.

► **To access the LUNs node Properties panel:**

1. In Unity's tree view, click the Site node.
2. Click the **Storage Pools** node.
3. Click the storage pool containing the LUNs for which you want to view space usage information.
4. Expand the LUNs node's Properties panel. The **LUNs** tab displays a grid that lists all the LUNs in a storage pool.

Figure 7-14: LUNs node's properties panel—LUNs tab

Name	Committed space	Snapshots	Reserved S...	Volume Size	Thin Provisi...	Replication...	LUN ID	Target	Initiator Gro...	Block size	Compression
lunb	77.63 GB	27.16 GB	1 GB	3 TB	Enabled	true	0			32 KB	95.46% (1.59 TB)
lun2	16 KB	0 B		1 GB	Enabled	false	1		iqn.1991-05.com	8 KB	0% (0 B)

Tip Double-click a LUN in the grid to automatically open the LUN's properties panel and display its child nodes.

▶ **To sort the list:**

- Click the sort pointer in the **Name** column heading until the arrow points down for descending order, or until the arrow points up for ascending order.

▶ **Columns related to space usage:**

- **Committed space:** The amount of space that is currently consumed by the host, excluding snapshots and reservation.
- **Snapshots:** The amount of the space consumed by snapshots, including the reservation added for snapshots.
- **Reserved space:** The current setting for reservation. For thick LUNs, reserved space is the same as the volume size. For more information, see [Understanding disk space consumption on page 214](#)
- **Volume size:** The size of the volume, as it appears to hosts.
- **Thin Provisioning:** Shows whether the LUN is thin or thick: **Disabled** (thick LUN) or **Enabled** (thin LUN).
- **Compression:** Displays the percentage of compressed data and its equivalent in megabytes or terabytes.

Setting up host connectivity

Unity allows you to restrict access to LUNs on the system based on the (iSCSI or Fibre Channel) initiator name. In other words, only the iSCSI or Fibre Channel initiators that you specify for the LUN are allowed to connect to the LUN through its target.

For a LUN to be visible to a host, you must create a LUN Mask and add that LUN to the mask. The LUN Mask also allows you to add target initiators (iSCSI or Fibre Channel) and assign the LUN to a target. A mask may include multiple LUNs. However, a LUN can only be part of one mask.

The LUN mask enables you to organize LUNs according to your storage and access needs. For example, if you need to provision a new application, you can create a LUN mask to gather the LUNs that will support the application, the hosts on which the application will reside, and the group of target ports (iSCSI or Fibre Channel) through which the application will access storage.

When you create LUN Masks, they are created on both controllers by default. Upon cluster failover, the LUN Masks are still available on Unity.



CAUTION: Replication and LUN Masking

LUN Masks are not replicated on the secondary site. If you ever need to make a pool on the secondary site the primary pool, you must create one or more LUN Masks on the secondary site for that pool so that it can be accessed by the same hosts as the current primary pool.

▶ **To view LUN masks:**

- Under the Site node, click **Host Connectivity** node to display its properties panel. The LUN Masks properties panel allows you to view all LUN Masks currently created on Unity. By default the **LUN Masks** tab is selected. At a glance, you can view all associations of targets, LUNs, and initiators.

Figure 7-15: Host Connectivity properties panel—LUN Masks tab

Name	Targets	Storage Pools	LUNs	Initiators Groups
pool33	pool33	pool33		
mask1				
mask3	target3		lun33	
lin2	lin2	lin2		
maskiscsi	lin1	lin1	linlun3	iqn.tara.com
lin1	lin1, tg1	lin1		
Fibre Channel	Fibre Channel	<All>	lin1lun0, lin2lun1, plun0, lin1Lun7, linLun5,	

► **To view initiators:**

- Click the **Initiator Groups** tab. It displays all initiators currently added to Unity, their type, and their associated LUNs.

Figure 7-16: Host Connectivity properties panel—Initiator Groups tab

Groups	IQN/WWN	Type	LUNs
wsdp86.evertrust.lia	iqn.1991-05.com.microsoft:wsdp86.evertrust.1	iSCSI	lunwithmaskdiffe
wsdp99.evertrust.lan	iqn.1991-05.com.microsoft:wsdp99.evertrust.1	iSCSI	lun111
wsdp61.evertrust.lan	iqn.1991-05.com.microsoft:wsdp61.evertrust.1	iSCSI	l1; lunwithmaskandC; newLunFor11599
wsdp22.evertrust.lan	iqn.1991-05.com.microsoft:wsdp22.evertrust.1	iSCSI	l2
wsdp88.evertrust.lan	iqn.1991-05.com.microsoft:wsdp88.evertrust.1	iSCSI	lun111

Refer to these topics to configure LUN masking on Unity:

- [Creating an Initiator group below](#)
- [Modifying an Initiator group on the facing page](#)
- [Deleting an Initiator group on page 236](#)
- [Adding a LUN mask on page 237](#)
- [Modifying a LUN mask on page 239](#)
- [Deleting a LUN mask on page 242](#)
- [Viewing LUN Masking information for a LUN on page 243](#)

Creating an Initiator group

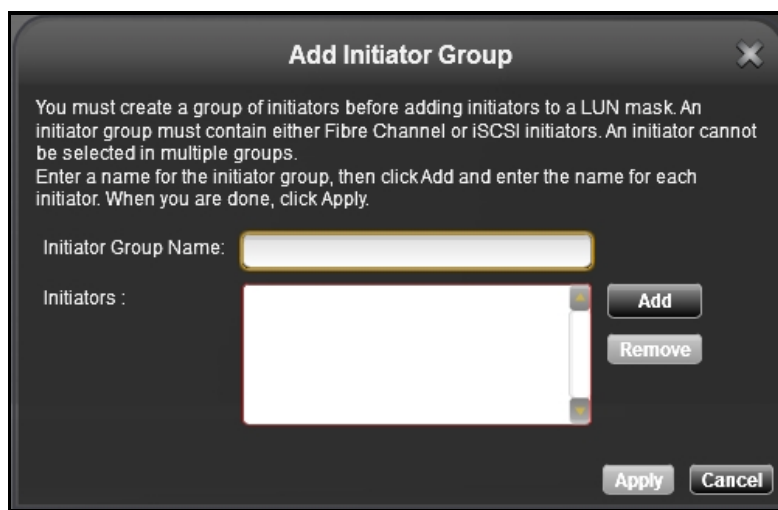
You must create a group of Initiators before adding initiators to a LUN mask. An initiator group must contain either Fibre Channel or iSCSI initiators. An initiator cannot be part of multiple groups.

► **To create an Initiator group:**

1. Under the Site node, click **Host Connectivity** node to display its properties panel.
2. Select the **Initiator Groups** tab. It displays all initiators currently added to Unity, their type, and their associated LUNs.

3. Click the **Add Initiator Group** button.

Figure 7-17: Add Initiator Group popup



4. Enter a name in the **Initiator Group Name** field.
5. Click **Add** to add an Initiator to the group.
6. Enter the Initiator IQN or WWN number:
 IQN format: `iqn.1999-05.com.microsoft:17bwmm1.nexsan.com`.
Tip To look for existing IQN numbers, see the iSCSI Target's properties panel—**Properties** tab. For targets that are connected but not defined on Unity, use the CLI command, `wwn`. This command will display all iSCSI targets connected to Unity.
7. Click **OK**.
8. Click **Add** again and repeat steps 6 and 7 for each Initiator to add to the group.
9. Click **Apply** to save your changes.

Modifying an Initiator group

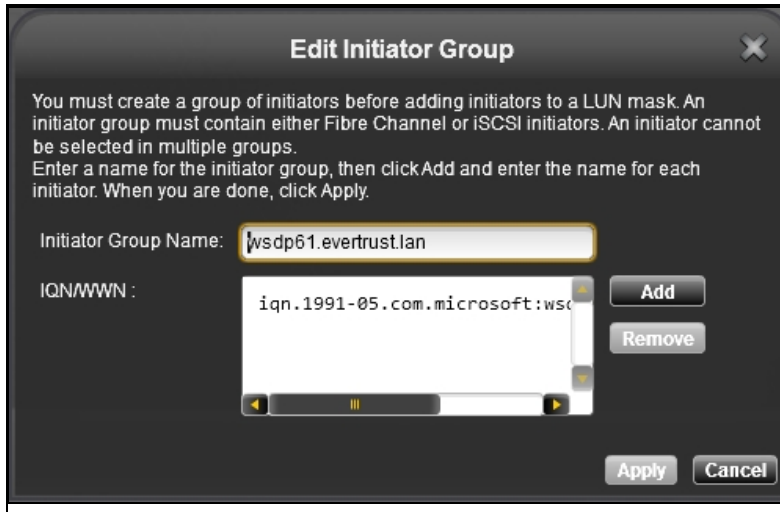
An initiator group must contain either Fibre Channel or iSCSI initiators. An initiator cannot be selected in multiple groups.

► **To modify an Initiator group:**

1. Under the Site node, click **Host Connectivity** node to display its properties panel.
2. Select the **Initiator Groups** tab. It displays all initiators currently added to Unity, their type, and their associated LUNs.
3. Select the Initiator Group to modify.

- Click the **Edit Initiator Group** button.

Figure 7-18: Edit Initiator Group popup



- Perform one or more of these actions:

To...	Do this
change the name	Enter a new name if the Initiator Group Name field.
add initiators	<ol style="list-style-type: none"> Click Add to add an Initiator to the group. Enter the Initiator IQN or WWN number: IQN format: <code>iqn.1999-05.com.microsoft:17bwmm1.nexsan.com</code>. Tip To look for existing IQN numbers, see the iSCSI Target's properties panel—Properties tab. For targets that are connected but not defined on Unity, use the CLI command, <code>wwn</code>. This command will display all iSCSI targets connected to Unity. Click OK. Repeat these steps for each Initiator to add to the group.
remove initiators	<ol style="list-style-type: none"> Select the IQN/WWN number of the Initiator to remove. Click Remove. Click OK. Repeat these steps for each Initiator to remove from the group.

- Click **Apply** to save your changes.

Deleting an Initiator group

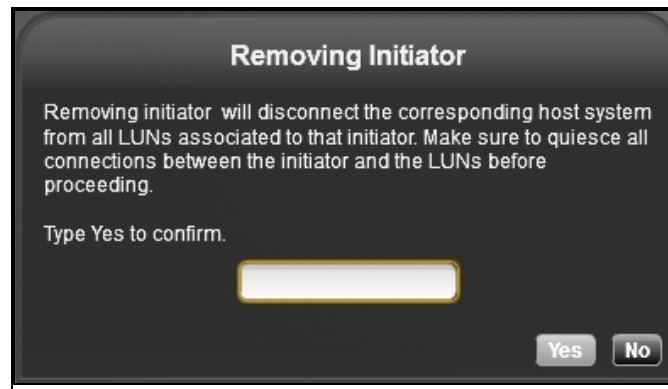
► **Before you begin:**

You must remove the Initiator group from all LUN Masks where it is used; see [Modifying a LUN mask on page 239](#). Removing an initiator group will disconnect the corresponding host systems from all LUNs associated to these initiators.

► **To create an Initiator group:**

1. Under the Site node, click **Host Connectivity** node to display its properties panel.
2. Select the **Initiator Groups** tab. It displays all initiators currently added to Unity, their type, and their associated LUNs.
3. Select the Initiator group to remove.
4. Click the **Delete Initiator Group** button.

Figure 7-19: Delete Initiator Group popup



5. Type **Yes** in the text field to confirm.
6. Click **Yes** to remove the Initiator group.

Adding a LUN mask

Before a LUN can be made visible to a host, you must create a LUN mask and assign that LUN to the mask. The LUN mask also allows you to add target initiators iSCSI (or Fibre Channel) and assign the LUN to a target. A mask may include multiple LUNs. However, a LUN can only be selected in one mask.

Notes:

- The mask will only display LUNs that have not been assigned to a target.
- Before creating a mask for iSCSI LUNs, you must create one or more iSCSI targets on the storage pool; see [Adding an iSCSI target](#) on page 288.
- LUN Masks are managed per site. If your storage pool is replicated, you must create corresponding LUN Masks on the remote site for the replica. This is so that the LUNs remain accessible in case of a failover.

► **To add a LUN mask:**

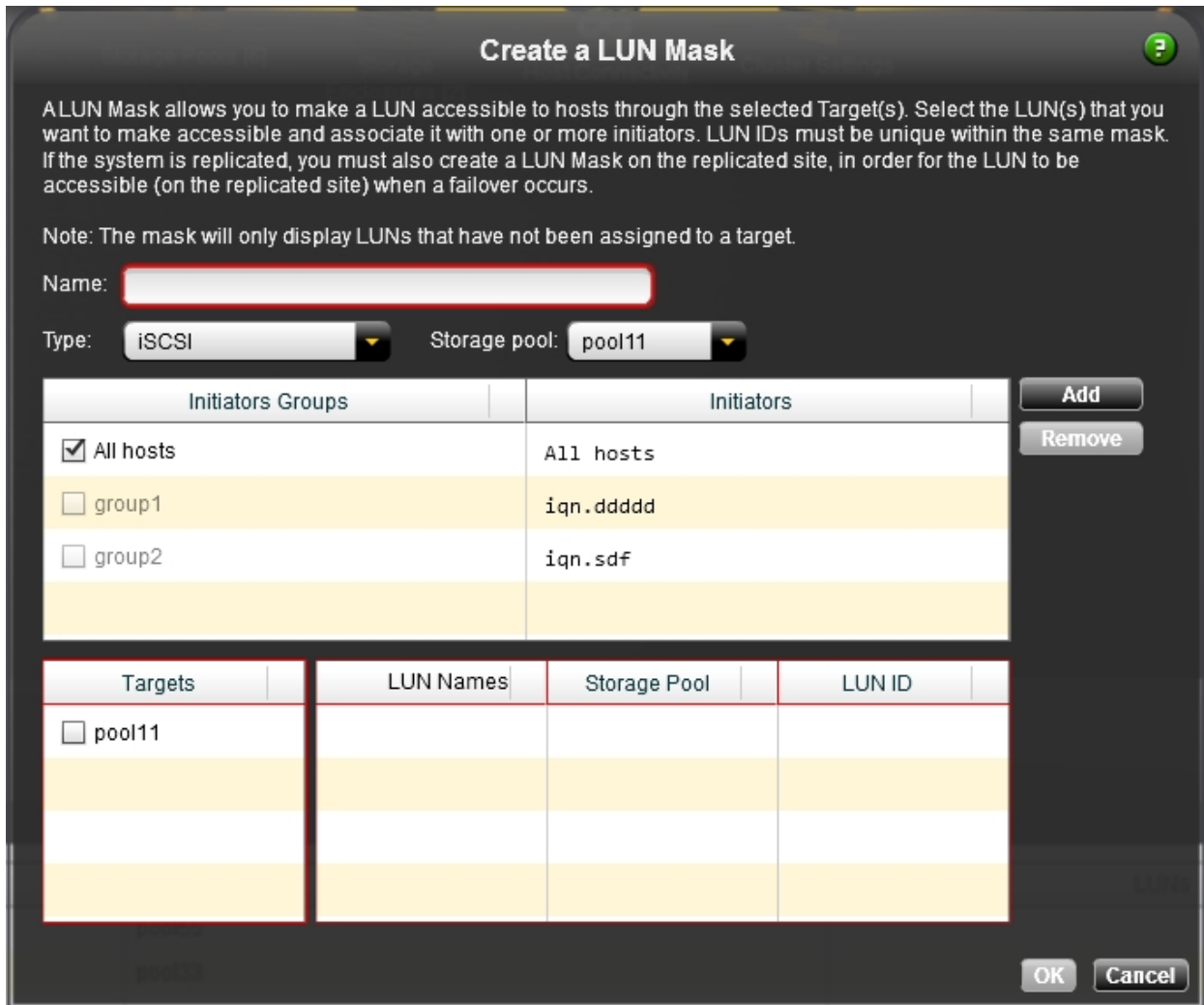
1. Click the Site node to display its child nodes.
2. Click the **Host Connectivity** node.

3. Perform one of these actions:

To...	Do this
use the LUN Masks context menu	<ol style="list-style-type: none"> a. Click the context menu button on the Host Connectivity node. b. When the node context menu opens, click Add a LUN Mask.
use the LUN Masks Properties panel	<ol style="list-style-type: none"> a. Expand the LUN Masks' Properties panel. b. Click the Add a LUN Mask button.

4. The Create a LUN Mask dialog box opens. Enter a meaningful name in the **Name** field.

Figure 7-20: Creating a LUN mask dialog box



5. From the **Storage Pool** drop-down list, select the name of the pool hosting the LUN(s) you will add to the mask. The list of targets in the **Targets** column gets automatically updated for the selected pool.
6. From the **Type** drop-down list, select **iSCSI** or **Fibre Channel**.

7

7. Under the **Initiators** list, **All hosts** is selected by default:
 - a. (Optionally) You can uncheck that option if you want to provide access to only selected initiators.
 - b. To add an Initiator Group, click the **Add** button. An initiator group must contain either Fibre Channel or iSCSI initiators. An initiator cannot be selected in multiple groups.

Figure 7-21: Add Initiator Group popup



- c. In the Add Initiator Group popup window, enter the IQN number.
 IQN format: `iqn.1999-05.com.microsoft:17bwmm1.nexsan.com`.
Tip To look for existing IQN numbers, see the iSCSI Target's properties panel—**Properties** tab. For targets that are connected but not defined on Unity, use the CLI command, `wwn`. This command will display all iSCSI targets connected to Unity.
 - d. Repeat the two steps above for each additional initiator.
 - e. Select one or more initiators.
 - f. Click **OK** to return to the Create a LUN Mask dialog box.
8. In the **Targets** column, select the desired targets. The LUNs present in the pool to which the target is associated become available for selection in the **LUN Names** column.
9. Select the LUN(s) that you want to make visible to the host.
10. Type a numeric value in the **LUN ID** field, or use the default value. The LUN ID is a number used to identify a LUN—from 0 to 254. Each LUN associated to the same target and the same initiators must have a unique LUN ID. However, if you associate each LUN to a different target or to different initiators (even if they are part of the same target), there is no need for the LUN IDs to be different. For LUN masking, the LUN ID has to be unique within the same mask.
11. Click **OK** to save your changes.

Modifying a LUN mask

You can modify these LUN mask settings:

- add new LUNs; available LUNs will depend on the target chosen as targets associated to a pool can only be used for LUNs associated to the same pool.
- rename LUN masks;
- assign new storage pools to the LUN mask;
- add or remove initiators;
- change target and LUN assignments;
- change LUN IDs.



CAUTION: Changing LUN Mask settings may impact connectivity to associated LUNs. Before proceeding, make sure to quiesce any connections between initiators that you plan to remove and their associated LUNs.

Notes:

- The mask will only display LUNs that have not been assigned to a target.
- Before editing a Mask for iSCSI LUNs, make sure all storage pools have iSCSI targets created; see [Adding an iSCSI target](#) on page 288.

▶ **To edit a LUN mask:**

1. Click the Site node to display its child nodes.
2. Click the **Host Connectivity** node.
3. Select the LUN Mask that you want to change.
4. Perform one of the following actions:

To...	Do this
use the LUN Mask context menu	<ol style="list-style-type: none"> a. Click the context menu button on the Host Connectivity node. b. When the node context menu opens, click Edit LUN Mask.
use the LUN Mask Properties panel	<ol style="list-style-type: none"> a. Expand the LUN Mask's Properties panel. b. Click the Edit LUN Mask button.

- The *Edit the LUN Mask* dialog box opens.

Figure 7-22: Editing the LUN Mask dialog box

Edit the LUN Mask ?

You can change any LUN Mask setting. If you remove an initiator associated to a LUN, make sure to assign this LUN to a new initiator. If you change the LUN ID, make sure it is unique within the mask. The mask will only display LUNs that have not been assigned to a target.

Note: Before editing a mask for iSCSI LUNs, make sure all storage pools have iSCSI targets created.

Warning: Changing LUN Masks settings may impact connectivity to associated LUNs. For example, clearing a selected initiator will disconnect the corresponding host system from the associated LUNs; make sure to quiesce the connection between the initiator and the LUNs before proceeding.

Name:

Type: Storage pool:

Initiators Groups	Initiators	
<input checked="" type="checkbox"/> All hosts	All hosts	<input type="button" value="Add"/> <input type="button" value="Remove"/>
<input type="checkbox"/> group1	iqn.ddddd	
<input type="checkbox"/> group2	iqn.sdf	

Targets	<input type="checkbox"/> LUN Names	Storage Pool	LUN ID
<input checked="" type="checkbox"/> pool99	<input type="checkbox"/> lun00_pool99	pool99	< 0 >
<input checked="" type="checkbox"/> t9	<input type="checkbox"/> lun01_pool99	pool99	< 0 >

6. Perform one or more of these actions:

To...	Do this
modify the LUN mask name	Enter a new name in the Name field.
change the storage pool	Select a new pool from the drop-down list. The list of targets in the Targets column gets automatically updated for the selected pool.
change the type	<ol style="list-style-type: none"> From the Type drop-down list, select iSCSI or Fibre Channel. Add initiators (see the procedure in the row below). Select targets from the Targets column. The LUNs present in the pool become available for selection in the LUN Names column. Select the desired LUNs from the LUN Names column. Enter the LUN ID. <p>Note LUN IDs must be unique within the same mask.</p>
add initiators	<ol style="list-style-type: none"> Click the Add button. In the Add Initiator pop-up window, enter the IQN number. IQN format: <code>iqn.1999-05.com.microsoft:17bwmm1.nexsan.com</code>. Tip To look for existing IQN numbers, see the iSCSI Target's properties panel—Properties tab. For targets that are connected but not defined on Unity, use the CLI command, <code>wwn</code>. This command will display all iSCSI targets connected to Unity. Repeat these steps for each additional initiator.
change initiators	<ul style="list-style-type: none"> In the Initiators list, uncheck one or more initiators and select other ones. If Everyone was selected, uncheck this option and select one or more initiators from the list.
change the LUN ID	Enter a new LUN ID for the selected LUN. Note LUN IDs must be unique within the same mask.

7. Click **OK** to save your changes.

Deleting a LUN mask

You can delete LUN masks at any time.



CAUTION: Deleting a LUN mask will make all associated LUNs inaccessible to their hosts. This will result in connection loss, and may also result in data loss. Make sure to quiesce all connections to the corresponding LUNs before proceeding.

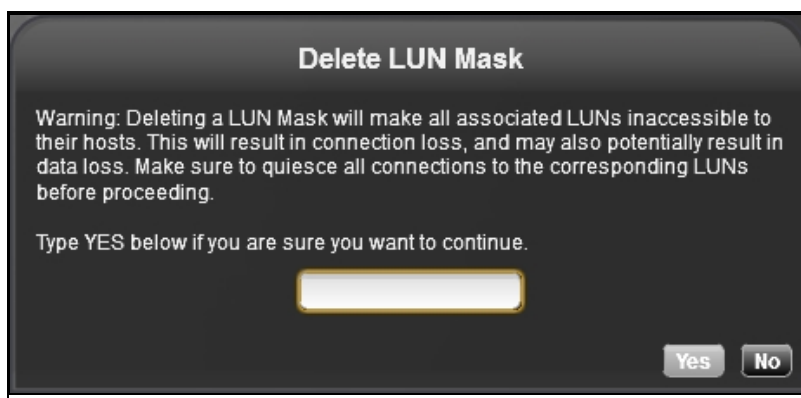
► **To delete a LUN mask:**

1. Click the Site node to display its child nodes.
2. Click the **Host Connectivity** node.
3. Perform one of these actions:

To...	Do this
use the LUN Masks properties panel	<ol style="list-style-type: none"> a. Expand the LUN Masks' Properties panel. b. Select the LUN Mask you want to delete from the LUN Masks tab. c. Click the Delete LUN Mask button.
use the LUN Mask Properties panel	<ol style="list-style-type: none"> a. Select the node of the LUN mask you want to delete. b. Expand the LUN Mask's Properties panel. c. Click the Delete LUN Mask button.

4. When prompted to confirm the action, type **Yes** in the text box.

Figure 7-23: Confirm LUN Mask deletion



5. Click the **Yes** button.

Viewing LUN Masking information for a LUN

The LUN Mask properties panel displays the initiators and their associated targets and LUNs. The same initiator can be used by multiple LUNs; likewise, a LUN can be accessed by multiple initiators. A LUN can also be associated to multiple targets. However, a LUN can only be selected in one LUN Mask, as opposed to initiators and targets.

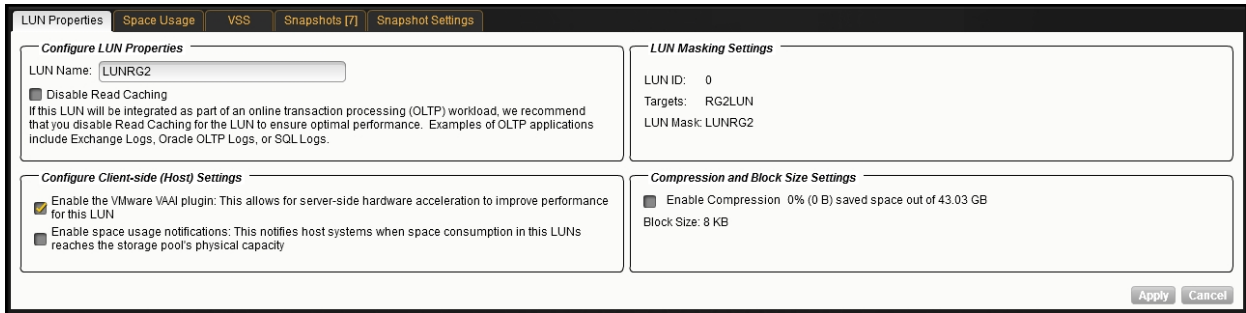
The LUN Mask's properties panel also allows you to edit or delete the LUN Mask. For procedural steps, see [Modifying a LUN mask](#) on page 239 and [Deleting a LUN mask](#) on the previous page.

► **To view LUN Mask information on a specific LUN:**

1. Click the **Storage Pools** node.
2. Select the pool hosting the LUN.
3. Select the **LUNs** node.
4. Select the node of the LUN for which you want to see LUN Masking information.

- Expand the LUN's properties panel. LUN Masking settings are displayed on the **LUN Properties** tab.

Figure 7-24: LUN's properties panel—LUN Properties tab



Adding an iSNS server

The Internet Storage Name Service (iSNS) protocol is designed to facilitate the automated discovery, management, and configuration of iSCSI devices on a TCP/IP network. You can configure iSCSI targets on Unity to use an iSNS server.

An iSNS server provides a central management point for LUNs on Unity by dynamically maintaining up-to-date information about their corresponding iSCSI target names.

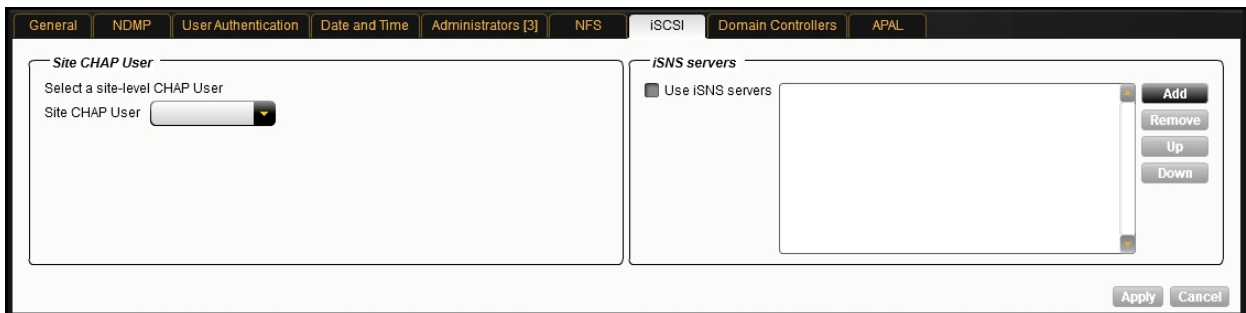
Note An iSNS server must already be set up and available on the network in order for Unity to access it.

Unity does not support the use of iSNS servers for Fibre Channel targets.

► **To add an iSNS server:**

- In Unity's tree view, click the Site node.
- Expand the Site node's Properties panel.
- Select the **iSCSI** tab.
- Select the **Use iSNS servers** option.

Figure 7-25: Site's properties panel—iSCSI tab



- Click the **Add** button.

- Enter the IP address of the iSNS server in the popup and click **OK**.

Figure 7-26: Adding an iSNS server popup



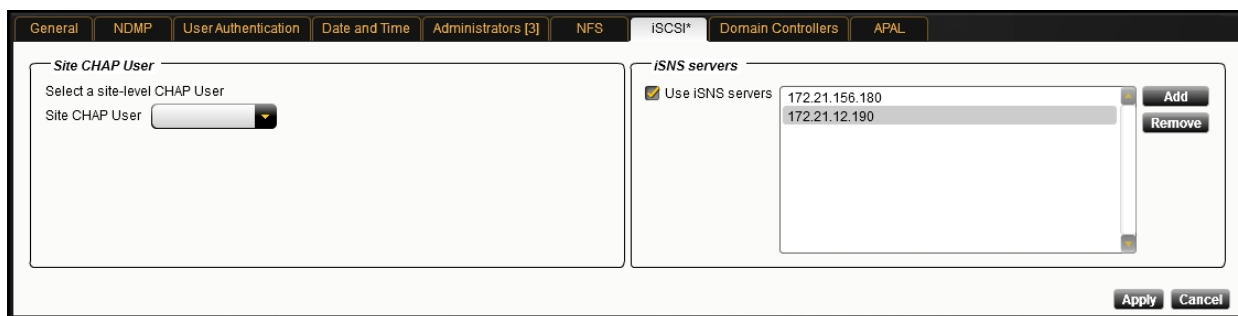
- Click **Apply**. All iSCSI targets on Unity will be managed by the specified iSNS server. For large networks, you can add additional iSNS servers.

Removing an iSNS server

► **To remove an iSNS server:**

- In Unity's tree view, click the Site node.
- Expand the Site node's Properties panel.
- Select the **iSCSI** tab.
- Select the IP address of the iSNS server to remove.

Figure 7-27: Site's properties panel—iSCSI tab



- Click the **Remove** button.
- Click **Apply**. The iSNS server is removed from Unity.

Managing snapshots for LUNs

Unity provides continuous data protection with the Snapshots feature, which allows you to capture, store, and access point-in-time copies of the data in your LUNs. Unity provides two ways for managing snapshots for LUNs:

- **Using the Snapshots node in Unity's tree view:**

You can enable browsing for a LUN's snapshot and then mount the browsed snapshot as an iSCSI volume just like you would the parent LUN. You can only connect to a LUN's snapshot using the corresponding storage pool's Management (mgmt) target, as opposed to the iSCSI target that you connect to the parent LUN through; for more information about the Management (mgmt) target, see [Adding a CHAP user to the Management target on page 259](#).

Once you connect to the browsed snapshot using the storage pool's Management (mgmt) target, you must set the corresponding volume as Online in Windows *Disk Management*.

- **Using Unity's VSS Hardware Provider:**

The VSS Hardware Provider enables a VSS host to create and manipulate shadow copies (point-in-time snapshots) of the data in LUNs on Unity. The VSS Hardware Provider supports Windows Volume Snapshot Service (or Volume Shadow Copy Service).

This section includes these topics:

[Using the LUN's Properties panel to manage LUN snapshots](#) below

[Using Windows VSS](#) on page 259

[Using both Nexsan Unity and VSS Hardware Provider to manage LUN snapshots](#) on page 279

Using the LUN's Properties panel to manage LUN snapshots

The LUN's Properties panel lists all the snapshots for the corresponding LUN; it also provides options and settings for configuring the snapshots schedule, taking manual snapshots, enabling and disabling snapshot browsing, and deleting snapshots.

▶ **To access the Snapshots tabs for a LUN:**

1. In Unity's tree view, click the Site node.
2. Click the **Storage Pools** node.
3. Click the storage pool containing the LUN for which you want to manage Snapshots.
4. Click its **LUNs** node.
5. Click the LUN for which you want to manage Snapshots.
6. Expand the LUN's properties panel.

The LUN's Properties panel includes two tabs for snapshots:

- [Snapshots tab](#) on page 249
- [Snapshot Settings tab](#) on page 251

Introduction to snapshots

A snapshot is a read-only copy of a share/LUN at a specific point in time. Think of a snapshot as a frozen image of the data in a share/LUN at the time the snapshot is recorded. You can use snapshots to maintain a set of previous versions of all the files in a share/LUN, which can serve as temporary backups of your data.

For example, if a set of files in a share/LUN are accidentally (or maliciously) deleted or overwritten, you can easily restore individual files from a snapshot of the share/LUN by browsing the snapshot (and accessing it from a Windows-based (CIFS) system and/or a UNIX/Linux-based (NFS) system). Or, if all the data in a share/LUN becomes corrupted, you can restore the data to a specific point-in-time snapshot using the rollback function.

Unity allows you to take manual snapshots of a share/LUN and also set a schedule for automatic snapshots. You can create a separate snapshots schedule for each share/LUN on Unity.

Snapshot concepts and terminology

This table describes replication concepts and terminology used in Unity.

Table 7-4: Snapshot concepts and terminology

Snapshot terminology	Description
Snapshot	<p>A snapshot is a read-only copy of a share/LUN at a specific point in time. You can use snapshots to maintain a set of previous versions of all the files in a share/LUN, which can serve as temporary backups of your data.</p> <p>The snapshot is created almost instantly, and initially consumes no additional disk space within the storage pool where the share/LUN resides. When data within the share/LUN changes—new data is added or existing data is updated—the snapshot maintains a reference to the previous copy of the data, and Unity updates the snapshot size accordingly. The Unity protects the file's original data blocks from being overwritten; it stores the new updates in a new location. The Unity maintains records and pointers to keep track of the data and file changes.</p> <p>This results in minimal disk space consumption and also allows for rapid recovery of data in case of a disk write error, a corrupted file, or a program malfunction.</p>
Automatic snapshot, or scheduled snapshots	<p>Unity takes periodic snapshots according to the schedule you define. Typically, you set a snapshot schedule when you initially create the share or LUN. You can then modify or disable the schedule in Unity.</p> <p>▶ Related topics:</p> <ul style="list-style-type: none"> ● Setting a schedule for automatic LUN snapshots on page 252 ● Setting a schedule for automatic file system snapshots on page 197
Manual snapshot	<p>You can take manual snapshots of a share or LUN at any time, even if you have automatic snapshots enabled. Manual snapshots allows you to record a copy of the dataset contents at any point in time.</p> <p>▶ Related topics:</p> <ul style="list-style-type: none"> ● Taking a manual LUN snapshot on page 253 ● Taking a manual file system snapshot on page 198
Browsing a snapshot, or mounting a snapshot	<p>Unity provides a mechanism that allows you to access a snapshot from a Windows-based system and/or a UNIX/Linux-based system and browse its contents—in the same way that you access a share or a LUN. A snapshot that you browse is a read-only copy of its parent share/LUN and its contents mirror the parent share/LUN's contents at the time the snapshot is recorded.</p> <p>You can use Unity's snapshot browsing mechanism to recover individual files from a snapshot in case the files are accidentally deleted or overwritten, or corrupted in the snapshot's parent share/LUN. Unity maintains all of the parent share/LUN's access-level attributes with the snapshots to ensure any recovery is authorized. This means that you can safely authorize all users—</p>

Snapshot terminology	Description
Rollback	<p>that have access to the share/LUN—to browse a snapshot and recover their own lost data from the snapshot.</p> <p>▶ Related topics:</p> <ul style="list-style-type: none"> ● Browsing a file system snapshot on page 199 ● Browsing a LUN snapshot on page 254 ● Browsing a VSS snapshot on page 273 ● Browsing replicated datasets and snapshots on page 439 <hr/> <p>The Unity allows you to roll back all the data in a share/LUN to a specific point-in-time snapshot of the share/LUN. The rollback function reverts a share/LUN's contents to what they were at the time the snapshot was taken, including all file- and folder-level permission settings and share/LUN-level access attributes. This function also automatically deletes all snapshots that are newer than the snapshot that you roll back to, including snapshots that have browsing enabled.</p> <p>Unity provides the rollback function for extreme circumstances: for example, if all the data in a share/LUN is corrupted and can no longer be recovered. The rollback function overwrites all the existing data in the share/LUN with the contents of the snapshot that you roll back to; any new data that was added after the snapshot is recorded, including updates to existing data, is lost during the rollback process.</p> <p>▶ Related topics:</p> <ul style="list-style-type: none"> ● Rolling back the data in a share to a snapshot on page 202 ● Rolling back data in a LUN to a snapshot on page 256 ● Rolling back data to a VSS snapshot on page 276
VSS , or Microsoft Volume Shadow Copy Service, Volume Snapshot Service, Volume Shadow Copy Service	<p>Microsoft Volume Shadow Copy is a technology included in Microsoft Windows that allows you to take manual or automatic backup copies or snapshots of data.</p> <p>If the Unity is joined to a Microsoft Active Directory domain, Unity automatically exposes all the snapshots for each share/LUN on the Unity to Microsoft Windows (CIFS) clients that access the share/LUNs—provided the Windows client computers support Microsoft VSS.</p> <p>You can then use Microsoft VSS on the Windows client computers to restore previous versions of files and folders from a snapshot of a share/LUN, or roll back a share/LUN to a specific point-in-time snapshot.</p> <p>▶ Related topics:</p> <ul style="list-style-type: none"> ● Using Windows VSS on page 259

Snapshots tab

The **Snapshots** tab displays a grid that lists all the snapshots recorded for the corresponding LUN.

Figure 7-28: LUN's properties panel—Snapshots tab

Browsing status	Name	Date	Time	Size	Type
	auto_2015-07-01-005955	2015/07/01	1:00:00 AM	0 B	Automatic
	auto_2015-07-02-005936	2015/07/02	12:59:00 AM	0 B	Automatic
	auto_2015-07-03-005915	2015/07/03	12:59:00 AM	0 B	Automatic
	auto_2015-07-04-005837	2015/07/04	12:58:00 AM	0 B	Automatic
	auto_2015-07-05-005838	2015/07/05	12:58:00 AM	0 B	Automatic

The grid shows this information for each snapshot:

- **Browsing status:** this column indicates whether or not browsing is enabled for the snapshot; it displays one of these icons:



Browsing is enabled



Browsing is disabled

- **Name:** this column displays the snapshot's name; the name displayed in this column varies depending on whether the snapshot is a scheduled (automatic) snapshot or a manual snapshot:
 - For a scheduled (automatic) snapshot, the snapshot name is prefixed with `auto_` and includes the date and time the snapshot is recorded; for example: Unity assigns this name for a scheduled snapshot recorded on June 15, 2011 at 1:01 AM: `auto_2011-06-15-010100`.
 - For a manual snapshot, the name can be a value that you define when taking the snapshot, or if you use the default snapshots naming convention, the name is prefixed with `manual_` and includes the date and time the manual snapshot is recorded; for example: if you take a manual snapshot on June 15, 2011 at 1:01 PM and you use the default snapshots naming convention, Unity assigns this name to the snapshot: `manual_2011-06-15-130101`.

If you are using VSS to manage your LUN snapshots, Unity displays the name with the `vss` prefix, as follows: `vss_client_FinancePool1`. For group snapshots, the naming convention adds `_grp`: `vss_grp_client_FinancePool1`. For information on VSS snapshots, see [Using Windows VSS on page 259](#).

- **Date:** this column displays the date the snapshot is recorded.
- **Time:** this column displays the time the snapshot is recorded.

Note Unity converts the date and time to local format; that is, the date and time on the system where Unity is currently running.
- **Size:** this column displays the size of the snapshot. When a snapshot is recorded it initially consumes no disk space; however, as data within the snapshot's parent LUN changes—for example, new data is added or existing data is updated—Unity updates the snapshot size accordingly.
- **Type:** this column indicates whether the snapshot is an **Automatic** (scheduled) or **Manual** snapshot.

Sorting the list of snapshots

You can sort the list of snapshots displayed in the grid in either ascending or descending (alphabetical) order by clicking the sort pointer in the **Name** column heading.



▶ **To sort the list in descending order:**

- Click the sort pointer until the arrow points down.

▶ **To sort the list in ascending order:**

- Click the sort pointer until the arrow points up.

You can also sort by **Browsing status**, **Date**, **Time**, **Size**, and **Type**; or a combination of **Name**, **Browsing status**, **Date**, **Time**, **Size**, and **Type**, in any particular sort order that you want: 1, 2, and 3.

For example, to sort by **Date** first, and **Name** second:

1. Click the sort pointer in the **Date** column heading until **1** is displayed (with the arrow pointing either up for ascending order, or down for descending order).
2. Click the sort pointer in the **Name** column heading until **2** is displayed (with the arrow pointing either up for ascending order, or down for descending order).

7

Filtering snapshots in the grid

You can filter the snapshots displayed in the grid by **Browsing status**, **Name**, **Date**, **Time**, **Size**, and **Type**, and you can also filter the snapshots to only display snapshots recorded within a specific time period.

To...	Do this
only display snapshots recorded within a specific time period	<ol style="list-style-type: none"> 1. Click the From date field above the snapshots grid, and select a starting date for the time period that you want to display snapshots from. <div style="border: 1px solid #ccc; padding: 2px; margin: 5px 0;"> From <input type="text" value="2011/06/07"/> To <input type="text" value="2011/06/08"/> </div> 2. Click the To date field, and select an end date for the time period.
only display snapshots with a specific Browsing status	<ol style="list-style-type: none"> 1. Open the drop-down list above the Browsing status column heading in the grid. 2. Select the browsing status (Browsing enabled or Browsing disabled) that you want to display snapshots for in the grid. The default filter setting is All.
only display snapshots of a specific type	<ol style="list-style-type: none"> 1. Open the drop-down list above the Type column heading in the grid. 2. Select the type (Manual or Automatic) that you want to display snapshots for in the grid. The default filter setting is All.
filter snapshots further	Combine filter settings. For example, if you only want to display snapshots that have Browsing enabled , of type Automatic , and which were recorded between May 15, 2015 and May 18, 2015, set these filter settings in the grid:

To...	Do this
	<ol style="list-style-type: none"> 1. Click the From date field above the snapshots grid, and select May 15 in the calendar. 2. Click the To date field, and select May 18 in the calendar. Unity filters the grid to only display snapshots recorded within the specified time period. 3. Open the drop-down list above the Browsing status column heading in the grid and select Browsing enabled. Unity filters the grid to only display snapshots that you enabled browsing for. 4. Open the drop-down list above the Type column heading in the grid and select Automatic. Unity filters the grid again to only display scheduled (automatic) snapshots.

Note To reset filter settings in the grid, click another node in Unity's tree view and then return to the Snapshots Properties panel by clicking the corresponding Snapshots node. All filter options in the grid revert to their default settings.

Searching for a specific snapshot in the grid

You can search for a specific snapshot in the grid by **Name**, **Date**, **Time**, or **Size**, simply by entering a search string in the text boxes above the corresponding column headings.

► **To search for a specific snapshot in the grid:**

- Enter a search string in the text boxes above the **Name**, **Date**, **Time**, or **Size** column headings.

For example, if you want to search for all snapshots that are 0 B in size, simply enter 0 in the text box above the **Size** column heading.

Figure 7-29: LUN's properties panel—Snapshots tab

Browsing status	Name	Date	Time	Size	Type
	auto_2015-07-01-005955	2015/07/01	1:00:00 AM	0 B	Automatic
	auto_2015-07-02-005936	2015/07/02	12:59:00 AM	0 B	Automatic
	auto_2015-07-03-005915	2015/07/03	12:59:00 AM	0 B	Automatic
	auto_2015-07-04-005837	2015/07/04	12:58:00 AM	0 B	Automatic
	auto_2015-07-05-005838	2015/07/05	12:58:00 AM	0 B	Automatic

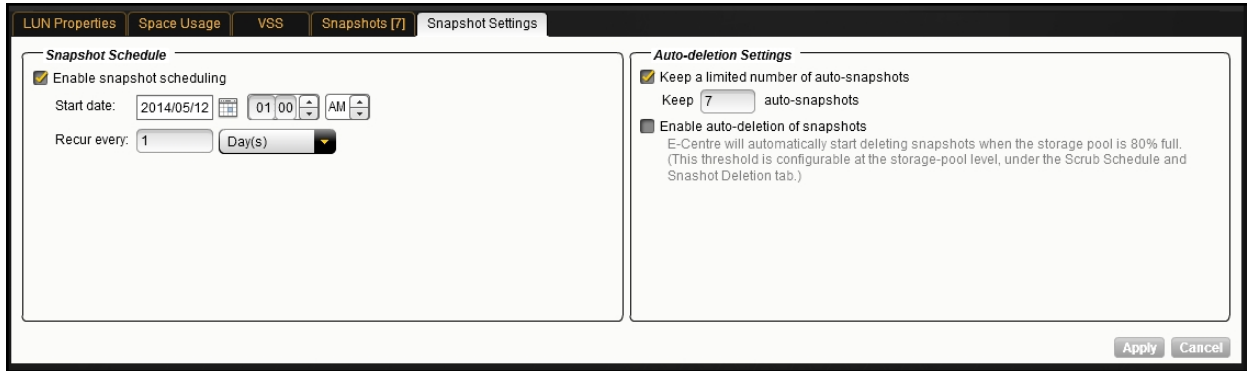
Snapshot Settings tab

The Snapshot **Settings** tab provides options for configuring a snapshots schedule and for specifying auto-deletion settings for snapshots.

When you set a snapshots schedule, Unity automatically takes periodic snapshots of the LUN according to the schedule you define; for more information, see [Setting a schedule for automatic LUN snapshots on the next page](#).

Auto-deletion settings allow you to specify the maximum number of snapshots that you want Unity to keep on the system for the corresponding LUN. These settings only apply to scheduled (automatic) snapshots. For more information, see [Setting auto-deletion settings for LUN snapshots](#) on page 258.

Figure 7-30: LUN's properties panel—Settings tab



Setting a schedule for automatic LUN snapshots

This section describes how to take automatic LUN snapshots. For instructions on taking a manual snapshot, see [Taking a manual LUN snapshot](#) on the facing page.

When you set a snapshots schedule, Unity automatically takes periodic snapshots of the LUN according to the schedule you define. Typically, you set a snapshots schedule when you initially create the LUN. You can then modify or disable the schedule in the Settings tab of the Snapshots Properties panel.

► **To set or modify a schedule for automatic snapshots:**

1. In Unity's tree view, click the Site node to display its child nodes.
2. Click the **Storage Pools** node.
3. Click the storage pool containing the LUN for which you want to set a snapshots schedule.
4. When the storage pool's child nodes are displayed, click its **LUNs** node.
5. Click the LUN for which you want to set a snapshots schedule.
6. Expand the LUN's properties panel.

7. Click the **Snapshot Settings** tab and configure the snapshots schedule for the LUN:
 - a. Select the **Enable scheduling** option to enable snapshots scheduling. This option is selected by default. Clearing the check box disables snapshot scheduling.
 - b. Adjust the snapshots schedule according to your preference. If you did not change the snapshots schedule for the LUN when you initially created the LUN, the default setting is once a day at 1 AM, with the start date set to the current date on Unity. This means that Unity will take an automatic snapshot of the LUN at 1 AM every day starting on the current date.
 - Specify the start date for the schedule by clicking the **Start date** field and selecting a date from the calendar.
 - Specify a recurrence pattern for the schedule by typing a value in the **Recur every** field.
 - Select the recurrence type from the drop-down list: **Minutes(s)**, **Hour(s)**, **Day(s)**, **Week(s)**, or **Month(s)**.
 - c. Click the **Apply** button to save your settings.

If you set the current date (or today's date) as the start date for the schedule, Unity takes an automatic snapshot of the LUN immediately after you set the schedule. Thereafter, Unity takes an automatic snapshot of the LUN according to the schedule you specify.

Note By default, Unity refreshes site information every 5 minutes; as a result, a scheduled snapshot that Unity records may not be immediately visible in the snapshots grid. You can manually refresh the list of snapshots displayed in the grid by clicking the **Refresh List** button on the **Snapshots** tab.

Taking a manual LUN snapshot

You can take manual snapshots of a LUN at any time, even if you have scheduled (automatic) snapshots enabled. This mechanism allows you to record a copy of the contents of a LUN at any point in time. For instructions on taking automatic snapshots, see [Setting a schedule for automatic LUN snapshots](#) on the [previous page](#).

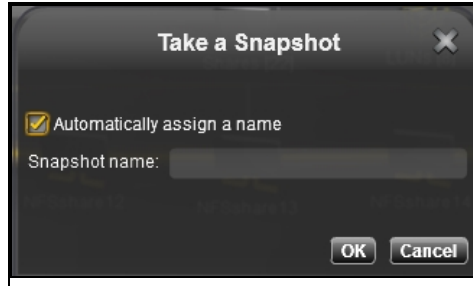
► **To take a manual snapshot:**

1. In Unity's tree view, click the **Site** node.
2. Click the **Storage Pools** node.
3. Click the storage pool containing the LUN for which you want to take a snapshot.
4. Click the **LUNs** node.
5. Click the LUN for which you want to take a snapshot.
6. Expand the LUN's properties panel.

- Click the **Take a Snapshot** button. Unity displays the Take a Snapshot dialog box.

Note You can also open this dialog box by opening the LUN node 's context menu and selecting **Take a Snapshot**.

Figure 7-31: Take a Snapshot dialog box



To...	Do this
specify a name for the manual snapshot	<ol style="list-style-type: none"> Clear the Automatically assign a name option (selected by default) and type a name for the snapshot in the Snapshot name field. When setting a name for a manual snapshot, the same naming restrictions apply as when you specify a name for a LUN. Click the OK button to set the name and close the Take a Snapshot dialog box. <p>Unity immediately takes a snapshot and adds it to the snapshots grid.</p>
To let Unity automatically assign a name to the manual snapshot	<ol style="list-style-type: none"> Make sure the Automatically assign a name option is selected (default selection). Click the OK button to close the Take a Snapshot dialog box. <p>Unity immediately takes a snapshot of the LUN and adds the manual snapshot to the snapshots grid. The snapshot is assigned a default name that is prefixed with <code>manual_</code> and includes the date and time the manual snapshot is recorded; for example: if you take a manual snapshot on May 15, 2013 at 1:01PM, Unity assigns this name to the snapshot: <code>manual_2013-06-15-130101</code></p>

Browsing a LUN snapshot

Setting [browsing for a snapshot](#) allows you to access the snapshot from a LUN and browse its contents—in the same way that you access a LUN.

You can use Unity's snapshot browsing mechanism to recover individual files from a snapshot in case the files are accidentally deleted or overwritten, or corrupted in the snapshot's parent LUN. Unity maintains all of the parent LUN's access-level attributes with the snapshot to ensure any recovery is authorized. This means that you can safely authorize all users—that have access to the LUN—to browse a snapshot of the LUN and recover their own lost data from the snapshot.



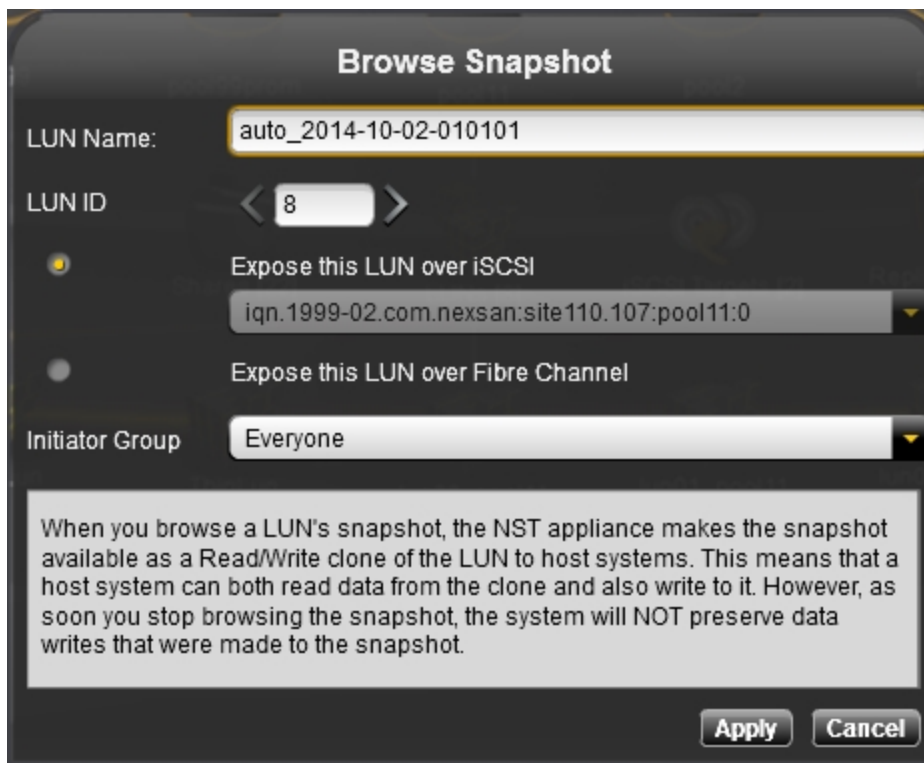
CAUTION: When you browse a LUN's snapshot in Unity, Unity makes the snapshot available as a Read/Write clone of the LUN to host systems. This means the host system can both read data from the clone and also write to it. However, as soon as you stop browsing the snapshot, Unity will NOT preserve data writes that were made to the snapshot. Therefore, it is important to ensure that you employ browsed LUN snapshots as read-only copies, and avoid writing new data to the snapshots.

Note If browsing for this snapshot is already enabled from the VSS Hardware Provider, the icon will display a status of browsing. For further details, see [Browsing a VSS snapshot](#) on page 273.

► **To set browsing for a snapshot:**

1. In Unity's tree view, click the **Site** node.
2. Click the **Storage Pools** node.
3. Click the storage pool containing the LUN for which you want to browse a snapshot.
4. When the storage pool's child nodes are displayed, click its **LUNs** node.
5. Click the LUN containing the snapshot that you want to browse.
6. Expand the LUN's properties panel.
7. Select the **Snapshots** tab. The Snapshots tab displays a grid that lists all the snapshots—both automatic (scheduled) and manual snapshots—that exist on the system for the LUN.
8. Highlight the snapshot that you want set browsing for by selecting the snapshot in the grid.
9. Click the **Browse Snapshot** button. Unity displays the Browse Snapshot dialog box where you specify the name that you and your users will use to access the snapshot, as well as the exposition method (iSCSI or Fibre Channel).

Figure 7-32: Browse Snapshot dialog box—LUN



Browse Snapshot

LUN Name: auto_2014-10-02-010101

LUN ID: < 8 >

Expose this LUN over iSCSI

iqn.1999-02.com.nexasan:site110.107:pool11:0

Expose this LUN over Fibre Channel

Initiator Group: Everyone

When you browse a LUN's snapshot, the NST appliance makes the snapshot available as a Read/Write clone of the LUN to host systems. This means that a host system can both read data from the clone and also write to it. However, as soon you stop browsing the snapshot, the system will NOT preserve data writes that were made to the snapshot.

Apply Cancel

10. Specify a browsing name for the snapshot and set its sharing method:
 - a. In the **LUN name** field, type a browsing name for the snapshot.

The name must start with an (upper-case or lower-case) alphabetic or numeric character; and, with the exception of the hyphen (-), and period (.), the name can only contain alphanumeric characters, without spaces.

These characters are NOT allowed:

“ / \ [] : ; | = , + * ? < >
 - b. Select the sharing method that you want to use to expose the snapshot to client computers on the network:
 - To expose the snapshot over iSCSI, select the **Expose this snapshot over iSCSI** option.
 - To expose the snapshot over Fibre Channel, select the **Expose this snapshot over Fibre Channel** option.
 - c. Click **Apply** to save your settings and close the Browse Snapshot dialog box.

Unity enables browsing for the snapshot. When complete, the **Browsing status** column in the snapshots grid displays the browsing enabled icon for the snapshot. If you mouse over the browsing enabled icon, Unity displays a Tool Tip identifying the browsing name that you set for the snapshot.

Note When you select a snapshot that has browsing enabled in the snapshots grid, the **Browse** button changes to **Stop browsing**.

7

Stopping LUN snapshot browsing

▶ **To disable browsing for a snapshot:**

1. In Unity's tree view, click the **Site** node.
2. Click the **Storage Pools** node.
3. Click the storage pool containing the parent LUN of the snapshot for which you want to disable browsing.
4. When the storage pool's child nodes are displayed, click its **LUNs** node.
5. Click the LUN containing the snapshot for which you want to disable browsing.
6. Expand the LUN's properties panel.
7. Select the **Snapshots** tab. The **Snapshots** tab displays a grid that lists all the snapshots—both automatic (scheduled) and manual snapshots—that exist on the system for the LUN.
8. Highlight the snapshot that you want to disable browsing for by selecting the snapshot in the grid.
9. Click the **Stop browsing** button.

Note The **Stop browsing** button is only displayed if you select a snapshot in the grid that has browsing enabled.

The **Browsing status** column in the snapshots grid displays the browsing disabled icon for the snapshot.

Rolling back data in a LUN to a snapshot

The rollback function reverts a LUN's contents to what they were at the time the snapshot was taken, including all file- and folder-level permission settings and access-level attributes. This function also automatically deletes all snapshots that are newer than the snapshot that you roll back to, including all manual snapshots of the LUN and snapshots that have browsing enabled.



CAUTION: Unity rolls back all the data in the LUN to the contents of the snapshot. This includes all file- and folder-level permission settings and LUN-level access attributes as they were when the snapshot was recorded. Additionally, Unity deletes all snapshots that are newer than the snapshot that you roll back to, including all manual snapshots of the LUN and snapshots that have browsing enabled.

► **Before you begin:**

Before rolling back a LUN, you must set the corresponding volume as offline. The steps to do this differ depending on whether the LUN is managed by VMware or by a Windows host.

For a LUN managed by VMware:

1. Power off all virtual machines hosted on the LUN.
2. Roll back the snapshot.
3. Rescan the datastores.
4. Power on the virtual machines hosted on the LUN.

For a LUN managed by Windows, set the corresponding volume as offline in Windows.

► **To roll back the data to a point-in-time snapshot:**

1. In Unity's tree view, click the **Site** node.
2. Click the **Storage Pools** node.
3. Click the storage pool containing the LUN that you want to roll back.
4. When the storage pool's child nodes are displayed, click its **LUNs** node.
5. Click the LUN containing the snapshot that you want to roll back to.
6. Expand the LUN's properties panel.
7. Select the **Snapshots** tab to display a grid that lists all the snapshots—both automatic (scheduled) and manual snapshots—that exist on the system for the LUN.
8. Highlight the snapshot that you want to roll back to by selecting the snapshot in the grid.
9. Click the **Rollback** button. Unity displays a confirmation dialog box.
10. Type **Yes** in the text box.
11. Click the **Yes** button.

Deleting LUN snapshots manually

This section describe how to delete snapshots for a LUN. You can delete both manual snapshots and automatic (scheduled) snapshots. For instructions to delete snapshots automatically, see [Setting auto-deletion settings for LUN snapshots](#) on the next page.

► **To manually delete snapshots for a LUN:**

1. In Unity's tree view, click the **Site** node.
2. Click the **Storage Pools** node.
3. Click the storage pool containing the LUN from which you want to delete snapshots.
4. Click the **LUNs** node.
5. Click the LUN from which you want to delete snapshots.
6. Expand the LUN's properties panel.

7. Select the **Snapshots** tab. The **Snapshots** tab displays a grid that lists all the snapshots—both automatic (scheduled) and manual snapshots—that exist on the system for the LUN.
8. Highlight the snapshot that you want to delete by selecting it in the grid. You can also select multiple snapshots: hold down SHIFT or CTRL and click the left mouse button; or, to select all the snapshots in the grid, click the **Select All** button.
9. Click the **Snapshot** button.
10. Unity prompts you to confirm deletion; click **Yes** to continue.

Setting auto-deletion settings for LUN snapshots

Auto-deletion settings allow you to specify the maximum number of snapshots that you want Unity to keep on the system for the corresponding LUN. For example, to keep only 7 snapshots on the system for the LUN, set the auto-deletion setting to 7; Unity automatically deletes the first, or oldest snapshot on the system when it records the next scheduled (or eighth) snapshot.

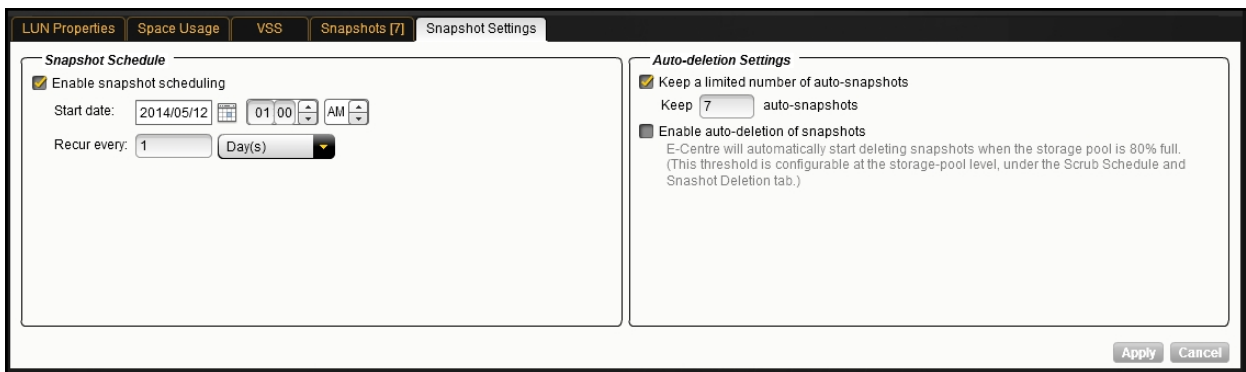
You can also enable automatic deletion of snapshots when space usage in the storage pool reaches 80% of its total capacity. Auto-deletion settings only apply to scheduled (automatic) snapshots; Unity does not automatically delete manual snapshots. The snapshot auto-deletion threshold is configurable at the storage pool-level; see [Modifying the snapshot auto-deletion setting for a storage pool](#) on page 112.

Note Snapshot auto-deletion settings are configured from the primary LUN only. If the LUN is replicated, the snapshots will also be automatically deleted from its replica using the same threshold, during a subsequent replication session.

▶ **To set auto-deletion settings for snapshots:**

1. In Unity's tree view, click the **Site** node.
2. Click the **Storage Pools** node.
3. Click the storage pool containing the LUN for which you want to set auto-deletion settings.
4. Click the **LUNs** node.
5. Click the LUN for which you want to set auto-deletion settings.
6. Expand the LUN's properties panel.
7. Select the **Snapshot Settings** tab.

Figure 7-33: LUN's properties panel—Snapshot settings tab



8. Under **Auto-deletion Settings**, select the **Keep a limited number of auto-snapshots** option (default setting).

9. Type a value in the **Keep auto-snapshots** field. For example, if you want Unity to keep only 5 snapshots on the system, type 5 in the field.
10. Optionally, if you want Unity to automatically delete snapshots when the used space in the storage pool reaches 80% of its total capacity, select the **Enable auto-deletion of snapshots** option. When this option is enabled, Unity automatically deletes snapshots for the LUN—starting with the oldest snapshot—until used space in the storage pool drops below 80%.

Using Windows VSS

Unity's VSS Hardware Provider serves as the interface between Windows Volume Shadow Copy Service running on a host system and Unity. Upon receiving instructions from a VSS host to create, mount, and restore snapshots, the VSS Hardware Provider sends the appropriate commands to Unity and returns the result of these commands to the host.

Note The VSS Hardware Provider supports both iSCSI and Fibre Channel LUNs.

► Prerequisites:

You must install the VSS Hardware Provider on a Windows Server host; it can be installed on any of the following operating systems:

- Windows Server 2016
- Windows Server 2012
- Windows Server 2008 R2
- Windows Server 2008
- Windows Server 2003 R2

Adding a CHAP user to the Management target

When you add a storage pool to Unity, the system assigns the storage pool a Management (mgmt) target, by default.

Unity's VSS Hardware Provider connects to a storage pool's Management target via iSCSI to view, create, and manage snapshots of all LUNs in the storage pool. Unlike a non-management target, the properties for the Management target are read-only; you cannot change any of the system-assigned properties for this target. You can, however, set a CHAP user for the Management target, in order to restrict access to LUN snapshots in a storage pool to specific VSS hosts.

► To set a CHAP user for a storage pool's Management target:

1. Access the storage pool's Management target:
 - a. Click the **Site** node.
 - b. Click the **Storage Pools** node.
 - c. Click the node corresponding to the relevant storage pool.
 - d. Click the **iSCSI Targets** node.
 - e. Click the **mgmt** node.
2. Expand the **mgmt** node's Properties panel.
3. Select the **Authentication** tab.
4. Select the **Use CHAP authentication** option to enable one-way CHAP authentication for the Management target.

5. Select the CHAP user that you want to set for one-way CHAP authentication:

To...	Do this
use the site-level CHAP user	Select the Use the Site CHAP User option. A site-level CHAP user must be set for this option to be enabled.
use a different CHAP user	<ol style="list-style-type: none"> Select the Use this CHAP User option. Select a CHAP user from the drop-down list.

6. To enable mutual CHAP authentication:
- Select the **Use Mutual CHAP** option.
 - Select a CHAP user from the drop-down list.
7. Click the **Apply** button to set the CHAP authentication configuration for the Management target.

Installing the VSS Hardware Provider

The installation of the VSS Hardware Provider is available on the Unity Discovery CD/DVD.

▶ **Before you begin:**

Make sure to review the list of supported operating systems in [Using Windows VSS](#) on the previous page.

If you install the VSS Hardware Provider on Windows Server 2003 R2, you will see several warning messages:

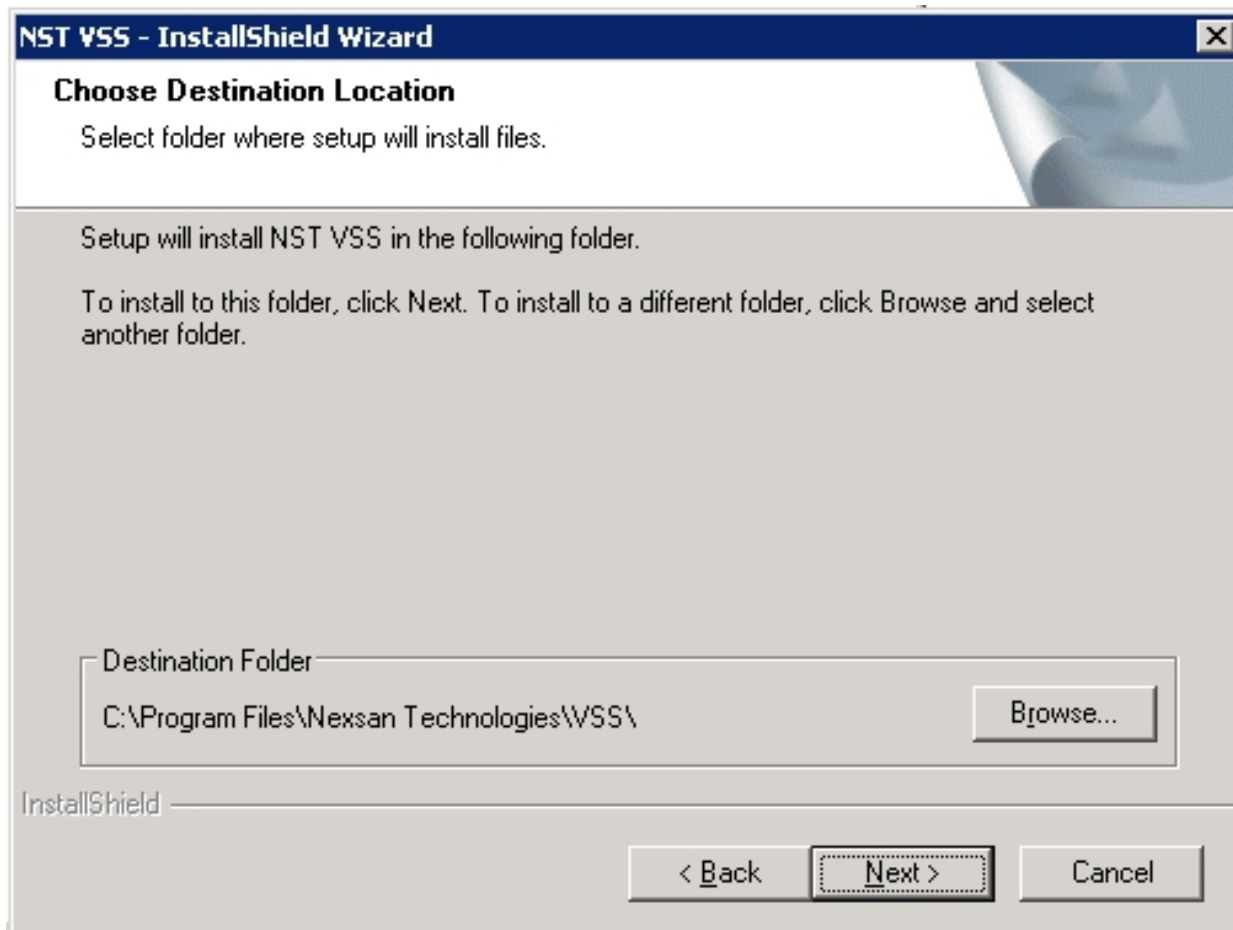
- For the **Run As** pop-up message, select **Current user** and uncheck the **Run this program with restricted access** option. This pop-up will appear multiple times. Perform the same steps as mentioned above each time.
- For any file replace warning, click **Yes**.
- For Windows logo verification warning, click **Continue**.

▶ **To install the VSS hardware provider:**

1. On the Unity Discovery CD/DVD, open the **VSS** folder and double-click **NSTVSS.exe**.
2. On the Welcome page, click **Next**.

3. On the Choose Destination Location page:
 - To select the default installation folder, click **Next**.
 - To select another folder, click **Browse** and navigate to the desired folder. Click **Next**.

Figure 7-34: Installing VSS Hardware Provider



4. On the Ready to Install page, click **Install**.
5. On the Installation Complete page, click **Finish** to exit the wizard.

6. Verify the VSS Hardware Provider installation:
 - a. Open a command prompt.
 - b. Type this command: `vssadmin list providers`
 - c. If the installation was successful, the list should display an entry for Nexsan VSS Hardware provider.

Figure 7-35: Verifying the VSS Hardware Provider installation

```

Administrator: Command Prompt
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\clusteruser>vssadmin list providers
vssadmin 1.1 - Volume Shadow Copy Service administrative command-line tool
(C) Copyright 2001-2005 Microsoft Corp.

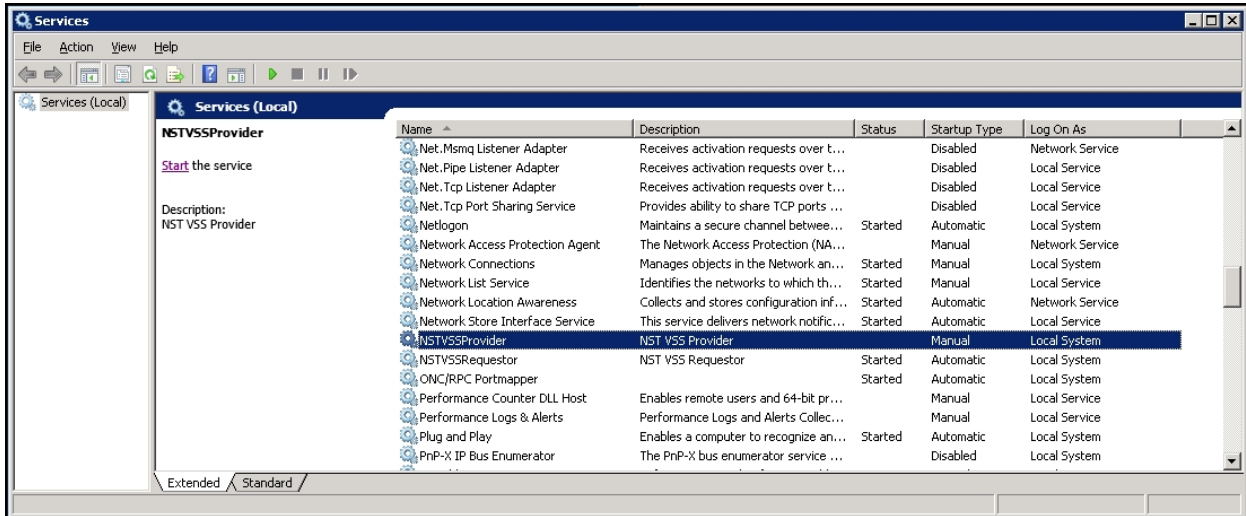
Provider name: 'Nexsan E5000 USS HW Provider'
  Provider type: Hardware
  Provider Id: {a21f8dd4-4d63-4030-882a-47cfa267cb1f}
  Version: 1.0.0

Provider name: 'Microsoft Software Shadow Copy provider 1.0'
  Provider type: System
  Provider Id: {b5946137-7b9f-4925-af80-51abd60b20d5}
  Version: 1.0.0.7

C:\Users\clusteruser>_
  
```

7. Start the VSS Hardware Provider service:
 - a. Open the *Services* application.
 - b. Locate and right-click the **NSTVSSProvider** service.

Figure 7-36: Starting the VSS Hardware Provider service



- c. Select **Start** from the context menu.
- d. Make sure the **NSTVSSProvider** service status indicates *Started*.
- e. Verify that the **NSTVSSRequestor** service status is *Started*.

► **What's next:**

[Enabling the Microsoft VSS client for LUNs below](#)

Enabling the Microsoft VSS client for LUNs

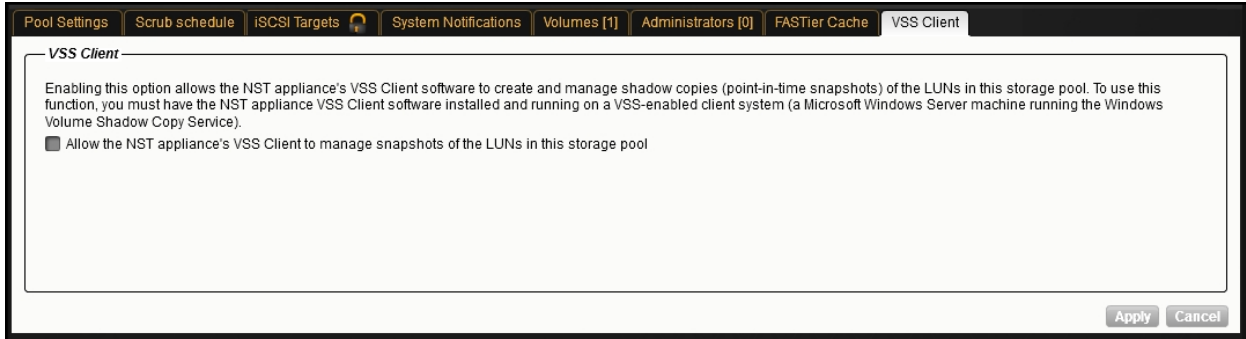
You can enable the VSS client on the pool hosting the LUNs that will be managed by VSS before or after installing the VSS Hardware Provider.

► **To enable the VSS Hardware Provider on a LUN:**

1. In Unity's tree view, click the **Site** node.
2. Click the **Storage Pools** node.
3. Select the pool hosting the LUN for which you want to enable VSS.
4. Expand the pool's Properties panel.

5. Select the **Properties** tab

Figure 7-37: Pool's properties panel—VSS Client tab



6. Select the option to allow Unity's VSS client to manage snapshots for LUNs hosted on this pool.
7. Click **Apply**.

► **Related topics:**

[Installing the VSS Hardware Provider on page 260](#)

[Discovering your LUNs with the Windows iSCSI Initiator below](#)

Discovering your LUNs with the Windows iSCSI Initiator

Before you can manage LUN snapshots using Unity's VSS Hardware Provider, you must discover the LUNs you created on Unity from the Windows Server host. These LUNs will appear as new disks in *Disk Management* and *Explorer*.

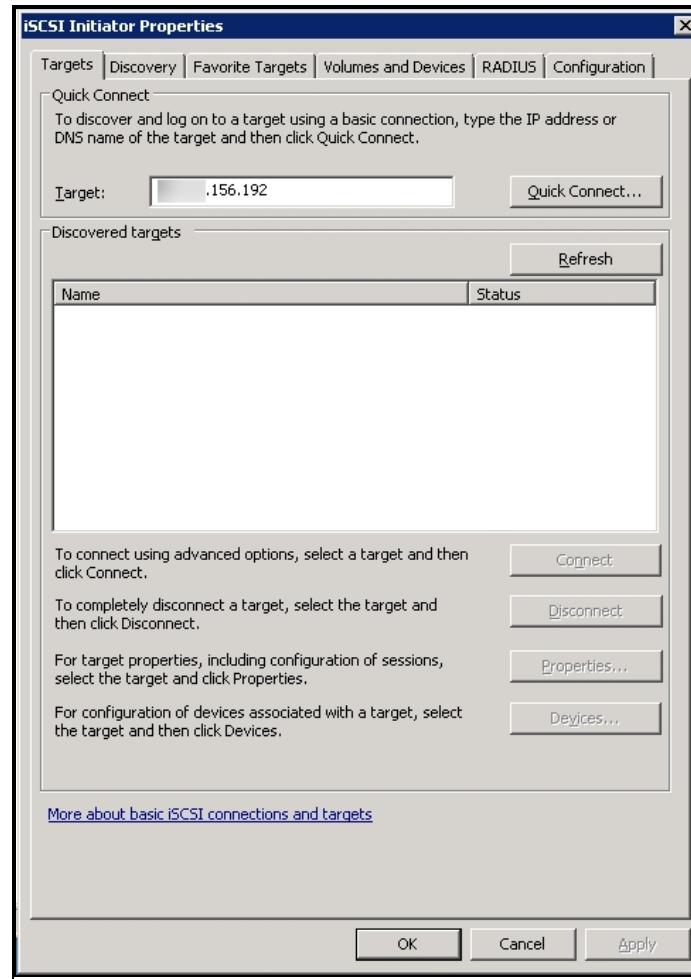
The VSS Hardware Provider connects to a storage pool's Management target via iSCSI to view, create, and manage snapshots of all LUNs in the storage pool. To discover the Management target, you must first enable the VSS feature in Unity; see [Enabling the Microsoft VSS client for LUNs on the previous page](#).

You can discover Unity targets using the **Targets** tab or the **Discovery** tab of the iSCSI Initiator Properties dialog box.

► **To discover the LUNs using the Targets tab:**

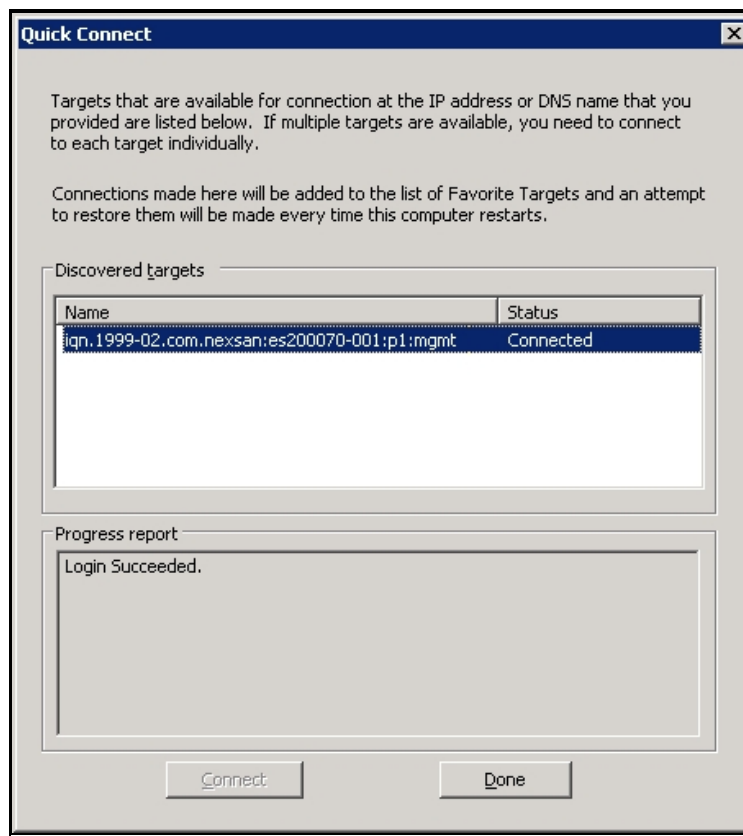
1. On the Windows server, select **Start> All Programs> iSCSI Initiator**.
2. In the **Target** field, type the Management virtual IP address of Unity.

Figure 7-38: iSCSI Initiator—Targets tab



3. Click **Quick Connect**. The discovered targets appear in the list.

Figure 7-39: iSCSI Initiator—Targets tab: Discovering targets



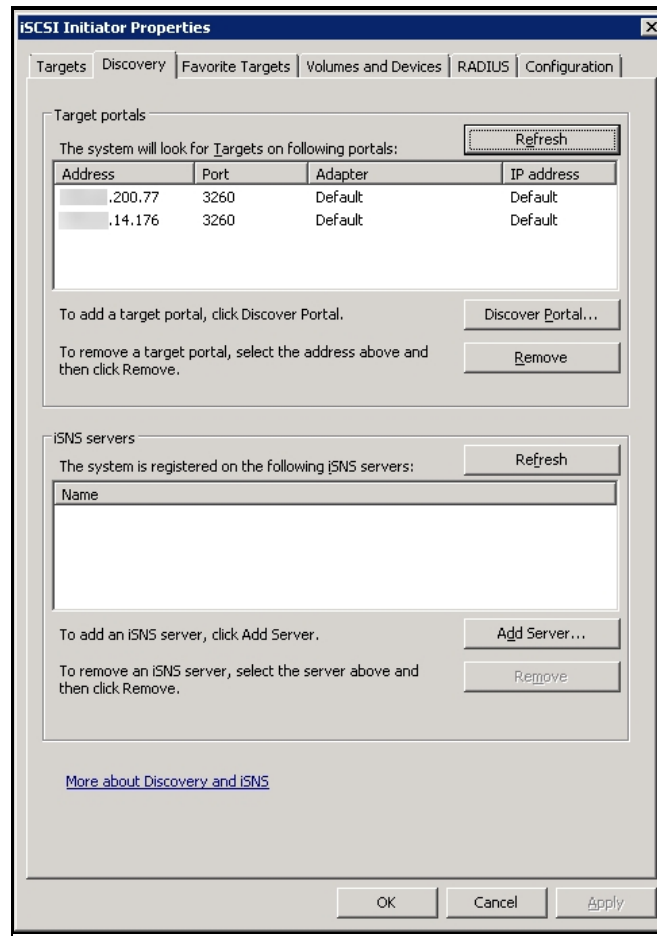
4. Click **Done** to close the Quick Connect dialog box.
5. The discovered target(s) appear(s) in the list. Click **OK** to exit the iSCSI Initiator.

► **To discover the LUNs using the Discovery tab:**

1. On the Windows server, select **Start> All Programs> iSCSI Initiator**.
2. Select the **Discovery** tab.

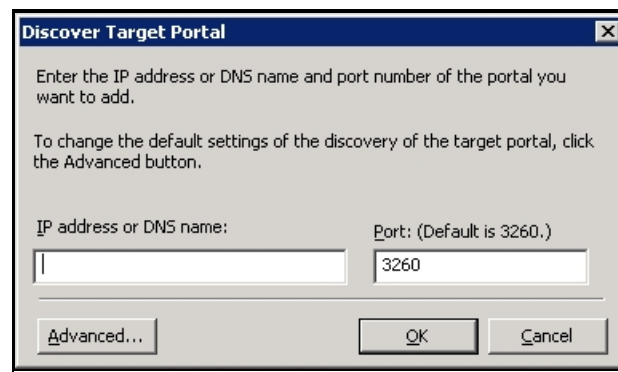
3. Click **Discover Portal**.

Figure 7-40: iSCSI Initiator—Discovery tab



4. In the **IP Address** or **DNS Name** field, type the Management virtual IP address of Unity and click **OK**.

Figure 7-41: iSCSI Initiator—Discovery tab: Discovering targets



5. The discovered target(s) appear(s) in the list. Click **OK** to exit the iSCSI Initiator.

► **Related topics:**

[Configuring the LUNs in Disk Management](#) on the next page

Configuring the LUNs in Disk Management

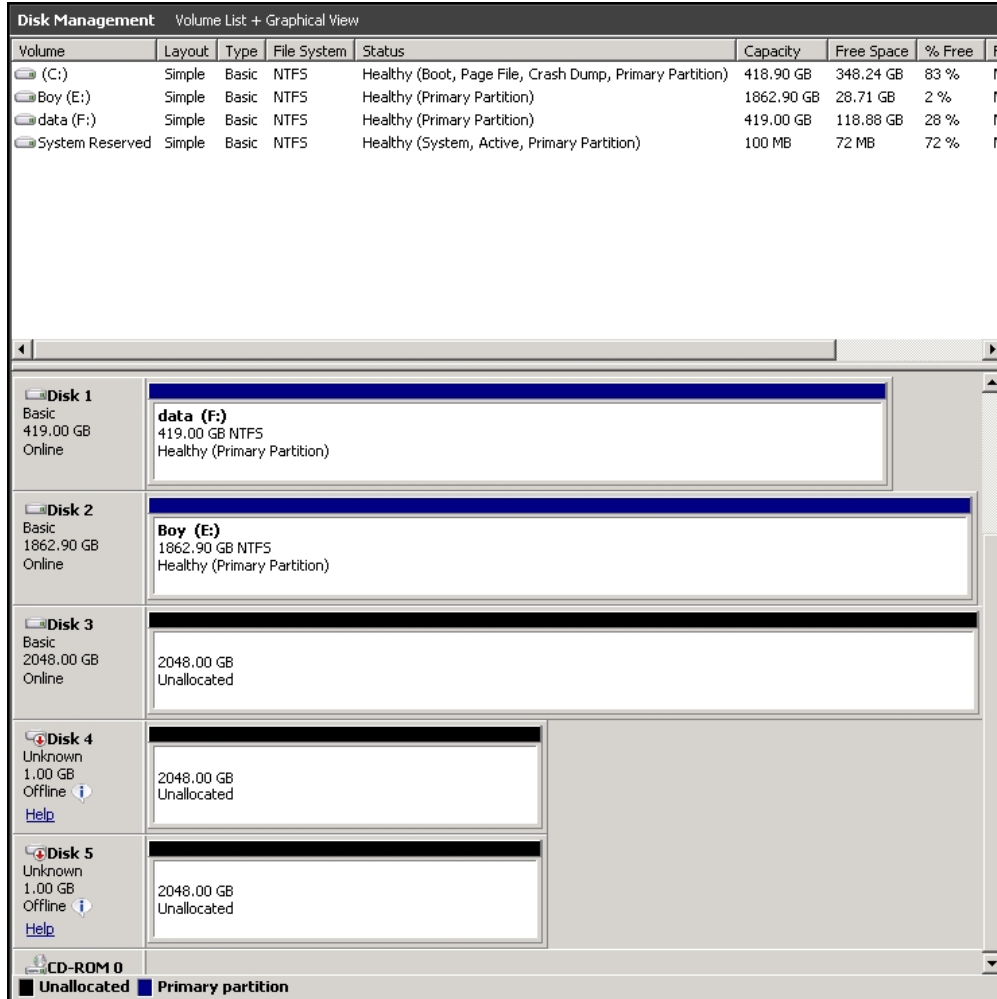
After discovering your LUNs with the Windows iSCSI Initiator, the LUNs appear as new disks, which you need to initialize and configure before you can use them.

► **To initialize and configure disks in *Disk Management*:**

1. Open *Disk Management*. The discovered targets appear as *Offline* and *Unallocated*.

This example shows two new disks, *Disk 4* and *Disk 5*, that correspond to two LUNs using the same iSCSI target on Unity.

Figure 7-42: Discovered targets in Disk Management

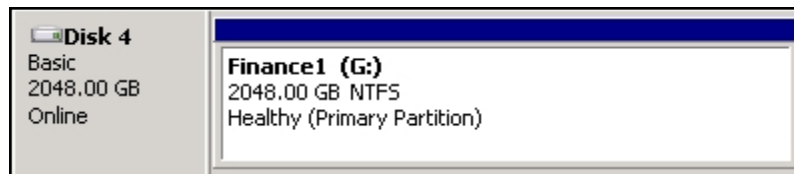


2. Right-click a disk on the left-hand side and select **Online**. The status changes to *Not Initialized* and *Online*.
3. Right-click the same disk on the left-hand side and select **Initialize Disk**.
 - For disks bigger than 2 TB, select **GPT (GUID Partition Table)**.
 - For disks smaller than 2 TB, leave the default option set to **MBR (Master Boot Record)**.

The status changes to *Basic*.

4. Right-click the initialized disk on the right-hand side. The context menu offers new options; select **New Simple Volume**.
5. Follow these steps in the New Simple Volume wizard:
 - a. Assign a volume size.
 - b. Assign a drive letter or mount the volume in an empty NTFS folder.
 - c. Format the volume as NTFS.
 - d. Give it a meaningful name.
 - e. Perform a quick format.
6. The volume appears as *Healthy* and displays your configuration settings.

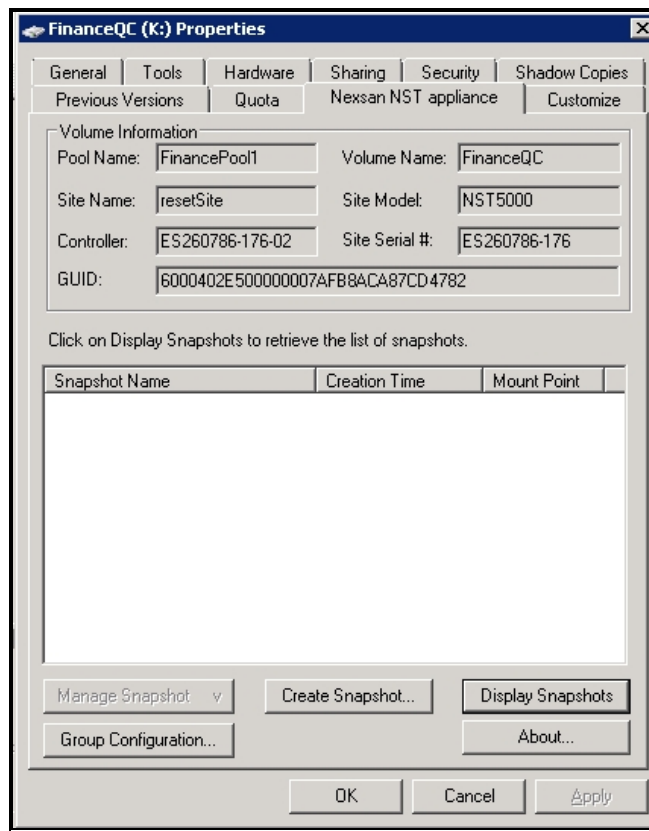
Figure 7-43: Configured volume in Disk Management



7. Repeat steps 2 to 5 for each discovered target disk.
8. Right-click a volume. The Properties dialog box displays a new tab called **Nexsan Unity** with the disk details, such as the pool name, Controller ID, and GUID.

Note The Properties panel will also display the **Nexsan Unity** tab when opened from *Explorer*.

Figure 7-44: Disk Properties—Nexsan Unity tab



► **What's next:**

You can now use your LUNs and manage the LUN snapshots; see [Creating a VSS snapshot](#) below.

Creating a VSS snapshot

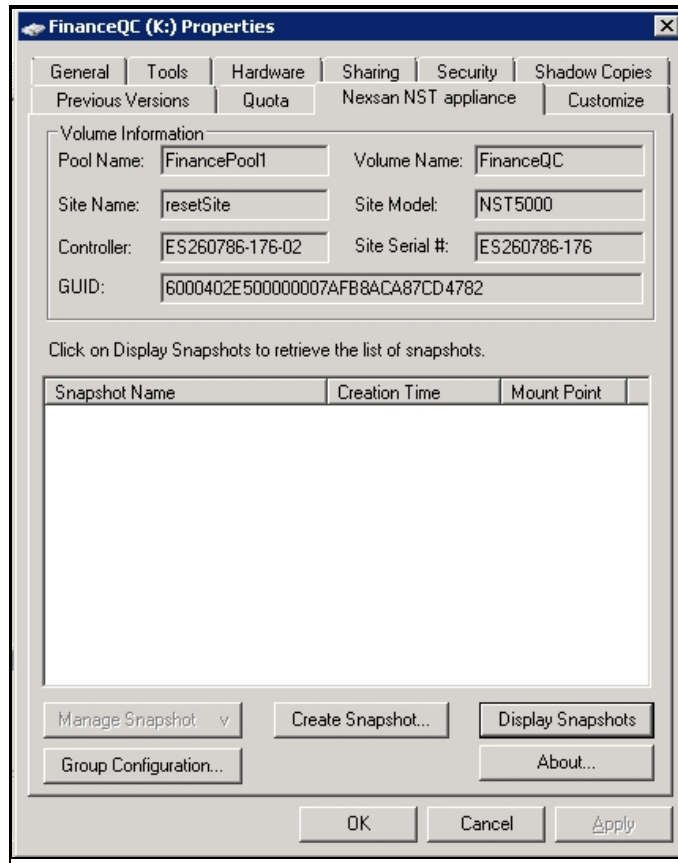
Unity's VSS Hardware Provider allows you to take snapshots of one or more LUNs. As opposed to Unity, the VSS Hardware Provider allows you to create groups of multiple LUNs and to take snapshots of these groups.

For applications running on multiple LUNs, such as an SQL Server database, you can create a snapshot of all the LUNs that are being used for the database. This enables you to restore the data residing on multiple LUNs at the same time, and not lose data integrity, such as database links.

► **To create a snapshot using the VSS Hardware Provider:**

1. On the Windows host, open *Explorer*.
2. Right-click a VSS-managed volume and select **Properties**.
3. Click the **Nexsan Unity** tab.
4. Click **Create Snapshot**.

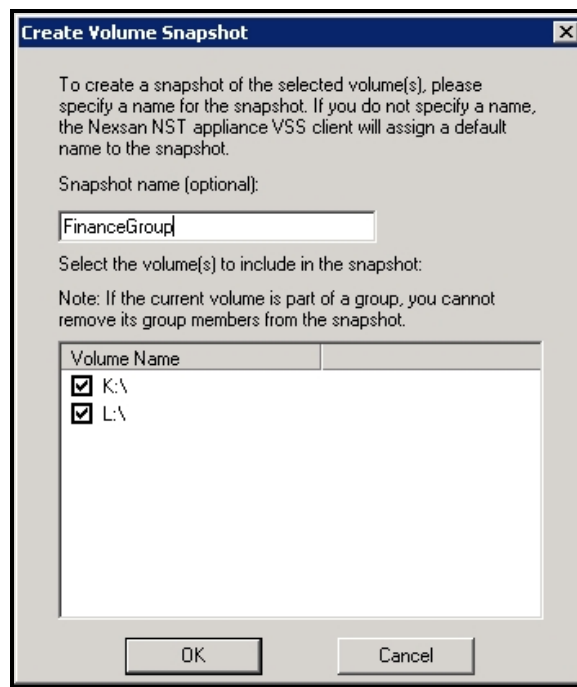
Figure 7-45: Creating VSS snapshots on the Windows host



5. By default, the volume from which you opened the Properties dialog box is selected. Optionally, enter a name for the snapshot. Do one of the following:
 - To take a snapshot of the current volume, click **OK**.
 - To take a snapshot of a group, select multiple LUNs from the list and click **OK**.

In this example, we create a group snapshot.

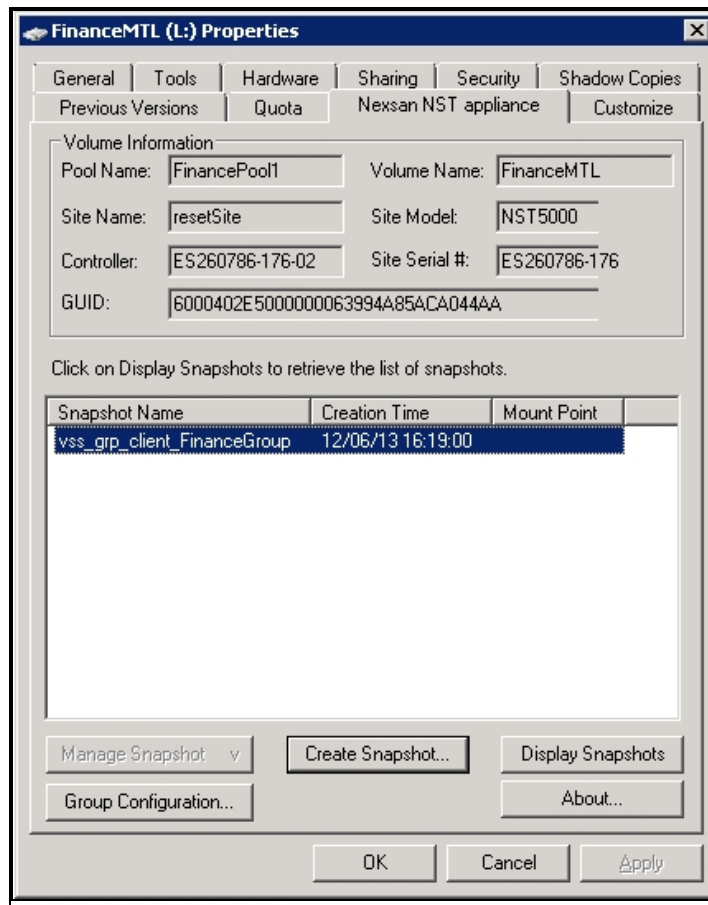
Figure 7-46: Creating a VSS group snapshot



6. After successful creation of the snapshot, you will see a confirmation message. Click **OK**.

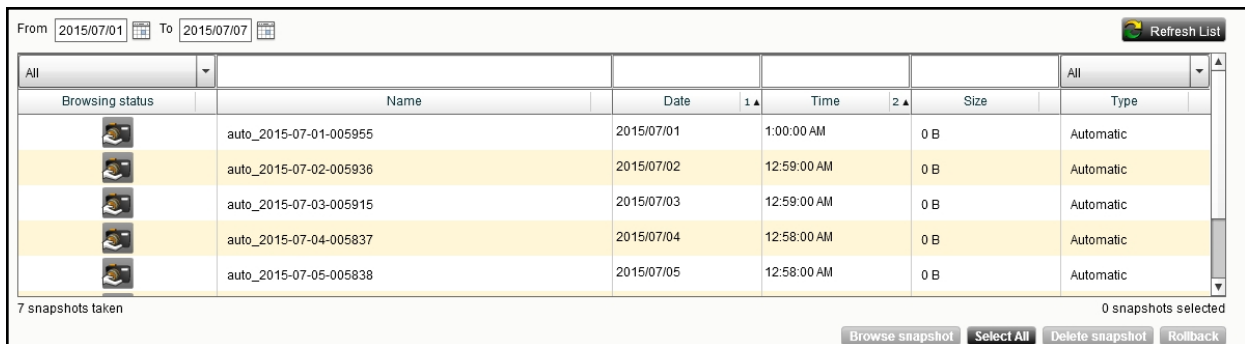
Back on the Properties page, you can see the new snapshot appearing in the list. Group snapshots include `_grp` in their name. This image provides an example of a group snapshot.

Figure 7-47: Viewing a VSS snapshot on the Properties page



You can also view the VSS snapshot from Unity.

Figure 7-48: Viewing a VSS snapshot in Unity



► **What's next:**

You can mount—also referred to as browse in Unity—unmount, rollback, and delete the snapshot as required.

► **Related topics:**

[Browsing a VSS snapshot on the facing page](#)

[Rolling back data to a VSS snapshot on page 276](#)

[Deleting a VSS snapshot on page 278](#)

Browsing a VSS snapshot

You can use the VSS Hardware Provider's [snapshot browsing](#) mechanism to recover individual files from a snapshot in case the files are accidentally deleted or overwritten, or corrupted in the snapshot's parent LUN.

Notes:

- The Management (mgmt) target must be connected for the **Manage Snapshot** button to be available and thus perform browsing.
- The VSS feature must be enabled for the storage pool in Unity.
- When you browse, or mount, a LUN snapshot using the VSS Hardware Provider on the Windows host, that same snapshot appears as *Browsing Enabled* in Unity.
- If the snapshot is already mounted in Unity, you will not be able to mount it with the VSS Hardware Provider.

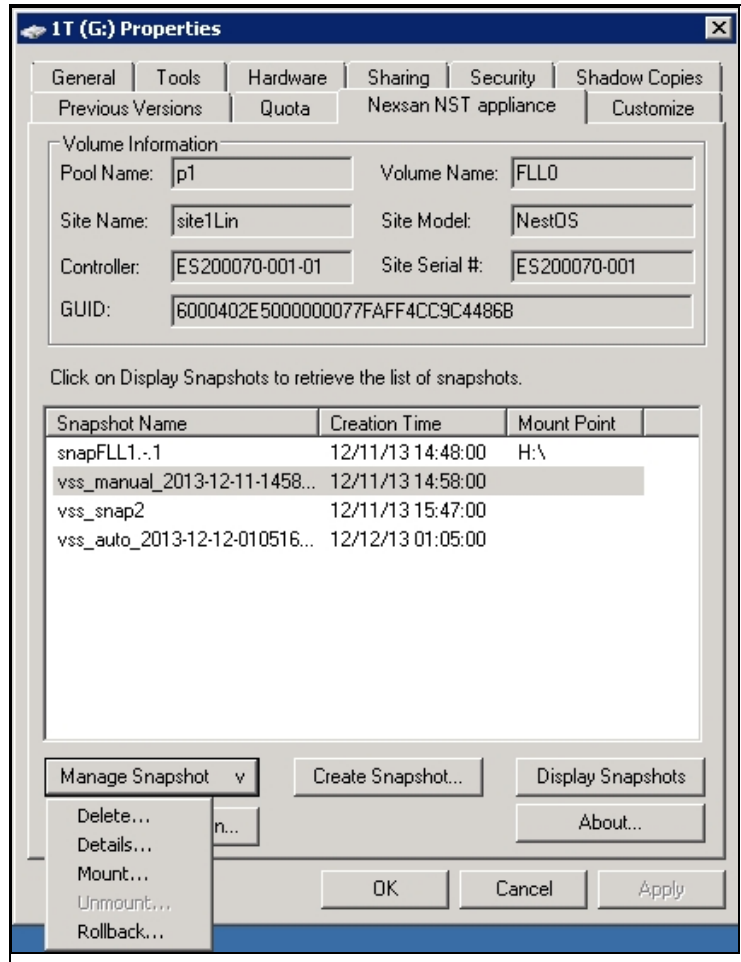
Note When browsing/mounting a LUN snapshot using the VSS Hardware Provider on Windows hosts, the disk is read-only. This applies to both iSCSI and Fibre Channel LUNs.

▶ **To mount a VSS snapshot:**

1. On the Windows Server host, open *Explorer*.
2. Right-click the volume where the snapshot to browse is hosted and select **Properties**.
3. Select the **Nexsan Unity** tab.
4. Click **Display Snapshots**.
5. Select the snapshot to mount.

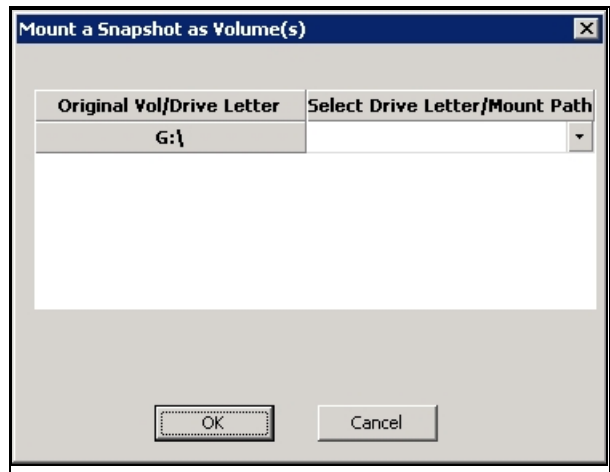
- From the **Manage Snapshot** drop-down list, select **Mount**.

Figure 7-49: Browsing a VSS snapshot



- A new window opens where you assign drive letter/mount path from the drop-down list. Click **OK**.

Figure 7-50: Assigning a drive letter to the VSS snapshot



8. You will see a confirmation message after successful mounting. Once refreshed, the list shows the Mount Point against the snapshot name.
 - a. Check if a new volume appears under **Hard Disk Drives** with the drive letter you provided in the previous step.
 - b. Verify that all files present in the original volume when the snapshot was taken are in the new volume.

▶ **To unmount a VSS snapshot:**

1. From the **Nexsan Unity** tab, select the snapshot you mounted.
2. From the **Manage Snapshot** drop-down list, select **Unmount**.
3. A confirmation message appears: *Snapshot successfully unmounted*. The volume that appeared with the assigned drive letter name under **Hard Disk Drives** is no longer present.

▶ **Related topics:**

[Creating a VSS snapshot on page 270](#)

[Rolling back data to a VSS snapshot on the next page](#)

[Deleting a VSS snapshot on page 278](#)

Viewing the VSS client information

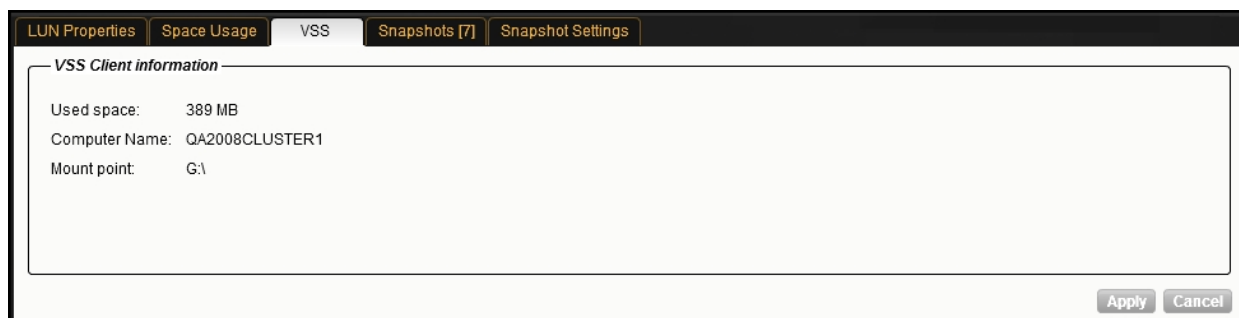
This section describes how to view the space currently used by LUN snapshots managed by the VSS Hardware Provider.

You can view the space consumption from Unity, along with the name of the Windows Server host, and the LUN mount point.

▶ **To view VSS client information for a LUN:**

1. Click the **Site** node to display its child nodes.
2. Click the **Storage Pools** node.
3. Click the node corresponding to the storage pool where the LUN is hosted.
4. Click the **LUNs** node.
5. Click the node corresponding to the LUN.
6. Expand the LUN's Properties panel.
7. Click the **VSS** tab.

Figure 7-51: LUN's properties panel—VSS tab



▶ **Related topics:**

[Creating a VSS snapshot on page 270](#)

[Browsing a file system snapshot on page 199](#)

Rolling back data to a VSS snapshot

The rollback function reverts a LUN's contents to what they were at the time the snapshot was taken, including all file- and folder-level permission settings and access-level attributes. This function also automatically deletes all snapshots that are newer than the snapshot that you roll back to, including all manual snapshots of the LUN and snapshots that have browsing enabled. The VSS Hardware Provider also allows you to roll back data for groups of LUNs, using the group snapshot.

Unity provides the rollback function for extreme circumstances: for example, if all the data in a LUN is corrupted and can no longer be recovered. The rollback function overwrites all the existing data in the LUN with the contents of the snapshot that you roll back to; any new data that was added after the snapshot is recorded, including updates to existing data, is lost during the rollback process and cannot be undone.

Notes:

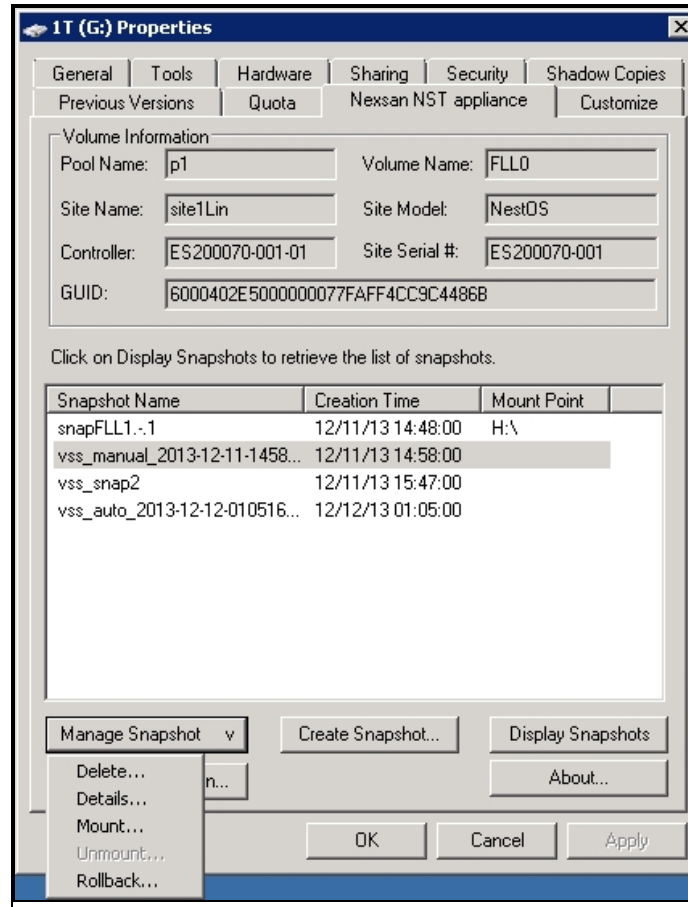
- The Management (mgmt) target must be connected for the **Manage Snapshot** button to be available and thus perform the rollback.
- The VSS feature must be enabled for the storage pool in Unity.

▶ **To roll back data to a VSS snapshot:**

1. On the Windows Server host, open *Explorer*.
2. Right-click the volume where the snapshot to roll back to is hosted and select **Properties**.
3. Select the **Nexsan Unity** tab.
4. Click **Display Snapshots**.
5. Select the snapshot that you wish to use for data restore.

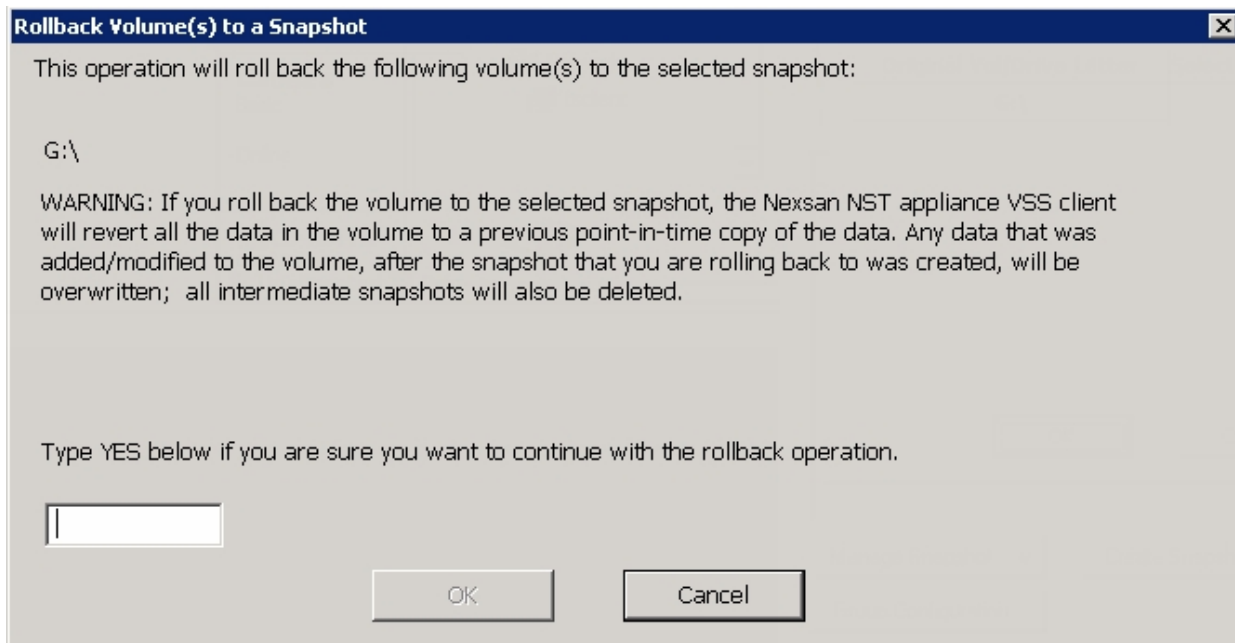
- From the **Manage Snapshot** drop-down list, select **Rollback**.

Figure 7-52: Rolling back data to a VSS snapshot



- You will be prompted to confirm the restore operation. Type **Yes** in the field and click **OK**.

Figure 7-53: Confirming the VSS snapshot rollback



7

- Restart these services:
 - Volume Shadow Copy
 - NSTVSSProvider
 - NSTVSSRequestor
- Verify that the data present in the volume correspond to the data in the snapshot.

Deleting a VSS snapshot

This section describes how to delete a LUN snapshot using Unity's VSS Hardware Provider.

Notes:

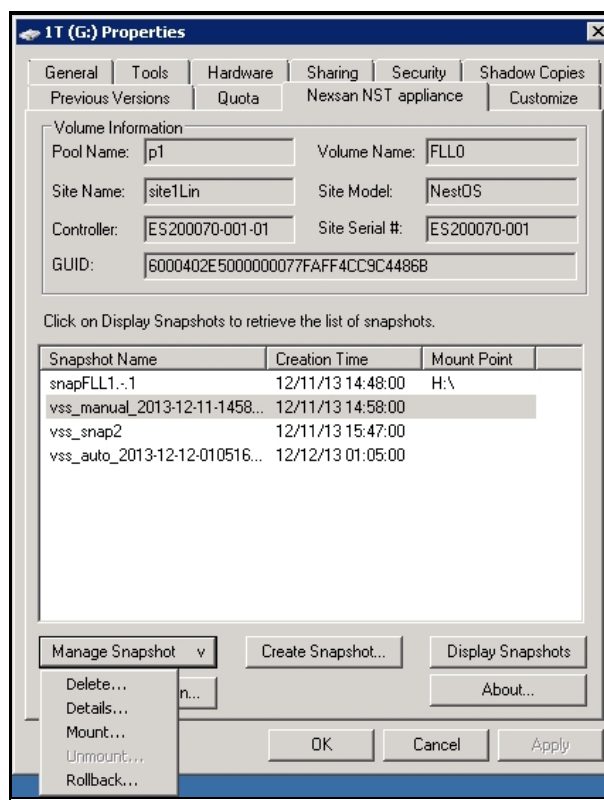
- The Management (mgmt) target must be connected for the **Manage Snapshot** button to be available and thus perform a deletion.
- The snapshot must be unmounted before it can be deleted; for steps to unmount a snapshot, see [Browsing a VSS snapshot on page 273](#).
- The VSS feature must be enabled for the storage pool in Unity.
- You can also delete a LUN snapshot created by the VSS Hardware Provider from Unity; see [Manually deleting file system snapshots on page 205](#).

▶ To delete a VSS snapshot:

1. On the Windows Server host, open *Explorer*.
2. Right-click the volume where the snapshot to delete is hosted and select **Properties**.
3. Select the **Nexsan Unity** tab.
4. Click **Display Snapshots**.
5. Select the snapshot to delete.

- From the **Manage Snapshot** drop-down list, select **Delete**.

Figure 7-54: Deleting a VSS snapshot



- A warning message will appear. Click **Yes** to confirm the deletion and refresh. The snapshot is no longer listed under the **Nexsan Unity** tab.

► **Related topics:**

[Enabling the Microsoft VSS client for LUNs on page 263](#)

[Discovering your LUNs with the Windows iSCSI Initiator on page 264](#)

Using both Nexsan Unity and VSS Hardware Provider to manage LUN snapshots

Unity provides two ways for managing snapshots for LUNs:

- Using Unity's tree view—see [Using the LUN's Properties panel to manage LUN snapshots on page 246](#)
- Using the VSS Hardware Provider—see [Using Windows VSS on page 259](#)

You can also use a combination of both methods to manage LUN snapshots. This table describes the actions performed using both methods and how the results display in each interface. Since both methods are linked by Unity, actions performed on a snapshot in Unity are reflected on the Windows host. However, browsing a snapshot using one method prevents that action against the same snapshot with the other method.

Table 7-5: Managing LUN snapshots using both Nexsan Unity and VSS Hardware Provider

Action performed	... in Nexsan Unity	... using VSS Hardware Provider on the Windows host
Create a snapshot	On the Windows host, the snapshot appears in the volume's properties when clicking Display Snapshots .	Prerequisites: <ol style="list-style-type: none"> 1. Install Unity's VSS Hardware Provider on the Windows host. 2. Enable the VSS Hardware Provider feature in Unity. In Unity, the snapshot appears under the Snapshots tab of the LUN.
Filter snapshots	Use the Snapshots tab of the LUN.	You cannot filter snapshots on the Windows host.
Search for a snapshot	Use the Snapshots tab of the LUN.	There is no search mechanism on the Windows host. In the volume's properties, you can only sort the names by clicking the Snapshot Name column.
Browse/mount a snapshot	When you enable browsing for a snapshot in Unity, the snapshot cannot be mounted using VSS.	When you mount a snapshot using VSS, that snapshot cannot be browsed in Unity; it will show as <i>Browsing Enabled</i> .
Disable browsing/unmount a snapshot	When you disable browsing for a snapshot in Unity, you can mount the snapshot on the Windows host.	When you unmount a snapshot using VSS, that snapshot can be browsed in Unity.
Roll back data to a snapshot	On the Windows host, newer data written to the disk is deleted.	In Unity, newer data written to the LUN is deleted.
Delete a snapshot	On the Windows host, the volume disappears from the list of drives in <i>Explorer</i> and <i>Disk Management</i> .	In Unity, the snapshot disappears from the grid in the Snapshots tab.

iSCSI Functions

When you add a LUN to a storage pool on Unity, you can assign the LUN to an iSCSI target in the storage pool. The [iSCSI target](#) presents the LUN(s) assigned to it to servers (initiators) on the network. The iSCSI target also allows Unity's VSS Hardware Provider to create and manage snapshots using the pool's Management (mgmt) target.

Each storage pool on Unity can have one, or multiple, iSCSI targets, with a maximum of 255 targets per storage pool (0 to 254).

During the LUN creation process, when you add a new LUN to a storage pool, you can assign the new LUN to the storage pool's default target; if a default target does not exist, Unity automatically creates the default target on the system. Alternately, you can create a new target to assign the LUN to—you can do this during the LUN creation process, or later, once you add the LUN to the system.

If your storage systems are connected to Unity using iSCSI, you can perform these functions for your iSCSI LUNs.

Note If you are mounting iSCSI LUNs on Windows hosts, do not enable or configure MPIO.

This section includes these topics:

[Configuring and managing CHAP authentication](#) below

[Adding an iSCSI target](#) on page 288

[Connecting to an iSCSI LUN from a Windows-based initiator](#) on page 290

Configuring and managing CHAP authentication

iSCSI initiators and targets prove their identity to each other using [CHAP](#).

Unity's iSCSI implementation provides three levels of CHAP authentication:

- **Site-level CHAP authentication:** with this level of security Unity authenticates the initiator (server). When an initiator tries to connect to Unity, it provides a user name and secret. Unity checks whether the user name and secret combination matches the site-level CHAP user account that you configured for the site in Unity. If they match, the initiator is authorized to connect to Unity and discover iSCSI targets that you configured on the system.
- **One-way CHAP authentication (target-level):** with this level of security the iSCSI target on Unity authenticates the initiator (server). When an initiator tries to connect to an iSCSI target on Unity, it provides a user name and secret to connect to the target. The iSCSI target on Unity checks whether the user name and secret combination matches the CHAP user account that you configured for the target in Unity. If they match, the initiator can connect to the target.
- **Mutual CHAP authentication:** with this level of security, the target and the initiator authenticate each other. When an initiator tries to connect to an iSCSI target on Unity, the target provides a user name and secret to the initiator (which you set on the initiator). The initiator compares the user name and secret to information it holds. If they match, the initiator can connect to the target.

You can implement one-way CHAP authentication without mutual CHAP authentication. However, you can only enable mutual CHAP authentication if one-way CHAP authentication is configured. Site-level CHAP authentication works independently of both one-way CHAP authentication and mutual CHAP authentication.

This section includes these topics:

[Adding a CHAP user](#) below

[Deleting a CHAP user](#) on page 283

[Modifying a CHAP user's secret](#) on page 284

[Setting the site-level CHAP user](#) on page 286

[Setting CHAP authentication for a target](#) on page 287

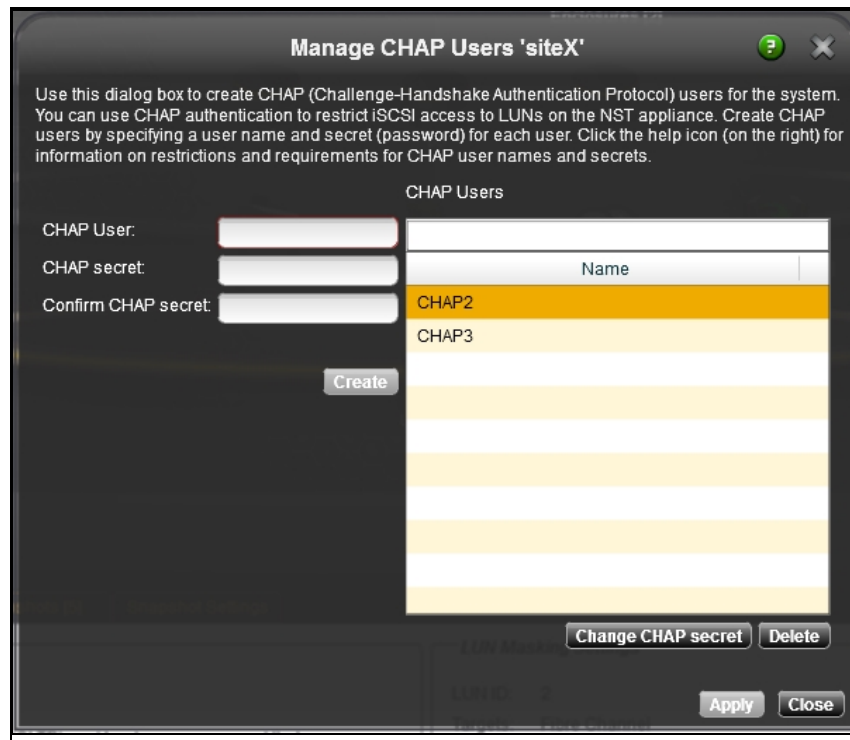
Adding a CHAP user

Before you can configure CHAP authentication for the site, or for targets on Unity, you must add CHAP users to the system.

► **To add a CHAP user:**

1. Open the Manage CHAP Users panel:
 - Select the **Manage CHAP users** option from the **Security and Permissions** menu in Unity's toolbar. The Manage Chap Users pop-up displays.

Figure 7-55: Manage CHAP Users dialog box



7

2. Type the CHAP user's name in the **CHAP User** field.

The CHAP user name can contain up to 16 characters and it must be unique to the system. It can contain any combination of upper-case or lower-case characters.

These characters are NOT allowed:

" / \ [] : ; | = , + * ? < >

A CHAP user name cannot consist solely of periods (.) and spaces.

Note CHAP user names are case-sensitive. When connecting to Unity, iSCSI initiators are required to type the CHAP user name using the same combination of lower- and upper-case letters that you entered when creating the corresponding CHAP user account.

3. Type a CHAP secret in the **CHAP secret** field.

The CHAP secret you specify must be at least 12 characters long, up to a maximum of 16. Spaces are allowed in a CHAP secret. You must use a combination of lowercase/uppercase letters, numbers and/or special characters.

For example, this is a valid password:

Strong Password!

Be sure to specify a strong CHAP secret that is not easily guessed.

Notes:

- CHAP secret passwords are case-sensitive.
 - If you intend to use mutual CHAP authentication, the CHAP user account that you set cannot have the same secret as the CHAP user that you set for one-way CHAP authentication (target-level). It is good practice to specify a unique secret for each CHAP user account on the system.
 - If you forget the secret for a CHAP user, the secret cannot be recovered. However, the secret can be reset.
4. Repeat the secret in the **Confirm CHAP secret** field.
 5. Click the **Create** button to add the CHAP user to Unity.

The new CHAP user appears in the list of CHAP users on the Manage CHAP Users panel.

Deleting a CHAP user

This section explains how to delete CHAP users.

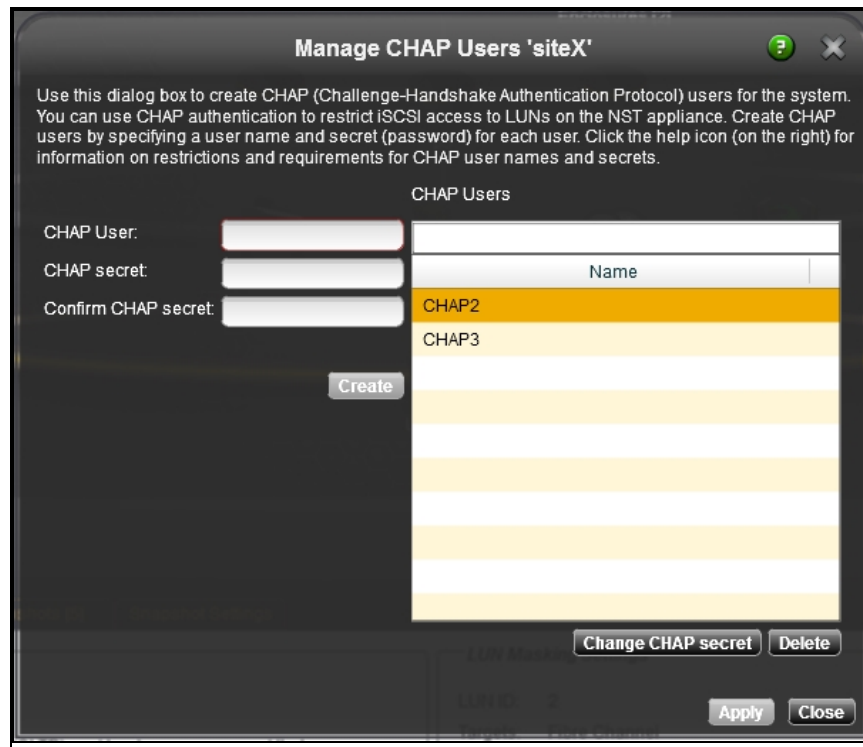


CAUTION: It is not recommended to delete *active* CHAP users from the system—specifically, CHAP users that are assigned to the site, or to targets on Unity, for CHAP authentication; this will result in initiators that have these CHAP users set for authentication to lose their connection to any corresponding LUNs on Unity.

▶ To delete a CHAP user:

1. Open the Manage CHAP Users panel: Select the **Manage CHAP users** option from the **Manage Users** menu in Unity's toolbar. The Manage CHAP Users panel displays.

Figure 7-56: Manage CHAP Users dialog box



7

2. From the CHAP users list, on the left-hand side of the Manage CHAP Users panel, select the CHAP user that you want to delete from the system.
3. Click the **Delete** button. Unity prompts you to confirm deletion.
4. Click **Yes** to delete the selected CHAP user. Unity removes the CHAP user from the list of users on the system.

Modifying a CHAP user's secret



CAUTION: It is not recommended to modify the secret for an *active* CHAP user on the system—specifically, a CHAP user that is assigned to the site, or to targets on Unity, for CHAP authentication. This will result in initiators that have this CHAP user set for authentication to lose their connection to any corresponding LUNs on Unity.

► To modify a CHAP user's secret:

1. Open the Manage CHAP Users panel: Select the **Manage CHAP users** option from the **Manage Users** menu in Unity's toolbar. The Manage CHAP Users panel displays.

Figure 7-57: Manage CHAP Users dialog box

Use this dialog box to create CHAP (Challenge-Handshake Authentication Protocol) users for the system. You can use CHAP authentication to restrict iSCSI access to LUNs on the NST appliance. Create CHAP users by specifying a user name and secret (password) for each user. Click the help icon (on the right) for information on restrictions and requirements for CHAP user names and secrets.

CHAP Users

CHAP User:

CHAP secret:

Confirm CHAP secret:

Name
CHAP2
CHAP3

- From the CHAP users list, on the left-hand side of the Manage CHAP Users panel, select the CHAP user that you want to modify the secret for.
- Click the **Change CHAP secret** button. The Change CHAP secret popup displays.

Figure 7-58: Change CHAP secret popup

Change CHAP secret

Enter the new CHAP secret:

New password:

Confirm password:

4. Type a new CHAP secret in the **New CHAP secret** field.

The CHAP secret you specify must be at least 12 characters long, up to a maximum of 16. Spaces are allowed in a CHAP secret. You must use a combination of lowercase/uppercase letters, numbers and/or special characters.

For example, this is a valid password:

Strong Password!

Be sure to specify a strong CHAP secret that is not easily guessed.

Notes:

- CHAP secret passwords are case-sensitive.
 - If you intend to use mutual CHAP authentication, the CHAP user account that you set cannot have the same secret as the CHAP user that you set for one-way CHAP authentication (target-level). It is good practice to specify a unique secret for each CHAP user account on the system.
 - If you forget the secret for a CHAP user, the secret cannot be recovered. However, the secret can be reset.
5. Repeat the new secret in the **Confirm CHAP secret** field.
 6. Click the **Save** button to set the new CHAP secret.

Setting the site-level CHAP user

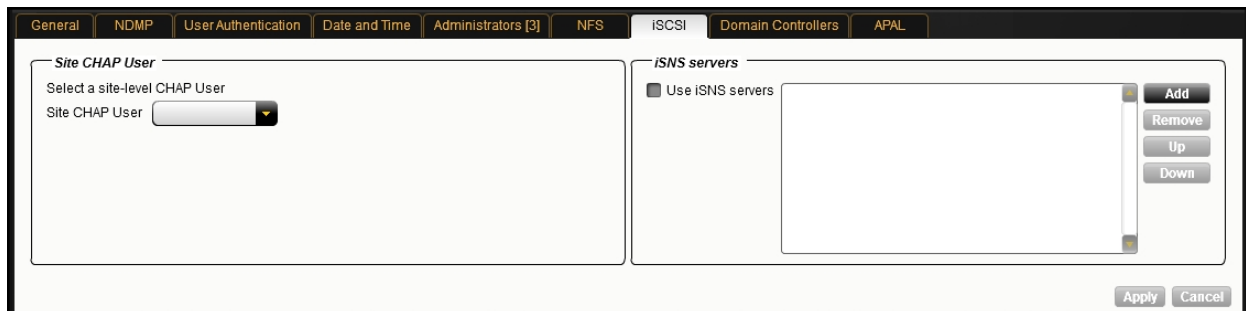
When you set a site-level CHAP user for Unity, you enable CHAP authentication at the site-level. This allows Unity to authenticate initiators that connect to the system.

More specifically, with site-level authentication, when an initiator tries to connect to Unity, it must provide a user name and secret. Unity then checks whether the user name and secret combination matches the site-level CHAP user that you configured for the site in Unity. If they match, the initiator is authorized to connect to Unity and discover iSCSI targets that you configured on the system.

► **To set a site-level CHAP user:**

1. In Unity's tree view, click the site node corresponding to the site that you want to set the site-level CHAP user for.
2. Expand the Site node's Properties panel.
3. Select the **iSCSI** tab.

Figure 7-59: Site node's properties panel—iSCSI tab



4. Open the Site CHAP user drop-down list, and select the CHAP user to set for site-level CHAP authentication.
5. Click the **Apply** button to set the CHAP user for the site.

Setting CHAP authentication for a target

When you set CHAP authentication at the target level, you prevent unauthorized initiators from connecting to LUNs assigned to the target. Unity supports both one-way CHAP authentication and mutual CHAP authentication at the target level:

- **One-way CHAP authentication (target-level):** with this level of security the iSCSI target on Unity authenticates the initiator (server). When an initiator tries to connect to an iSCSI target on Unity, it provides a user name and secret to connect to the target. The iSCSI target on Unity checks whether the user name and secret combination matches the CHAP user account that you configured for the target in Unity. If they match, the initiator can connect to the target.
- **Mutual CHAP authentication:** with this level of security, the target and the initiator authenticate each other. When an initiator tries to connect to an iSCSI target on Unity, the target provides a user name and secret to the initiator (which you set on the initiator). The initiator compares the user name and secret to information it holds. If they match, the initiator can connect to the target.

Note Disabling CHAP authentication at the iSCSI target level results in client/host systems that have an active connection to any LUN(s) associated with the initiator(s) to be immediately disconnected and lose access to their data. This may also result in data loss.

► To enable CHAP authentication for a target:

1. In Unity's tree view, navigate down to the target that you want to set CHAP authentication for:
 - a. Click the **Site** node to display its child nodes.
 - b. Click the **Storage Pools** node.
 - c. Click the node corresponding to the storage pool where the target that you want to set CHAP authentication for exists.
 - d. Click the **iSCSI Targets** node.
 - e. Click the node corresponding to the target that you want to set CHAP authentication for.
2. Expand the target's Properties panel.
3. Select the **Authentication Settings** tab.

Figure 7-60: iSCSI target's properties panel—Authentication tab



4. Select the **Use CHAP authentication** option to enable one-way CHAP authentication for the target.
5. Select the CHAP user that you want to set for one-way CHAP authentication:
 - To use the site-level CHAP user, select the **Use the Site CHAP User** option; a site-level CHAP user must be set for this option to be enabled (see [Setting the site-level CHAP user](#) on the previous page).
 - To specify a different CHAP user, select the **Use this CHAP User** option, and then select a CHAP user from the drop-down list.

6. To enable mutual CHAP authentication, select the **Use Mutual CHAP** option, and then select a CHAP user from the drop-down list.
7. Click the **Apply** button to set the CHAP authentication configuration for the target.

Adding an iSCSI target

Unity provides the Target Setup Wizard to guide you through the process of adding a Target to a storage pool.

▶ **To start the Target Setup Wizard:**

1. Under the site node, click the **Storage Pools** node to select it and display its child nodes.
2. Click the storage pool that you want to add a target to.
3. Select the **iSCSI Targets** node.
4. Perform one of these actions:
 - Click the context menu button on the iSCSI targets node to open the node context menu, or
 - Expand the Properties panel for the iSCSI targets node.
5. Click **Add an iSCSI Target**.

The Target Setup Wizard guides you through the process of adding a target to a storage pool.

This section includes these steps:

[Step 1: Specifying the IQN and public alias for the iSCSI target](#) below

[Step 2: Verifying configuration settings](#) on the facing page

[Step 3: Viewing configuration results](#) on the facing page

Step 1: Specifying the IQN and public alias for the iSCSI target

Step 1 of the Target Setup Wizard prompts you to specify the iSCSI target's IQN and public alias.

- **IQN:** an IQN (iSCSI qualified name) is the unique identifier of a device in an iSCSI network. iSCSI uses the form `iqn.date.authority:uniqueid` for IQNs. For example, Unity uses this IQN to identify iSCSI targets:

```
iqn.1999-02.com.nexsan:<site name>:<pool name>:<unique ID>
```

This name indicates that this is an iSCSI device from Nexsan, which was registered as a company in February of 1999. The naming authority is simply the DNS name of the company reversed; in this case, `com.nexsan`. Following this is the site name, the storage pool name where the target exists, and a unique ID that you must specify to identify the target.

Note IQN is always forced to lower case by Unity, in accordance with RSF conventions.

- **Public alias:** this is a symbolic name that you can assign to a target on the Unity. The public alias is seen by some iSCSI initiators; it can help you identify the target. You can change a target's public alias at any time.

Figure 7-61: Target Setup Wizard, Step 1: Specifying the iSCSI target's IQN and public alias

Create an iSCSI Target

Follow the steps to create an iSCSI Target in the storage pool, including setting an IQN and PublicAlias for the target.

IQN: iqn.1999-02.com.nexasan:

Public alias:

► **To specify the IQN and public alias for the iSCSI target:**

1. Type a unique ID in the text box next to the **IQN:** field. The ID must start with an (upper-case or lower-case) alphabetic or numeric character; spaces are not allowed.
2. Type a public alias for the target in the **Public alias** text box. The public alias can contain up to a maximum of 16 characters, and it must start with an (upper-case or lower-case) alphabetic character; with the exception of the underscore (_), hyphen (-), and period (.), the public alias can only contain alphanumeric characters.
3. Once you specify the IQN and public alias for the target, click the forward arrow on the panel to continue

Step 2: Verifying configuration settings

This step of the Target Setup Wizard summarizes the settings you selected for the new iSCSI target and creates the target in the storage pool when you click **Start**. Review the summary carefully before applying the configuration settings.

Figure 7-62: Target Setup Wizard, Step 2: Verify Settings

Verify Settings

Please verify your configuration settings. If you want to change a setting, click the back arrow to navigate to the relevant configuration panel. Or, click the step identifier at the top of the wizard panel to go back to a specific step.

IQN: iqn.1999-02.com.nexasan:finance12.22:financemr:1
Public alias: FinanceSite

► **To change a configuration setting:**

- Click the back arrow to navigate back to the corresponding configuration step.
- Or
- Click the corresponding step identifier at the top of the Target Setup Wizard panel. For example, if you want to change the IQN for the target, click **Step 1**.

If you are satisfied with the configuration settings, click the **Start** button at the bottom of the panel. The Target Setup Wizard automatically proceeds to [Step 3: Viewing configuration results](#) below, where you can view progress as Unity creates the new iSCSI target.

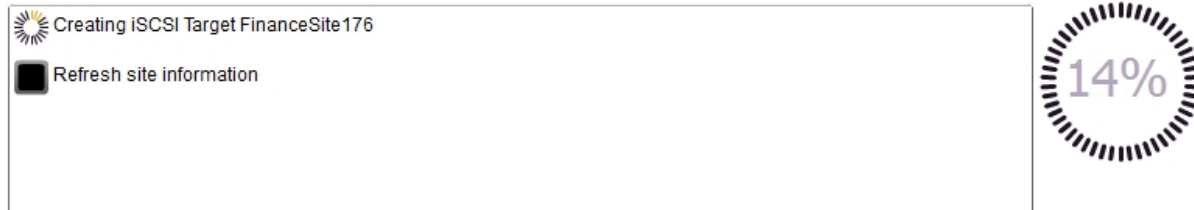
Step 3: Viewing configuration results

The last step of the Target Setup Wizard displays progress as Unity creates the new iSCSI target.

The Target Setup Wizard displays error events that the system encounters during the target creation process. You can view more details about an error event by expanding the corresponding entry.

Figure 7-63: Target Setup Wizard, Step 3: Viewing progress
Configuration Results

Applying settings:



► **To view more details for an error event:**

- Click the plus (+) sign corresponding to the error event.

Unity informs you when it successfully creates the target. It also asks you if you want to create another target in the storage pool:

Click **Yes** if you want to create a new target; the Target Setup Wizard scrolls back to [Step 1: Specifying the IQN and public alias for the iSCSI target](#) on page 288 and resets all configuration settings to their defaults.

Connecting to an iSCSI LUN from a Windows-based initiator

Notes:

- The procedures provided here are specific to Microsoft Windows 7; the process for connecting to an iSCSI LUN on Unity may differ depending on the version of Windows from where you are initiating the connection.
- In addition, some iterations of Microsoft Windows, such as Windows XP, do not come pre-installed with Microsoft's iSCSI Initiator; you may have to download Microsoft's iSCSI Initiator, and then install and configure it before connecting to an iSCSI LUN on Unity.

► **Step 1: Connect the iSCSI LUN from a Microsoft Windows-based initiator**

1. On the Windows system from where you want to connect to an iSCSI LUN on Unity, select **Start > Search**, and type **iSCSI**.
2. In **Programs**, click **iSCSI Initiator**.
3. If this is the first time you are launching Microsoft iSCSI Initiator, you receive a prompt that says the Microsoft iSCSI service is not running. Click **Yes** to start the service.
4. The Microsoft iSCSI Initiator Properties dialog box opens, and the **Targets** tab displays. Click the **Discovery** tab.
5. To add Unity as a target portal, click **Discover Portal**.
6. In the Discover Portal dialog box, type the virtual IP address of the Pool Resource Group where the LUN exists.
7. Select the discovered targets (LUNs) that you want to connect to and click **Connect**. The initiator adds the iSCSI LUN to Windows.
8. Click **Done**.
9. Click **OK** to close the Microsoft iSCSI Initiator Properties dialog box.

You must now initialize the LUN on the Windows system and add it as a disk volume to the system.

► Step 2: Initialize the LUN

1. Click **Start > Search**, type **Disk Management**
2. In **Programs**, click **Disk Management**.
3. *Disk Management* starts and informs you that a new disk has been found; it also instructs you to initialize the new disk before you use it. Click **OK** to initialize the new disk.
4. The new disk is displayed in Storage Manager as Disk 1 (although this designation may vary depending on the configuration of your system. The new disk is identified as **Online**, but **Unallocated**. To allocate the disk, right-click the disk and select **New Simple Volume**.
5. In the New Simple Volume Wizard, you define how much disk space to allocate to the volume and you specify its drive letter.
6. Specify the disk space to allocate to the new simple volume, and then click **Next**.
7. Specify the drive letter to assign to the volume, and then click **Next**.
8. Format the volume using NTFS, and then click **Next**.
9. Disk Management prompts you to confirm the settings. Click **Finish** to continue.
10. Disk Management formats the volume and once the format process completes, it displays a new Healthy (Primary Partition) formatted with NTFS.

You can access the new volume as you would a hard disk attached locally to the system.

Deleting a LUN



CAUTION: When you delete a LUN from a storage pool, you also permanently remove all the data contained in the LUN, including snapshots of the data. If the LUN is replicated to a remote Nexsan Unity site, the replicated LUN, including all the data in the replicated LUN is permanently removed as well.

► To delete a LUN:

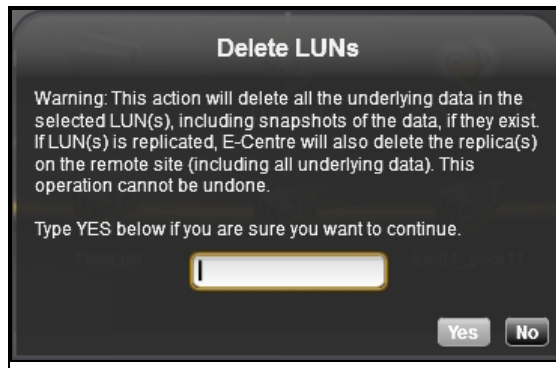
1. In Nexsan Unity's tree view, click the **Site** node to display its child nodes.
2. Click the **Storage Pools** node.
3. Click the storage pool that you want to delete a LUN from.
4. Click the **LUNs** node.

- Perform one of these actions:

To...	Do this
use the LUNs node Properties panel	<ol style="list-style-type: none"> Expand the LUNs node's Properties panel. The LUNs node's Properties panel displays all the LUNs on the storage pool. In the grid, select the LUN that you want to delete from the system.
use the LUN's Properties panel	<ol style="list-style-type: none"> Select the LUN that you want to delete from the storage pool. Expand the LUN's Properties panel.
use the LUN's node context menu	<ol style="list-style-type: none"> Select the LUN that you want to delete from the storage pool. Click the context menu button to open the node context menu.

- Click the **Delete LUN** button. Unity prompts you to confirm the action.

Figure 7-64: confirm LUN deletion



- Type **Yes** in the text box.
- Click the **Yes** button.

Chapter 8

Clustering

The Nexsan Unity has built-in Active/Active Clustering capability, whereby both controller nodes on Unity operate in *active* mode—that is, both controllers can actively serve data in parallel—in addition to providing full redundancy in the event that one of the controller nodes fails.

This section includes these topics:

Clustering overview	294
Viewing cluster health status and controller information	300
Understanding heartbeats	302
Moving cluster resources	304
Restarting the cluster or individual controller nodes	306
Shutting down the cluster or individual controller nodes	307
Modifying IP configuration settings	309
Setting or modifying IPMI settings	316
Enabling jumbo frames	318
Enabling LACP	320
Configuring TCP flow control	324

Clustering overview

The Unity's [Active/Active](#) Clustering configuration provides both high-availability and load balancing for your Nexsan storage infrastructure.

- [High-availability](#) ensures minimal down-time by eliminating a single point of failure with a second controller node. If one controller fails, the Unity automatically fails over system operations and redirects I/O to the second controller on the system.
- [Load balancing](#) allows you to distribute data equally among both controller nodes in the [cluster](#).

To help you achieve load balancing, the Unity uses *Pool Resource Groups*: When you create a storage pool on the Unity, you assign it to one of the two Pool Resource Groups in the cluster. In turn, each Pool Resource Group, along with the storage pools assigned to it, is hosted on one of the two controller on the Unity. End users and client systems on the network access their data (through file systems and/or iSCSI LUNs) in the storage pools using the corresponding Pool Resource Group's *virtual* IP address.

By default, each controller node on the Unity hosts a single Pool Resource Group. This configuration ensures a balanced load on the system. If needed, you can easily modify or reconfigure load balancing on the cluster in Unity: for example, you can move a storage pool from one [Pool Resource Group](#) to the other to balance or rebalance I/O between Pool Resource Groups; or, you can move an entire Pool Resource Group, along with the storage pools assigned to it, from one controller node to the other. In a [failover](#) situation, where one of the controller nodes in the cluster fails, or needs to be shut down for maintenance, the Unity automatically transitions any Pool Resource Group(s) on the [passive](#) controller, along with all its underlying storage pools, to the [active](#) controller.

The process for transitioning Pool Resource Groups between physical controller nodes has no impact on data accessibility, since end users and client systems on the network access their data (through file systems and/or iSCSI LUNs) in storage pools using the corresponding Pool Resource Group's *virtual* IP address, instead of the controller node's *physical* IP address. In other words, the virtual end point through which end users and client systems access their data always remains constant, regardless of the physical controller node that is currently serving up the data. It is important to note, however, that transitioning a storage pool from one Pool Resource Group to the other impacts data accessibility since the virtual end point through which end users and client systems access their data in the storage pool changes.

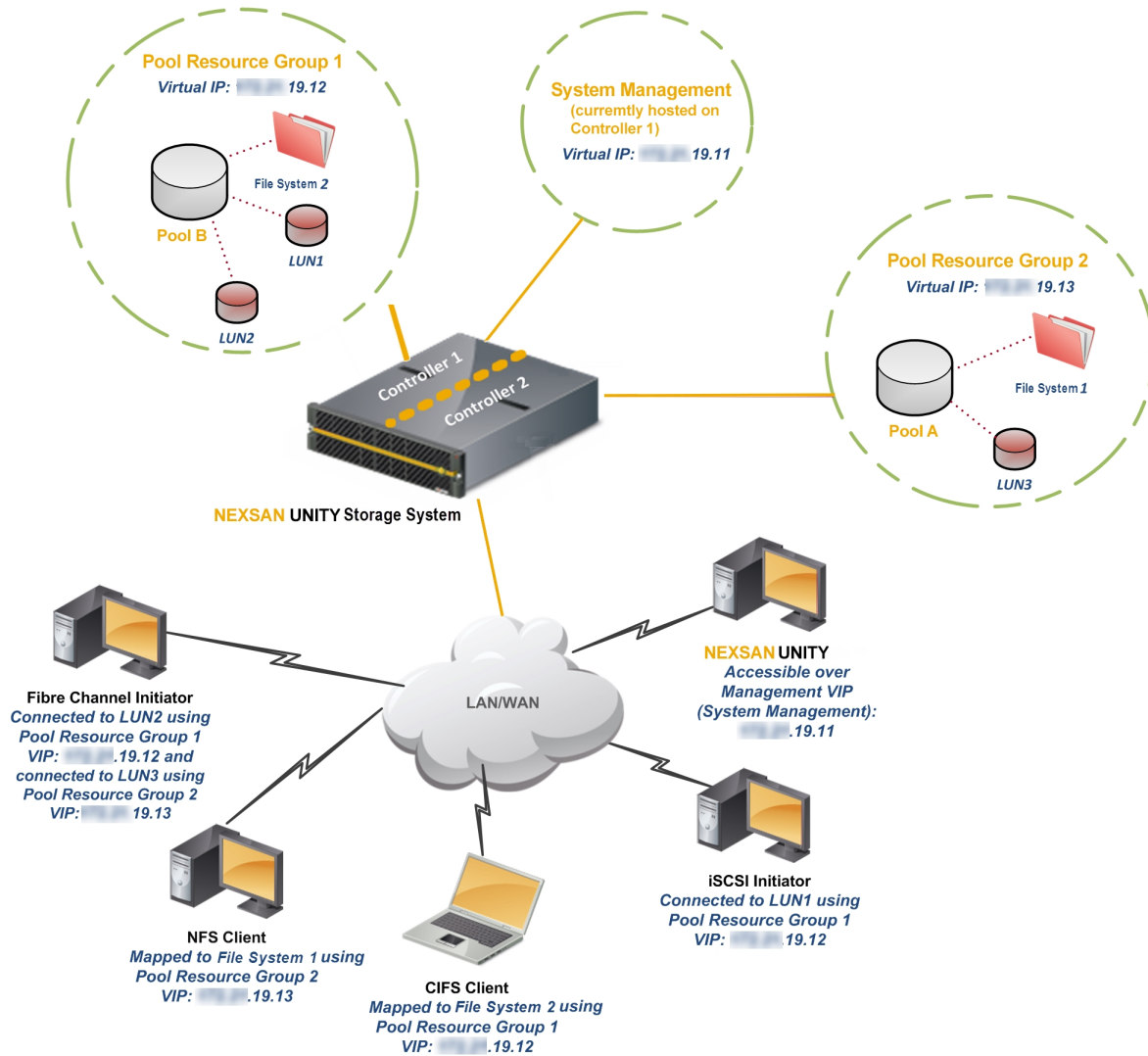
In addition to allowing you to customize load balancing on the cluster, the mechanism for transitioning Pool Resource Groups from one controller to the other gives you the flexibility to plan for and perform hardware maintenance on a specific controller node, with minimal down time and virtually no impact to data accessibility.

Unity 2000P/Unity 4000 Clustering

This diagram illustrates an Active/Active Clustering configuration for the Unity 2000P/Unity 4000; it includes examples demonstrating how client systems access data sets (file systems and/or LUNs) in Pool Resource Groups. The / provides Fibre Channel support, and all LUNs can be accessed through all Fibre Channel ports.

The LUNs hosted by each controller can be accessed through the controller's Fibre Channel ports and iSCSI connections. The direct connection between the controller managing the LUNs and the Fibre Channel host is referred to as the *Optimized Path*. The *All Ports / All LUNs* feature creates an additional access path from one controller to the set of LUNs hosted by the other controller; this is referred to as the *Non-Optimized Path*. As a result, this feature provides uninterrupted access to LUNs by using multipathing.

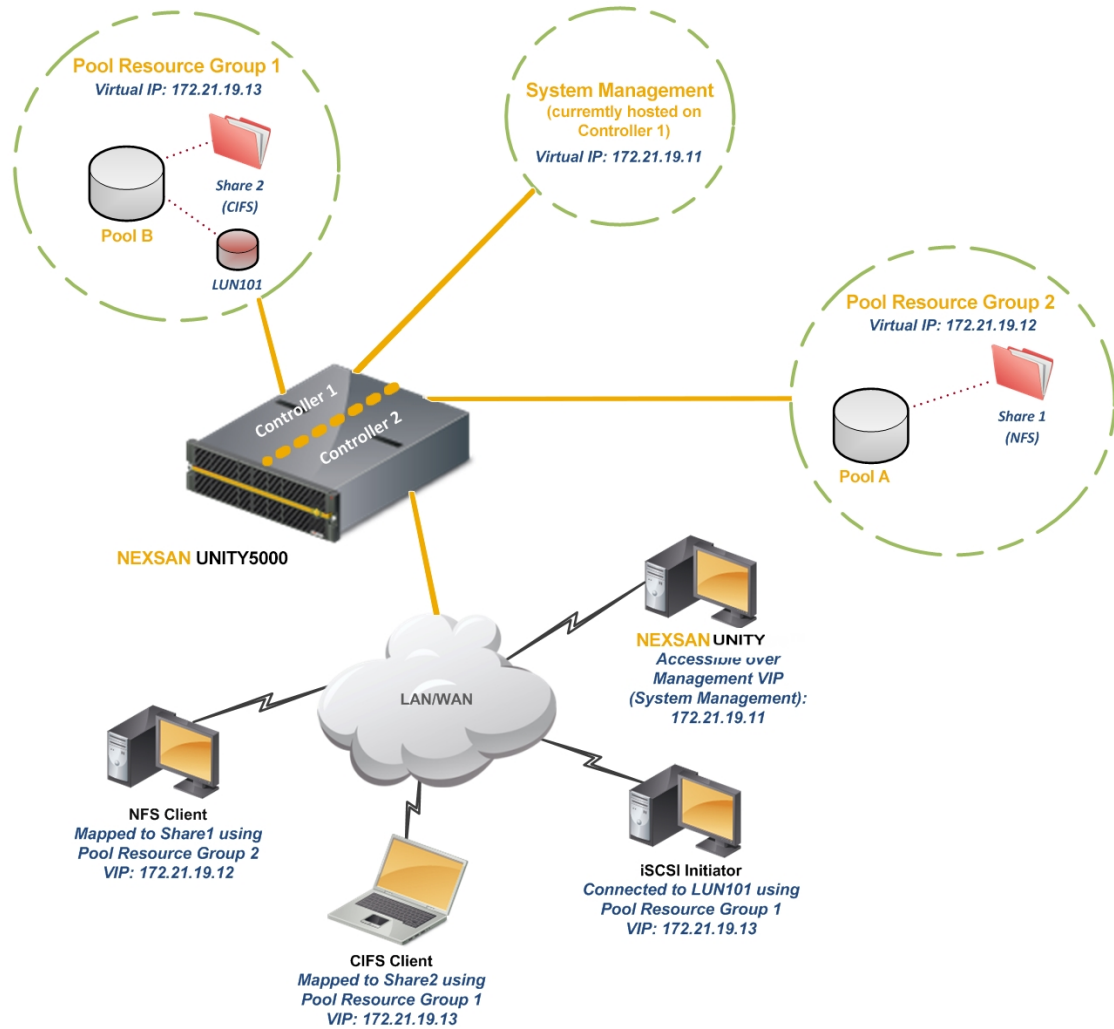
Figure 8-1: Illustration of Active/Active Clustering for the Unity 2000P/Unity 4000



Unity 2000C/Unity 5000 Clustering

This diagram illustrates an Active/Active Clustering configuration for the Unity 2000C/Unity 5000; it includes examples demonstrating how client systems access data sets (shares and/or iSCSI LUNs) in Pool Resource Groups.

Figure 8-2: Illustration of Active/Active Clustering for the Unity 2000C/Unity 5000



Unity 6000 Clustering

The Nexsan Unity 6000 configuration consists of two Active/Active Unity 6000 controllers attached to Nexsan storage devices to provide high-availability during failover. The Unity 6000 provides Fibre Channel support, and all LUNs can be accessed through all Fibre Channel ports.

The Unity 6000 configuration includes the same core technologies for data protection as the standard Unity Active/Active Cluster configuration: Data Replication, Snapshots, automatic controller failover, etc. Each controller can have one or more Nexsan storage systems allocated to it over Fibre Channel or SAS.

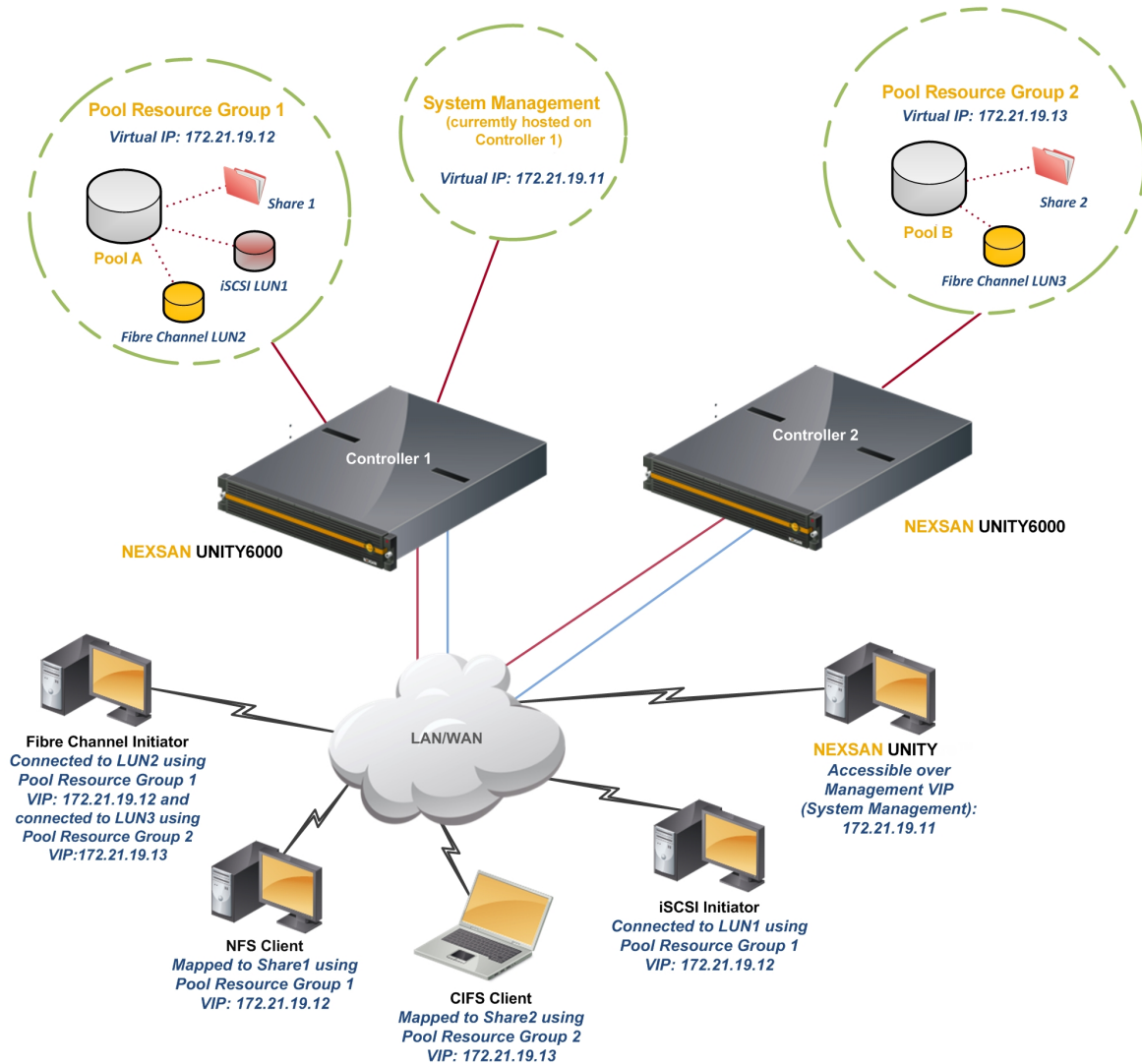
The LUNs hosted by each controller can be accessed through the controller's Fibre Channel ports and iSCSI connections. The direct connection between the Unity 6000 controller managing the LUNs and the Fibre Channel host is referred to as the *Optimized Path*. The *All Ports / All LUNs* feature creates an additional access path from one controller to the set of LUNs hosted by the other controller; this is referred to as the *Non-Optimized Path*. As a result, this feature provides uninterrupted access to LUNs by using multipathing.

The Unity 6000 comes equipped with FASTier write cache—non-volatile high-speed cache memory—which keeps a certain amount of I/O operations in memory in case of:

- power outage: the data gets written to disk while the Unity Vault Protection Module provides power to the Unity 6000.
- controller failure or network connection loss between the controllers: the data gets written to disk while the failover process occurs on the other controller.

This diagram illustrates the Nexsan Unity 6000 Active/Active configuration.

Figure 8-3: Illustration of Active/Active Clustering for the Unity 6000

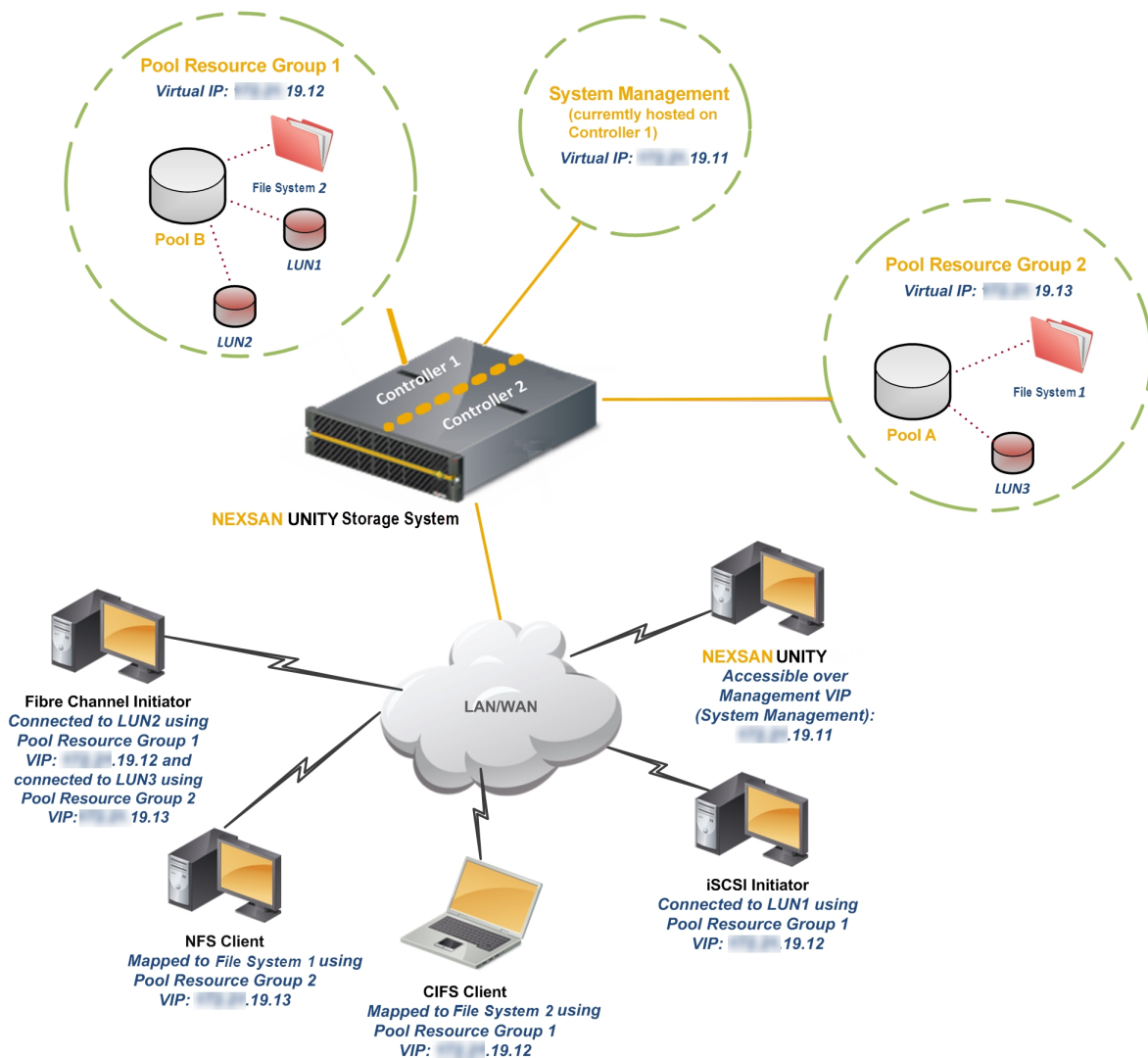


Unity2200 Clustering

This diagram illustrates an Active/Active Clustering configuration for the Unity2200; it includes examples demonstrating how client systems access data sets (file systems and/or LUNs) in Pool Resource Groups. The Unity2200 provides Fibre Channel support, and all LUNs can be accessed through all Fibre Channel ports.

The LUNs hosted by each controller can be accessed through the controller's Fibre Channel ports and iSCSI connections. The direct connection between the controller managing the LUNs and the Fibre Channel host is referred to as the *Optimized Path*. The *All Ports / All LUNs* feature creates an additional access path from one controller to the set of LUNs hosted by the other controller; this is referred to as the *Non-Optimized Path*. As a result, this feature provides uninterrupted access to LUNs by using multipathing.

Figure 8-4: Illustration of Active/Active Clustering for the Unity2200

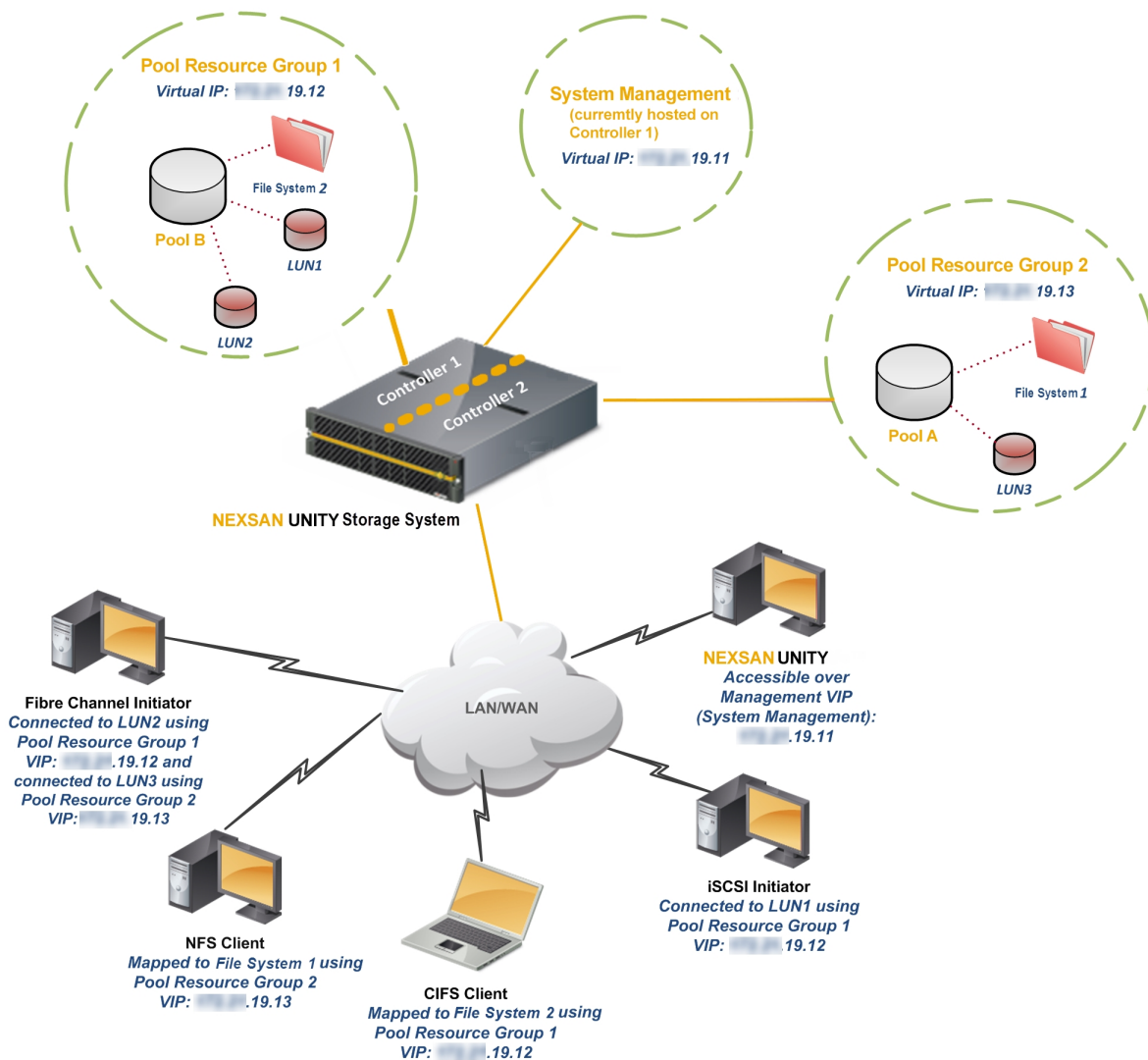


Unity4400 and Unity6900 Clustering

This diagram illustrates an Active/Active Clustering configuration for the Unity4400 and the Unity6900; it includes examples demonstrating how client systems access data sets (file systems and/or LUNs) in Pool Resource Groups. The Unity4400 and the Unity6900 provide Fibre Channel support, and all LUNs can be accessed through all Fibre Channel ports.

The LUNs hosted by each controller can be accessed through the controller's Fibre Channel ports and iSCSI connections. The direct connection between the controller managing the LUNs and the Fibre Channel host is referred to as the *Optimized Path*. The *All Ports / All LUNs* feature creates an additional access path from one controller to the set of LUNs hosted by the other controller; this is referred to as the *Non-Optimized Path*. As a result, this feature provides uninterrupted access to LUNs by using multipathing.

Figure 8-5: Illustration of Active/Active Clustering for the Unity4400 and the Unity6900



Example of data access in a typical Unity cluster implementation

This table represents a typical Unity cluster configuration where each controller node in the cluster hosts a single Pool Resource Group; in turn, each storage pool on the system is assigned to a specific Pool Resource Group:

Controller 1, Physical IP: xxx.xx.19.10	Controller 2, Physical IP: xxx.xx.19.11
Pool Resource Group 1, Virtual IP: xxx.xx.19.12	Pool Resource Group 2, Virtual IP: xxx.xx.19.13
<ul style="list-style-type: none"> Storage Pool(s) assigned to Pool Resource Group 1: <ul style="list-style-type: none"> FinancePool1, containing these data sets: <ul style="list-style-type: none"> share1 (CIFS/NFS) share2 (NFS) LUN101 	<ul style="list-style-type: none"> Storage Pool(s) assigned to Pool Resource Group 2: <ul style="list-style-type: none"> FinancePool2, containing these data sets: <ul style="list-style-type: none"> share3 (CIFS) LUN201

In order for a client system on the network to access *share3* in *FinancePool2* (on physical Controller 2 in the cluster), the client must use the virtual IP address for Pool Resource Group 2; in this case, **xxx.xx.19.13**.

The CIFS mount point for *share3* is, therefore, represented as:

```
\\xxx.xx.19.13\share3
```

This mount point remains constant even if we transition Pool Resource Group 2 to Controller 1.

However, if we reassign *FinancePool2* to Pool Resource Group 1 (by moving it out of Pool Resource Group 2), the mount point for *share3* changes:

```
\\xxx.xx.19.12\share3
```

Viewing cluster health status and controller information

This section explains how to view status information for a Unity cluster, including the:

- health of the cluster
- status of each controller node (whether each node is up or down)
- cluster license status
- cluster type
- chassis inter-connect card status (Unity 2000, Unity 4000, Unity 6000)

▶ To view cluster status information:

- If you are managing multiple sites (multi-site management of remote systems): in Unity's tree view, click the Site node representing Unity that you want to view cluster status information for.
- Click the **Cluster Settings** node.

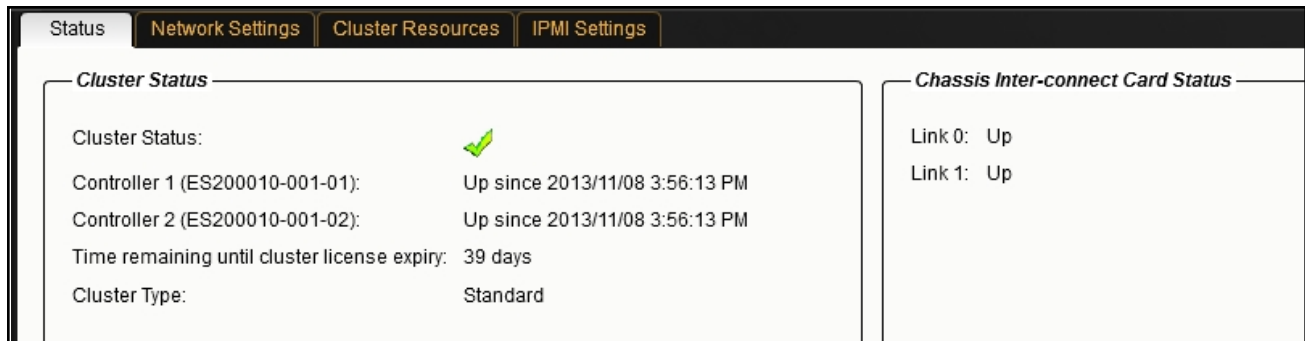
- Click the node representing the two controllers on Unity.

Note When hovering the mouse over the node, a tool tip displays to provide information about the current Cluster health, such as the Unity Vault Module status, APAL status and APAL channel, and network connection status. This information also appears in the Event Viewer.

```
Press Ctrl+C to copy to clipboard.
Network connection ixgbe0 (in aggregate nx0) on
ES606100-001-01 is not connected or is malfunctioning.
Network connection nx0 on ES606100-001-01 is partially
disconnected or is malfunctioning.
Network connection ixgbe1 (in aggregate nx0) on
ES606100-001-02 is not connected or is malfunctioning.
Network connection nx0 on ES606100-001-02 is partially
disconnected or is malfunctioning.
```

- Expand the controller node's Properties panel.

Figure 8-6: Cluster Settings Properties panel—Status tab



- Select the **Status** tab. The **Status** tab provides this information for the cluster:

- the health of the cluster: a check mark next to **Cluster Status** indicates the cluster is healthy—that is, both controller nodes on Unity are operating within normal parameters. An **X** indicates that the cluster is unhealthy: one of the controller nodes is down, or not responding. When the cluster is in an unhealthy state, the error condition trickles down Unity's tree view: a red **X** is superimposed over the Site, Clusters, and controller nodes to indicate the error condition and help you identify the source.
- the status and position of each controller: the **Status** tab identifies the host id of each controller and whether each controller is **Up** (operational) or **Down** (non-responsive). In addition, the **Status** tab indicates the physical position/location of each controller node in the Unity 5000 chassis: left or right side of the chassis, when viewing the chassis from the front.
- the cluster type: the **Status** tab also displays the license type and status, that is, the amount of time remaining until the license expires. If the license is about to expire, you will see a warning icon.
- the chassis inter-connect card status (Unity 2000, Unity 4000, Unity 6000): The chassis inter-connect card ensures a constant and direct connection between with the two controllers, with two cables connected to the HBA card on the back of each controller's chassis. For connection details, see the *Nexsan Unity Hardware Reference Guide*.

Each card is represented by a link number. Both links should display *Up*. If the status is *Down* or *Unknown*, verify your cable connections. To see if the chassis inter-connect card is enabled, see [Viewing APAL status](#) on page 403.

Note Unity prevents you from performing some tasks and operations when the cluster is an unhealthy state—that is, when one of its controller nodes is **Down** (non-responsive); for more information, see [List of tasks and operations that you cannot perform when one of the controller nodes is down](#) below.

List of tasks and operations that you cannot perform when one of the controller nodes is down

These are the tasks and operations that you cannot perform in Unity when the cluster is an unhealthy state—that is, when one of its controller nodes is **Down** (non-responsive):

- Adding or deleting storage pools
- Modifying network settings
- Unjoining, joining a domain, or modifying domain settings
- Moving, or transitioning, cluster resources between controller nodes
- Moving storage pools from one controller node to the other

Understanding heartbeats

Unity uses heartbeats and reservations to enable communication between the two cluster nodes, thus increasing cluster reliability. There are two layers of cluster heartbeats, and at least one layer of heartbeat must be active:

- **Private network (Private0) layer:** This is the network layer for private communication between the two controller nodes. Disk heartbeats sent and received between controller nodes over the private network ensure that they are communicating with each other.
- **Disk layer:** The disk layer provides an additional heartbeat path for the cluster on top of the heartbeat validation provided by the private network layer. For Unity Storage Expansions, each Unity controller node periodically writes to and reads from dedicated regions of a data disk. For Nexsan E-Series, each controller node periodically writes to and reads from a dedicated volume (a virtual LUN).

If the private network connection fails, Unity relies on the Disk layer to allow heartbeats to continue normally, thus preventing a failover situation. When all heartbeats are down on both the Private0 and Disk layers, the controller assumes that its peer is down and restarts the service group. If a heartbeat is detected, no failover occurs.

Transient and persistent reservations with disk heartbeats

Disk heartbeats can prevent a split-brain situation on Unity, where both controllers are active and both try to manage storage, which results in data corruption. The Active/Passive state is applied at the pool resource group level. For example, a node can be active for Pool Resource Group 1 and passive for Pool Resource Group 2.

Unity supports two reservation types: Transient and persistent. Both reservation types store reservation data on three volumes or drives per storage pool.

Each controller writes its state on a shared disk and reads the state of the peer. A reservation flag is set on a separate shared disk for persistent reservations, and on the same disk for transient reservations. The reservation prevents corruption if a split brain occurs by triggering a failure mechanism and causing a controller reboot.

Transient reservation

Unity Storage Systems with Unity Storage Expansions or NST Storage Expansions use transient reservation.

Transient reservation is temporary and expires automatically after two seconds if a heartbeat is detected on the peer controller. If one controller node fails, the peer controller makes a reservation and becomes the active controller. When the failed controller comes back online, it becomes the passive controller and does not make a reservation. See [Disk heartbeating—Comparison between transient and persistent reservation](#) below.

Persistent reservation

Unity Storage Systems with an attached Nexsan E-Series Storage System (head unit) with firmware version 1204 or higher use persistent reservation.

For persistent reservation, heartbeats are stored on virtual LUNs, which are Random Access Memory (RAM) volumes. Heartbeats are stored on one virtual LUN per E-Series enclosure.

Persistent reservation is preserved until removed, either by the owning controller when failing over gracefully, or by the peer controller when failing over ungracefully. The active controller writes heartbeats on disk and makes a reservation. If the active controller fails, the passive controller removes the existing reservation and makes its own reservation. It thus becomes the active controller. When the failed controller comes back online, it will not make a reservation and becomes the passive controller.

For both transient and persistent reservations, if the controller that fails is the passive controller, it remains passive. You can change the Unity configuration to make the passive controller active if required, or leave it as passive. With transient reservations, if the passive controller is not responding, that is, becomes "frozen", and makes a reservation on disk, Unity will have two active controllers and a split-brain, which results in data corruption.

The main difference between transient and persistent reservations occurs when a controller freezes. If the frozen controller is the active controller, it may reboot again after it comes back online. Specifically, when the former active controller attempts to access the storage pool, a reservation conflict occurs since it does not own the reservation anymore, causing it to reboot and resulting in potential data corruption. When the controller is back online, it sees that the peer controller has taken over, and assumes the passive state. In systems using persistent reservation, the peer node becomes the active controller and makes the reservation.

The following table provides details when controllers are in normal, failed, and frozen states, and the differences in the behavior of transient and persistent reservation. The scenarios assume Controller 1 is the active controller and Controller 2 is the passive controller.

Table 8-1: Disk heartbeating—Comparison between transient and persistent reservation

State	Transient reservation	Persistent reservation
Normal	<ol style="list-style-type: none"> 1. Controller 1 makes a reservation. 2. Controller 1 sets the failure flag (failure mechanism if there is a reservation conflict). 3. Controller 1 waits 2 seconds and removes reservation. 4. Controllers 1 and 2 exchange heartbeats periodically. 	<ol style="list-style-type: none"> 1. Controller 1 makes a reservation. 2. Controller 1 sets the failure flag. 3. Controllers 1 and 2 exchange heartbeats periodically.

State	Transient reservation	Persistent reservation
Controller failure	<ol style="list-style-type: none"> 1. Controller 1 fails and does not send a heartbeat. 2. Controller 2 starts the Pool Resource Group. 3. Controller 2 makes a reservation (devices are not reserved at this point). 4. Controller 2 sets the failure flag. 5. Controller 2 removes reservation after 2 seconds. 6. Controller 1 comes back online. 7. Controllers 1 and 2 exchange heartbeats. 8. Controller 1 sees Controller 2 is now the active controller and remains passive. 	<ol style="list-style-type: none"> 1. Controller 1 fails and does not send a heartbeat. 2. Controller 2 starts the Pool Resource Group. 3. Controller 2 makes a reservation by overwriting Controller 1's reservation. 4. Controller 2 sets the failure flag. 5. Controller 1 comes back online. 6. Controllers 1 and 2 exchange heartbeats. 7. Controller 1 sees Controller 2 is now the active controller and remains passive.
Controller freeze	<ol style="list-style-type: none"> 1. Controller 1 freezes and does not send a heartbeat. 2. Controller 2 starts the Pool Resource Group. 3. Controller 2 makes a reservation (devices are not reserved at this point). 4. Controller 2 sets the failure flag. 5. Controller 2 removes its reservation. 6. Controller 1 unfreezes. 7. Controller 1 does not get a reservation conflict, because the reservation was removed. <p>This results in a split-brain situation.</p>	<ol style="list-style-type: none"> 1. Controller 1 freezes and does not send a heartbeat. 2. Controller 2 starts the Pool Resource Group. 3. Controller 2 makes a reservation by overwriting Controller 1's reservation. 4. Controller 2 sets the failure flag. 5. Controller 1 unfreezes. (<i>how?</i>) 6. Controller 1 gets a reservation conflict and reboots (since Controller 2 now owns the reservation). 7. Controller 1 comes back up and is now passive. <p>The split brain situation is avoided.</p>

Moving cluster resources

If one of the controller nodes fails for any reason, the Unity automatically fails over all system operations and redirects I/O to the second controller on the system. This includes failing over cluster resources—for example, Pool Resource Groups or the System Management component—if they are currently hosted on the failed, or inactive, controller. This process is completely automated, and requires no user intervention.

You can manually move cluster resources—including Pool Resource Groups and the System Management component—from one controller node to the other if you need to perform routine or emergency maintenance on a controller node—for example, to replace a failed component, or upgrade a component.



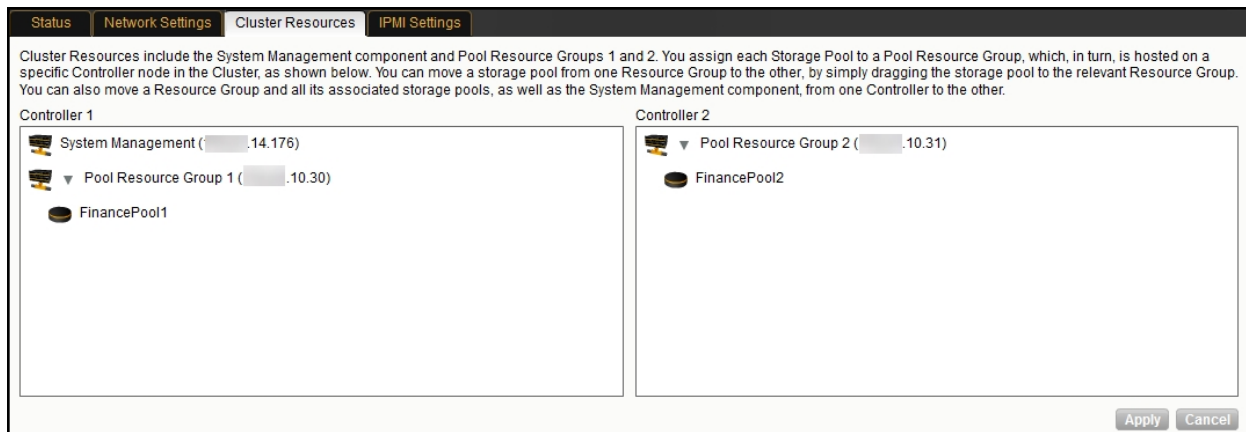
CAUTION: When you move cluster resources from one controller to the other, client systems and applications on the network will temporarily lose connection to data sets (file systems and/or iSCSI LUNs) onUnity—until the move operation completes and the cluster comes back online; this could result in delays, or potentially timeouts.

Before moving cluster resources, make sure that client systems with an active connection to any file systems or iSCSI LUNs onUnity are disconnected; also make sure to quiesce any applications with an active connection toUnity.

► **To move cluster resources from one controller node to the other:**

1. If you are managing multiple sites (multi-site management of remote systems): in Unity's tree view, click the Site node representing the clustered Unity that you want to perform a manual switchover on.
2. Click the **Cluster Settings** node.
3. Expand the **Cluster Settings** node's Properties panel.
4. Select the **Cluster Resources** tab. The Cluster Resources tab provides a visual representation of where each resource in the cluster is currently hosted: Controller 1 or Controller 2. In addition, the Cluster Resources tab indicates the Pool Resource Group that each storage pool on the systems is currently assigned to.

Figure 8-7: Site node's properties panel—Cluster Resources tab



5. Select the cluster resource that you want to move to by clicking it in the corresponding Controller box, and then drag the resource to the controller that you want to move the resource to.

Note You can also move storage pools from one Pool Resource Group to other; see [Moving a storage pool on page 116](#).

6. If needed, move additional cluster resources.
7. Click the **Apply** button.
8. Unity prompts you to confirm the action. Click **Yes** to continue.

Unity informs you when the process completes.

Restarting the cluster or individual controller nodes

You may need to occasionally restart the Unity, or one of its controller nodes—for example, when you make changes to the configuration of the Unity that requires a reboot.

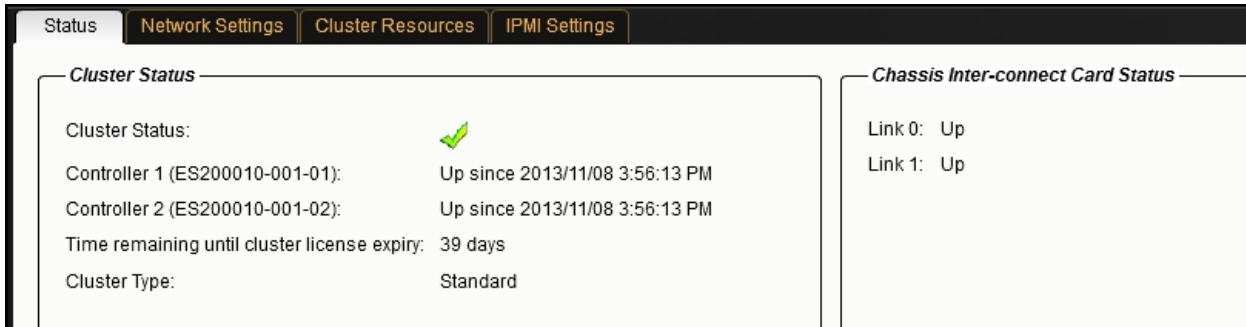


CAUTION: When you restart the Unity, or one of its controller nodes, client systems and applications on the network will temporarily lose connection to the Unity—until the cluster comes back online; this could result in host delays, or potential timeouts. Before restarting the Unity, or one of its controller nodes, make sure that client systems with an active connection to any data set (file systems and/or iSCSI LUNs) on the Unity are disconnected; also make sure to quiesce any applications with an active connection to the Unity.

► **To restart the Unity, or one of its controller nodes:**

1. If you are managing multiple sites (multi-site management of remote systems): in Unity's tree view, click the Site node representing the clustered Unity that you want to restart.
2. Click the **Cluster Settings** node.
3. Expand the controller node's Properties panel, by clicking the **Properties** tab.

Figure 8-8: Cluster Settings properties panel—Status tab



4. Click the **Restart Controllers** button. This displays the Restart Controllers popup.

Figure 8-9: Restart Controllers popup



5. Select one of the available options:
 - To restart the entire cluster (both controllers on the Unity): Select the **Both** option.
 - To restart only one controller: Select the corresponding controller: **Controller 1** or **Controller 2**.
6. Click **Yes** to continue.

Unity restarts the clustered Unity, or the selected controller. This process may take some time to complete.

Notes:

- If you restart both controllers on the Unity, client systems and applications on the network will temporarily lose connection to the Unity—until the cluster comes back online.
- If you restart only the *passive* controller—that is, the controller node where the System Management component is currently NOT hosted—Unity transitions any Pool Resource Group on the controller, along with the storage pools assigned to it, to the other controller node; Unity also changes the status of the controller as being *Down*, and a warning condition trickles down through Unity's tree view—until the controller comes back online.
- If you restart only the *active* controller—that is, the controller node where the System Management component is currently hosted—Unity transitions the System Management component to the other controller—making it the active node in the cluster. Nexsan Unity also transitions any Pool Resource Group on the controller, along with the storage pools assigned to it, to the new active controller. In addition, Nexsan Unity changes the status of the controller node that you restart as being *Down*, and a warning condition trickles down through Nexsan Unity's tree view—until the controller comes back online.

Shutting down the cluster or individual controller nodes

You may need to shut down the Unity, or one of its controller nodes, to perform maintenance on the system, such as, replacing a faulty hardware component, or upgrading a component.



CAUTION: When you shut down the Unity, or one of its controller nodes, client systems and applications on the network will temporarily lose connection to the Unity—until the cluster comes back online; this could result in host delays or potentially timeouts. Before restarting the Unity, or one of its controller nodes, make sure that client systems with an active connection to any data set (file systems and/or iSCSI LUNs) on the Unity are disconnected; also make sure to quiesce any applications with an active connection to the Unity.

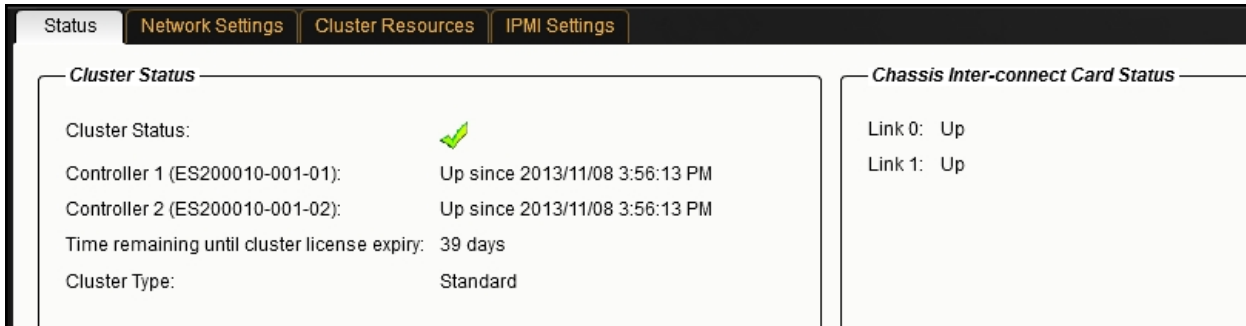
The shut down process quiesces system services on the Unity; it does not physically shut down the system. When you shut down the Unity, wait a few minutes, and then press the power button on the front of the Unity chassis for 1.5 seconds to completely shut off the system; if you shut down one of the controller nodes in the cluster, wait a few minutes, and then remove the corresponding controller node's power cable from the back of the Unity Storage System.

► To shut down the Unity, or one of its controller nodes:

1. If you are managing multiple sites (multi-site management of remote systems): in Unity's tree view, click the Site node representing the clustered Unity that you want to shut down.
2. Click the **Cluster Settings** node.

- Expand the controller node's Properties panel, by clicking the **Properties** tab.

Figure 8-10: Cluster Settings properties panel—Status tab



- Click the **Shut Down Controllers** button. This displays the Shut Down Controllers dialog box.

Figure 8-11: Shut Down Controllers popup



- Select one of the available options:
 - To shut down the entire cluster (both controllers on the Unity): Select the **Both** option.
 - To shut down a controller node: Select the corresponding controller: **Controller 1** or **Controller 2**.
- Click **Yes** to continue. Unity shuts down the Unity, or the selected controller. This process may take some time to complete.

The shut down process quiesces system services on the Unity; it does not physically shut down the system:

- If you shut down the Unity (both controllers in the cluster), wait a few minutes, and then press the power button on the front of the Unity chassis for 1.5 seconds to completely shut off the system;
- If you shut down one of the controller nodes in the cluster, wait a few minutes, and then remove the corresponding controller node's power cable from the back of the Unity Storage System.

Notes: If you shut down...

- both controllers on the Unity, client systems and applications on the network will lose connection to the Unity—until you bring the system back online.

- only the *passive* controller—that is, the controller node where the System Management component is currently NOT hosted—Unity transitions any Pool Resource Group on the controller, along with the storage pools assigned to it, to the other controller node; Unity also changes the status of the controller as being *Down*, and a warning condition trickles down through Unity's tree view—until the controller comes back online
- the *active* controller—that is, the controller node where the System Management component is currently hosted—Unity transitions the System Management component to the other controller—making it the *active* node in the cluster. Unity also transitions any Pool Resource Group on the controller, along with the storage pools assigned to it, to the new *active* controller. In addition, Unity changes the status of the controller node that you shut down as being *Down*, and a warning condition trickles through Unity's tree view—until the controller comes back online.

Modifying IP configuration settings

This section describes the process for modifying Unity network settings. You can modify network settings for both the primary data network interface (nx0) and the management interface (nx99). For more information about nx0 and nx99, see the Nexsan Unity Software User Guide.



CAUTION: Client systems using these IP addresses will lose connection to Unity. Before modifying IP addresses, disconnect client systems, and quiesce any applications with an active connection to Unity.

If you modify Resource Group virtual IP addresses, you will need to manually update all file system and LUN mappings on client systems to reflect the new virtual IP addresses.

▶ To modify network settings on Unity:

1. From the **Unity dashboard**, select **Cluster Settings**. The Cluster Settings panel opens.
2. Select **Status > IP Configuration**.
3. Modify the relevant IP address for the primary data network interface (nx0) by changing the values in the corresponding fields.
4. Optionally, modify IP address settings for the management interface (nx99).
5. If needed, modify IP address settings for the Default gateway for Unity, as well as for the preferred DNS server; and (optionally) the IP address of the alternate DNS server. These settings are applied globally to all network interfaces on the system.
6. If an E-Series storage system is connected to Unity, and you want Unity to automatically set the new IP addresses for the subnet mask, default gateway, and DNS server on the storage system, select the **Set the Subnet Mask, Default Gateway, and DNS on all externally-attached Unity Storage Systems** option; this option is only displayed if Unity has a Nexsan E18, Nexsan E48, or Nexsan E60 storage system attached to it via SAS (or Fibre Channel), and allocated to the site.
7. Click the **Apply** button to set the new IP and network settings on Unity, and if applicable, on any Nexsan E18, Nexsan E48, or Nexsan E60 storage system attached to Unity.
Unity modifies the network settings on Unity; it informs you once the process completes.
8. Depending on the network settings you modified, you may be required to restart Nexsan Unity.

Understanding IP address requirements

In a typical configuration, Unity requires a total of 8 IP addresses:

- 3 for the management interface (nx99), and
- 5 for the primary data network interface (nx0).

These 8 IP addresses include a combination of physical and virtual IP addresses. You use virtual IP addresses for accessing Nexsan Nexsan Unity on the management interface (nx99) and for accessing data (file systems and/or LUNS) in Pool Resource Groups on the primary data network interface (nx0). Virtual IP addresses allow end users and client systems on the network to access Unity as a single entity.

IP addresses are also required for Nexsan E-Series storage. Nexsan E-Series enclosures shipped for use with Unity are DHCP-enabled. During the Site Setup process, you must specify static IP addresses for all E-Series storage enclosures.

The IPMI interface also requires 2 additional IP addresses: 1 per controller.

These tables list the IP addresses required for the network interfaces on Unity, including information about what each IP address is used for.

Table 8-2: Management interface (nx99) IP addresses

Management Interface (nx99)	Required IP addresses
The management interface requires 3 IP addresses.	
1. <u>Management Virtual IP address</u>	You use this IP address to manage Unity via Nexsan Unity: simply type the IP into your internet browser's address bar to access Nexsan Unity. The management virtual IP is set for the cluster as a single entity; thus, if a controller node fails, the system always remains accessible.
2. <u>Controller 1 (physical) IP address</u>	Physical IP that you must set on the management interface (nx99) for the first controller node in the Cluster.
3. <u>Controller 2 (physical) IP address</u>	Physical IP that you must set on the management interface (nx99) for the second controller node in the Cluster.

Table 8-3: Primary data network interface (nx0) IP addresses

Primary data network interface (nx0)	Required IP addresses
The primary data network interface (nx0) is the entry point for accessing data in file systems and LUNs. This is the network interface that client systems on the network use to connect to the system for data access.	
The primary data network interface requires 5 IP addresses.	
1. <u>Intersite Virtual IP address</u>	This IP address enables connectivity between 2 or more Unity Systems for data replication and inter-site communication. Specifically, when you set up data replication, the system prompts you to specify the intersite virtual IP of Unity to replicate data to. This IP address is required even in single-site implementations.
2. <u>Controller 1 (physical) IP address</u>	Physical IP that you set on the primary data network interface (nx0) for the first controller node in the Cluster.
3. <u>Controller 2 (physical) IP address</u>	Physical IP that you set on the primary data network interface (nx0) for the second controller node in the Cluster.

Primary data network interface (nx0)	Required IP addresses
<ol style="list-style-type: none"> 4. <u>Pool Resource Group 1 Virtual IP address</u> 5. <u>Pool Resource Group 2 Virtual IP address</u> 	<p>When you create a storage pool on Unity, you assign it to one of the two Pool Resource Groups in the cluster. End users and client systems on the network use the corresponding Pool Resource Group's virtual IP to access their data in the storage pool. For load balancing, each Pool Resource Group is hosted on one of the two controller nodes in the cluster.</p> <p>If a controller node fails, Unity transitions the Pool Resource Group(s) on the failed controller, along with all its underlying storage pools, to the surviving controller. Data accessibility is NOT impacted, since end users and client systems can continue accessing their data using the corresponding Pool Resource Group's virtual IP.</p>

Understanding Network interfaces and required IP addresses

Network interfaces and required IP addresses

Unity provides these network interfaces:

1. Management interface (nx99): Management traffic only

You use the management interface to manage Unity Storage Systems using the Unity software. Unity allows the management interface to be on a different subnet without requiring explicit routing. The dedicated management interface only carries management traffic; for example: access to Nexsan Unity, SMTP, SNMP, and SSH. All network traffic related to data access (file systems and iSCSI LUNs) is restricted to the other interfaces on the system.

On the Unity 6000 and next generation Unity Storage Systems, the on-board NIC 1 GigE port is dedicated to Unity's management interface (as well as the IPMI interface).

2. Primary data network interface (nx0): Data traffic only

You use the primary data network interface to access data on Unity (via file systems and/or iSCSI LUNs). On some systems, depending on the model and configuration of the system, the on-board LAN 1 port (top-most port) is configured as the primary data network interface.

If the Unity 5000 is equipped with one of the optionally available GigE or 10GigE network interface cards, the primary data network interface is always set on the add-on card.

On the Unity 6000 and next generation and Unity Storage Systems, the 10GigE I/O module serves as the primary data network interface (nx0).

3. Private0: Between peer controllers on a Unity Storage System or Unity Storage Enclosure only

This is the network layer for private communication between the two controller nodes on Unity. You MUST never delete or modify this entry, nor any of the ports assigned to it; doing so will break the system.

On the Unity 2000, Unity 4000, and Unity 5000, private connectivity is internal.

On the Unity 6000 and next generation Unity Storage Systems, private connectivity is performed by plugging the chassis inter-connect HBA cables/network cables between the two controllers.

By default, all ports on an optionally available GigE or 10GigE network interface cards are aggregated as one interface for redundancy. For example, all 4 RJ-45 ports on the optionally available 1GigE Quad-port Network

PCIe card are aggregated as a single interface; this provides redundancy in the event that data connectivity on one of the ports is interrupted.

Note Connecting a 10GigE network interface card to a 100 Mbps switch is NOT supported.

This section covers the following topics:

Understanding link layers

The nxadmin Command-line interface (CLI) provides the `nic` command to view and configure link layer and aggregation information on Unity. The information provided in this section assumes that Unity has the management interface (nx99) connected and configured.

The Unity 2000C and Unity 2000P have a 2-port onboard network interface with one port configured as primary data network interface (nx0)—on each controller node

The Unity 4000 has a 2-port or 4-port network interface (add-on) card configured as the primary data network interface (nx0)—on each controller node.

The Unity 5000 has a 4-port network interface (add-on) card configured as the primary data network interface (nx0)—on each controller node.

The Unity 6000 uses a 10GbE I/O module configured as the primary data network interface (nx0)—on each controller node.

► **To view link layer information on Unity:**

1. Access the nxadmin CLI as described in the *nxadmin Command-line Interface Reference Guide*.
2. At the prompt, type:
`nic show-link`
3. Press the Enter key.

This is the typical output of this command on an Unity with the management interface (nx99) and a 4-port network interface (add-on) card configured as the primary data network interface (nx0).

Figure 8-12: Viewing link layer information

```
ES200100-001-02:P:/> nic show-link
LINK          CLASS      MTU      STATE    BRIDGE      OVER
igb0          phys      1500    up       --          --
igb1          phys      1500    unknown --          --
ixgbe0        phys      1500    up       --          --
ixgbe1        phys      1500    up       --          --
ixgbe2        phys      1500    up       --          --
ixgbe3        phys      1500    up       --          --
nx0           aggr      1500    up       --          ixgbe2 ixgbe3
private0      aggr      1500    up       --          ixgbe0 ixgbe1
nx99          aggr      1500    up       --          igb0
ES200100-001-02:P:/>
```

This list provides detailed information about the entries displayed in the link layer output:

- `private0`: This is the network layer for private communication between the two controller nodes on Unity. You **MUST** never delete or modify this entry, nor any of the ports assigned to it; doing so will break the system.
- `nx0`: This is the primary data network interface; it must always exist.
- `nx99`: This is the management interface; it must always exist.

- **nx#**: This identifies secondary data network interfaces (if configured)—typically, nx1, nx2, and so on. You **MUST** configure each interface on a separate subnet. Additionally, each interface **MUST** exist on both controller nodes; this is required to use Unity’s network configuration utility (`setip`) to configure network settings on the interfaces.
- **igb#**, **ixgbe#**: These identify physical ports. The ports are assigned to these interfaces:
 - **ixgbe0** and **ixgbe1**: These ports are assigned to the **private0** interface. You **MUST** never delete or modify these ports.
 - **igb0**: This is the on-board LAN1 port, located at the bottom of each controller node, closest to the bottom-edge of the controller box. It is assigned to the management interface (nx99).
 - **igb1**: This is the on-board LAN2 port, located just above the LAN1 port on each controller node; it is unused.
 - **ixgbe2** and **ixgbe3**: These are the 2 ports on a 2-port, add-on network interface card (NIC)—if installed. The number and designation of these ports differ depending on the type of add-on NIC installed on Unity. If the add-on card has 4 ports, you will also see **ixgbe4** and **ixgbe5**.
 In a typical configuration, all ports on the add-on NIC are aggregated under **nx0** (primary data network interface).

Setting up a secondary network interface

This section describes the process for creating a secondary network interface on Unity using the Unity CLI.

Setting up new network interfaces is useful in these scenarios:

- To be able to use different subnets, in which case you separate the ports into different aggregations (there must be at least one port available to create an aggregation);
- To add and use a new network card, in which case you create one or more aggregations with the ports of the new network card.

This procedure provides an example for separating the default aggregation on a 4-port network card, using two ports for one aggregation and the other two ports for the second aggregation. Since the ports must not be currently assigned to another interface, you must remove them from that interface first, then you add them to the new network interface.



CAUTION: Each new network interface **MUST** be on a different subnet. However, the nx99 (management interface) can coexist with one other network interface in the same subnet.

► To set up a secondary network interface:

1. On **BOTH** controller nodes, remove ports from the nx0 (primary data network interface):
 - a. On the first controller node, for example, to remove **igb4** and **igb5** from **nx0**, type:


```
nic remove-aggr -l igb4 -l igb5 nx0
```
 - b. Press the Enter key.
 - c. Repeat these steps on the other controller node.
 - d. Use the `nic show-link` command to ensure that the link layer configuration is identical on both nodes.

2. On BOTH controller nodes, use the ports you remove from the nx0 interface to create a secondary network interface, typically, *nx1* (all network interfaces must start with **nx**):
 - a. On the first controller node, type this command to add the ports you removed from nx0 to create nx1, in our example, *igb4* and *igb5* :

```
nic create-aggr -l igb4 -l igb5 nx1
```
 - b. Press the Enter key.
 - c. Repeat these steps on the other controller node.
 - d. Use the `nic show-link` command to ensure that the link layer configuration is identical on both nodes.

3. Configure network settings on the secondary network interface:

Note You need only perform this operation on one controller node in the cluster; the `setip` utility automatically applies the network settings to the second controller node.

- a. On ANY controller node, type:

```
setip
```

- b. Press the Enter key. This displays the IP configuration screen where you set or modify the network settings for all network interfaces on Unity.

```

NST IP Configuration Utility
- Use the Enter key or the arrow keys to navigate between fields
- Use the Tab key to navigate between fields and buttons
- Selecting OK prompts the system to validate all IP settings
  even if changes were not made

Default Gateway           : ██████████.12.254
Domain Name               : qadomain.net
DNS Server 1              : ██████████.14.30
DNS Server 2              :
Management Interface (nx99)
  Controller 1 Physical IP : ██████████.200.10
  Controller 2 Physical IP : ██████████.200.11
  Management Virtual IP   : ██████████.200.12
  Subnet Mask              : 255.255.0.0

Primary Data Interface (nx0)
  Controller 1 Physical IP : ██████████.200.10
  Controller 2 Physical IP : ██████████.200.11
  Intersite Virtual IP    : ██████████.200.12
  Resource Group 1 Virtual IP : ██████████.200.13
  Resource Group 2 Virtual IP : ██████████.200.14
  Subnet Mask              : 255.255.0.0

Secondary Data Interface (nx1)
  Controller 1 Physical IP :
  Controller 2 Physical IP :
  Intersite Virtual IP    :
  Resource Group 1 Virtual IP :
  Resource Group 2 Virtual IP :
  Subnet Mask              :

                                                                    100%
  < OK >      <Validate>      < Cancel >      < Help >

```

- c. Use the Tab key to navigate down to the **Controller 1 IP** field under **Network nx1**, and enter a valid IP address. Repeat this process for each field under **Network nx1**.
- d. When you finish configuring network settings for Network nx1, tab to the **<Validate>** option and press the Enter key; Unity validates the network settings.
- e. Once the validation process completes successfully, tab to the **<OK>** option and press Enter to apply the network settings to the system.

Note For more details on the `nic` and `setip` commands, refer to the *nxadmin Command-line Interface Reference Guide*.

Setting or modifying IPMI settings

Unity supports [IPMI](#) over LAN. To enable IPMI for Unity, you must connect a network cable to the second on-board 1 Gb LAN port at the back of each controller on Unity chassis; this second LAN port is located at the bottom of each controller node, closest to the bottom-edge of the controller box.

► **To set IPMI settings:**

1. If you are managing multiple sites (multi-site management of remote systems): in Unity's tree view, click the Site node representing Unity that you want to modify IPMI network settings for.
2. Click the **Cluster Settings** node.
3. Expand the controller node's Properties panel.

Figure 8-13: Cluster Settings properties panel—IPMI tab

4. Select the **IPMI** tab.
5. Modify IPMI network settings for Unity by overwriting any existing values in the relevant fields:
 - a. Type a new IPMI IP address for each controller node on the system.
 - b. Specify new IPMI subnet and/or IPMI gateway addresses or Unity.
6. If needed, type a new password for Unity IPMI web-based interface in the **Password** field; you need this password to access Unity IPMI web-based interface. The default password is **ADMIN** (all upper case).
7. Click the **Apply** button to set the new IPMI network settings on Unity.

Accessing the IPMI web-based interface

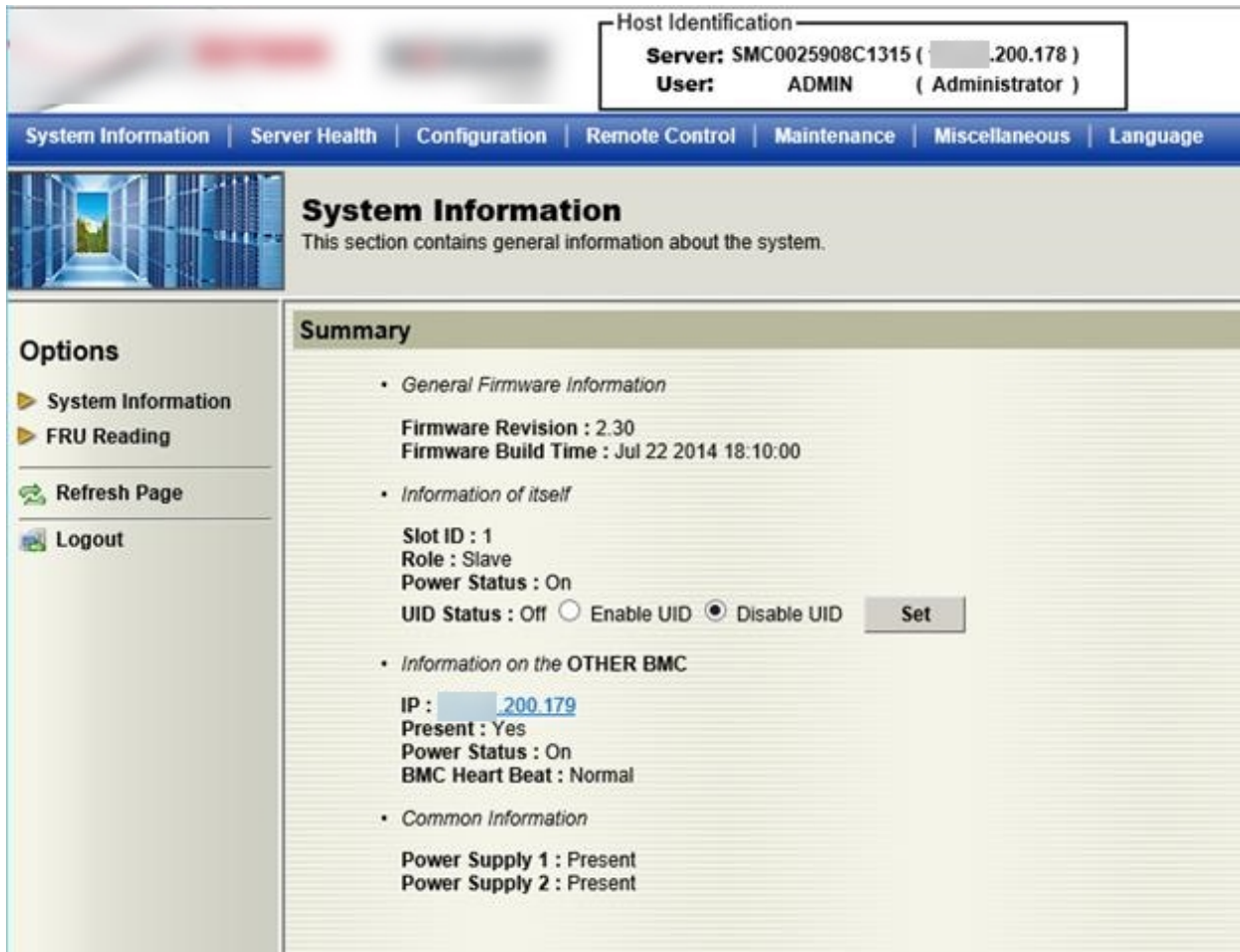
This section explains how to access Unity's IPMI web-based interface.

► **To access the IPMI web-based interface:**

1. Open a web browser on a system that is installed on the same network (and subnet) as Unity.
2. In the web browser's address bar, type the IPMI IP address for the *active* controller on Unity.
To determine which node is *active* on a clustered system, see [Viewing cluster health status and controller information](#) on page 300.
3. Press Enter. This launches the IPMI web-based interface and displays the log on dialog.
4. In the **Username** field, type **ADMIN** (all upper case).

- In the **Password** field, type the IMPI password (the default is **ADMIN**—all upper case). This displays the IPMI web-based interface main screen.

Figure 8-14: Accessing Unity’s IPMI web-based interface



Enabling jumbo frames

Enabling [jumbo frames](#) on Unity can significantly increase network throughput while consuming fewer CPU cycles on the system.

► **Before you begin:**

- You must make sure to enable jumbo frames on the switch(es) that Unity is connected to, as well as on all client systems that access Unity.
- You must make sure that the 10 GigE interface is set as the primary interface (nx0) on Unity (for example: ixgbe1, ixgbe2, etc.).
- Enabling jumbo frames over the network will cause disconnection. Perform these steps through a KVM or IPMI console. Client systems and applications on the network will temporarily lose connection to Unity during the reboot and switchover operations. Make sure that client systems with an active connection to any shares on Unity are disconnected; also make sure to quiesce any applications with an active connection to Unity.

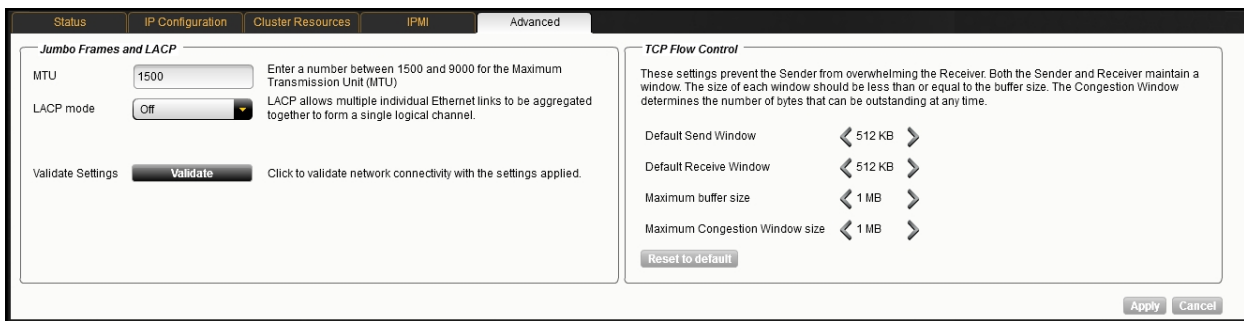
- We recommend that IPMI settings be configured for Unity if you are connected to Unity with a system on a separate management network.

This section describes how to enable jumbo frames using Unity. You can also enable jumbo frames using the `nxadmin` CLI; see [Enabling jumbo frames using the menu-driven `nxadmin` CLI](#) below.

► **To enable jumbo frames on Unity:**

1. Click the Site node.
2. Click the **Cluster Settings** node.
3. Expand the controller node's Properties panel.
4. Select the **Advanced** tab.

Figure 8-15: Cluster properties panel: Advanced tab



5. Enter a number between 1500 and 9000 in the **MTU** field.
6. (Optionally) Click the **Validate** button to verify if all requirements are met.

In the Validate MTU dialog box:

 - a. Enter the IP address of a device with the desired MTU to confirm network connectivity with Unity.
 - b. Click **Validate**.
 - c. When the validation is complete, click **Close**.

When the process completes, the Validation Result dialog box shows you whether the validation was successful or not; in the case of failure, the specific reasons are indicated.

Note If you specify an MTU and enable the LACP mode, Unity will validate both features at the same time. In the validation dialog box, perform the same steps as mentioned above.
7. Click the **Apply** button to save your changes.

Enabling jumbo frames using the menu-driven `nxadmin` CLI

Enabling [jumbo frames](#) on Unity can significantly increase network throughput while consuming fewer CPU cycles on the system.

► **Before you begin:**

- You must make sure to enable jumbo frames on the switch(es) that Unity is connected to, as well as on all client systems that access Unity.
- You must make sure that the 10 GigE interface is set as the primary interface (`nx0`) on Unity (for example: `ixgbe1`, `ixgbe2`, etc.).

- Enabling jumbo frames over the network will cause disconnection. Perform these steps through a KVM or IPMI console. Client systems and applications on the network will temporarily lose connection to Unity during the reboot and switchover operations. Make sure that client systems with an active connection to any file systems on Unity are disconnected; also make sure to quiesce any applications with an active connection to Unity.
- We recommend that IPMI settings be configured for Unity if you are connected to Unity with a system on a separate management network.

▶ **To enable jumbo frames on Unity:**

1. Access the nxadmin CLI.
2. Type this command to set the MTU for the nx0 interface to 9000 bytes (jumbo frames) and press Enter:

```
nic set-linkprop -p mtu=9000 nx0
```
3. Repeat these steps for any other network interfaces on Unity (such as, nx1); for example:

```
nic set-linkprop -p mtu=9000 nx1
```
4. Restart the system or the controller node:
 - a. Type **menu** and press Enter.
 - b. When the NestOS Admin Menu displays, type **2 (Shutdown and Reboot Menu)**, and press Enter.
 - c. Type **1**, and press Enter. The system or controller node reboots; this process may take some time to complete.
5. Once the system or controller node reboots, test and confirm network connectivity to Unity.
6. Repeat these steps on the second controller node after you transition cluster resources back to the node you finished configuring.

Enabling LACP

LACP (Link Aggregation Control Protocol) allows multiple individual Ethernet links to be aggregated together to form a single logical channel. LACP allows a network device to negotiate an automatic bundling of links by sending LACP packets to the peer (directly connected device that also implements LACP).

LACP is typically used for two purposes:

1. Load balancing: bundling two or more links together provides increased throughput and a level of load balancing for when the speed of individual Ethernet lines is limited.
2. Redundancy: links in a LACP aggregation provide an automatic fallback should one of the links fail, providing enhanced resilience. All traffic is routed from the failed link to the remaining links.

Unity supports both active and passive LACP modes:

- Active mode: places a port into an active negotiating state in which the port initiates negotiations with other ports by sending LACP packets.
- Passive mode: places a port into a passive negotiating state in which the port responds to LACP packets that it receives but does not initiate LACP packet negotiation.

This section explains how to enable and configure LACP on Unity.

Requirements and guidelines for implementing LACP

This section lists network and infrastructure requirements for implementing LACP, as well as guidelines/best practices for configuring the Ethernet switch(es) for LACP.

- LACP only operates point-to-point between two partner devices connected together: for example, Unity and the Ethernet switch(es).
- LACP must be enabled at both ends of the link to be operational. Refer to the Ethernet switch manufacturer's documentation for information on setting up LACP on the Ethernet switch(es).
- The link between Unity and the Ethernet switch(es) must be Full-Duplex.
- Both Unity and the Ethernet switch(es) must be running at the same speed (1Gbps or 10Gbps).
- The Ethernet switch(es) must support the IEEE 802.3ad Link Aggregation Standard.
- To prevent a single point-of failure in your configuration, make sure to connect each controller node to a different Ethernet switch, as illustrated in this diagram.

Figure 8-16: Connecting controllers to Ethernet switches on the Unity 2000C

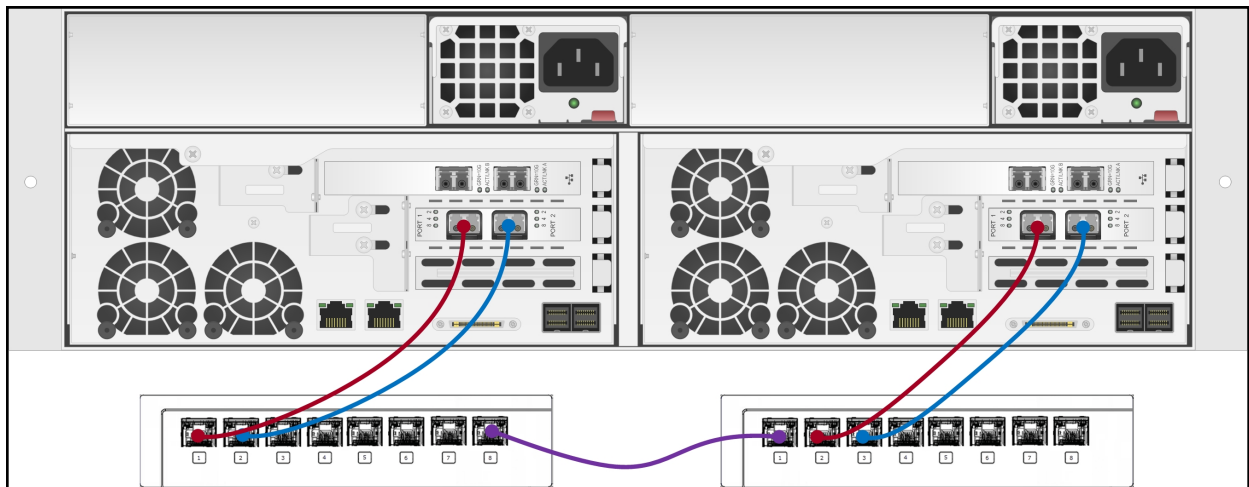


Figure 8-17: Connecting controllers to Ethernet switches on the Unity 2000P/Unity 4000

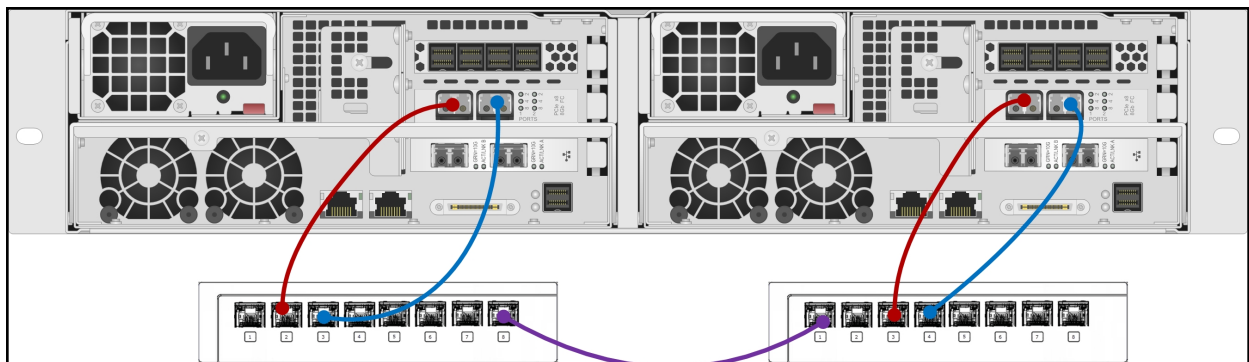


Figure 8-18: Connecting controllers to Ethernet switches on the Unity 5000

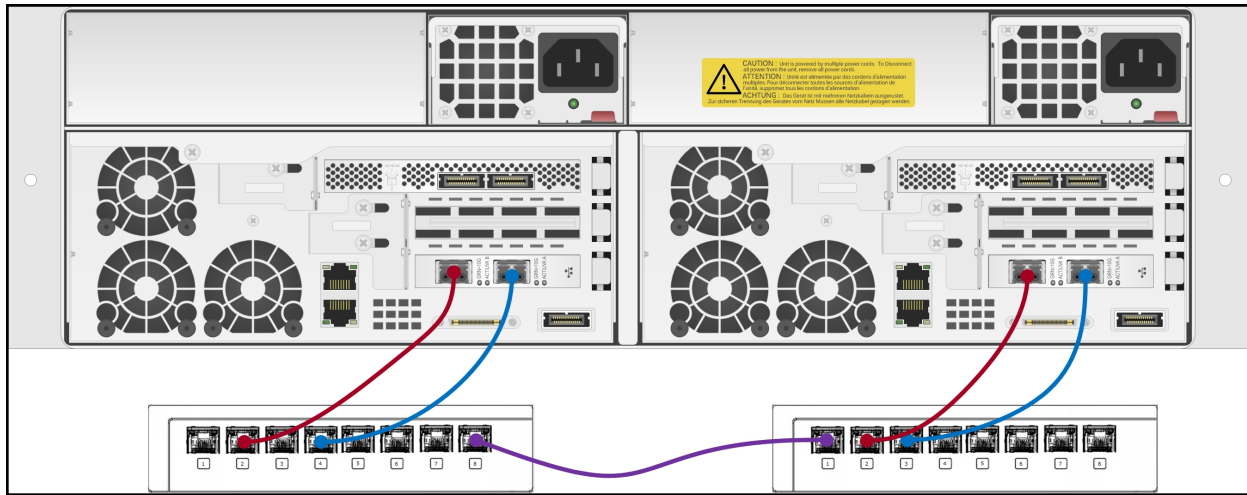
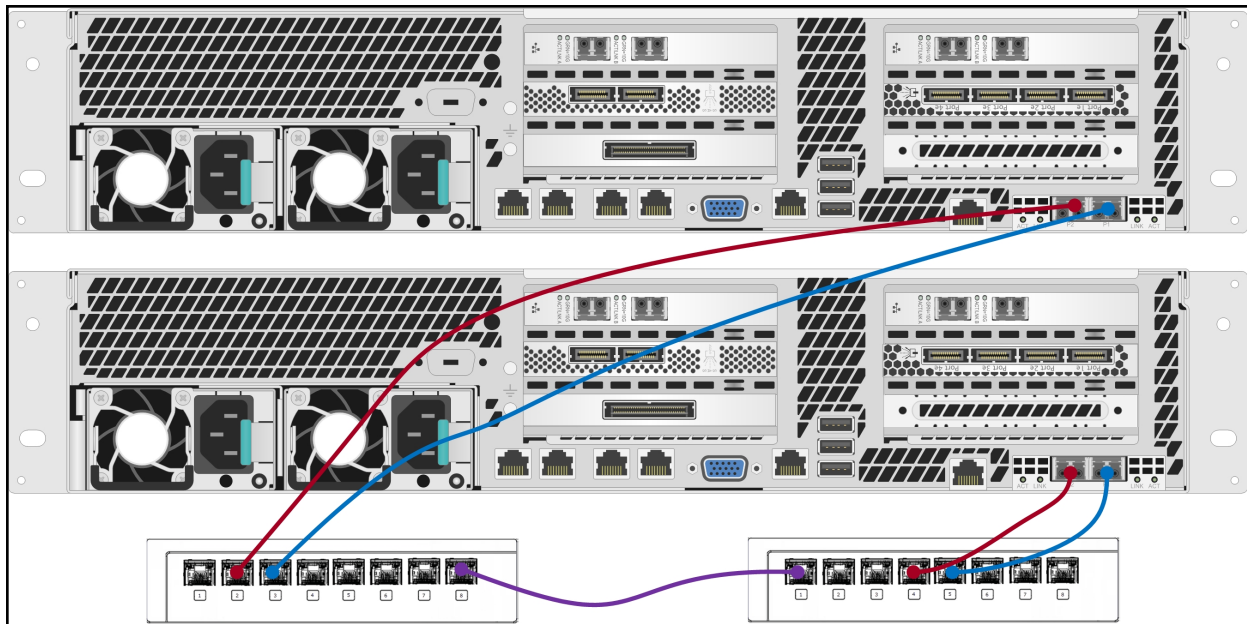


Figure 8-19: Connecting controllers to Ethernet switches on the Unity 6000



Understanding link aggregation

Link aggregation does NOT work by passing packets across all the links in an aggregate group in a round-robin fashion. When a packet arrives, LACP calculates the source and destination address hash (which can be L2, L3, or L4 policies, with L4 being the default), and automatically assigns any given source-destination pair to one of the links in the aggregate. As a result, a single TCP connection can never achieve speeds surpassing the throughput of a single link.

For example, while you might aggregate 4x 1Gbps links into a single aggregate, you'll never get more than 1Gbps in any single data transfer. Even in the case of multiple sessions at the same time from multiple clients, 50/50 load balancing is almost never achieved in real-life implementations; around 70/30 is more common.

For more information about LACP, see:

http://en.wikipedia.org/wiki/Link_aggregation

Enabling LACP using Unity

► Before you begin:

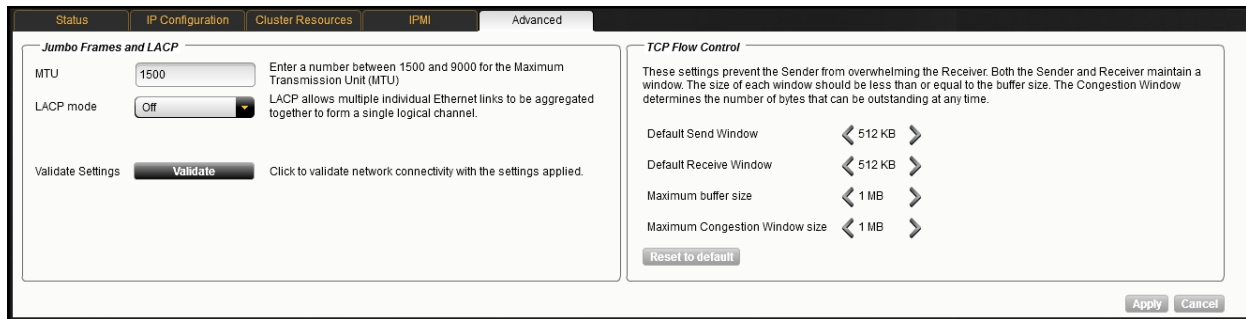
- Read the requirements for LACP; see [Requirements and guidelines for implementing LACP](#) on page 320.
- To learn how link aggregation works, see [Understanding link aggregation](#) on the previous page.

Note The LACP mode is applied to both nodes on the cluster.

► To enable LACP on Unity:

1. Click the Site node.
2. Click the **Cluster Settings** node to display its child node.
3. Expand the controller node's Properties panel, by clicking the **Properties** tab.
4. Select the **Advanced** tab.

Figure 8-20: Cluster Settings properties panel—Advanced tab



5. From the **LACP mode** drop-down list, select **On**.
6. (Optionally) Click the **Validate** button to verify if all requirements are met. Unity will apply the selected mode and then will revert back to the original setting.

When the Validate LACP Mode dialog box displays, click **Validate**. When the process completes, the LACP Validation Result dialog box shows you whether the validation was successful or not; in the case of failure, the specific reasons are indicated.

Note If you enabled both LACP and specified an MTU for Jumbo Frames, Unity will validate both features at the same time. In the validation dialog box:

- a. Enter the IP address of a device with the desired MTU enabled to confirm network connectivity with Unity.
 - b. Click **Validate**.
 - c. When the validation is complete, click **Close**.
7. Click the **Apply** button to save your changes.

Enabling LACP using the nxadmin CLI

Unity provides the `nic` command in Unity's menu-based nxadmin CLI for enabling and monitoring LACP on Unity.

► Before you begin:

- Enabling LACP over the network will cause disconnection. Perform these steps through KVM console, or through IPMI console. For complete details on using the nxadmin menu and CLI commands, refer to the

Nexsan Unity Command-line Interface Reference Guide.

- You must not enable LACP on nx99 otherwise you will lock yourself out of the system.



CAUTION: On a clustered system, you must enable LACP on each controller node individually. Before you enable LACP on a controller node, however, you must transition any Pool Resource Groups and/or the System Management component to the second controller in the system. You must then repeat this process to enable LACP on the second controller.

► **To enable and configure LACP on Unity:**

1. Access the nxadmin CLI.
2. When the NestOS Admin Menu displays, type **5 (Run a Command)**, and then press Enter.
3. At the command: prompt, type one of these command to enable LACP on Unity, in either active or passive mode:

- Active mode:

```
nic modify-aggr -L active nx0
```

Where nx0 represents the primary interface on Unity. You can also enable LACP on the secondary interface, if available: to enable LACP on the secondary interface, replace nx0 with nx1.

- Passive mode:

```
nic modify-aggr -L passive nx0
```

Where nx0 represents the primary interface on Unity. You can also enable LACP on the secondary interface, if available: to enable LACP on the secondary interface, replace nx0 with nx1.

4. Press Enter. Unity disconnects from the network.
5. Configure the Ethernet switch to set the ports that you want to combine into a logical channel. Unity comes back online once LACP negotiation is complete.
6. Test and confirm network connectivity to Unity.

Configuring TCP flow control

TCP flow control settings prevent the Sender from overwhelming the Receiver. In a connection between a client and a server, the client tells the server the number of bytes it is willing to receive at one time from the server; this is the client's *receive* window, which becomes the server's *send* window. Likewise, the server tells the client how many bytes of data it is willing to take from the client at one time; this is the server's *receive* window and the client's *send* window.

When the server receives data from the client, it places it into a buffer. The server must then send an acknowledgment back to the client to indicate that the data was received, and process the data, transferring it to the destination application process.

Data is acknowledged when received, but not necessarily immediately transferred out of the buffer. This means that is possible for the buffer to fill up with received data faster than the receiving TCP can empty it. When this occurs, the receiving device may need to adjust its window size to prevent the buffer from being overloaded.

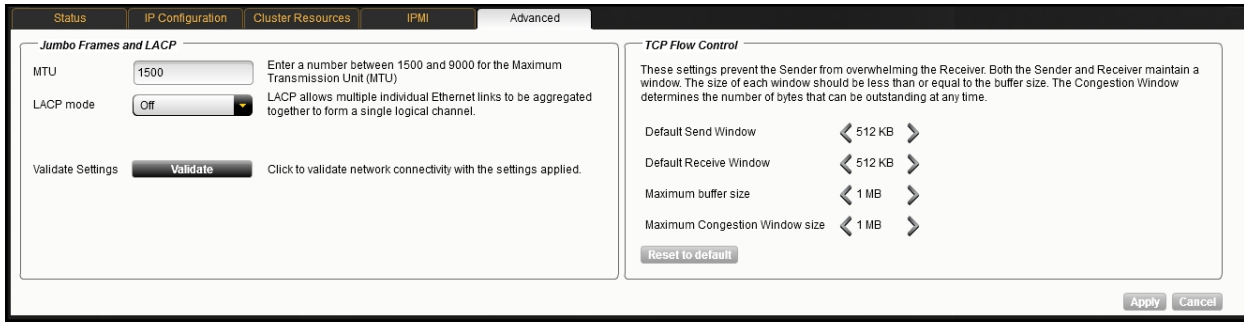
TCP separates receiver congestion from network congestion, and uses flow controls for each (receiver window and congestion window). The congestion window determines the number of bytes that can be outstanding at any time.

Note The TCP flow control settings are applied to both nodes on the cluster.

► **To configure TCP flow control:**

1. Click the Site node.
2. Click the **Cluster Settings** node.
3. Expand the controller node's Properties panel.
4. Select the **Advanced** tab.

Figure 8-21: Cluster Settings properties panel—Advanced tab



5. Set the **Default Send Window** parameter; specify a value ranging from 4 KB to 1 GB. The default value is 512 KB.
The size of the Send window should be less than or equal to the buffer size.
6. Set the **Default Receive Window** parameter; specify a value ranging from 2 KB to 1 GB. The default value is 512 KB.
The size of the Receive window should be less than or equal to the buffer size.
7. Set the **Maximum buffer size** parameter; specify a value ranging from 8 KB to 1 GB. The default value is 1 MB.
8. Set the **Maximum congestion window size** parameter; specify a value ranging from 128 B to 1 GB. The default value is 1 MB.
9. Click the **Apply** button.

Tip To revert back to the default settings, click the **Reset to Default** button and click **Apply**.

Chapter 9

Storage

Managing storage for Unity involves: allocating a new storage system to the system; reconfiguring the RAID level on storage, including specifying the number of RAID sets (or volumes) that you want Unity to create on the system, as well as the number of disks that you want to assign as hot spares; and setting or modifying network settings on a Nexsan storage enclosure.

Allocating new storage to the site	328
Modifying IP settings for a Nexsan E-Series Storage System	330
Resetting the RAID configuration for storage	331
Renaming a storage enclosure	332
Adding new drives to a Nexsan storage enclosure	333
Removing a storage enclosure	335
Shutting down a Nexsan storage enclosure	335
Powering the systems back on	337
Using Self-Encrypting Drives (SEDs)	340
Disabling SEDs encryption	341

Allocating new storage to the site

When you connect a Unity Storage System or a Nexsan Unity Storage Expansion to Unity, you must allocate the storage system to the site and configure its [RAID settings](#). This is also true when you add new disk drives to a Unity Storage System, a Nexsan Unity Storage Expansion, or to internal storage on the Nexsan Unity 5100™ Storage System.

► **Before starting the Add Storage Systems Wizard:**

- Make sure the storage system that you want to allocate to the site is properly connected to Unity, and that it is powered on.
- Read about performance limitations when mixing volumes with different RAID levels; see [Mixing volumes with different RAID levels](#) on page 98.

Note All Unity Storage System and Nexsan Unity Storage Expansions are hot-pluggable, so Unity does not need to be powered off when plugging in a new storage enclosure.

► **To start the Add Storage Systems Wizard:**

1. Under the site node where you want to add the storage system, click the **Storage Enclosures** node to select it.
2. Perform one of the following actions:

To...	Do this
use the Storage Enclosures' node context menu	<ol style="list-style-type: none"> a. Click the context menu button on the Storage Enclosures node. b. When the node context menu opens, click Add.
use the Storage Enclosures Properties panel	<ol style="list-style-type: none"> a. Click the Properties tab at the bottom of the screen to expand the Devices node's Properties panel. b. Click the Add a Storage Enclosure button on the Properties panel.

This section includes these steps:

Step 1: Discovering new storage and configuring RAID settings	328
Step 2: Verifying settings	330
Step 3: Viewing results	330

Step 1: Discovering new storage and configuring RAID settings

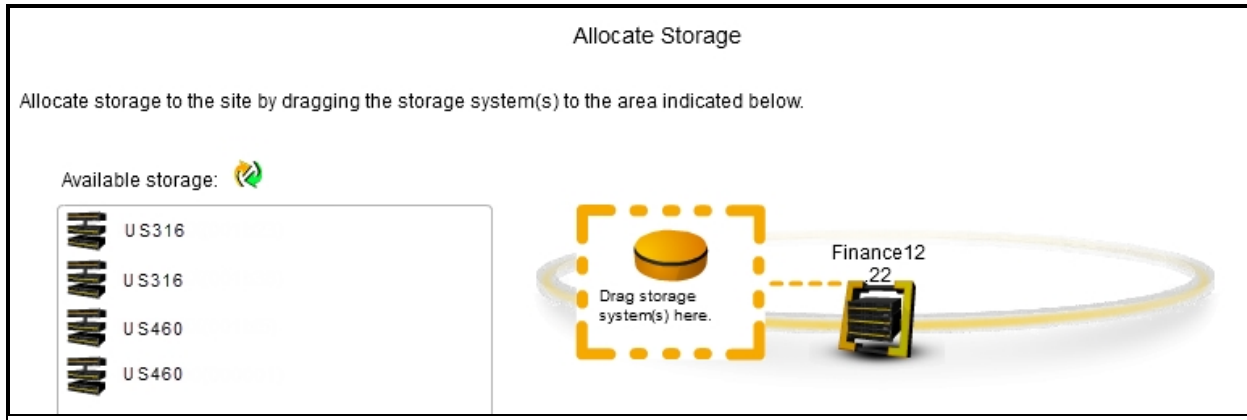
In *Step 1*, the Add Storage Systems Wizard automatically discovers any new storage connected to Unity and then displays the Storage Configurator.

Note If the Add Storage Systems Wizard fails to discover new storage, make sure the storage is properly connected to Unity, and that it is powered on.

If you are adding new disk drives to a Unity Storage System, a Nexsan Unity Storage Expansion, or to internal storage on the Nexsan Unity 5100™ Storage System, you must add the minimum amount of disk drives for the new drives to be discoverable, depending on the [RAID configuration](#) of the storage enclosure.

Then, click the refresh button .

Figure 9-1: Add Storage Systems Wizard, step 1: discovering new storage and configuring RAID settings



Note If the Add Storage Systems Wizard discovers a Nexsan storage enclosure that has DHCP enabled (default configuration), the Add Storage Systems Wizard prompts you to specify a static IP address(es) for the controller(s) on the storage enclosure. You **MUST** set a static IP address(es) for the storage system.

► **To set a static IP address(es) for Nexsan storage:**

1. Type a valid IP address in the **Controller 1** field.
2. If applicable, type a valid IP address in the **Controller 2** field.
3. Click the **Apply** button.

Note Unity automatically sets the Subnet mask, Default gateway, and Preferred DNS server on the storage system according to the values that you configured for Unity.

Once the Add Storage Systems Wizard sets static the IP address(es) on the Nexsan storage system, the Storage Configurator opens.

► **To configure RAID settings for the storage system:**

1. From the **RAID level** drop-down list in the Storage Configurator, select the RAID level—5, 6, or 10. The Storage Configurator automatically recommends the optimal RAID settings (**Number of RAID sets** and **Hot spares**) for the RAID level you select. You can adjust these settings or keep the recommended (optimal) settings.
2. From the **Number of RAID sets** drop-down list, select the number of RAID sets that you want to create on the storage enclosure. The Storage Configurator creates a volume for each RAID set that you specify. A volume represents a virtual subset of the aggregated disk space available on the storage system.
3. From the **Hot spares** drop-down list, select the number of hot spare disks that you want to assign to the storage enclosure. If a disk on the system fails, Unity automatically replaces the failed disk with the hot spare, allowing the system to continue operating. Depending on your RAID level and RAID sets selections, and the number of disks available on the system, you may only be able to assign one disk as a hot spare.

Note The Storage Configurator automatically assigns any unallocated disks as hot spares. For example, if you have 2 hot spare disks available after setting the RAID level and RAID sets, and you select only 1 disk as a hot spare assignment, the Storage Configurator automatically assigns the second unallocated disk as a hot spare to the RAID array.

As you select the RAID level, the number RAID sets, and the number of hot spares to create on the storage system, the Summary section on the Storage Configurator panel automatically updates to display how your selections impact disk assignment on your storage.

- (Optionally) Enter a friendly name for the storage enclosure.
- Click **OK** to save your selections and close the Storage Configurator.
- When you finish configuring and allocating storage, the Add Storage Systems Wizard automatically moves forward to [Step 2: Verifying settings](#) below.

Step 2: Verifying settings

Step 2 of the Add Storage Systems Wizard summarizes your configuration settings and allocates the storage system to the site when you click **Start**. Review the summary carefully before proceeding.

▶ **To change a configuration setting:**

- Click the back arrow to navigate back to the corresponding configuration step.
Or
- Click the step identifier at the top of the Add Storage Systems Wizard panel to go back to a specific step. For example, if you want to change the RAID setting for the storage system, click **Step 1**.

Figure 9-2: Add Storage Systems Wizard, step 2: verifying settings

Verify Settings

Please verify your configuration settings. If you want to change a setting, click the back arrow to navigate to the relevant configuration panel. Or, click the step identifier at the top of the wizard panel to go back to a specific step.

```
List of allocated storage devices:  
US360  
RAID Level: RAID 6  
RAID Sets: 2
```

If you are satisfied with the configuration settings, click the **Start** button at the bottom of the panel. The Add Storage Systems Wizard automatically moves forward to [Step 3: Viewing results](#) below.

Step 3: Viewing results

Step 3 of the Add Storage Systems Wizard displays progress while it configures the storage system and allocates the storage system to Unity.

The Add Storage Systems Wizard displays any error events that the system encounters during the configuration process. You can view more details about an error event by expanding the corresponding entry.

▶ **To view more details for an error event:**

- Click the plus (+) sign corresponding to the error event.

Once the Add Storage Systems Wizard finishes configuring the new storage system and allocates it to the site, Unity adds a corresponding node for the storage system under the Storage Enclosures node in Unity's tree view.

Modifying IP settings for a Nexsan E-Series Storage System

You can modify the controller IP addresses and network settings for a Nexsan E-Series Storage System connected to Unity.

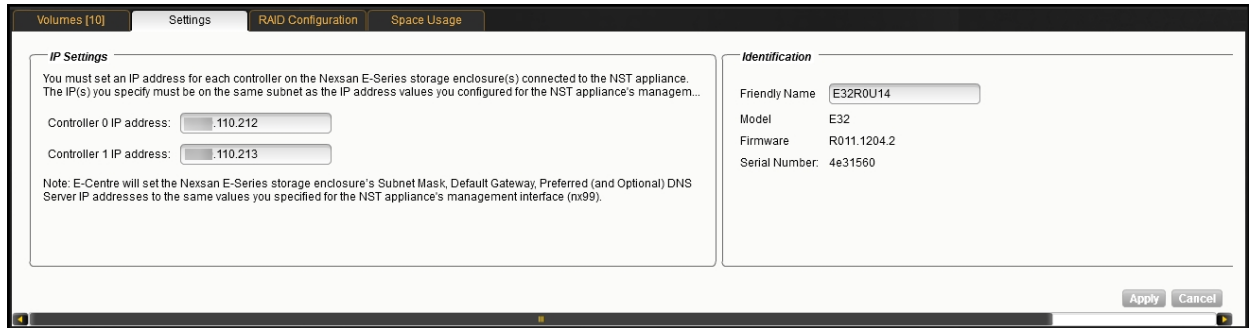
▶ **To modify the IP addresses:**

- If you are managing multiple sites (multi-site management of remote systems): in Unity's tree view, click the Site node where the Nexsan E-Series Storage System that you want to modify network settings for

exists.

2. Click the **Storage Enclosures** node.
3. Select the node representing the E-Series Storage System.
4. Expand the storage system's Properties panel.
5. Select the **Settings** tab.

Figure 9-3: Storage enclosure properties panel—Settings tab



6. Modify network settings by overwriting any existing values in the relevant fields:
 - a. Type a new IP address for Controller 1.
 - b. Type a new IP address for Controller 2.
7. Click the **Apply** button to set the new network settings.

Resetting the RAID configuration for storage

You can reset the [RAID configuration](#) on storage connected to Unity, including both externally-attached storage systems and internal storage (on the Nexsan Unity 5100™ Storage System).

When you reset RAID settings on storage, the system releases the volumes and hot spares on the corresponding storage system, and resets the disk drives to non-RAID status.

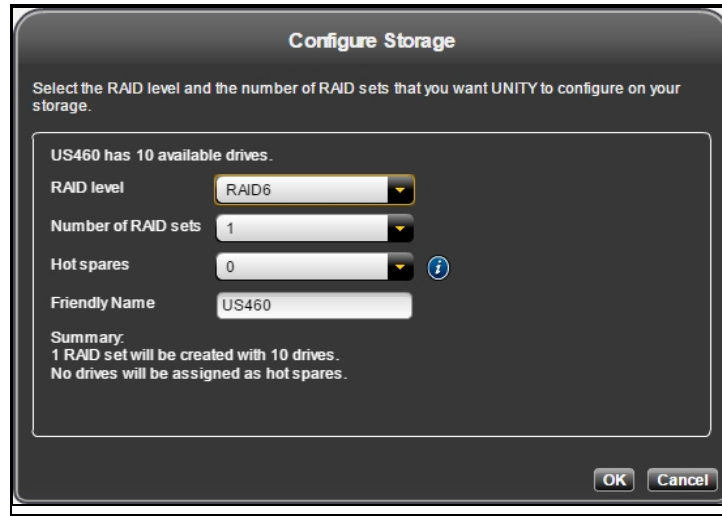
You perform this operation if you want to specify a new RAID configuration for your storage. This operation can only be performed on a storage system where no storage pool exists, or where a volume is not currently allocated to a storage pool.

▶ To reset the RAID configuration on storage connected to Unity:

1. If you are managing multiple sites (multi-site management of remote systems): in Unity's tree view, click the Site node where the Nexsan storage system that you want to reset RAID settings for exists.
2. Click the **Storage Enclosures** node.
3. Select the node representing the Nexsan storage system that you want to reset RAID settings for.
4. Expand the storage system's Properties panel.

- Click the **Configure RAID** button. This displays the Storage Configurator.

Figure 9-4: Storage Configurator: reset RAID



- From the **RAID level** drop-down list in the Storage Configurator, select the RAID level—5, 6, or 10—that you want Unity to configure on your storage. The Storage Configurator automatically recommends the optimal RAID settings (**Number of RAID sets** and **Hot spares**) for the RAID level you select; you can adjust these settings, or keep the recommended (optimal) settings.
- From the **Number of RAID sets** drop-down list, select the number of RAID sets that you want to create on the storage system. Unity creates a volume for each RAID set that you specify. A volume represents a virtual subset of the aggregated disk space available on the storage system.
- Next, from the **Hot spares** drop-down list, select the number of hot spare disks that you want to assign to the storage system. If a disk on the system fails, Unity automatically replaces the failed disk with the hot spare, allowing the system to continue operating. Depending on your RAID level and RAID sets selections, and the number of disks available on the system, you may only be able to assign one disk as a hot spare.

Note The Storage Configurator automatically assigns any unallocated disks as hot spares. For example, if you have 2 hot spare disks available after setting the RAID level and RAID sets, and you select only 1 disk as a hot spare assignment, the Storage Configurator automatically assigns the second unallocated disk as a hot spare to the RAID array.

As you select the RAID level, the number RAID sets, and the number of hot spares to create on the storage system, the Summary section on the Storage Configurator panel automatically updates to display how your selections impact disk assignment on your storage.

- Once you finish configuring RAID settings for the storage system, click the **OK** button to save your selections and close the Storage Configurator.

Renaming a storage enclosure

You can rename a storage enclosure at any time. Unity will update the new name for the site, for all storage pools using that storage enclosure.

The name must start with an (upper-case or lower-case) alphabetic or numeric character; and, with the exception of the hyphen (-), and period (.), the name can only contain alphanumeric characters, without spaces.

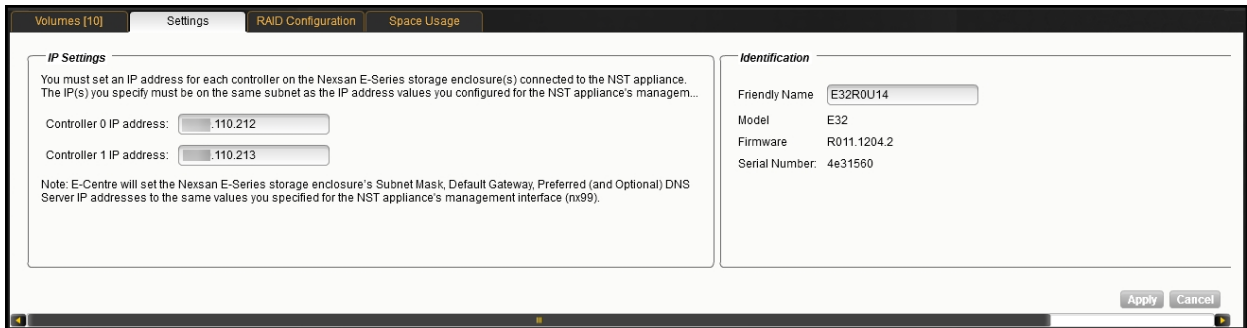
These characters are NOT allowed:

" / \ [] : ; | = , + * ? < >

► **To rename a storage enclosure:**

1. If you are managing multiple sites, in Unity's tree view, click the Site node where the storage enclosure to remove exists.
2. Select the **Storage Enclosures** node.
3. Click the node corresponding to the storage enclosure.
4. Expand the storage enclosure's properties panel.
5. Select the **Settings** tab.

Figure 9-5: Storage enclosure properties panel—Settings tab



6. In the **Friendly Name** field, enter a new name for the storage enclosure.
7. Click **Apply**.

Adding new drives to a Nexsan storage enclosure

You can add new drives to a Nexsan external storage (Nexsan Unity Storage Expansion or Nexsan E-Series), or internally on the Unity 5100.

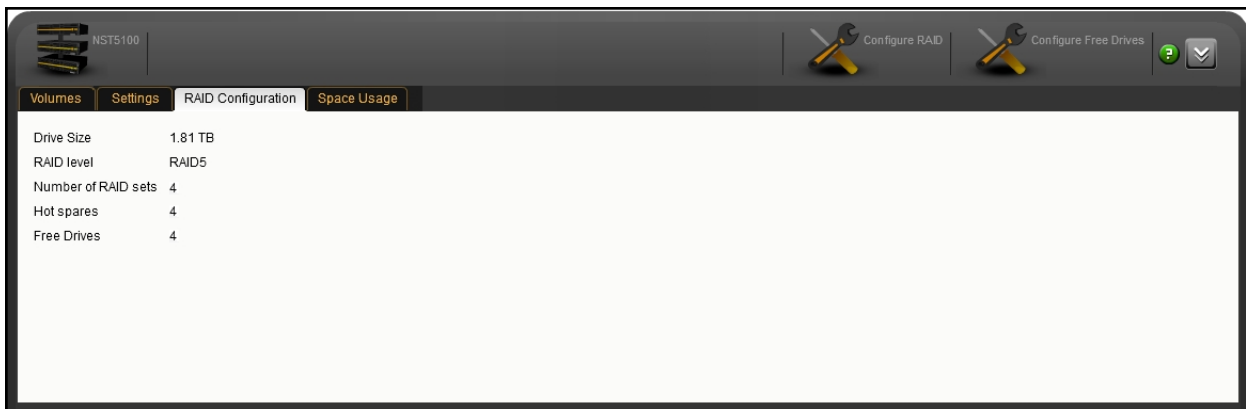
Once the drives are physically added on the Nexsan storage enclosure, Unity will automatically detect them and Nexsan Unity will display a new button on the storage properties panel.

► **To configure the new drives:**

1. Click the **Storage Enclosures** node.
2. Select the node representing the Nexsan storage system for which you are adding drives.
3. Expand the storage system's Properties panel.

4. Select the **RAID Configuration** tab to view the free drives. In the example below, Unity detects 4 free drives.

Figure 9-6: Storage enclosure's properties panel—RAID Configuration tab

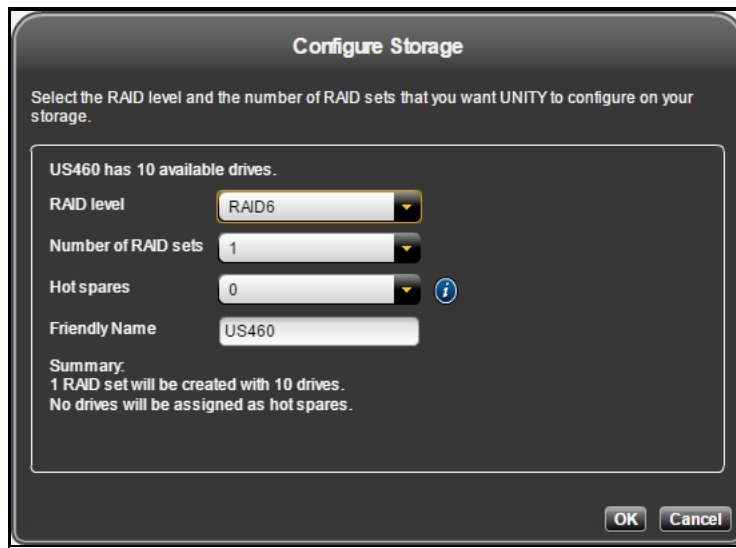


5. Click the **Configure Free Drives** button. This button only appears when Unity detects new drives.
6. In the **Configure Storage** dialog box, select the number of RAID sets and, if you have enough drives, select the number of hot spares. Unity keeps the same RAID level for the new drives since the storage system is already configured.

Optionally, enter a friendly name for the storage device.

In our example, Unity automatically assigns the 4 drives to one RAID set.

Figure 9-7: Configuring Storage dialog box



7. Click **OK** to apply the settings and close the dialog box.

8. On the storage system's Properties panel, click the **Volumes** tab. You should see the new volume with a status of *Free* since it is not assigned to a pool yet.
 - To add the volume to a new pool, see [Adding a storage pool](#) on page 100.
 - To add the volume to an existing pool, see [Adding volumes to a storage pool to expand capacity](#) on page 107.

Figure 9-8: Storage enclosure's properties panel—Volumes tab

Name	Space	Status	Associated storage pool
Volume 0 3.63 TB	336 KB used out of 3.63 TB	Pool Member	FinancePool1
Volume 1 3.63 TB	271 KB used out of 3.63 TB	Pool Member	FinancePool1
Volume 2 3.63 TB	354 KB used out of 3.63 TB	Pool Member	FinancePool1
Volume 3 3.63 TB	0 B used out of 3.63 TB	Free	

Removing a storage enclosure

Before you can physically remove a storage enclosure, you must:

1. Remove all volumes on the storage enclosure that are allocated to storage pools.
 - For Nexsan Unity Storage System, you must remove the storage pools hosted on the unit, as described in [Deleting a storage pool](#) on page 120.
 2. Remove the storage enclosure from Nexsan Unity, as described in this section.
- ▶ **To remove a storage enclosure from Unity:**
1. If you are managing multiple sites, in Unity's tree view, click the Site node where the storage enclosure to remove exists.
 2. Select the **Storage Enclosures** node.
 3. Click the node corresponding to the storage enclosure.
 4. Expand the storage enclosure's properties panel.
 5. Click the **Remove Enclosure** button.
 6. Click **OK**.

▶ **What's Next:**

You can now remove the storage enclosure physically, as described in the *Nexsan Unity Storage Expansion Reference Guide*.

Shutting down a Nexsan storage enclosure

You may need to shut down a storage enclosure for maintenance or replacement. If the storage enclosure hosts volumes associated to one or more storage pools, these storage pools and all underlying datasets will be unavailable until the storage enclosure comes back online.

Note This does not apply to mirrored pools in a synchronous replication. If the mirror is online, the storage pool will continue to function.

Note You cannot shut down any Nexsan Unity Storage Expansions from Unity. They must be shut down physically by turning off the switches on the power supply units.

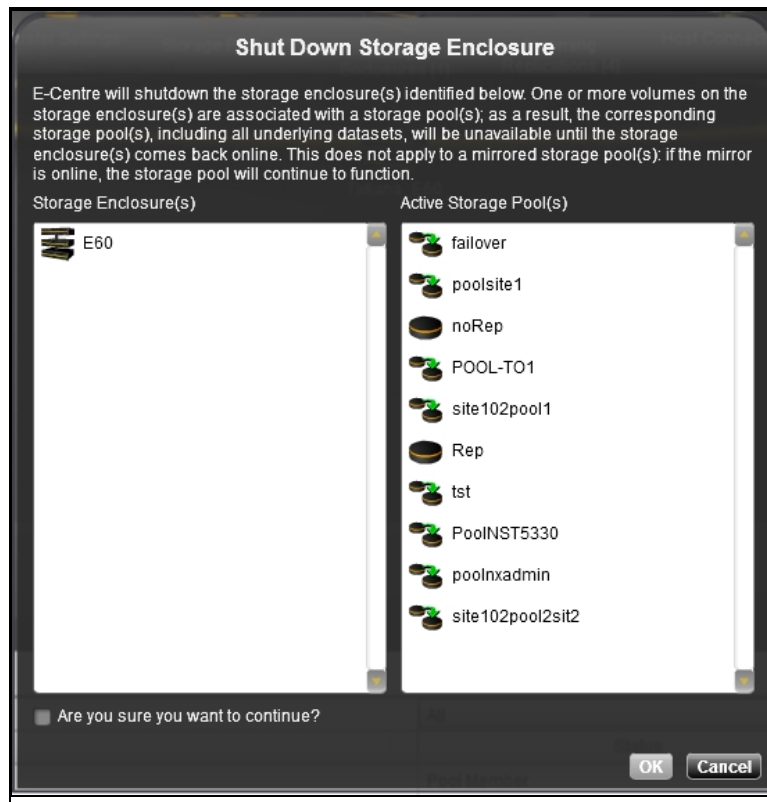


CAUTION: You must not shut down or restart Nexsan E-Series storage enclosures using the E-Series graphical user interface. This could result in storage pools being unavailable or data loss.

► **To shut down a storage enclosure:**

1. If you are managing multiple sites, in Unity's tree view, click the Site node where the storage enclosure to shut down exists.
2. Select the **Storage Enclosures** node.
3. Click the node corresponding to the storage enclosure.
4. Expand the storage enclosure's properties panel.
5. Click the **Shut down** button.

Figure 9-9: Shut Down Storage Enclosure dialog box



6. Unity displays all storage pools that are currently active. Check the **Are you sure you want to continue?** option.
7. Click **OK**.

► **Related topic:**

[Powering the systems back on](#) on the facing page

Powering the systems back on

This topic describes how to restart the systems after a planned shut down operation and to recover from power outage.

If you shut down one or more storage enclosures as part of a maintenance/replacement operation, you can simply restart the storage enclosure(s) from Unity.

If you experienced a power outage and all systems are down, you must follow a specific order sequence to ensure data integrity. In this case, you must power on the systems in this order:

1. If an E18X™, E48X™, or E60X™ Unity Storage Expansion(s) is connected to the Nexsan E-Series, power on each Unity Storage Expansion first, and then wait 2 minutes.
2. Power on the Nexsan E-Series, and then wait 2 minutes.






Note If a drive carrier activity LED does not light up, check to make sure the corresponding drive is properly seated in the chassis.







3. For the Unity 6000, power on the Unity Vault Protection Modules.
4. Power on Unity.



CAUTION: You must not restart Nexsan E-Series storage enclosures using the E-Series graphical user interface. This could result in storage pools being unavailable or data loss.

▶ To power the systems back on:

1. If a Nexsan E-Series Unity Storage Expansion(s) is connected to the Nexsan E-Series, power on each Unity Storage Expansion first, and then wait 2 minutes.
2. Power on the Nexsan E-Series storage enclosures and wait 2 minutes.
3. For the Unity 6000, power on the Unity Vault Protection Modules:
 - a. Press and hold the power button  located on the right side of the LCD screen until the power turns on.
 - b. Wait for the Unity VPM to boot up. The LCD screen should display  *Normal mode* with a green status.
 - c. Repeat these steps on the second Unity VPM.
4. Power on the Unity 2000C/Unity 2000P.
 - a. Press and hold the power button  located on the right front panel of the chassis until the power LED lights up.
 - b. Verify the power LEDs  on the LEFT and RIGHT front control panels are illuminated to ensure that the controller nodes are receiving power and the power modules are functioning properly.
 - c. Verify that the heartbeat LED  is blinking yellow in 2-3 second intervals.
 - d. Verify that the drive carrier LEDs are illuminated in green.

5. Power on the Unity 4000/ Unity 5000.
 - a. Press and hold the power button  located on the right front panel of the chassis until the power LED lights up.
 - b. Verify the power LEDs  on the left and right front control panels to ensure that the controller nodes are receiving power and the power modules are functioning properly.
 - c. Verify that the heartbeat LED  is blinking yellow in 2-3 second intervals.
 - d. Verify that the drive carriers LEDs are illuminated in green.
6. Power on the Unity 6000.
 - a. Press and hold the power button  located on the right front panel of the chassis until the power LED lights up.
 - b. On each controller node, verify that the power LED  on the right of the front control panel is illuminated to ensure that it is receiving power and the power modules are functioning properly.
 - c. Verify that the system status LED  is illuminated in solid green.
 - d. Verify that the drive carriers LEDs are illuminated in green.

7. Reboot the Nexsan E-Series storage enclosures in Unity:
 - a. Log in to Unity.
 - b. If you are managing multiple sites, in Unity's tree view, click the Site node where the storage enclosure to reboot exists.
 - c. Select the **Storage Enclosures** node.
 - d. Click the node corresponding to the storage enclosure and expand the storage enclosure's properties panel.
 - e. Click the **Restart** button.

Figure 9-10: Restarting an E-Series storage enclosure



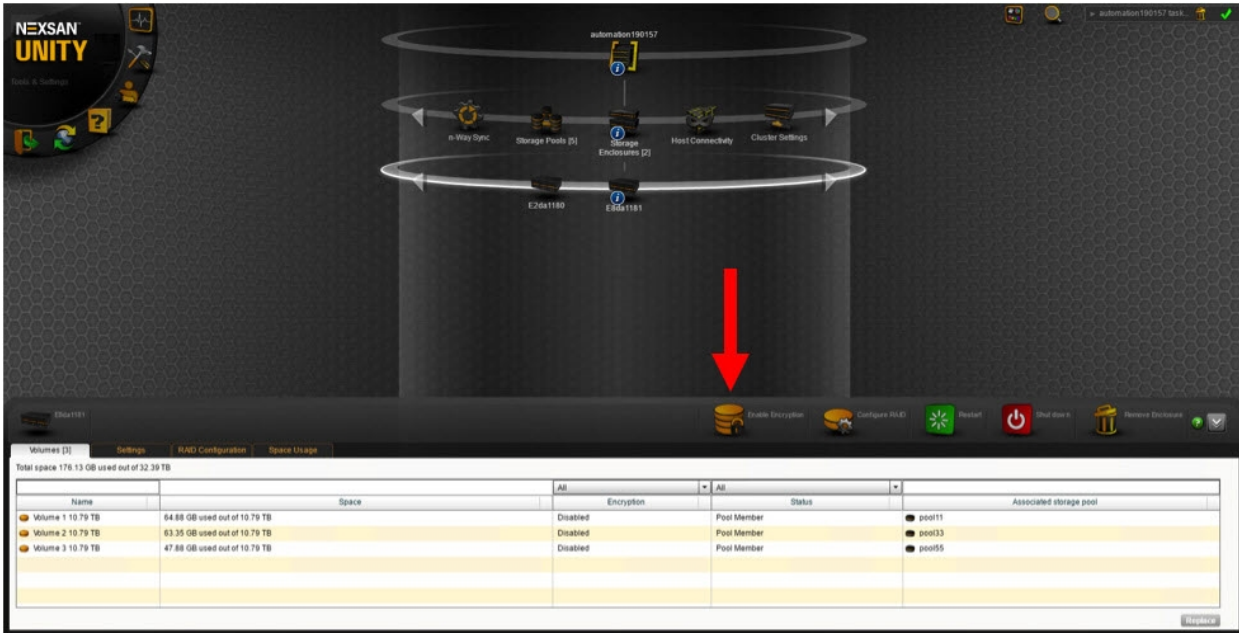
- f. Check the **Are you sure you want to continue?** option.
- g. Click **OK**.

Using Self-Encrypting Drives (SEDs)

When using Unity with SEDs-capable drives, you may now enable SEDs encryption.

► Enabling SEDS encryption

1. From the **Storage Enclosures** node, select an enclosure with SED-capable hardware.
2. Click the **Enable Encryption** button.



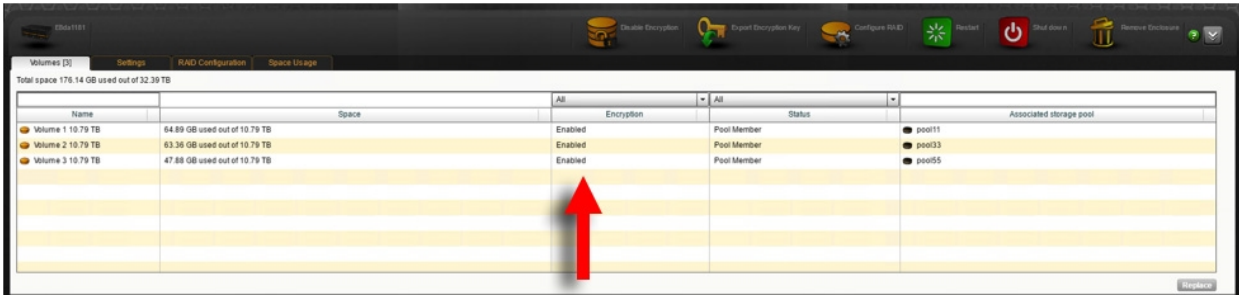
3. In the **Enable Data Encryption** dialog, click the **Export Encryption Key(s)** button.



Warning: You must back up the keys to a secure location. Loss of keys may result in loss of all data.

4. Select a location for the exported keys, then click Save.
5. Select the checkbox indicating that you have backed up the keys.

6. Click **Apply**.
7. In the **Volumes** pane, verify that encryption is enabled for individual volumes.



Disabling SEDs encryption

1. From the **Storage Enclosures** node, select an the enclosure on which you wish to disable SEDs.
2. Click the **Disable Encryption** button.
3. In the **Disable Data Encryption** dialog, click OK.
4. Verify that encryption is disabled.

Chapter 10

Using Active Archive

When using Active Archive in conjunction with an Assureon Server you now have the ability to set data retention policies to automatically offload stale data and release primary storage. This allows you to increase the performance of your primary storage without increasing its primary size.

If you require data retention policies for compliance and data management you now have the ability to leverage Nexsan tier one storage for your compliance needs. Archiving is useful if you want to:

- Use life-cycle management
- Utilize Assureon features to have better control of your corporate data
- Reduce risk of data loss or corruption
- Use Assureon to store sensitive data which would otherwise require a separate solution from your primary storage

Connecting to an Assureon Server

Assureon can be configured to use certificate authentication. This mode encrypts the traffic between the Assureon Client and the server using an SSL certificate issued by the Assureon server. This certificate also determines the data that users have access to. In order to access files in the Assureon Explorer tool, users will need to have a certificate installed. Assureon shortcuts are protected using standard NTFS security. If the certificate allows access to the data in Assureon, then users who have access to the shortcuts will have access to the data.

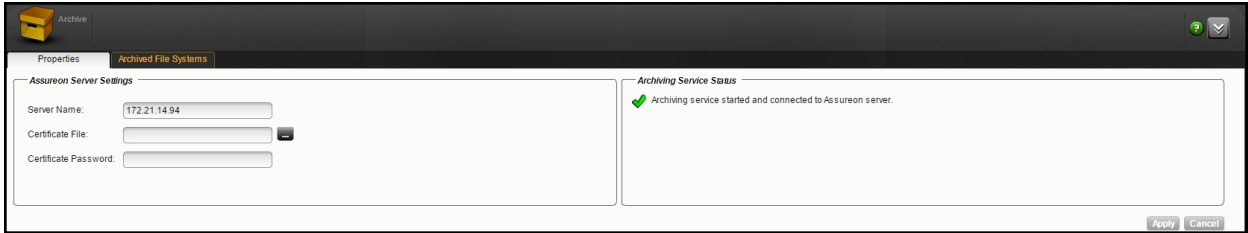
Note Certificate authentication may also be used alongside Active Directory (AD) authentication. For example, some clients may use certificate authentication while others use AD authentication.

▶ **To configure a connection to an Assureon Server:**

1. If you are managing multiple sites, in Unity's tree view, click the Site node.
2. Select the Archive node.
3. Expand the properties panel.

4. Select the **Properties** tab.

Figure 10-1: Archive properties panel—Properties tab



5. Configure your Assureon settings:
 - **Server Name:** The name of the Assureon server being used for archiving purposes.
 - **Certificate File:** The certificate being used to authenticate use of this Assureon Server. You can use another certificate if needed.
 - **Certificate Password:** The password used to authenticate the certificate file. For more information on certification files, see the *Using Certificates for Authentication* section of the *Assureon Administration Guide*.

Managing Active Archive settings for file systems

Nexsan's Assureon allows you to retain data, using Nexsan's Assureon archiving capabilities.

Use the instructions in this procedure for:

- Viewing and updating Active Archive settings on the Assureon Server
- Enabling or disabling Active Archive for a file system
- Viewing archiving statistics

Prerequisites

- You must have the optional Assureon Active Archive service enabled.
- For details about configuring Assureon Server and to configure settings such as watches, archive folders and methods, and generating reports or viewing events, please refer to the *Assureon Administration Guide* on the [Nexsan Assureon Documentation & Online Help](#) Web page.

▶ To manage Active Archive settings for a file system:

1. On the **Unity** node from the tree, select **Storage Pools > Pools**.
2. Click the **File Systems** node, then open a link to a file system.
3. Click the link to the file system you want to manage archive settings for. The **File Systems** panel opens. Note available space, and the CIFS and NFS Mount Points, where the files for the file system will be archived.
4. Click the **Archive Settings** tab. The **Active Archive** panel opens.

5. Select the **Enable Active Archive** button

Figure 10-2: File Systems Active Archive panel

The following Active Archive settings are the settings on Assureon Server by which data from your file system will be archived. The options that appear here are defined on the Assureon Server.

Table 10-1: Assureon Server Settings

Setting	Description
Archive Organization	Select the Assureon organization to be used for archiving. An organization is a group of one or more file systems which share retention rules, access classifications, and reports.
Archive File System	Select the file system in the Archive Organization to be used for archiving. A file system consists of a database, storage location (the stores), manifest and audit files as well as replication options. Think of it as a self-contained archive that shares properties with the other file systems within an organization.
Retention Rule	Select the retention rule to be used for data archived from this file system. Retention rules specify how long a file is kept under management. The default is 180 days, but the range is from 90 days to 99 years.
Access Classification	Select the access classification to be used for data archived from this file system. When a file is placed under Assureon management, it is stored using classification and sub classification information. Classifications enable you to control access to files. They also provide an intuitive way to search, audit, and dispose of files.
Action After Archiving	Define what is to happen to files once they have been archived: Shortcut , Leave , or Remove . Note Files will not be converted to shortcuts, or removed if asynchronous replication is enabled.

- Optionally, click the **Advanced Settings on Assureon Server** link to configure settings directly on Assureon.

► **To disable Active Archive:**

- Deselect the **Enable Active Archive** checkbox.
- Click the **Apply** button to save your changes.

Chapter 11

Site-level tasks

Unity provides several tools and functions for managing Unity and your Nexsan storage infrastructure. This section describes the management tools and functions available in Unity, as well as some of the administrative tasks you can perform to manage Unity.

To configure Asynchronous Replication settings, see the *Nexsan Unity Snapshots and Replication Guide*.

This section includes these topics:

Modifying the site name	348
Disabling automatic FASTier write cache assignment	348
Modifying the time server	348
Setting NDMP configuration options	349
Modifying site preferences	351
Modifying system preferences	355
Modifying the date, time, and time zone settings	356
Adding a remote site for multi-site management	357
Disconnecting a remote site	360
Disconnecting sites in a multi-site implementation	360
Updating Unity	363
Modifying authentication settings	371
Troubleshooting site-level warning and error conditions	401
Configuring NFS settings	402
Viewing APAL status	403
Viewing the Unity Vault Protection Module status	404
Viewing NVDIMM status	404
Enabling FTP support	405
Understanding the CallHome feature	406
Enabling Internet Connectivity	414

Modifying the site name

You set the [site name](#) for Unity during the Site Setup process. You can change the site name at any time.

► **To modify the site name for Unity:**

1. Click the Site node representing the site that you want to modify the site name for.
2. Expand the Site node's Properties panel.

Figure 11-1: Site node's General tab: modifying the site name

3. Type a new name for the site in the **Site name** field; make sure that the new name adheres to these restrictions and conventions:
 - Spaces are allowed
 - The site name can contain up to a maximum of 16 characters—including spaces.
 - The name must start with an (upper-case or lower-case) alphabetic or numeric character; and, with the exception of the hyphen (-), and period (.), the name can only contain alphanumeric characters, without spaces.

These characters are NOT allowed:

" / \ [] : ; | = , + * ? < >

4. Click **Apply**.

Disabling automatic FASTier write cache assignment

By default, [FASTier](#) write cache is assigned automatically on the Unity 2000, Unity 4000 and the Unity 6000.

You can disable the automatic assignment of FASTier write cache in the event that some of your pools would become degraded, or if you want to shut down your system.

On the Unity 2000, FASTier write cache can be manually unassigned and reassigned as it uses SSD rather than NVRAM.

► **To automatically allocate FASTier write cache:**

1. In Unity's tree view, click the Site node.
2. Expand the Site node's Properties panel.

Figure 11-2: Site node's properties panel—General tab

3. Under **FASTier Write Cache**, uncheck the **Automatically allocate FASTier Write Cache to storage pools** option.
4. Click **Apply**.

Modifying the time server

Unity uses a [time server](#), or NTP (Network Time Protocol) server, to synchronize its date and time with. By default, Unity synchronizes its date and time with the Microsoft Active Directory server or the LDAP Directory Server that it is connected to.

Notes:

- Unity supports multiple time servers: if you specify a time server, as opposed to using the Microsoft Active Directory/LDAP Directory server for date and time synchronization for Unity, we highly recommend that you specify at least two time servers. This ensures that date and time synchronization on Unity remains unaffected in the event that one of the time servers you specify is no longer available.

- Although a time server is not a strict requirement for the Unity authentication mode, it is still good practice to specify a time server so that the date and time on Unity is always synchronized with other network resources.

You can modify time server settings for Unity at any time.

▶ **To modify the time server for Unity:**

1. In Unity's tree view, click the Site node representing the site that you want to set, or modify, the time server for.
2. Expand the Site node's Properties panel.
3. Select the **User Authentication** tab.

Figure 11-3: Site node's properties panel—User Authentication tab

4. Type a time server for the site in the **Time Server** field. To specify multiple time servers, use a comma to separate each entry, for example: `tick.utoronto.ca,time.nrc.ca`.
5. Click **Apply** to update time server settings for Unity.

Setting NDMP configuration options

Network Data Management Protocol (NDMP) is used to transport data between network attached storage (NAS) devices and backup devices. This removes the need for transporting the data through the backup server itself, thus enhancing speed and removing load from the backup server.

Unity includes a NDMP plug-in that allows you to back up data from Unity to an industry-standard backup and restore solution that supports NDMP. The plug-in preserves all access rights for CIFS and NFS shares on Unity, and uses background snapshots for fast backups.

You can set, or modify, NDMP configuration options for Unity at any time.

Note When you set up NDMP backup for Unity, make sure to configure your backup and restore solution (or backup server) to connect to Unity using the Pool Resource Group virtual IP address that the storage pool, from where data is to be backed up, is assigned to. If you have 2 or more storage pools equally distributed between both Pool Resource Groups on the system, and you want to back up the data in all storage pools, you will need to establish 2 separate connections on your backup server to both Pool Resource Groups.

▶ **Setting advanced NDMP configuration options using the nxadmin CLI:**

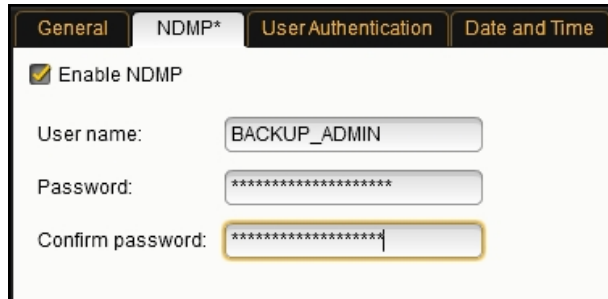
Unity provides advanced configuration options for setting up the NDMP plug-in on Unity, through the nxadmin command line interface (CLI). These options include: setting the NDMP protocol version (2, 3, or 4—the default is 4), setting the password encryption (cram-md5 or cleartext), and so on; for more information, see the `nstndmp` command in the CLI.

▶ **To configure NDMP in Unity:**

1. In Unity's tree view, click the Site node representing the site that you want to set, or modify, NDMP settings for.

- Expand the Site node's Properties panel.

Figure 11-4: Site node's properties panel—NDMP tab



- Select the **NDMP** tab.
- Select the **Enable NDMP** option—if this option is not already selected—to enable NDMP on Unity.
- Type the NDMP user name in the **User name** field.
- Type the password for the NDMP user in the **Password** field.
- Re-type the password for the NDMP user in the **Confirm password** field.

Note The user name and password combination must be consistent between Unity and the NDMP backup and restore application that you intend to use for backing up the data on Unity. The user name and password combination does not need to be defined on Unity as a local user, nor does it need to be defined on the Microsoft Active Directory, or LDAP Directory, server that Unity is connected to. The NDMP user name and password combination is used only for NDMP operations.

- Click **Apply** to set the NDMP configuration options for Unity.
- If needed, set or configure advanced options for NDMP in the nxadmin command line interface (CLI); see the `nstndmp` command in the CLI.

Modifying site preferences

Unity provides the **Nexsan Unity Preferences** panel in the **Tools & Settings** menu in Unity's global toolbar for configuring the auto-refresh interval for the site, date and time.

This section includes these topics:

Modifying the auto-refresh interval for the site	351
Scaling Unity to the screen resolution	352
Modifying the date and time formats displayed in Nexsan Unity	353
Modifying the Initial View	354

Modifying the auto-refresh interval for the site

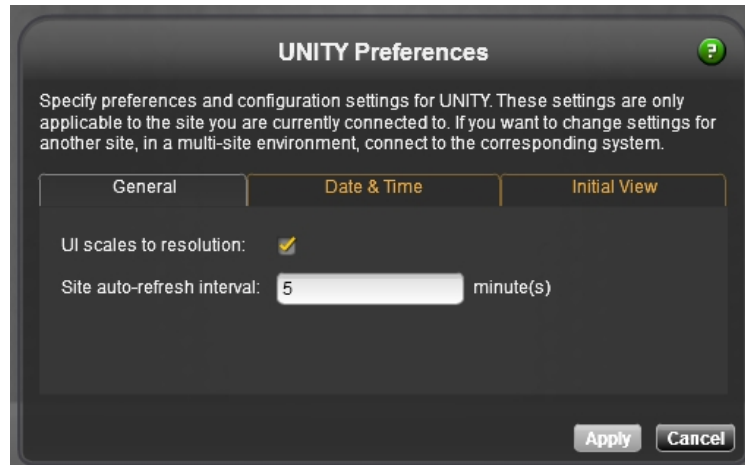
By default, Unity automatically updates configuration and status information for the Unity every 5 minutes, and then displays the updated information in Unity's tree view. You can increase or decrease the auto-refresh interval for the site, as needed.

You can also manually refresh configuration and status information for the site; for more information, see [Manually refreshing site- or file system-level information](#) on the next page.

► To modify the auto-refresh interval for the site:

1. If you are managing multiple sites (multi-site management of remote systems): in Unity's tree view, click the Site node representing the site that you want to modify the auto-refresh interval for.
2. Open the **Tools & Settings** menu in Unity's global toolbar, and select the **Unity Preferences** menu option. This opens the Nexsan Unity Preferences panel.

Figure 11-5: Nexsan Unity Preferences panel—General tab



3. Select the **General** tab.
4. Type a value—in minutes—for the auto-refresh interval in the **Site auto-refresh interval** text box; the default is 5 minutes. As an example, if you want Unity to automatically update configuration and status information for Unity every 2 hours, type 120 in the text box.

Note Setting too low an interval may cause network congestion and affect the overall performance of the system. If you need to refresh configuration and status information for Unity, you can perform a manual refresh at the site-level—or, at the file system-level, to obtain updated information for file systems on the

system; see [Manually refreshing site- or file system-level information below](#).

5. Click the **Apply** button to save the new auto-refresh interval, and close the Preferences panel.

Manually refreshing site- or file system-level information

You can manually refresh site-level, or file system-level, information on Unity. This does not impact the auto-refresh schedule.

▶ **To manually refresh site-level information:**

1. If you are managing multiple sites (multi-site management of remote systems): in Unity's tree view, click the Site node representing the site that you want to manually refresh.
2. Click the context menu button to open the Site node's context menu.
3. Select the **Refresh** option. Nexsan Unity updates configuration and status information for the selected site.

Tip You can also click the **Refresh** button on the Site node's Properties panel.

▶ **To manually refresh file system-level information:**

1. If you are managing multiple sites (multi-site management of remote systems): in Unity's tree view, click the Site node representing the site where the file systems that you want to manually refresh exist; this displays the Site node's child nodes.
2. Click the File Systems node.
3. Click the context menu button to open the File Systems node's context menu.
4. Select the **Refresh** option. Nexsan Unity updates configuration and status information for all the file systems on the selected site.

Tip You can also click the **Refresh** button on the File Systems node's Properties panel.

Scaling Unity to the screen resolution

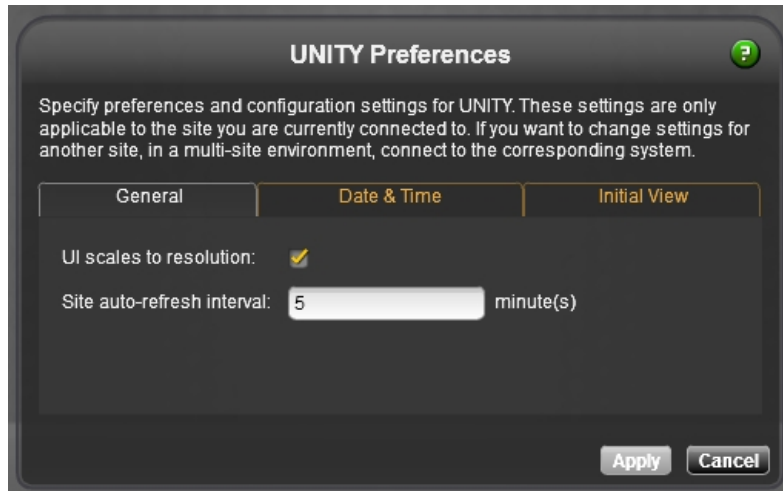
For best screen resolution to view Unity, we recommend that your screen size resolution be set to 1280 x 720 minimum. However, if you cannot change your screen resolution to this setting or higher, you have the possibility to make Unity scale to your resolution automatically for better viewing.

Note The setting is only applied to the site you are currently connected to. To change settings for another site in a multi-site environment, connect to the corresponding system.

► **To configure Unity scaling:**

1. In Unity's tree view, click the Site node.
2. Open the **Tools & Settings** menu in Unity's global toolbar, and select the **Preferences** menu option. This opens the Nexsan Unity Preferences panel.

Figure 11-6: Nexsan Unity Preferences panel—General tab



3. Select the **General** tab.
4. Select the **UI scales to resolution** option.
5. Click the **Apply** button to save the changes and close the panel.

Modifying the date and time formats displayed in Nexsan Unity

By default, Unity uses the YYYY/MM/DD format to display date information, and the h:mm:ss AM/PM format to display time; you can change the date and/or time formats for dates and times that for displayed in Unity.

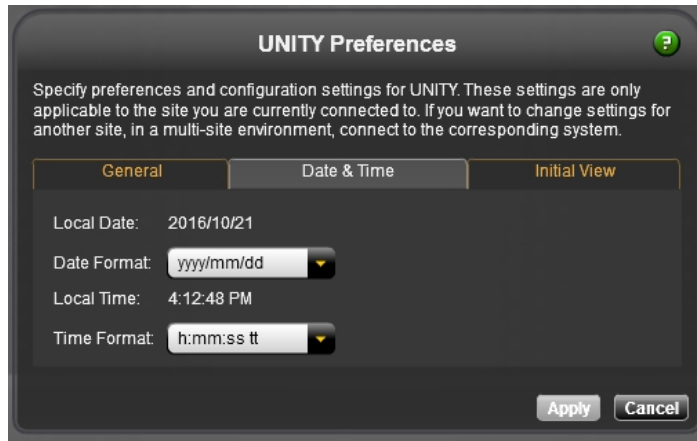
Note To change the date, time, or time zone, see [Modifying the date, time, and time zone settings on page 356](#).

► **To modify the date and time formats displayed in Unity:**

1. If you are managing multiple sites (multi-site management of remote systems): in Unity's tree view, click the Site node representing the site that you want to modify date and time formats for.

2. Open the **Tools & Settings** menu in Unity's global toolbar, and select the **Unity Preferences** menu option. This opens the Unity Preferences panel.

Figure 11-7: Unity Preferences panel—Date & Time tab



3. Select the **Date & Time** tab.
4. Adjust the date and time formats according to your preference:
 - To change the date format for the site: Open the **Date Format** drop-down list and select one of the available formats.
Unity adjusts the Local Date displayed above the **Date Format** drop-down list to illustrate the date format you select.
 - To change the time format for the site: Open the **Time Format** drop-down list and select one of the available formats.
Unity adjusts the Local Time displayed above the **Time Format** drop-down list to illustrate the time format you select.
5. Click the **Apply** button to save the new date and/or time format, and close the Preferences panel.

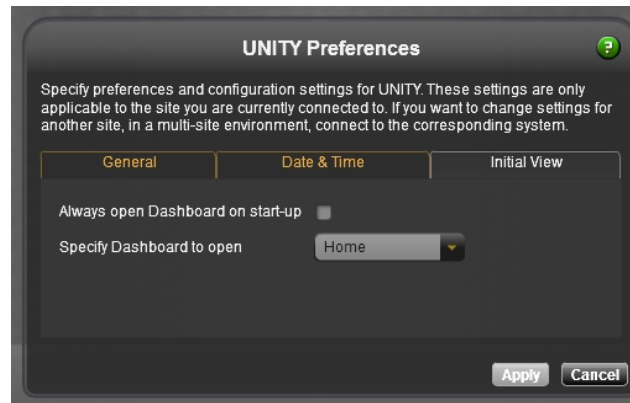
Modifying the Initial View

By default, when you start Unity, the Dashboard view gets displayed, more specifically, the Home dashboard. If you wish to change the dashboard to display or if you prefer to see the Tree view instead, you can modify Unity's initial view from the **Tools** menu.

► **To modify Unity's initial view:**

1. From the **Tools & Settings** menu in the Global Toolbar, select **Unity Preferences**.

Figure 11-8: Unity Preferences panel—Date & Time tab



2. The Unity Preferences dialog box displays. Click the **Initial View** tab.
3. Perform one of these actions:
 - To see the Tree view when you start Unity, clear the **Always open Dashboard on start-up** option.
 - To change the Dashboard to display in the Dashboard view, select another dashboard from the drop-down list.
4. Click **Apply** to save your changes.

Modifying system preferences

Unity provides the **System Preferences** panel in the **Tools&Settings** menu to set the background task retention settings.

This section covers this topic:

[Modifying background tasks settings below](#)

Modifying background tasks settings

Background tasks are asynchronous tasks that are scheduled, or they can be one-time manual tasks. These tasks include pool/file system/LUN deletion, site promotion/demotion, scrubbing, snapshots, pool resilvering, node or site failover, and replication.

By default, Unity deletes background tasks automatically. Five tasks are deleted every week. You can reduce or increase the number of tasks to delete, as well as changing the duration of tasks. You can also disable the auto-deletion setting if you want to keep the tasks running. Background Task retention settings apply for individual categories of tasks; for example, if you specify 2, the system will retain the last 2 completed tasks for each task type: pool scrub, replication, system or controller reboot, etc.

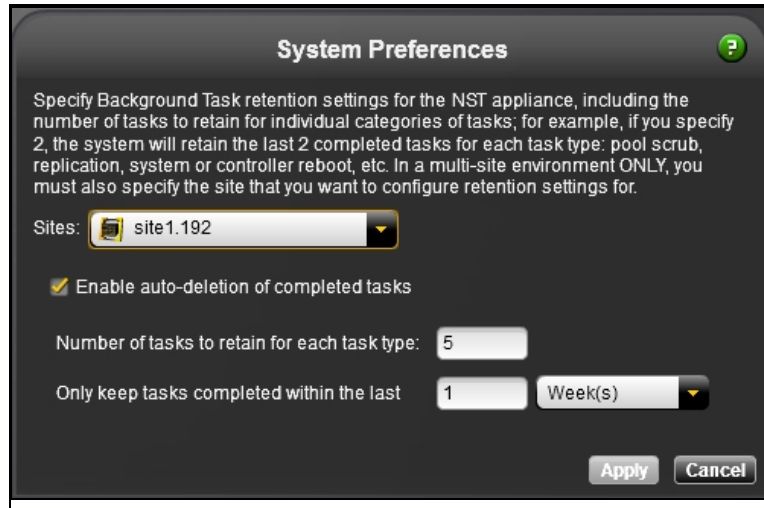
In a multi-site environment **ONLY**, you must also specify the site that you want to configure retention settings for.

You can modify the task auto-deletion settings at any time from the **System Preferences** menu.

► **To modify background task settings:**

1. Open the **Tools & Settings** menu in Unity's global toolbar, and select the **System Preferences** menu option. This opens the System Preferences panel.

Figure 11-9: System Preferences panel



2. If you are managing multiple sites (multi-site management of remote systems), select the desired site from the **Sites** drop-down menu. If there is only one site, the drop-down list does not display.
3. Perform some of these actions:

To...	Do this
disable auto-deletion of tasks	Clear the Enable Auto Delete of asynchronous tasks option.
change the quantity of tasks	Enter a new number in the Quantity field. The maximum value is 512.
change the duration of tasks	<ol style="list-style-type: none"> a. Enter a new number in the Duration field. The duration range is 15 days to 1 year. b. Change the Week(s) to Minute(s), Hour(s), or Day(s).

4. Click the **Apply** button to save the changes and close the System Preferences panel.

Modifying the date, time, and time zone settings

Typically, you set the time zone for Unity during the Site Setup process (see [Step 2: Configuring the site information](#) on page 40); if needed, you can modify the time zone at any time from the Site's properties panel.



CAUTION: After you change the time zone for the site, you must reboot the system for the time zone change to take effect: client systems and applications on the network will lose connection to Unity during the reboot process, which could result in data loss. Before changing the time zone and rebooting the system, make sure that client systems with an active connection to any file systems on Unity are disconnected; also make sure to quiesce any applications with an active connection to Unity.

► **To modify date, time, and/or time zone settings:**

1. If you are managing multiple sites (multi-site management of remote systems): in Unity's tree view, click the Site node representing the site for which you want to modify date and time settings.
2. Expand the Site's properties panel.

3. Select the **Date and Time** tab.

Figure 11-10: Site's properties panel—Date and Time tab

Changing the time zone on the UNITY appliance requires you to reboot the system for the time change to take effect. Client s
UNITY appliance.

Server Time Zone:
(GMT-05:00) Eastern Time (US & Canada)

Server Time:
2016/10/21 4 48 52 PM

Time Server: **time.nist.gov** **Synchronize**

4. Adjust the date and time settings according to your preference:

To change the...	Do this
server time zone	Select a new time zone from the drop-down list.
server date	Click the calendar icon next to the date and choose a new date.
server time	Type new numbers in the appropriate boxes or use the up and down arrows to modify the time.
synchronize the time with the Time Server	Click the Synchronize button. Note You can change the Time Server used by Unity using the User Authentication tab; see Modifying authentication settings on page 371.

5. Unity will display a warning, click **OK** to continue.
6. Click the **Apply** button to apply your changes on both nodes.

Adding a remote site for multi-site management

Unity provides single pane-of-glass management for multiple Unity on the network. This allows you to manage multiple Unity sites from a single Unity browser session; or, more specifically, from a single Unity that you designate as the central management hub for all other Unity installed on your LAN or WAN.

For example, if you have 3 systems installed in 3 different geographic locations: Hong Kong, Montreal, and San Diego, you can designate the system in Montreal as the management hub for your Nexsan storage infrastructure; and then, to enable multi-site management, you add the systems in Hong Kong and San Diego to Unity in Montreal using Unity. You can now administer all 3 sites from an Unity session running on the system in Montreal, by simply navigating between systems.

▶ **To add a remote Unity:**

1. In a web browser, launch Unity for Unity that you want to use as the management hub for your infrastructure.
2. Select the **Add a site** menu option from the **Tools & Settings** menu in Unity's global toolbar. This opens the Connect to a site popup.

Figure 11-11: Connect to a Site popup



3. In the **Intersite virtual IP** field, type the Intersite virtual IP address configured on the primary data network interface (nx0) of the remote site.

4. Click **Connect** to establish a connection to the remote Unity.

Unity connects to the remote Unity and checks the system to make sure it is configured properly: the remote system must be properly set up using the Site Setup Wizard (see the *Nexsan Unity hardware Reference Guide*). Depending on the speed of your network connection, this process can take some time to complete.

If the user account you are currently logged on with on the current system does not exist on the remote Unity that you are attempting to add, or if the user account is not assigned the Site Administrator role on the remote site, Unity prompts you for user credentials to connect to the remote system.

You must either provide the Unity Administrator (**nxadmin**) credentials for the remote Unity, or the user name and password of a Site Administrator configured on the remote system:

To...	Do this
log on as a Site Administrator	<ol style="list-style-type: none"> a. In the User name field, type the user name of a Site Administrator on the remote Unity. b. In the Password field, type the password for the Site Administrator on the remote Unity. c. (For systems connected to a Microsoft Active Directory domain or LDAP Directory server) From the Domain drop-down list, select the domain where the Site Administrator user account exists. d. Click the Log on button.
log on as the Unity Administrator (nxadmin) Note (For systems connected to a Microsoft Active Directory domain or LDAP Directory server) When logging on as the Unity Administrator (nxadmin), you must also enter credentials for a domain user account. Otherwise, you will be unable to access domain user accounts on the remote Unity; as a result, you will be unable to configure security for the site, storage pools, and file systems on the remote site, including assigning Site or Storage Pool Administrators and configuring file system-level access permissions.	<ol style="list-style-type: none"> a. In the User name field, type the user name of a Site Administrator on the remote Unity. b. In the Password field, type the password for the Site Administrator on the remote Unity. c. (For systems connected to a Microsoft Active Directory domain or LDAP Directory server) From the Domain drop-down list, select the domain where the Site Administrator user account exists. d. Click the Expand button next to the Login as: nxadmin field; this displays the Password field. e. In the Password field, type the password for the Unity Administrator (nxadmin) on the remote Unity. f. Click the Log on button.

Unity informs you when it successfully connects to the remote Unity and adds the remote system to the current site.

5. Click the **Close** button.

Disconnecting a remote site

You can disconnect a remote site from the current Unity.

▶ **To disconnect a remote Unity:**

1. In Unity's tree view, click the node representing the remote Unity that you want to disconnect.
2. Click the node context menu button to open the Site node's context menu.
3. Select the **Disconnect Site** option.
4. Click **Yes** when prompted to confirm.

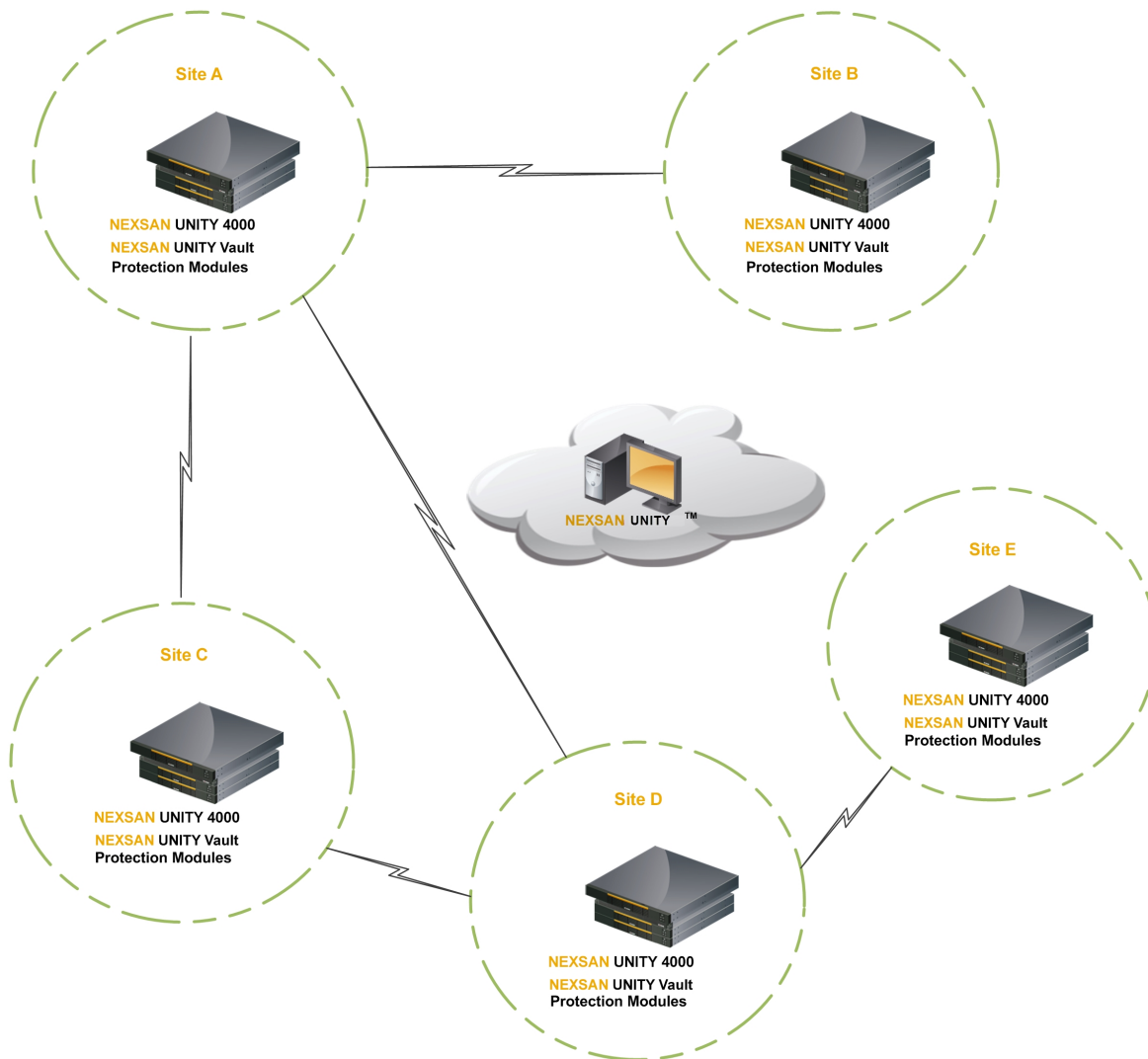
Tip You can also click the **Disconnect Site** button on the Site node's Properties panel.

Disconnecting sites in a multi-site implementation

In a multi-site implementation, a site can be connected to multiple sites. You can choose to remove a connection between two sites while keeping the connection between others. When you disconnect a site, it will still appear as being connected to other sites. To completely remove a site from your multi-site implementation, you must disconnect it from all sites to which it is connected. If a selected site is connected to only one site, it is removed from Unity immediately.

As an example, Site A is connected to Site B, C, and D. Site D is connected to C and E. When you select Site A to disconnect it, Unity displays the list of connected sites, so B, C, and D in our example. If you select Site C, Unity removes its connection from Site A. However, it will still appear in Unity because Sites C and D remain connected. When you select the node of Site A, Site C appears as grayed out. When you select the node of Site D, Site C appears with a regular icon. To completely remove Site C from the multi-site implementation, you must disconnect it from Site D as well.

Figure 11-12: Site connections in a multi-site implementation



► **Before you begin:**

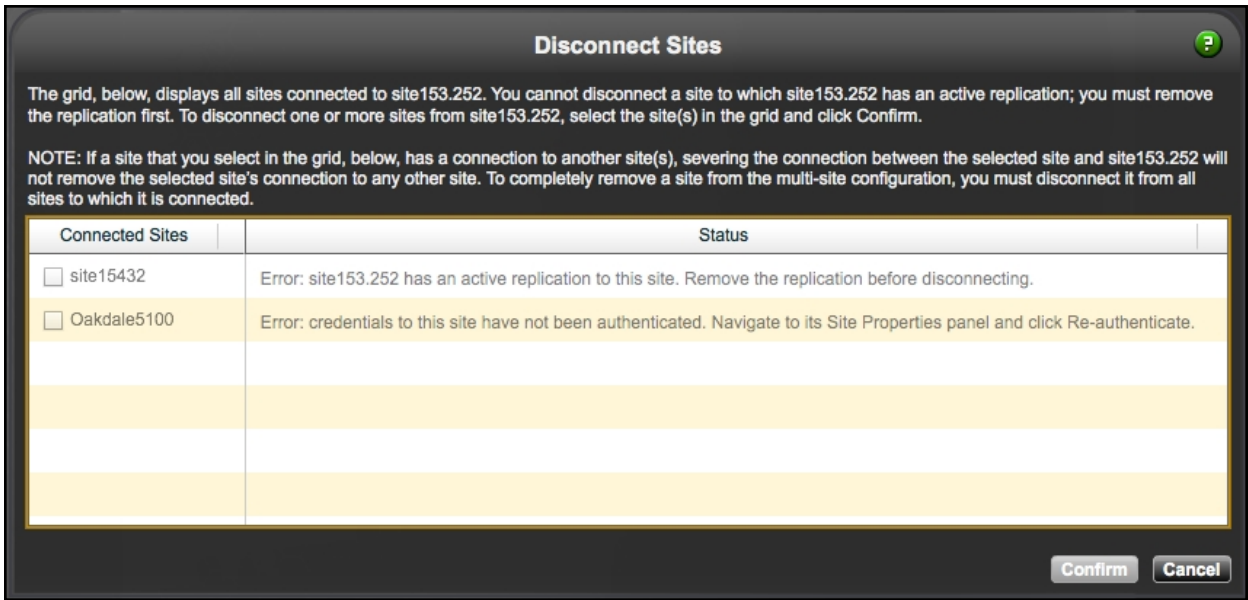
- If the site has replication set up, you must remove the replication for all storage pools on that site first, as described in the *Nexsan Unity Snapshots and Replication Guide*.
- You must be authenticated to the site.

► **To disconnect sites in a multi-site implementation:**

1. In Unity's tree view, select the node representing the remote site.
2. Click the node context menu button to open the Site node's context menu.

3. Select the **Disconnect Site** option. Unity displays the list of sites that are currently connected to the selected site.

Figure 11-13: Disconnecting sites



4. Select one or more sites and click **Confirm**.
- Note** If you get an error message because the site is inaccessible, proceed only if you expect the site to be permanently inaccessible.

The selected site(s) are no longer connected to the site.

Updating Unity

The Unity firmware upgrader provides three options that enable you to:

- upgrade firmware components on Unity. This also upgrades the firmware upgrader itself.
- add new features to Unity
- upgrade the cluster license to a permanent license.

Topics in this section:

Upgrading to the latest firmware	364
Adding new features	366
Upgrading the cluster license	369

Upgrading to the latest firmware

The Unity firmware upgrader provides three methods for upgrading firmware: by connecting to the Unity License Server, from a USB key if you do not have Internet access, or by uploading a file from a directory located on your network.

The firmware update you are entitled to perform on Unity depends on whether or not you have a maintenance plan for Unity:

- With a maintenance plan, you can update firmware components on Unity to a major release version; for example: 5.x.x to 6.x.x.
- Without a maintenance plan, you can only update firmware components to a minor release; for example: 5.1.x to 5.1.2.

For more information about maintenance plans, please contact your Nexsan Reseller or Support representative.



CAUTION: The Nexsan Unity firmware upgrader reboots Unity. For Clustered systems, the firmware upgrader also performs a cluster failover operation to the other node in the cluster. As a result, client systems and applications on the network will temporarily lose connection to Unity during both the reboot and failover operation.

Before upgrading, we recommend the following:

- That you disconnect any client system with an active connection to datasets (file systems and/or iSCSI LUNs) on Unity.
- That you quiesce any applications with an active connection to Unity.

Note If there is an attached E-Series that also needs a firmware update your Unity will need to be off lined.

▶ **To perform a firmware update:**

1. In the Unity tree view, click the Unity System node representing the Unity that you want to perform the upgrade on.


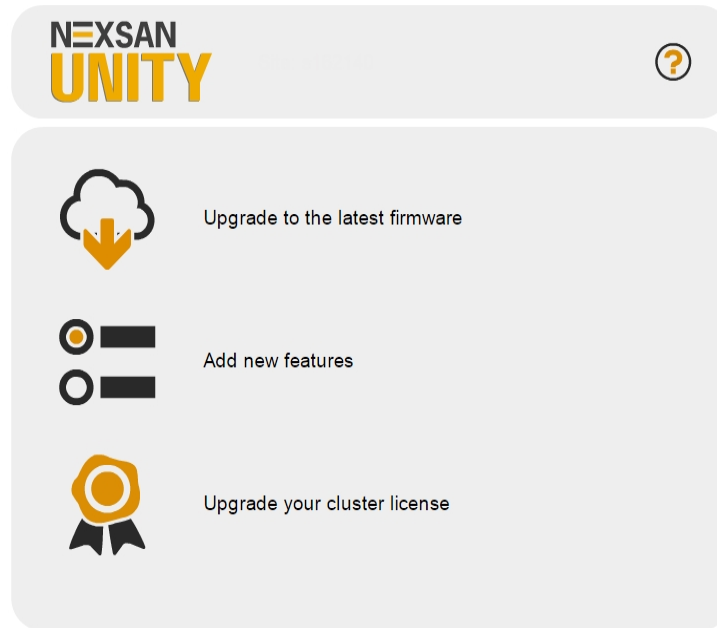
- From the Global Toolbar, select the **Check for Updates** icon . Unity checks the system health and if both controllers are healthy, prompts you to **log on**. If either controller is in an unhealthy state, review the error messages and proceed as indicated (restart the controller, free disk space, and so on).

Figure 11-14: Nexsan Unity firmware upgrader



- Select **Upgrade to the latest firmware**.
- Select the relevant firmware update option:
 - **Connect to the Unity License Server** to check for updates on the Nexsan Unity License Server using the Internet.
 - **Plug in a USB drive** to upgrade firmware components from a USB key loaded with the update files provided to you by Nexsan Support. Before performing the upgrade, you must plug the USB key into one of the available USB ports at the back of Unity chassis.
 - **Upload from your browser** to browse for the upgrade package file (.tgz) and select it from a directory located on your network.
- The firmware upgrader downloads the version you selected in the previous step, and displays the version running on the local Unity System and the latest available update for your system. Click **Next** to proceed. Unity prepares the package for installation.
- Click **Proceed** to start the upgrade. The firmware upgrader displays a summary of the steps to be completed. Click **Start** to proceed with the upgrade.
- After successfully upgrading the first controller, the firmware upgrader pauses before upgrading the peer controller. Click **Proceed** when you are ready to continue the upgrade.
- After the upgrade on the peer controller completes, click **Start Unity**.

► **Related Topics:**

[Adding new features](#) on the next page

[Upgrading the cluster license](#) on page 369

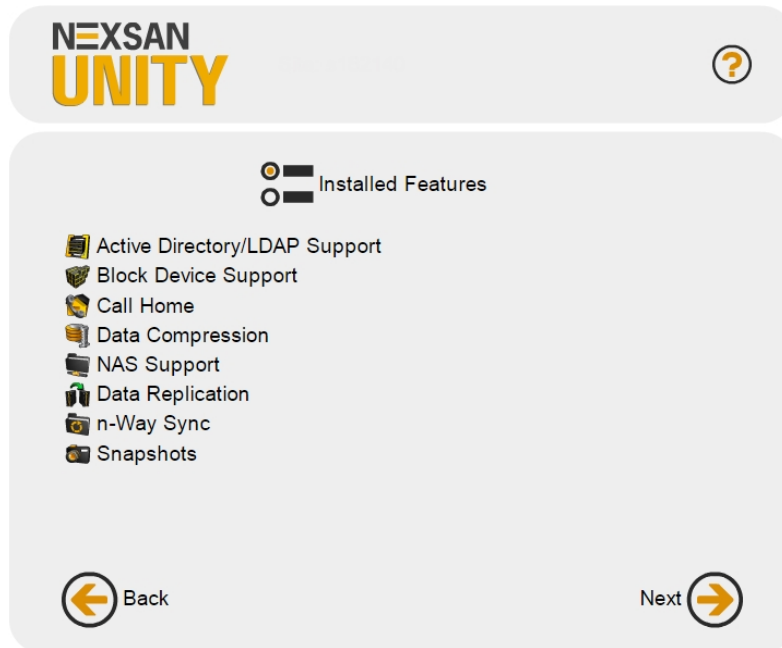
Adding new features

The Unity firmware upgrader allows you to add new features to Unity.

▶ **To add features:**

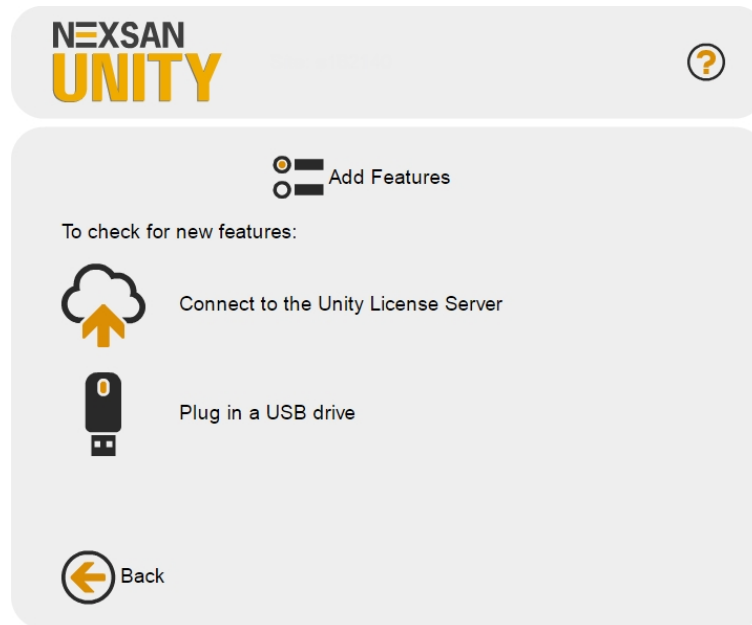
1. Launch the firmware upgrader as described in [Upgrading to the latest firmware](#) on page 364.
2. Select **Add new features**.
3. Unity displays the features currently installed in your site. Click **Next** to continue.

Figure 11-15: Viewing installed features



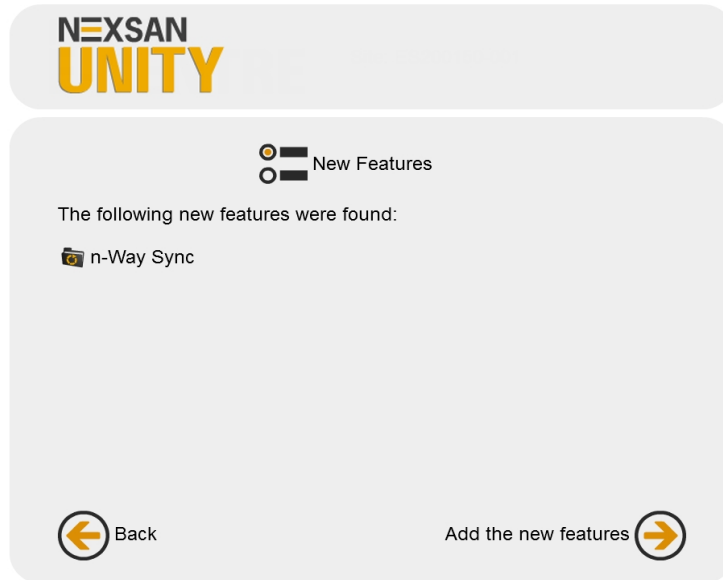
4. To check if new features are available, select the relevant feature update option:
 - **Connect to the Unity License Server** checks for new features on the Nexsan Unity Update Server.
 - **Plug in a USB drive** checks for new features from a USB key with the update files provided to you by Nexsan Support. Before performing the upgrade, you must plug the USB key into one of the available USB ports at the back of Unity chassis.

Figure 11-16: Checking for new features



5. The firmware upgrader verifies if new features are available on the Update Server and displays the results. Perform one of these actions:
 - If new features are found, click **Add the new features**.
 - If no new features are found, click the left arrow to go back to the main screen and close the upgrader.

Figure 11-17: Adding new features



Upgrading the cluster license

The Unity firmware upgrader allows you to upgrade the type of license you purchased for Unity.

An expiration date displays if the cluster license is set to *Evaluation*, otherwise *Permanent License* displays if the system has been converted to a permanent deployment.

► **To convert a temporary cluster license to permanent:**

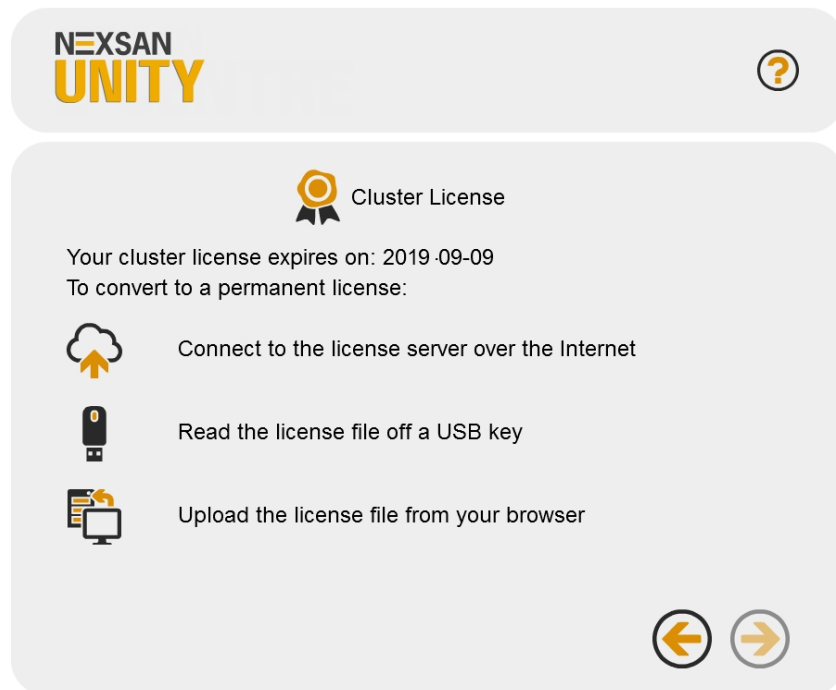
1. Launch the firmware upgrader as mentioned in [Upgrading to the latest firmware](#) on page 364.
2. Click **Update your license**.
3. Unity displays the current license status.

If your license has expired or is about to expire, choose one of these options:

- Connect to the license server over the Internet to download the a permanent license from the Nexsan Unity License Server.
- Plug in a USB drive to read the license package file from a USB key with the update files provided to you by Nexsan Support. Before performing the upgrade, you must plug the USB key into one of the available USB ports at the back of Unity chassis.
- From your browser: you can browse for and select the package file from a directory located on your network. By default, the firmware upgrader will look for a `.nxi` file.

If you have a permanent license, no action is required. Click the left arrow to go back to the main screen and close the upgrader.

Figure 11-18: Viewing cluster license status



4. The firmware upgrader reads the license file from the License Server or the USB key and displays a confirmation message once the license is converted to permanent.

Perform one of these actions:

- If the cluster license was upgraded successfully, click the right arrow to finish.
- If an error occurred, read the error information and try to resolve the issue accordingly.

Modifying authentication settings

By default, Unity configures the Unity authentication mode during the initial site setup. With Unity authentication, a user enters a user name and password to log on to Unity, and Unity verifies that they match a user name and password stored locally on Unity.

With authentication through a Microsoft Windows Active Directory domain or an LDAP Directory service, a user enters a user name and password in the same Unity log on window and Unity checks the Microsoft Windows Active Directory server or LDAP Directory server for a matching user record.

Note In a multi-site environment, the user authentication mode must be the same for all sites. If a remote site is on a different domain and/or requires authentication with different credentials than the logged in user, you must click the Site node of the site you want to access, open its properties panel, and click the **Re-authenticate** button to enter the credentials for that site.

Note SMBv1 must be enabled on Domain Controllers when using Active Directory Authentication on Unity.

This section includes these topics:

- Active Directory:
 - [Joining an Active Directory Domain](#) below
 - [Managing domain controllers](#) on page 385
 - [Enabling Kerberos for accessing CIFS file system](#) on page 386
 - [Unjoining Unity from an Active Directory domain](#) on page 396
- LDAP: [Connecting to an LDAP Directory service](#) on page 398
- Local: [Setting up Unity authentication](#) on page 400

Joining an Active Directory Domain

This section includes these topics:

- [Microsoft Active Directory domain requirements](#) below
- [Delegating control to the non-Administrator user account](#) on page 376
- [Creating computer objects on the Active Directory server](#) on page 373
- [Joining an Active Directory domain using Unity](#) on page 380

Microsoft Active Directory domain requirements

This section describes the Microsoft Active Directory support requirements for Unity. Carefully review this table before [joining](#) Unity to a Microsoft Active Directory domain.

Requirement	Description
Operating Systems	<ul style="list-style-type: none"> ● Windows Server 2012 ● Windows Server 2008 R2 ● Windows Server 2008 x86 or x64, including: <ul style="list-style-type: none"> ● Windows Server 2008 with Service Pack 1 ● Windows Server 2008 with Service Pack 2 ● Window Server 2003 R2 x86 or x64

Requirement	Description
Reverse DNS	The Microsoft Active Directory implementation must be configured with a reverse DNS lookup zone.
Global catalog and LDAP catalog ports	The primary domain controller that Unity connects to must have both the global catalog port (3268) and the LDAP catalog port (389) open. In a Microsoft Active Directory forest implementation, all domain controllers must have these ports open.
Time server	<p>The primary domain controller that Unity connects to must be configured as a reliable time source (time server capability) for the domain. In a Microsoft Active Directory forest implementation, all domain controllers must have this capability.</p> <p>If the Microsoft Active Directory implementation does not provide, or is not configured for, time server capability, you must specify a valid Network Time Protocol (NTP) source for Unity to synchronize its date and time with.</p>
Domain administrator privileges	<p>You will need to provide domain credentials for a domain administrator, or of a user who has full domain administrative privileges.</p> <p>If the user account does not have domain administrator privileges, you must create computer objects for Unity in the Active directory domain, and give the corresponding user account management access to the objects before joining the domain.</p> <p>For procedural steps, see:</p> <p>Delegating control to the non-Administrator user account on page 376, and Creating computer objects on the Active Directory server on the facing page.</p>
DNS alias for non-standard domain names	<p>Use a DNS alias if the domain controller name starts with a digit, or contains nonstandard characters. If the name of the primary domain controller that you configure Unity to connect to starts with a digit, or contains nonstandard characters, you must set up an alias—made up of only standard characters—for the domain controller on the DNS server; standard characters include: (A-Z, a-z), digits (0-9), and hyphens (-).</p> <p>You must also add a resource record for the alias in the reverse DNS lookup zone. Later, when you configure the Unity to join the Microsoft Active Directory domain, you must specify the domain controller’s alias, including its fully qualified domain name (FQDN), in the Domain Controller (optional) field.</p> <p>As an example, if the domain controller uses this name: 1MYDC_001.mydomain.lan,</p> <ol style="list-style-type: none"> 1. Create this alias for the domain controller on the DNS server: MYDC-001 2. Add a resource record for the alias in the reverse DNS lookup zone. 3. During the Site Setup process, when configuring Unity to join the Microsoft Active Directory domain, specify the domain controller’s alias, including its fully qualified domain name (FQDN), in the Domain Controller (optional) field: MYDC-001.mydomain.lan

Requirement	Description
LM Manager authentication level	By default, Unity uses NTLM level 2 authentication. If your Active Directory Domain Controller uses a different authentication level, you must change this setting by selecting another LM Compatibility Level in Step 7 .
Creation of machine accounts	The Microsoft Active Directory implementation must support the creation of machine accounts in the default Organizational Unit (OU). To change the Organizational Unit of computer objects, click the Advanced button when joining a domain .

Creating computer objects on the Active Directory server

In a typical deployment, Unity requires Domain Administrator privileges to join a Microsoft Active Directory domain. This process allows Unity to automatically create and configure computer objects for Unity on the Microsoft Active Directory server, without any manual intervention from a network administrator.

In some environments, specifying Domain Administrator credentials to integrate Unity with the Microsoft Active Directory Domain is not desirable, or possible. For these deployments, a network administrator can join Unity to a Microsoft Active Directory Domain using a user account with limited domain administrative privileges.

To allow this, you must manually perform configuration steps for creating and configuring computer objects for Unity on the Microsoft Active Directory server:

- Determine or create the non-Administrator domain user account that you want to use to join Unity to the Microsoft Active Directory Domain. [Delegate full control](#) to this user before joining the Active Directory domain.
- Create a computer object(s) for Unity on the corresponding Active Directory Server for each controller node, as described in this procedure.
- Configure the attributes for the computer object(s) according to the settings described in this procedure.
- Use the **Advanced** button [join Unity](#) to the Microsoft Active Directory Domain using the credentials for the non-Administrator domain user account.



CAUTION: RISK OF OUTAGE

Do not join Unity with Active Directory to Domain Controllers hosted on VMware. Domain Controllers used with Unity and Active Directory must either be a physical device or hosted externally to Unity.

▶ **To create a computer object for a non-Administrator user account:**

1. On the relevant Active Directory Server, add a new computer object for Unity, using each controller node's host name.



CAUTION: When creating the computer object, make sure to enter the host name exactly as it is configured on Unity, or on each of its controller nodes.

To obtain the host name for Unity controller nodes:

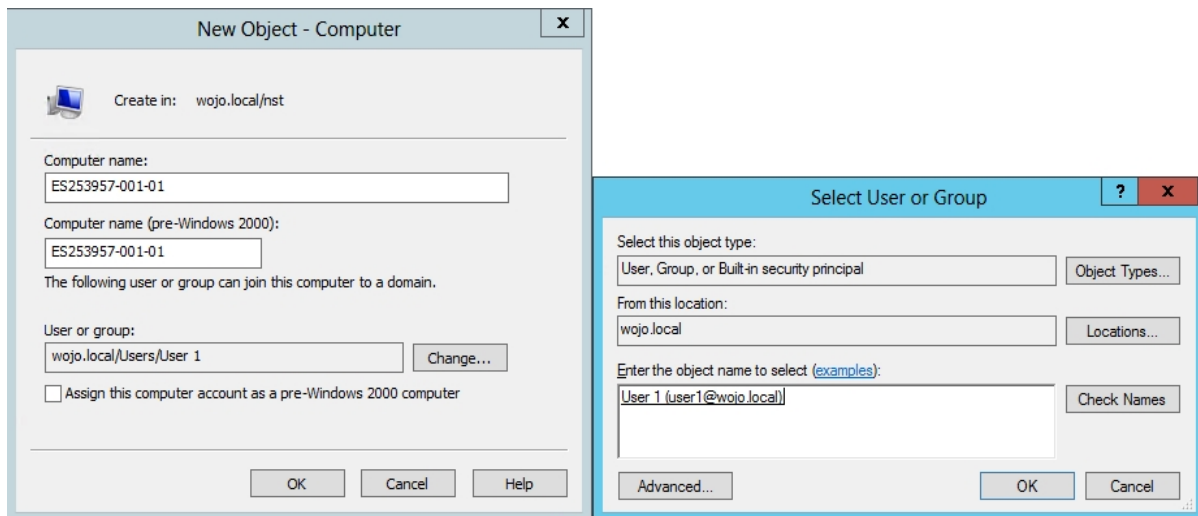
- a. Access the nxadmin CLI on Unity via SSH or remote console. Download and install an SSH client of your choice on a client machine that has network connectivity to Unity. You can use Putty, which is a (free) open source telnet and SSH client, available for download at this URL:

<http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html>

- b. Once you download and install an SSH client, launch it, and enter the IP address of a controller node.
 - c. When the login prompt displays, type **nxadmin**, and press Enter.
 - d. When you are prompted for the password, type the nxadmin (Nexsan Unity Administrator) password configured on Unity, and then press Enter. If you are connecting to a system that has not yet been configured using the Nexsan Unity Site Setup Wizard—that is, an uninitialized Unity—you must type the default password for the nxadmin (Nexsan Unity Administrator) account: **PASSWORD** (all upper-case).
 - e. On each controller node, run the `hostname` command.
 - f. Take note of the Unity host name; for example, `ES253957-001-01`.
2. Give the non-Administrator domain user account the ability to perform the operation for integrating Unity with the Active Directory Domain. You must give the non-Administrator domain user account the ability to join each controller node to the Active Directory Domain.

It is important that you perform this step, since, by default, the privileges for joining a new computer object to the Active Directory Domain are automatically assigned to the Domain Administrator user/group account.

Here is an example:



3. Set the following attributes for the computer object that you added for Unity to the Active Directory Server. You must set these attributes separately for each controller node.



CAUTION: Use the Active Directory Service Interfaces Editor (ADSI Edit) to set the attributes for the computer object(s). For each attribute, make sure to specify the value using the exact letter case, as shown.

Table 11-1: Computer object attributes

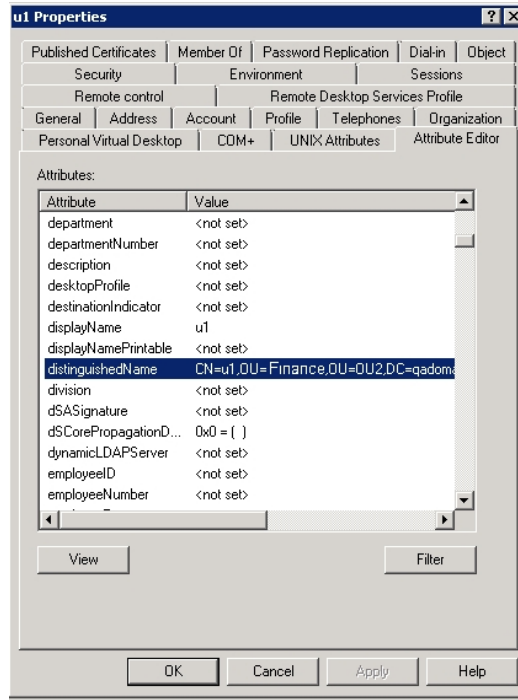
Attribute	Value to set...
dNSHostName	<NESTHOSTNAME>.<domainname> For example: ES777666-001-01.qadomain.net
msDS-SupportedEncryptionTypes	31
servicePrincipalName	<ul style="list-style-type: none"> ● cifs/<NESTHOSTNAME>.<domainname> For example: cifs/ES777666-001-01.qadomain.net ● host/<NESTHOSTNAME>.<domainname> For example: host/ES777666-001-01.qadomain.net ● HTTP/<NESTHOSTNAME>.<domainname> For example: HTTP/ES777666-001-01.qadomain.net ● nfs/<NESTHOSTNAME>.<domainname> For example: nfs/ES777666-001-01.qadomain.net ● root/<NESTHOSTNAME>.<domainname> For example: root/ES777666-001-01.qadomain.net ● host/<NESTHOSTNAME> For example: host/ES777666-001-01
userPrincipalName	host/<NESTHOSTNAME>.<domainname>@<DOMAINNAME> For example: host/ES777666-001-01.qadomain.net@QADOMAIN.NET
userAccountControl	4130

Note If the domain you are joining is `department.company.com`, make sure to use that whole name in *Step 7*.

- In the **distinguishedName** attribute of the computer object, take note of the Organizational Unit names, in this format: *OU=name1,OU=name2*, etc. You will need this for *Step 7*.

Note You can create a new OU at the root of the domain tree or use an existing user-defined OU.

In the example below, you would use *OU=Finance,OU=OU2*.



- Repeat **step 3** above for the computer object that you added for the 2nd controller node.
- Configure Unity using the Nexsan Unity Site Setup Wizard (if not already configured).
- Join Unity to the Microsoft Active Directory Domain in Nexsan Unity.

Make sure you specify the user name and password for the non-Administrator domain user account that you granted the ability to perform the operation for integrating Unity with the Active Directory Domain; see **step 5** of [Joining an Active Directory domain using Unity](#) on page 380.

Make sure to use the same (whole) domain name as in *Step 3*.

- At the Configure User Authentication Mode step, click the **Advanced** button.
 - Enter the Organizational Unit (OU) names obtained in *Step 4*.
 - Select the **Use pre-defined computer objects** option.
 - Click **Apply**.
- After configuring Unity and successfully joining the system to the Microsoft Active Directory Domain, reset the **userAccountControl** attribute to **69632**—for each Unity computer object that you added to the Active Directory Server: DONT_EXPIRE_PASSWORD | WORKSTATION_TRUST_ACCOUNT.

Delegating control to the non-Administrator user account

After [creating a computer object](#) in the Active Directory server, you must give full control to the non-Administrator user account for the selected Organization Unit (OU), so that this user can operate Unity in your Active Directory environment.

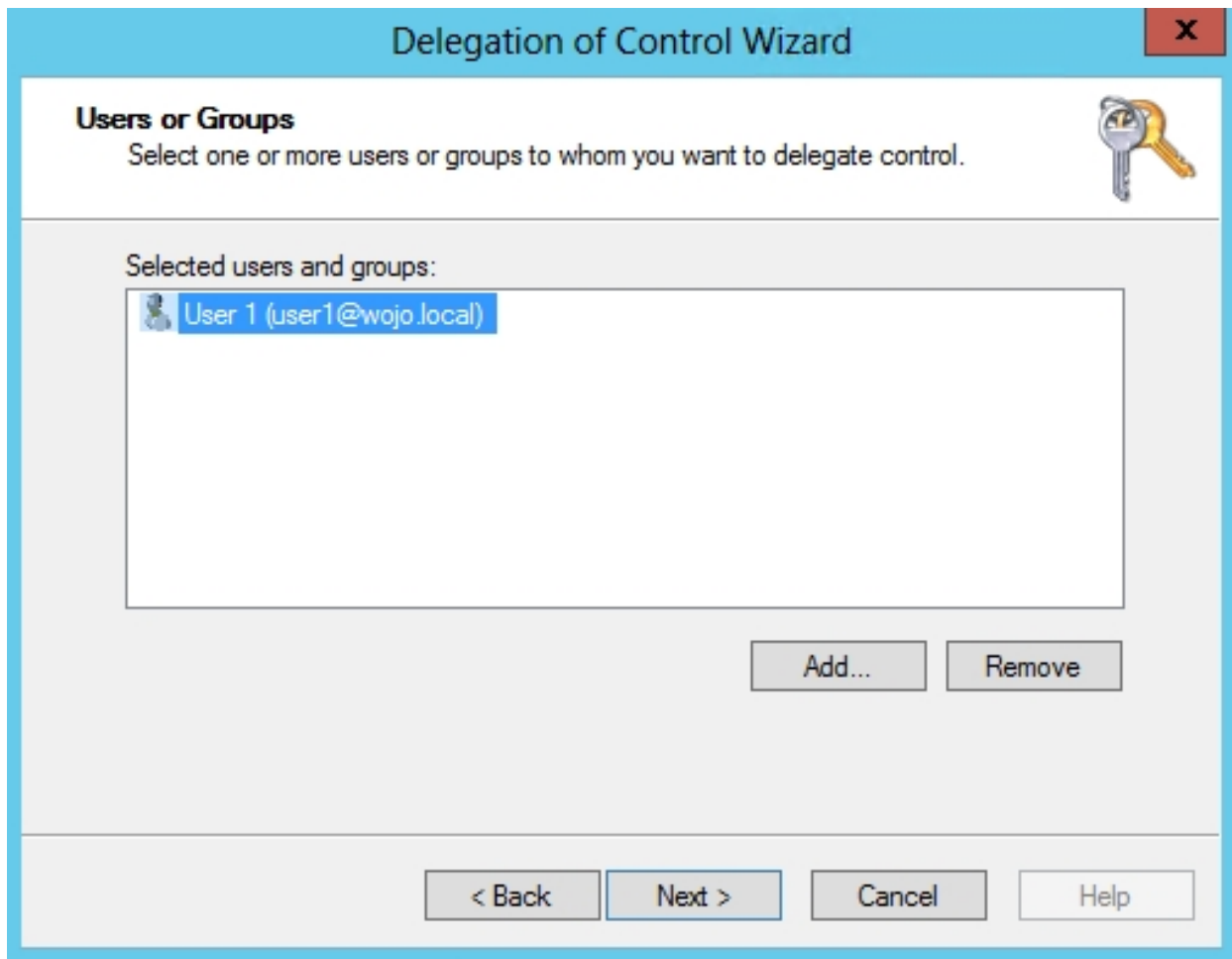
► **To delegate control:**

1. To open Active Directory Users and Computers:
 - a. Click **Start** then select **Control Panel**.
 - b. Double-click **Administrative Tools**.
 - c. Double-click **Active Directory Users and Computers**.

To open Active Directory Users and Computers in Windows Server 2012, click **Start** , and type `dsa.msc`.

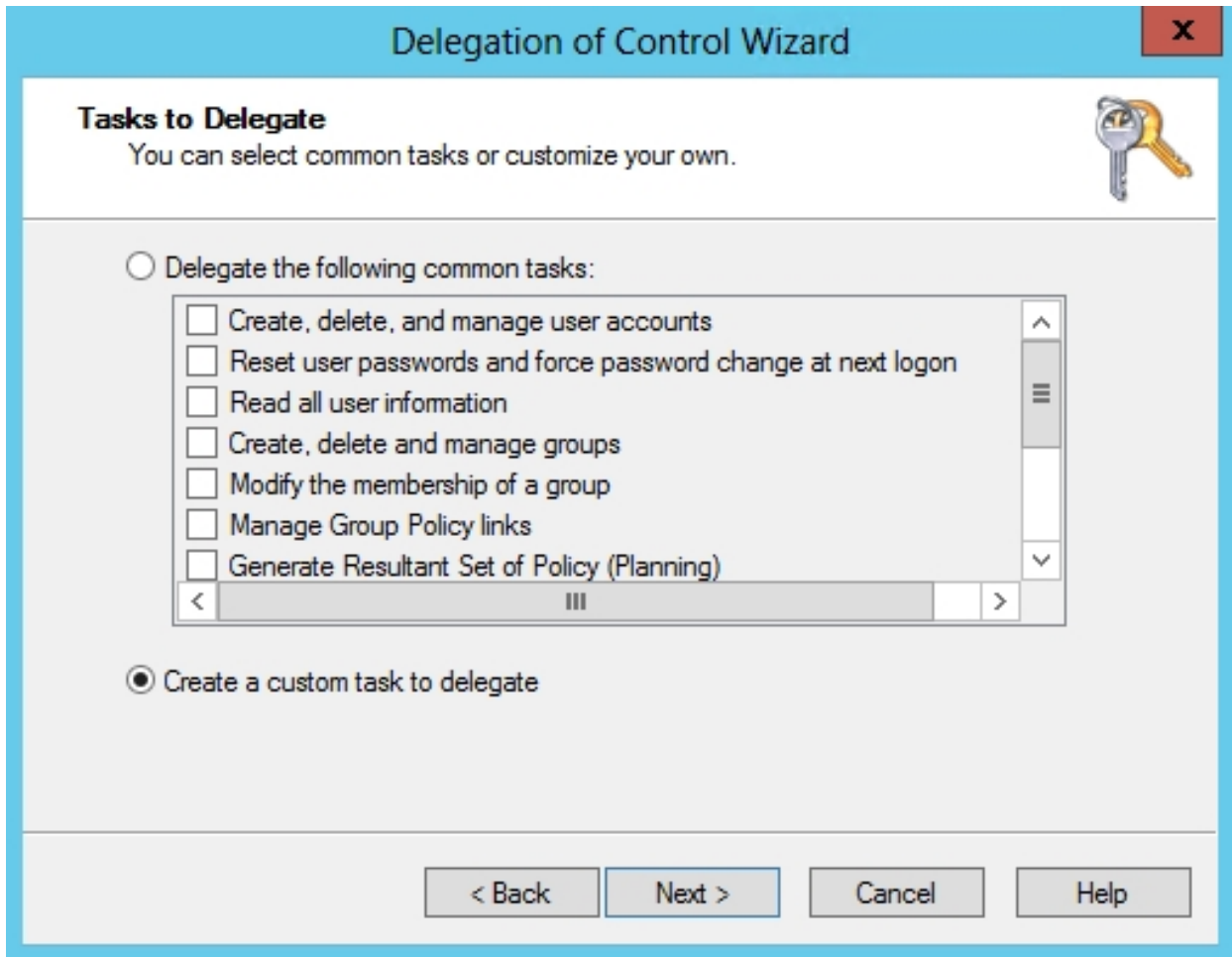
2. In the console tree, right-click the organizational unit (OU) for which you want to delegate control, under *Active Directory Users and Computers\ domain node*.
3. Click **Delegate Control** to start the Delegation of Control Wizard.
4. Click **Add** and select the non-Administrator user account used in the previous section. Click **Next**.

Figure 11-19: Active Directory - Delegation of Control Wizard: select a user



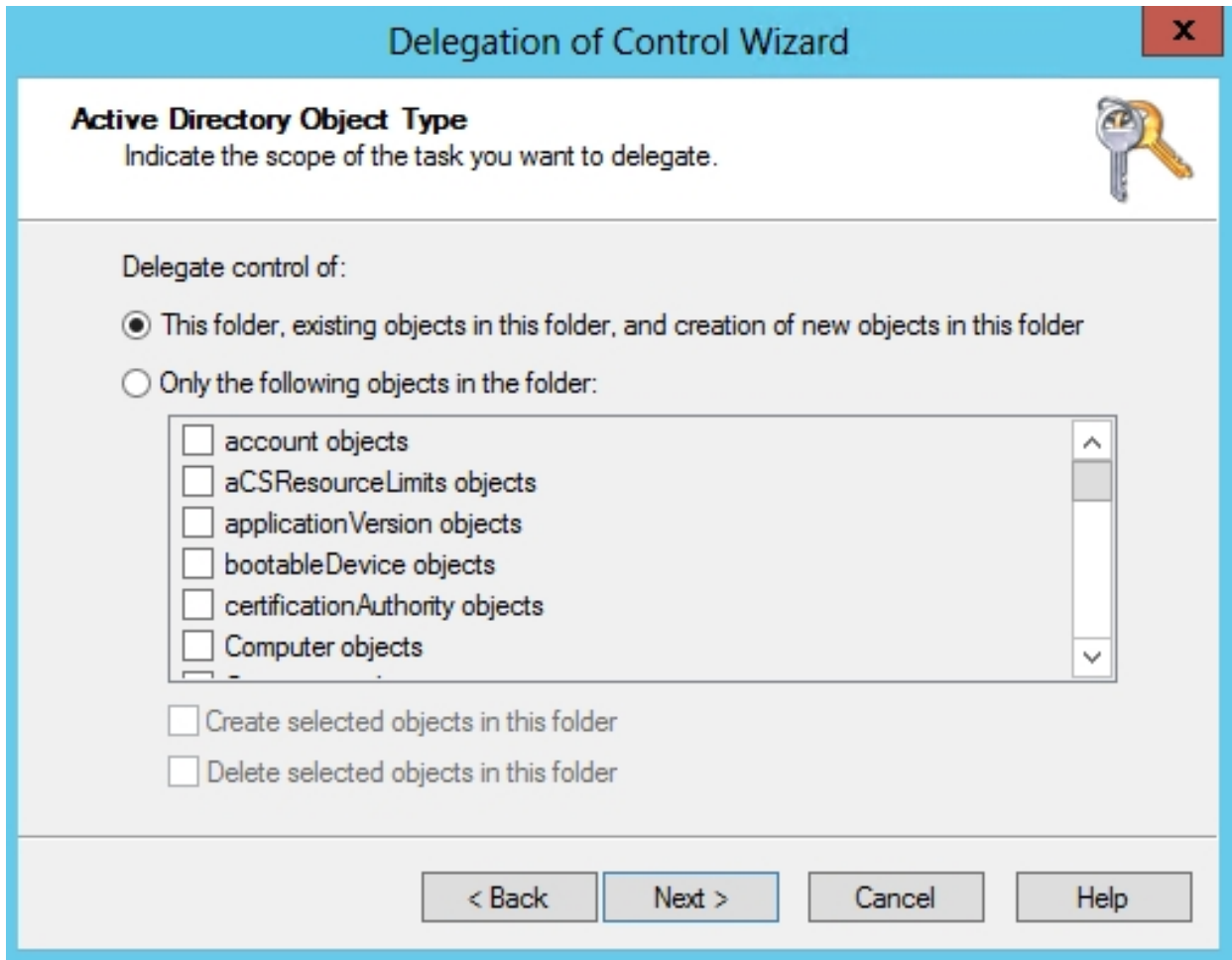
5. Select **Create a custom task to delegate** and click **Next**.

Figure 11-20: Active Directory - Delegation of Control Wizard: select tasks to delegate



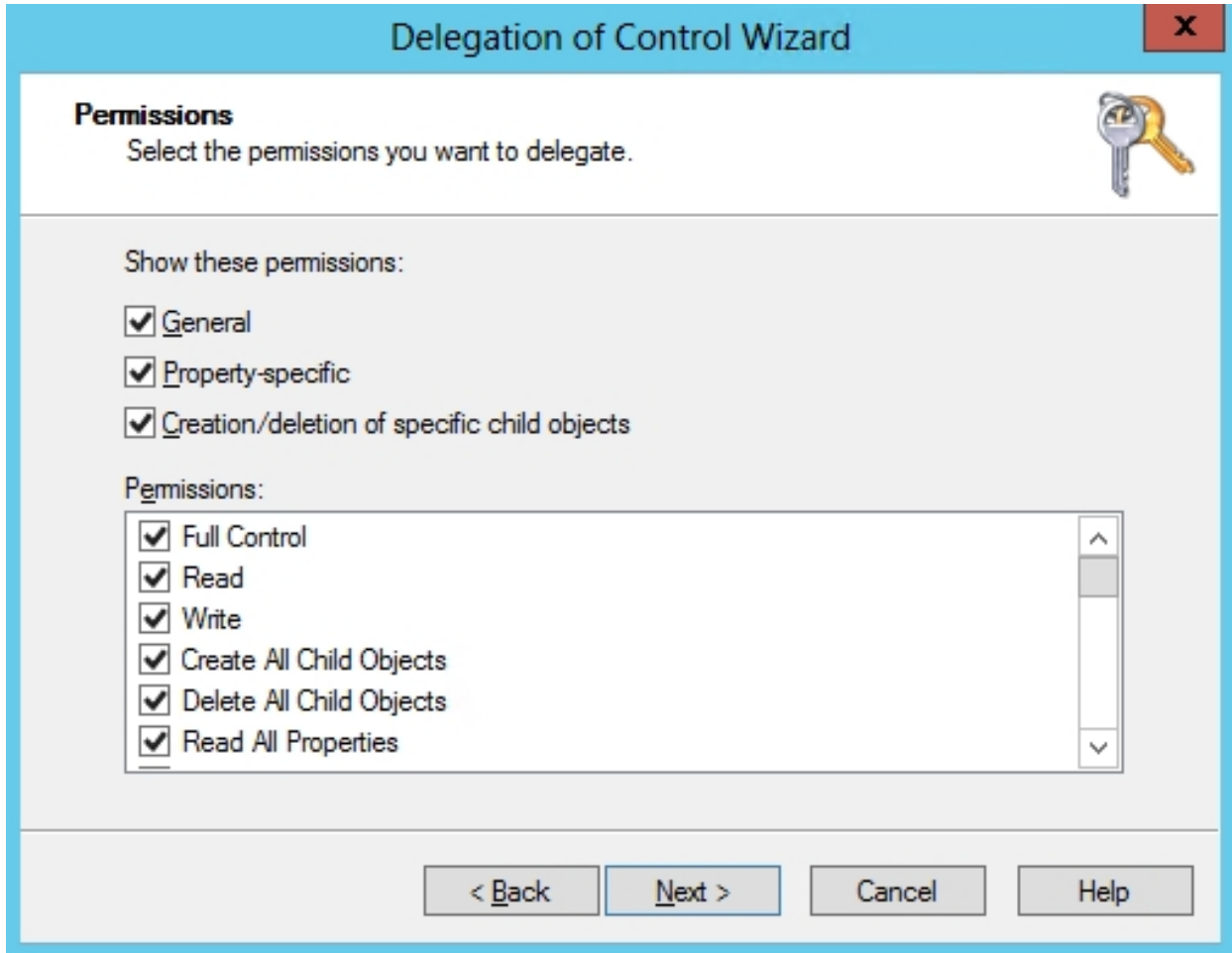
6. Select **This folder...** and click **Next**.

Figure 11-21: Active Directory - Delegation of Control Wizard: select the task scope



7. Give **Full Control** access to the non-Administrator user account and click **Next**.

Figure 11-22: Active Directory - Delegation of Control Wizard: select permissions



8. Click **Finish**.

Joining an Active Directory domain using Unity

This section describes the process for joining Unity to a new domain. For information about supported domain controllers and connectivity requirements, see [Microsoft Active Directory domain requirements](#) on page 371



CAUTION: If Unity is currently connected to a domain, and you subsequently join Unity to a new domain, all Site and Storage Pool Administrators configured on the system are removed. All file system-level access permissions are also removed, although file- and folder-level ACLs (CIFS) and permissions (NFS) remain unchanged.

However, when you rejoin the previous domain that Unity was connected to, or if the new domain has the same set of user and/or group accounts as the previous domain, Unity restores Site and Storage Pool Administrators, as well as all file system-level access permissions on the system.



CAUTION: Joining a new domain or rejoining a former domain

If Kerberos is configured to access file systems, the Kerberos configuration gets disabled when unjoining a domain. After joining a new domain or rejoining an old domain, you must reconfigure Kerberos as described in [Enabling Kerberos for accessing CIFS file system](#) on page 386.

► **To join Unity to a Microsoft Active Directory domain:**

1. If you are managing multiple sites: in Unity's tree view, click the Site node representing Unity that you want to join to a new domain.
2. Expand the Site node's Properties panel.
3. Select the **User Authentication** tab.

Figure 11-23: Site node's Properties: User Authentication tab

The screenshot shows the 'User Authentication' tab selected in the 'Site node's Properties' panel. The 'Join a Microsoft Active Directory Domain' option is selected. The form contains the following fields and controls:

- Active Directory Domain Name:
- Time Server (optional):
- User name:
- Password:
- LM Compatibility Level: (with a dropdown arrow and an information icon)
- Buttons: Unjoin, Advanced, Apply, Cancel
- Radio buttons:
 - Connect to an LDAP Directory Service
 - Use UNITY authentication

4. Click **Modify**.
5. Select the **Join a Microsoft Active Directory Domain** option and click the right arrow.
6. If you are currently connected to a domain (Microsoft Active Directory or LDAP), you will be required to enter the user name and password for the domain administrator in the corresponding fields to unjoin the current domain. Click the right arrow to continue.
7. Unity then prompts you to enter DNS settings for the new domain. Type the IP address for the preferred DNS server, and (optionally) the IP address of the alternate DNS server, in the relevant fields.
8. In the next step, enter the name of the **Active Directory Domain Name**. For example, `domain.net`.
9. Type the user name (for example, `administrator`) and password for the domain administrator in the corresponding fields.

10. From the **LM Compatibility Level** drop-down list, select a level from 2 to 5. The NTML levels supported by Unity are explained below:

Security Level	Setting	Description
2	Send NTLM response only	Client computers use NTLMv1 authentication, and they use NTLMv2 session security if the server supports it. Domain controllers accept LM, NTLM, and NTLMv2 authentication.
3	Send NTLM2 response only	Client computers use NTLMv2 authentication, and they use NTLMv2 session security if the server supports it. Domain controllers accept LM, NTLM, and NTLMv2 authentication.
4	Send NTLM response only. Refuse LM.	Client computers use NTLMv2 authentication, and they use NTLMv2 session security if the server supports it. Domain controllers refuse to accept LM authentication, and they will accept only NTLM and NTLMv2 authentication.
5	Send NTLM response only. Refuse LM and NTLM.	Client computers use NTLMv2 authentication, and they use NTLMv2 session security if the server supports it. Domain controllers refuse to accept LM and NTLM authentication, and they will accept only NTLMv2 authentication.

11. (Optional) Click the **Advanced** button to perform one or more of these actions.

Figure 11-24: Joining a Microsoft Active Directory domain - advanced settings

- To connect to a specific domain controller: If you are working in a multiple domain environment (Microsoft Active Directory forest implementation), enter the IP address of the domain controller in the **Domain Controller to connect to** field. This step may also be required if the fully qualified domain name (FQDN) of the Microsoft Active Directory domain server that you specify in the **Active Directory Domain Name** field does not resolve to the IP address of the domain controller that you want Unity to connect to.

- To change the default location where the Unity adds its computer objects on your Active Directory server: Computer objects are stored under `Computers` by default. In the Organizational Unit (OU) for the computer objects field, enter the names of the Organizational Unit (OU), in this format: `OU=NAME1, OU=NAME2`

If the names do not exist, the wizard will create them. If they already exist, the OU names are part of the existing **distinguishedName** attribute of the Organizational Unit (OU).

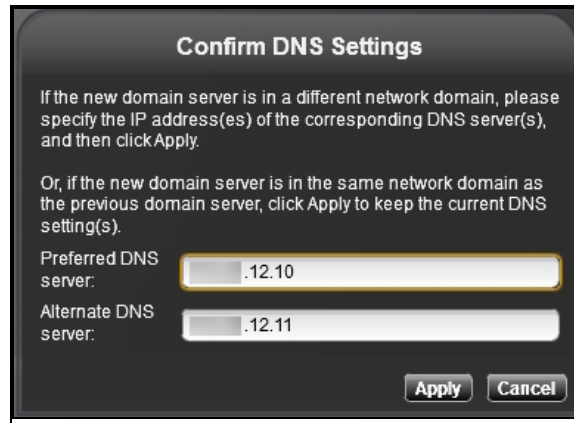
Note IDMU is not supported in AD environments containing multiple top-level organizational units.

- To use pre-defined computer objects: If you are joining the Active Directory domain with a user that has domain administrator privileges: you do not need to select this option since the Organizational Unit path (mentioned above) you provide will create the computer objects. If you want to use the system defaults, check this option without entering a path.

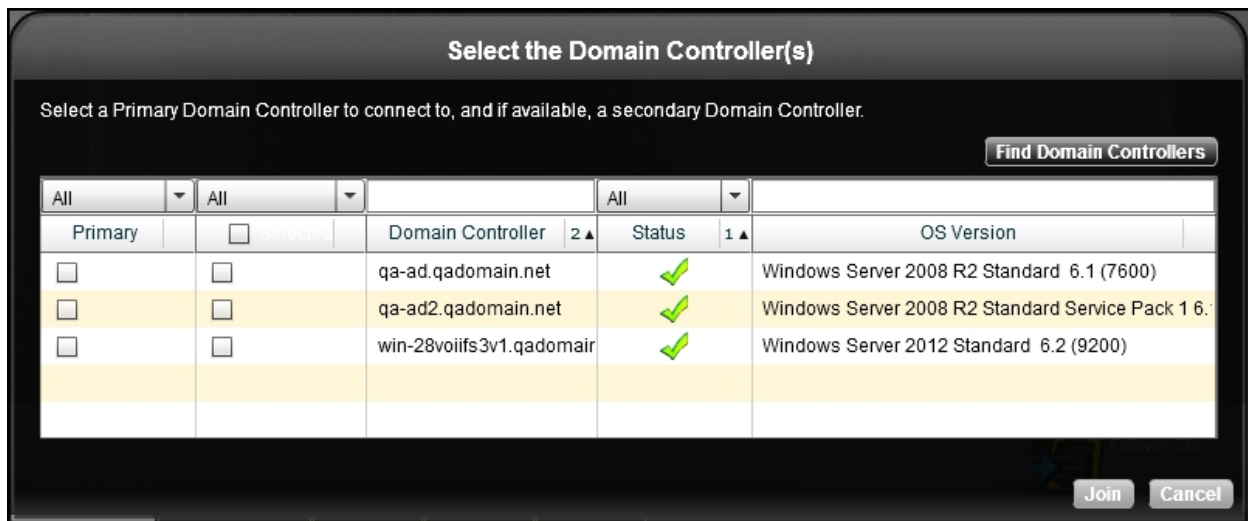
If you are joining the Active Directory domain with a user that does NOT have domain administrator privileges: you must select this option in addition to entering the OU path mentioned above to use computer objects already created on your Active Directory server.

12. Click the **Apply** button.
13. If Unity is currently connected to a domain, and you did not previously unjoin the system from the domain, Unity prompts you for domain administrator credentials; this is required to remove Unity entries from the current domain and unjoin Unity from that domain. Type the user name and password for the domain administrator, and then click the **Submit** button.

14. Unity then prompts you to confirm DNS settings for the new domain. Type the IP address for the preferred DNS server, and (optionally) the IP address of the alternate DNS server, in the relevant fields.



15. Click the **Apply** button.
Once the connection to the new domain controller you specified in a previous step is established, Unity discovers all domain controllers in the domain, and it checks each domain controller for supportability with Unity.
16. The discovered domain controllers are displayed in the Select the Domain Controller(s) dialog box. A check mark in the **Status** column indicates the corresponding domain controller meets all relevant requirements for supportability, and an **X** indicates that the domain controller does NOT meet connectivity requirements.



If a specific domain controller does not appear in the grid, click the **Find Domain Controllers** button to restart the discovery process.

- a. Select a primary domain controller by clicking its corresponding check box in the **Primary** column of the grid.
 - b. (Optional) For redundancy, select one or more secondary controllers. In the event that the primary domain controller becomes unavailable, Unity automatically establishes connectivity to the domain through the secondary domain controller.
17. Click **Join**.

- Click the **Restart Unity** button when prompted.

Managing domain controllers

When you connect Unity to a Microsoft Active Directory or an LDAP Directory server, Unity automatically discovers all domain controllers in the domain; during the discovery process it checks each domain controller for supportability with Unity. The discovered domain controllers are displayed in Unity in the Site node's Properties panel, under the **Domain Controllers** tab.

Figure 11-25: Site's properties panel—Domain Controllers tab

Primary	Selected	Domain Controller	Status	OS Version
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	qa-ad.qadomain.net	✔	Windows Server 2008 R2 Standard 6.1 (7600)

The **Domain Controllers** tab contains a grid that displays all discovered controllers in the domain; the grid identifies the primary domain controller that Unity is currently connected to, and, if applicable, the secondary domain controller currently selected for the system.

For each discovered domain controller, the grid indicates whether or not the domain controller is supported by Unity: a check mark in the **Status** column indicates the corresponding domain controller meets all relevant requirements for supportability, and an **X** indicates the domain controller does NOT meet connectivity requirements for Unity; for more information about supported domain controllers and connectivity requirements, see [Microsoft Active Directory domain requirements on page 371](#).

When you double-click a domain controller in the grid that does NOT meet connectivity requirements for Unity—that is, a domain controller with an **X** in its **Status** column—Unity displays a pop-up that provides detailed information as to why the domain controller is not supported.

This section includes these topics:

- [Discovering new domain controllers below](#)
- [Selecting alternate primary and/or secondary domain controllers on the next page](#)

Discovering new domain controllers

This section explains how to discover new domain controllers in the domain.

► To discover domain controllers:

- Access the **Domain Controllers** tab:
 - If you are managing multiple sites: in Unity's tree view, click the **Site** node representing Unity system that you want to discover new domain controllers for.
 - Expand the Site node's Properties panel.
 - Select the **Domain Controllers** tab.
- Click the **Find Domain Controllers** button to start the discovery process.

Unity discovers all new domain controllers in the domain, and checks each domain controller for supportability with Unity.

Selecting alternate primary and/or secondary domain controllers

This section explains how to select alternate primary and/or secondary domain controllers for the Unity.

► **To select alternate primary and/or secondary domain controllers:**

1. Access the **Domain Controllers** tab:
 - a. If you are managing multiple sites (multi-site management of remote systems): in Unity's tree view, click the **Site** node representing Unity that you want to discover new domain controllers for.
 - b. Expand the Site node's Properties panel.
 - c. Select the **Domain Controllers** tab.
2. Click the **Discover all domain controllers** button to start the discovery process. Unity discovers all new domain controllers in the domain, and checks each domain controller for supportability with Unity.
3. Select a new primary domain controller by clicking its corresponding check box in the **Primary** column of the grid.
4. (Optionally) Select a new secondary domain controller, if available, by clicking its corresponding check box in the second column (under the **Selected** column heading). You can select multiple secondary domain controllers, if your infrastructure supports this.
5. Click the **Update Domain Controllers** button.

Unity updates controller connectivity settings for Unity; this process may take some time to complete.
6. Once Unity updates controller connectivity settings for Unity, it may prompt you to restart Unity; click the **Restart Unity** button.

Enabling Kerberos for accessing CIFS file system

To enable Kerberos support on Unity, you must perform these configuration tasks:

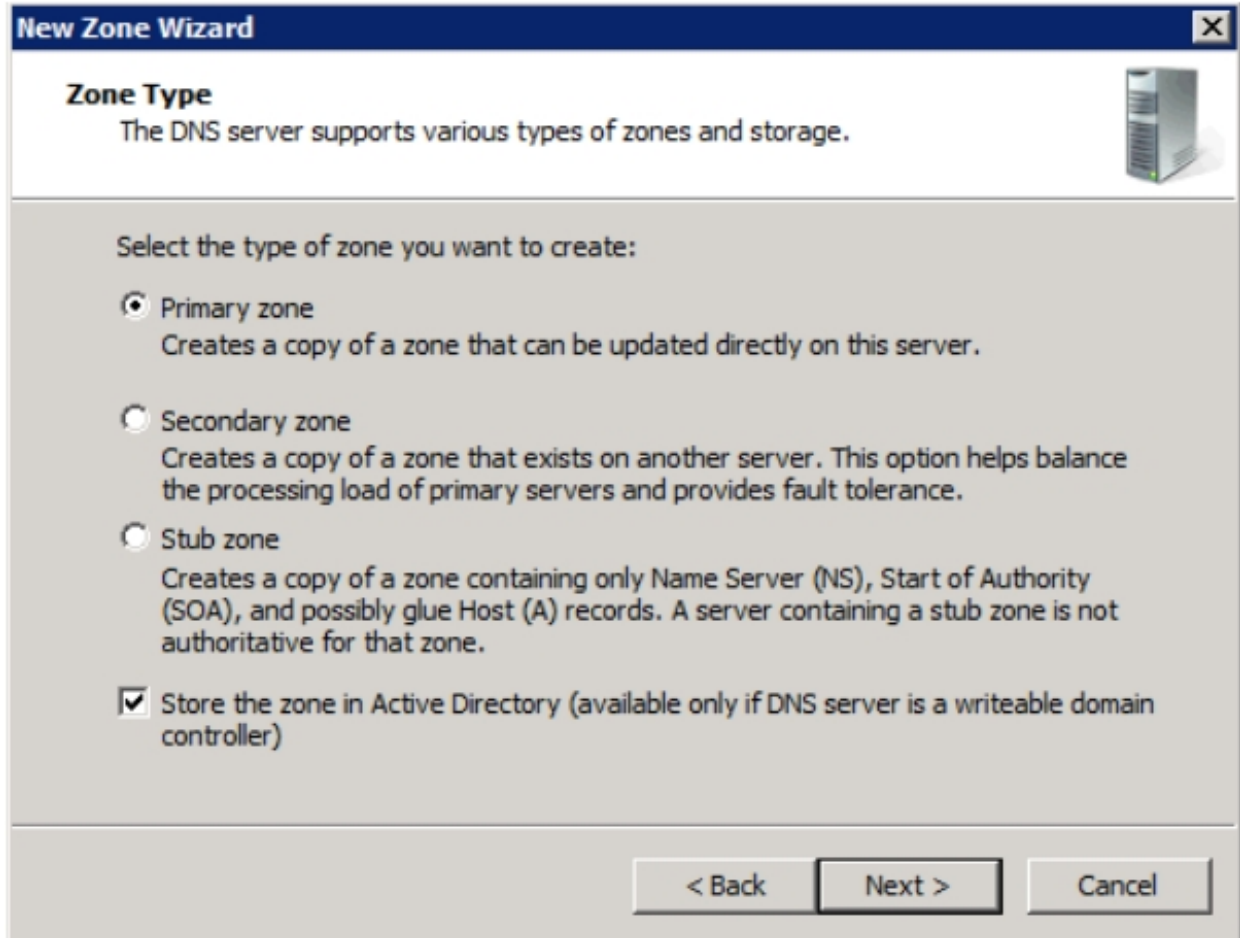
1. [Add a Reverse Lookup Zone](#) for the subnet of your Resource Groups in DNS Manager on your Active Directory domain.
2. [Add a host in DNS Manager](#) for each Resource Controller.
3. [Configure the host](#) in Active Directory Users and Computers.

Note Your Unity must have CIFS server version 2.1 to be able to use Kerberos.

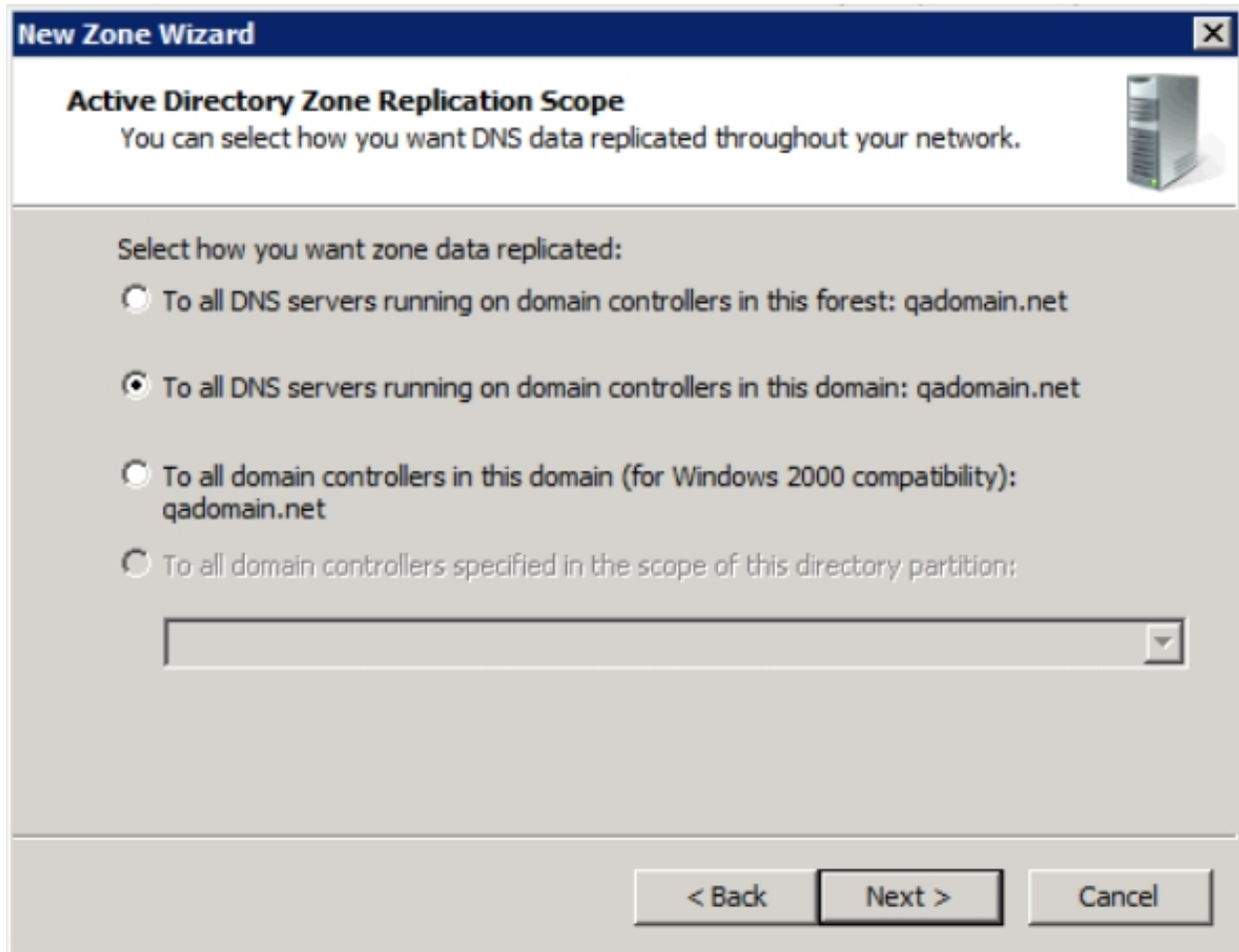
Adding a Reverse Lookup Zone in DNS Manager

► **To add a Reverse Lookup zone:**

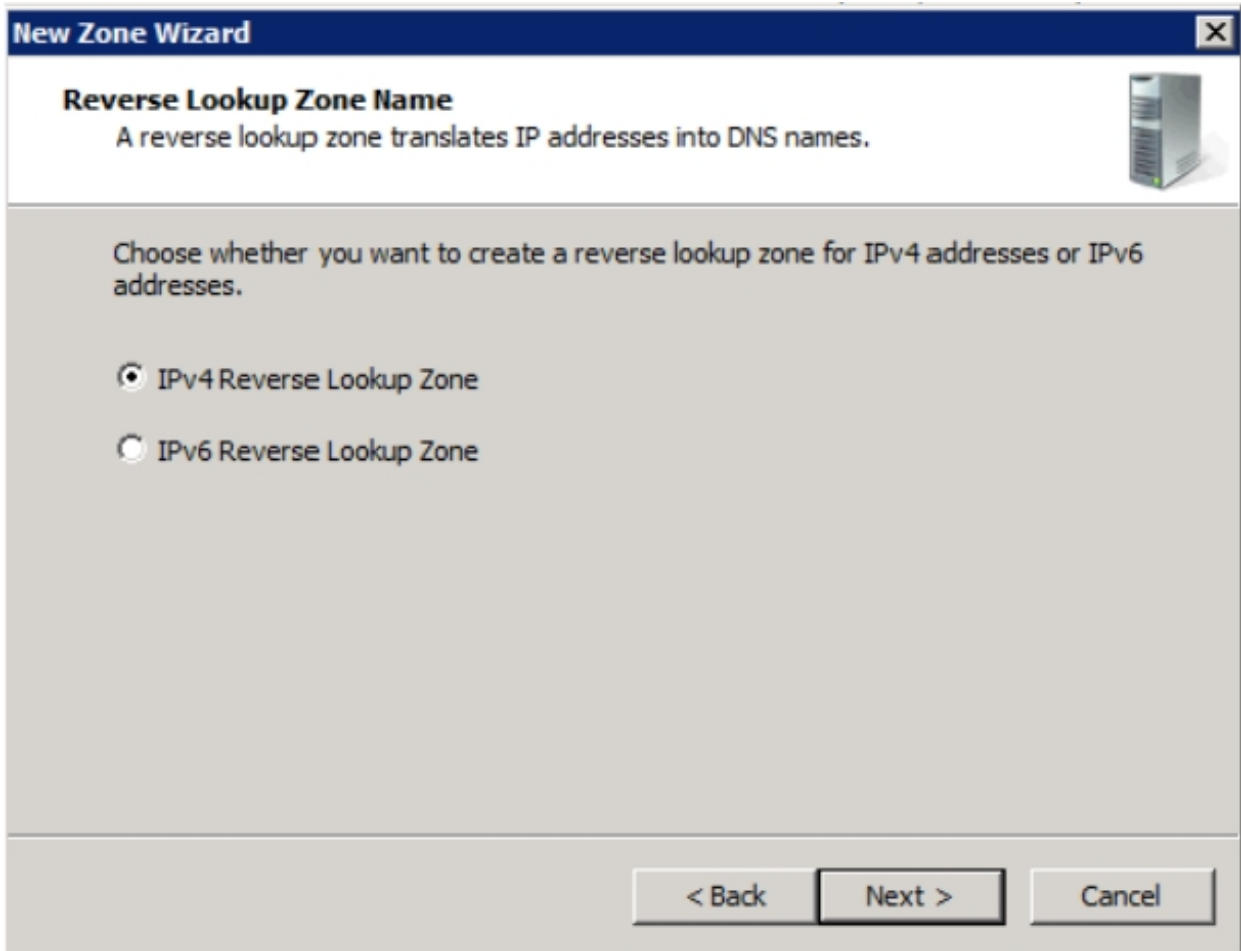
1. In DNS Manager, right-click **Reverse Lookup Zones** and select **Add Reverse Lookup Zone**.
2. The New Zone wizard opens. Select the **Primary Zone** and click **Next**.



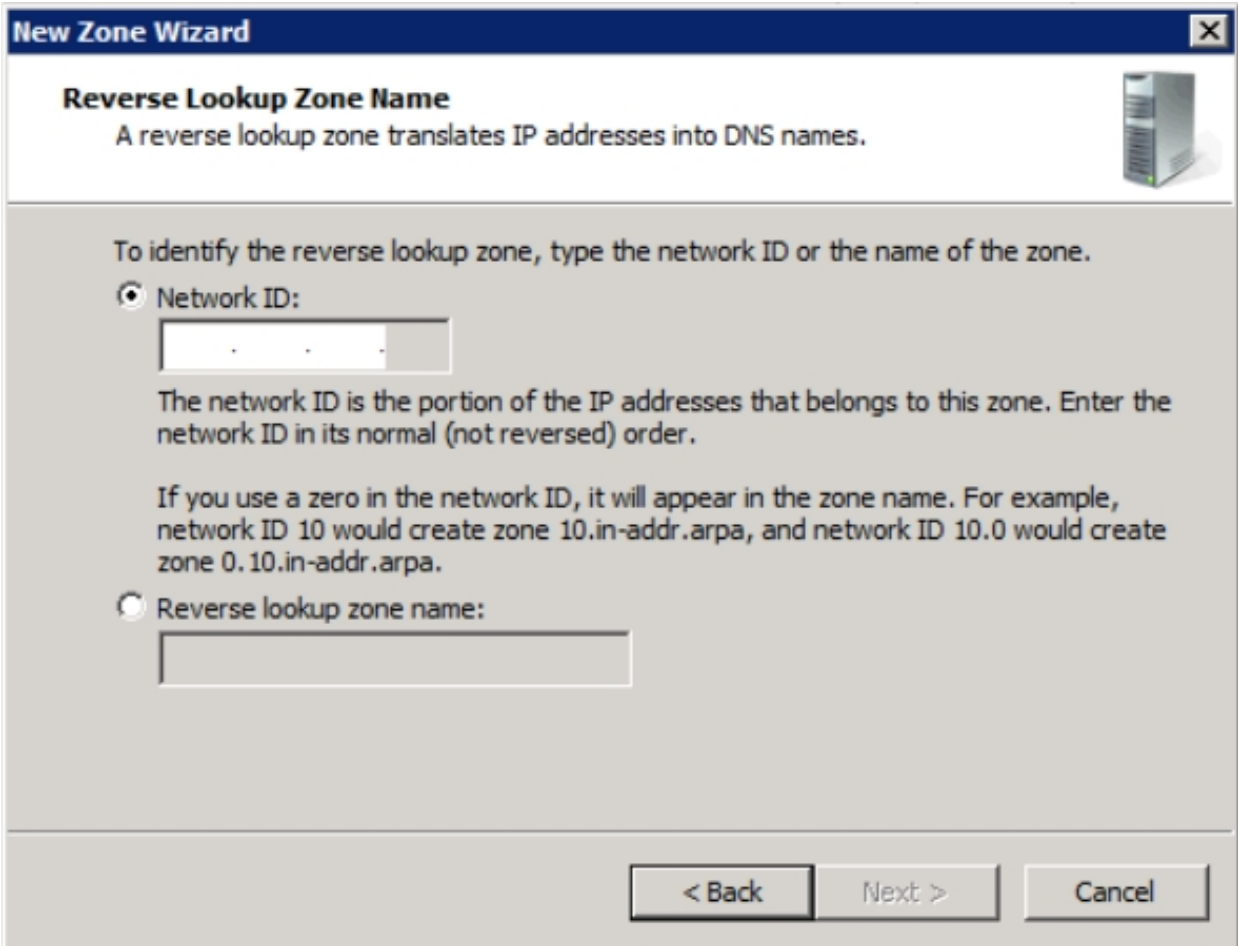
3. Select the zone replication scope, as applicable in your Active Directory domain, and click **Next**.



4. Select the version of IP addressing and click **Next**.

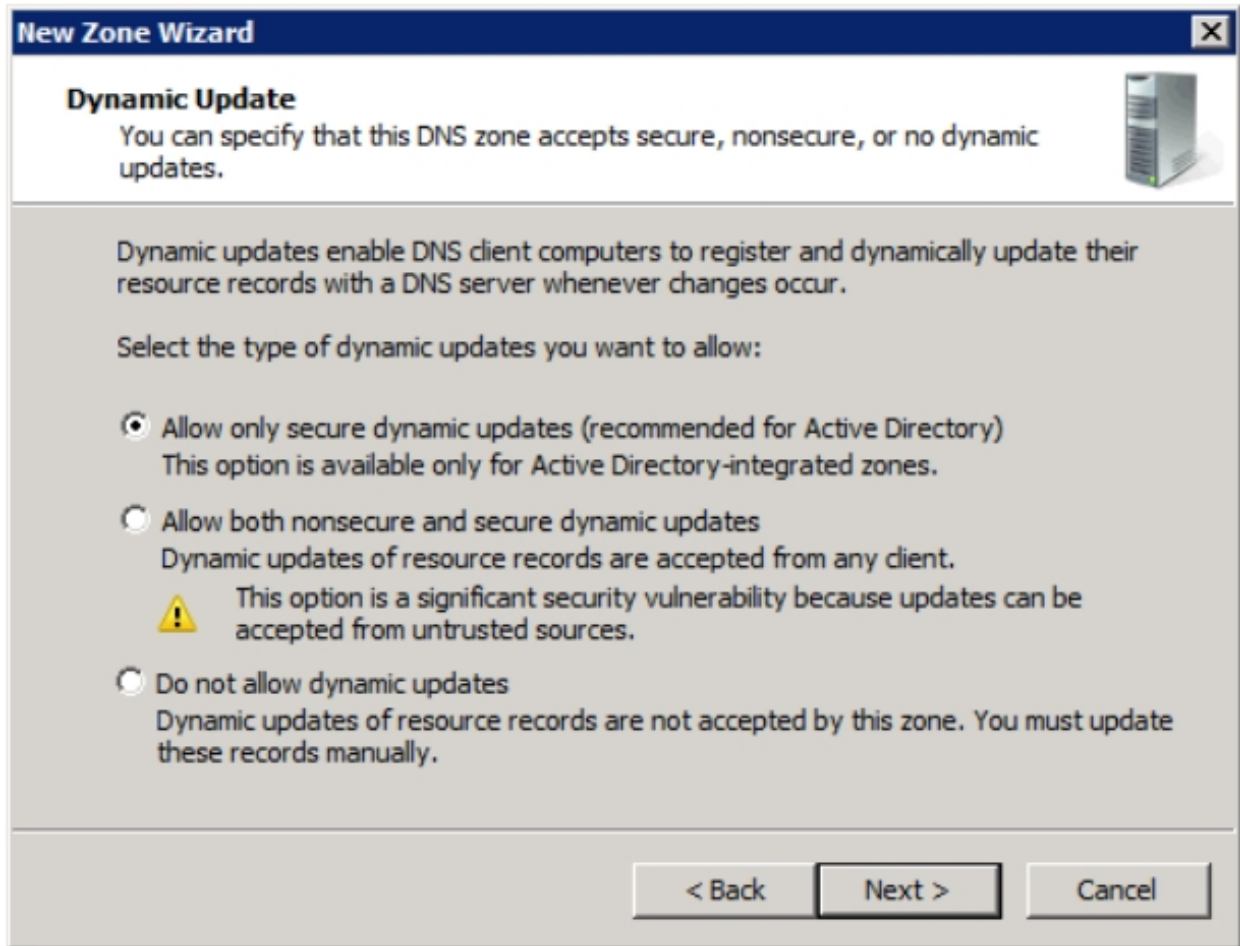


5. Enter the portion of IP address that belongs to this zone and click **Next**.

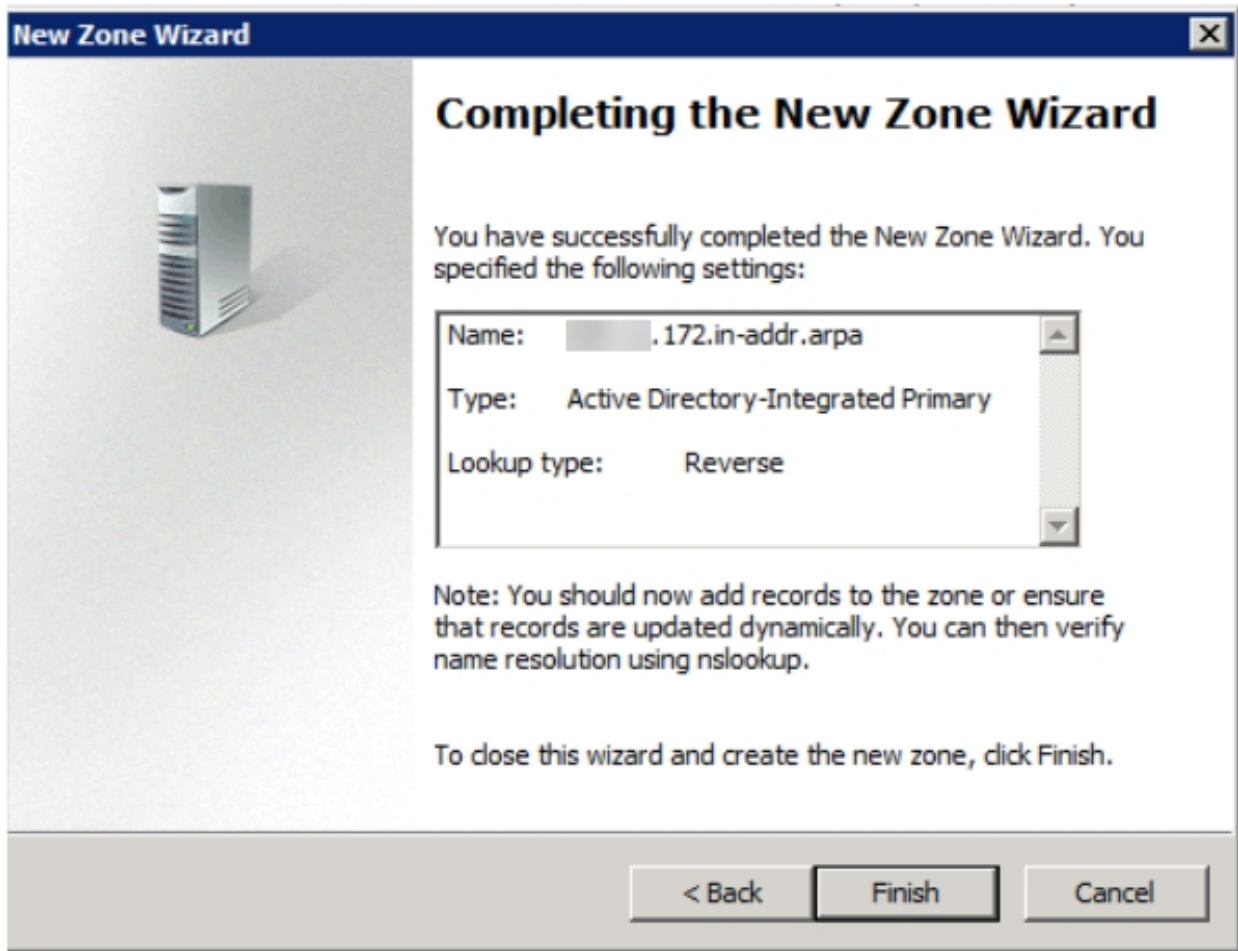


The screenshot shows a Windows-style dialog box titled "New Zone Wizard" with a close button (X) in the top right corner. The main heading is "Reverse Lookup Zone Name" with a sub-heading "A reverse lookup zone translates IP addresses into DNS names." and a server icon on the right. Below this, a text box says "To identify the reverse lookup zone, type the network ID or the name of the zone." There are two radio button options: "Network ID:" (which is selected) and "Reverse lookup zone name:". The "Network ID:" option has a text input field containing "10.10.10.10". Below the input field, there is explanatory text: "The network ID is the portion of the IP addresses that belongs to this zone. Enter the network ID in its normal (not reversed) order." and "If you use a zero in the network ID, it will appear in the zone name. For example, network ID 10 would create zone 10.in-addr.arpa, and network ID 10.0 would create zone 0.10.in-addr.arpa." The "Reverse lookup zone name:" option has an empty text input field. At the bottom right, there are three buttons: "< Back", "Next >", and "Cancel".

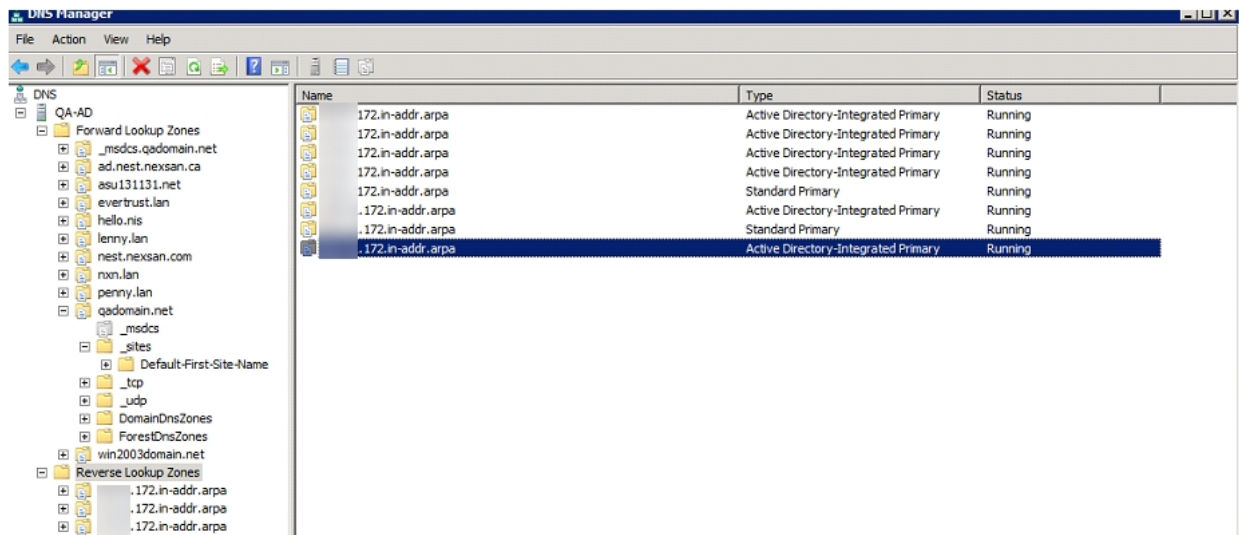
6. Select secure dynamic updates and click **Next**.



7. Click **Finish**.



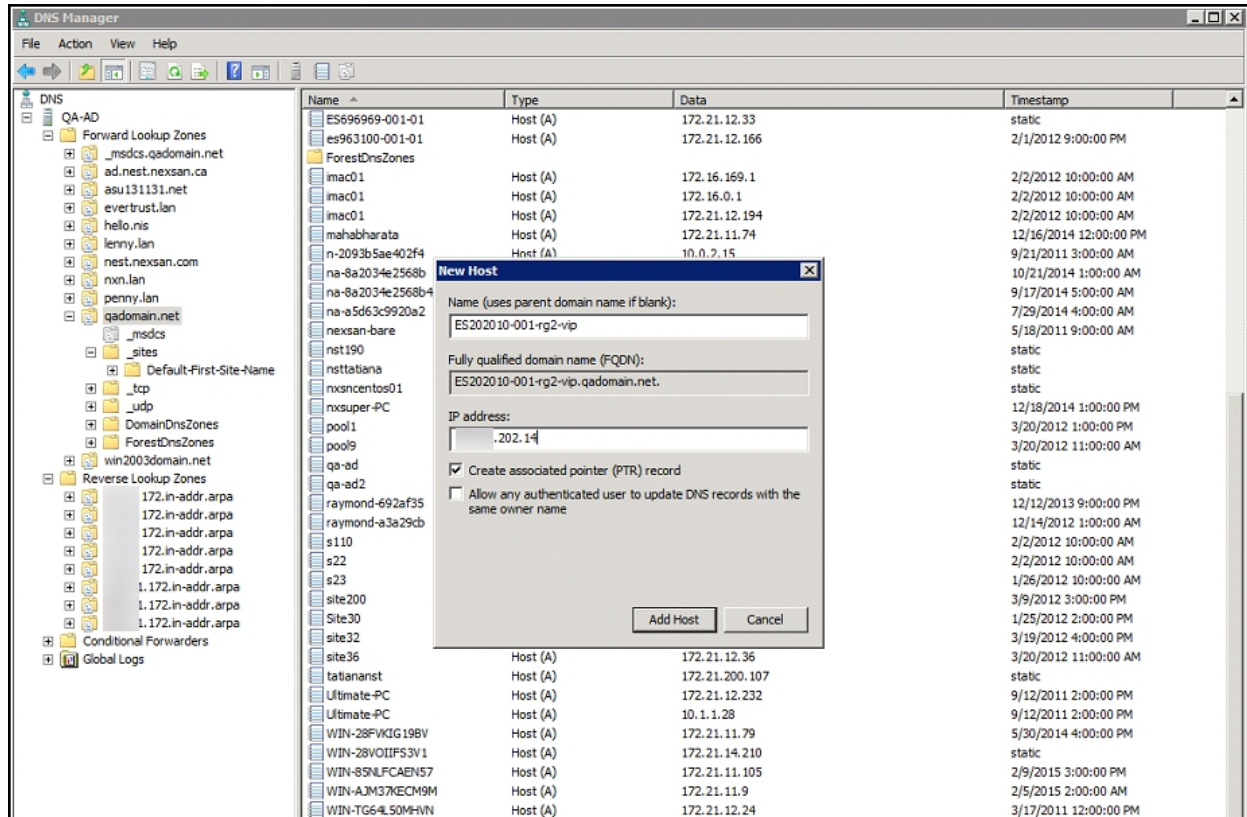
The new DNS lookup zone is listed in DNS Manager.



Adding a host for each Resource Controller in DNS Manager

► To add a host:

1. Right-click your domain name and select **New Host**.
2. Enter the host name of your Resource Group 1.
3. Enter the IP address of your Resource Group 1.
4. Click **Add Host**.
5. Repeat these steps for Resource Group 2.

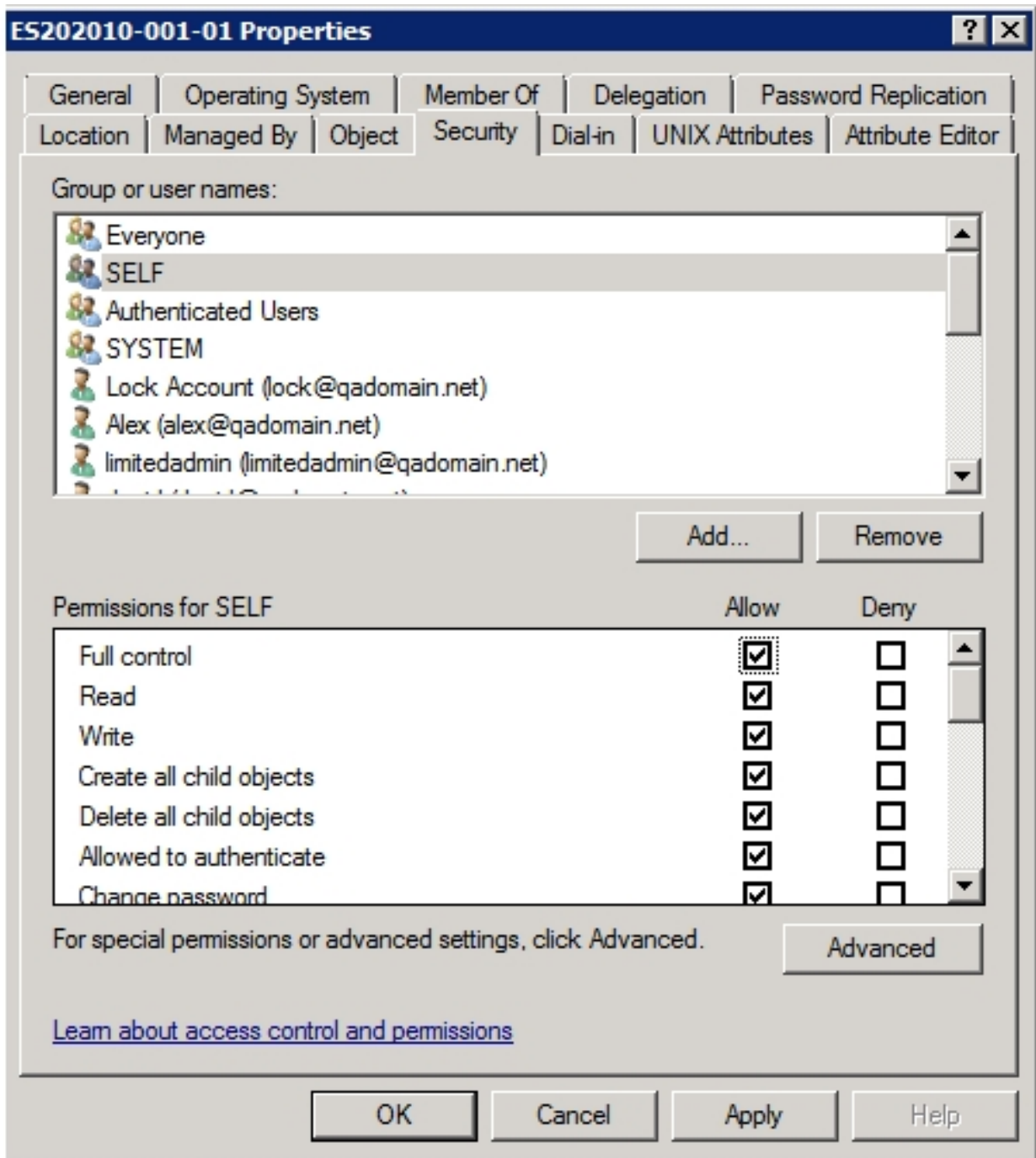


Configuring the host in Active Directory

► To configure the host:

1. In *Active Directory Users and Computers*, select the **Computers** organization unit.
2. Locate the computer object for Unity. It is named after the Unity node name (ES202010-001-01 for Controller 1 in our example.). Right-click the computer object and select **Properties**.

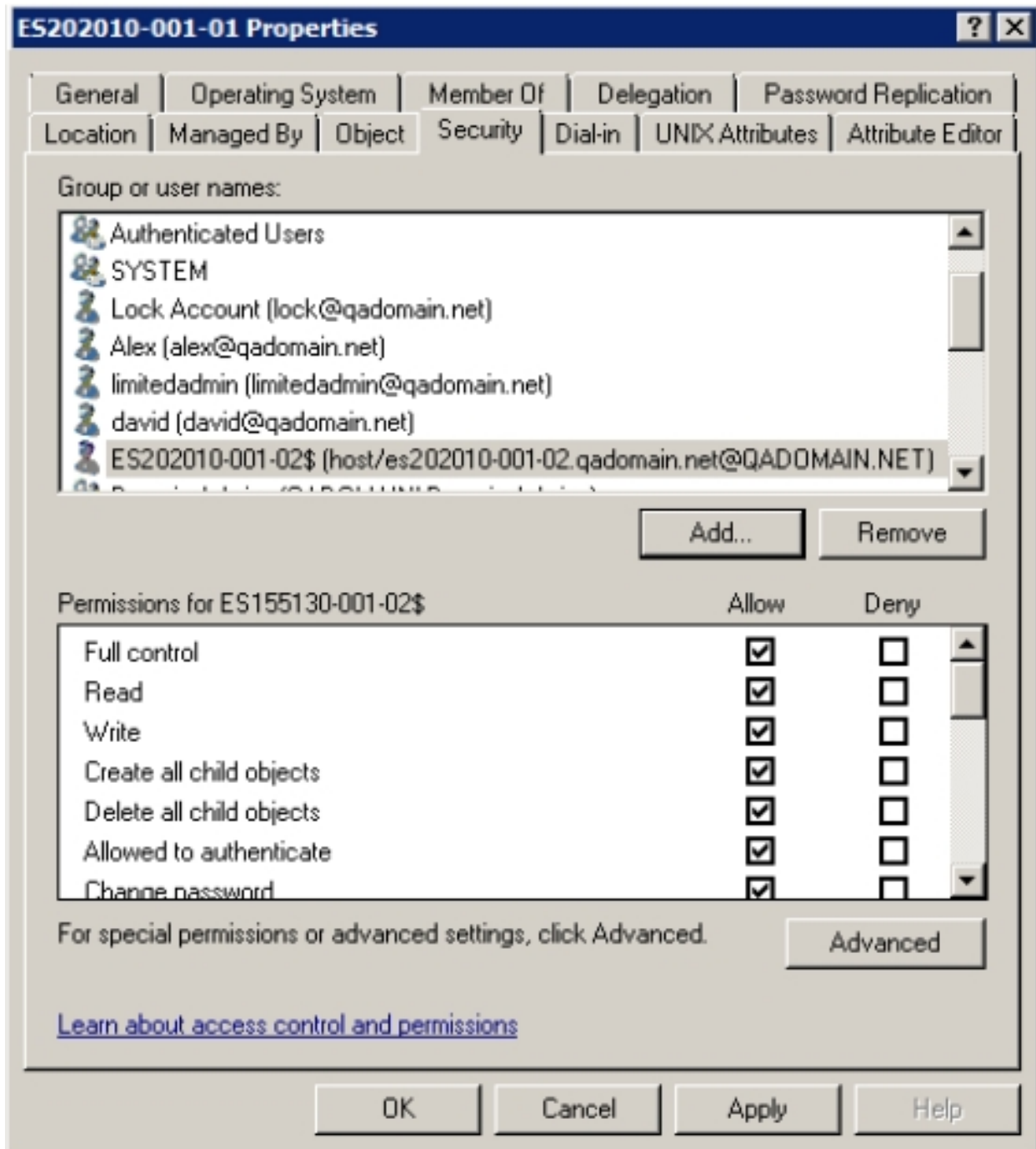
3. Under the **Security** tab:
 - a. Select **SELF**.
 - b. Select **Full Control**.
 - c. Click the **Apply** button.



4. Click the **Add** button.
5. In the Select Users, Computers, Service Accounts, or Groups window, click the **Object Types** button.

6. In the Object Types window, select the **Computers** check box and click **OK**.
7. Back in the Select Users, Computers, Service Accounts or Groups window:
 - a. Enter the account name of the PEER NODE (*ES202010-001-02* in our example).
 - b. Add the **\$** sign at the end of the node name.
 - c. Click **OK**.

- The peer node is added to the list in the Properties dialog box. Select the **Full Control** option and click **OK**.



- Repeat steps 2 to 8 to modify the permissions for Controller 2.

You can now use Kerberos if you connect to the share using the Resource Group's host name.

Unjoining Unity from an Active Directory domain

If you are making structural changes to the domain—including retiring or relocating a domain server, or moving Unity to another domain—you may need to unjoin Unity from the Microsoft Active Directory Domain that the

system is currently connected to.

Note If you select Unity authentication, when Unity restarts, you can only log on to the system as the Unity Administrator (**nxadmin**), since all previous Site and/or Storage Pool administrators configured on the system are removed during the unjoin process. Once you log on the system as the Unity Administrator (**nxadmin**), you can add local users and/or group accounts to the system, and then configure Site and Storage Pool administrators, as needed. For more information about adding local users and/or group accounts to the system, see [Users and access rights](#) on page 65.



CAUTION: All file system-level access permissions are also removed, although file- and folder-level ACLs (CIFS) and permissions (NFS) remain unchanged. However, when you rejoin the same domain that you unjoined Unity from, or join a new domain with the same set of user and group accounts as the previous domain, Unity restores Site and Storage Pool Administrators, as well as all file system-level access permissions on the system.

► **To unjoin Unity from a domain:**

1. If you are managing multiple sites: in Unity's tree view, click the Site node representing Unity that you want to unjoin from the domain.
2. Expand the Site node's Properties panel.
3. Select the **User Authentication** tab.

Figure 11-26: Site's properties panel—User Authentication tab

The screenshot shows the 'User Authentication' tab in the Site's properties panel. It features a tabbed interface with 'User Authentication' selected. Below the tabs, there are two radio button options: 'Join a Microsoft Active Directory Domain' (selected) and 'Connect to an LDAP Directory Service'. Under the selected option, there are input fields for 'Active Directory Domain Name' (containing 'domain.net'), 'Time Server (optional):' (containing 'time.nist.gov'), 'User name:', 'Password:', and 'LM Compatibility Level:' (set to '2'). At the bottom of this section are buttons for 'Unjoin', 'Advanced', 'Apply', and 'Cancel'. Below the radio buttons, there is another 'Use UNITY authentication' option which is not selected.

4. Click the **Unjoin** button, under the **Join a Microsoft Active Directory Domain** option.
5. Enter the Active Directory credentials and click **OK**.

6. Unity prompts you for domain administrator credentials; this is required to remove Unity entries from the Microsoft Active Directory Domain server and complete the unjoin process.

Figure 11-27: Microsoft Active Directory Domain Credentials dialog box



7. Type the user name for the domain administrator in the **User name** field.
8. Type the password for the domain administrator in the **Password** field.
9. Click the **Submit** button. Unity begins the process for unjoining Unity from the domain; this process may take some time to complete.
10. Once Unity completes the process for unjoining the domain, it prompts you to restart Unity; click the **Restart Nexsan Unity** button.

Connecting to an LDAP Directory service

The Unity Authentication service is preconfigured by default during initial system setup. Use this procedure if you want to instead connect to an LDAP Directory Service.

► **To connect to an LDAP Directory service:**

1. If you are managing multiple sites: in Unity's tree view, click the Site node representing Unity that you want to unjoin from the domain.
2. Expand the Site node's Properties panel.
3. Select the **User Authentication** tab.
4. Select the **Connect to an LDAP Directory Service** option.

If the site is using Active Directory authentication, you'll need to unjoin from AD. See [Unjoining Unity from an Active Directory domain](#) on page 396

The Site Setup Wizard displays the settings for connecting to an LDAP Directory service on the network; you must configure these settings to connect to the LDAP Directory server.

- In the **LDAP Domain Name** field, type the name of the LDAP domain and extension for the domain that you want Unity to connect to. For example, `domain.com`

The screenshot shows a configuration dialog box with the following elements:

- Radio buttons: Join a Microsoft Active Directory Domain, Connect to an LDAP Directory Service, Use UNITY authentication
- LDAP Domain Name:
- LDAP Host Name:
- Time Server (optional):
- Proxy DN:
- Password:
- Buttons: **Connect**, **Cancel**

- (Optional) In the **LDAP Host Name** field, type the host name of the LDAP Directory server and the domain name and extension that you want Unity to connect to. For example, `ldapserverservername.domain.com`.

This step is only required if:

- the domain name you specify in the **LDAP Domain Name** field does not resolve to the IP address of the LDAP Directory server, or
- the LDAP domain name you specify is an identification label for multiple resources in your LDAP implementation.

If you do not specify an LDAP host name, Unity automatically connects to the LDAP Directory server that you specify in the **LDAP Domain Name** field.

- (Optional) In the **Time Server** field, type the IP address or the fully qualified domain name of the time server that you want Unity to synchronize its date and time with. A time server is required to ensure that the date and time settings on Unity are synchronized with LDAP Directory server that the system connects to. By default, a time server is already defined.

Note Unity supports multiple time servers: if you specify a time server in the **Time Server** field, as opposed to using the LDAP Directory server for date and time synchronization for Unity, we highly recommend that you specify at least two time servers; this ensures that date and time synchronization on Unity remains unaffected in the event that one of the time servers you specify is no longer available. To specify multiple time servers, use a comma to separate each entry, for example:

`tick.utoronto.ca,time.nrc.ca`.

- In the **Proxy DN** field, type the Proxy identity's distinguished name (DN) configured on your LDAP Directory server (for example, `cn=asmith,dc=domain,dc=com`), where `cn` denotes common name, and `dc` denotes domain component. The Proxy identity is a user on the LDAP Directory server that has restricted authority to required information on the server; Nexsan Unity binds to the LDAP Directory server using the Proxy user's DN.

Note The LDAP Directory server must have a Proxy identity configured before you connect Unity to the server.

- Type the Proxy identity's password in the **Password** field.
- Click the **Connect** button.

The progress panel informs you if the system is unable to connect to the domain. You can click an error message in the progress panel to obtain more information about the error; take any corrective action, if applicable, and click the **Connect** button again to retry the connection.

Setting up Unity authentication

With Unity authentication, Unity is not connected to a user directory or authentication service on the network; you must manually create user and group accounts on Unity for user authentication.

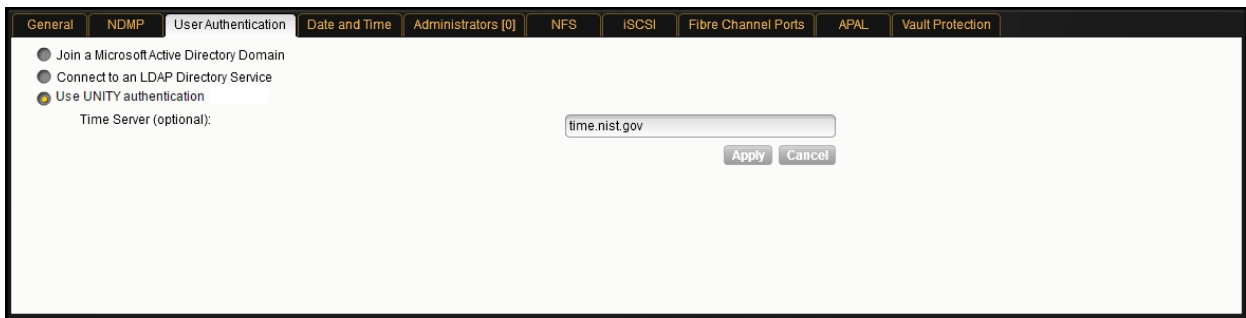


CAUTION: If Unity is currently connected to a domain, and you subsequently configure Unity authentication for the system, all Site and Storage Pool Administrators configured on the system are removed. All file system-level access permissions are also removed, although file- and folder-level ACLs (CIFS) and permissions (NFS) remain unchanged. However, when you rejoin the previous domain that Unity was connected to, Unity restores Site and Storage Pool Administrators, as well as all file system-level access permissions on the system.

► **To set up Unity authentication:**

1. If you are managing multiple sites: in Unity's tree view, click the Site node representing Unity that you want to set up Unity authentication on.
2. Expand the Site node's Properties panel.
3. Select the **User Authentication** tab.

Figure 11-28: Site's properties panel—User Authentication tab



4. Select the **Use the Unity authentication** option.
5. Optionally, specify a time server in the **Time Server** field.
6. Click the **Connect** button.
7. If Unity is currently connected to a domain (Microsoft Active Directory or LDAP), Unity prompts you for domain administrator credentials. This is required to remove Unity entries from the current Microsoft Active Directory Domain server and unjoin Unity from that domain.

Type the user name and password for the domain administrator, and then click the **Submit** button.

The process for unjoining Unity may take some time to complete.
8. When prompted to restart Unity, click the **Restart Unity** button.

Note When Unity restarts, you can only log on to the system as the Unity Administrator (**nxadmin**), since all previous Site and/or Storage Pool administrators configured on the system were removed when you unjoined the previous domain. Once you log on the system as the Unity Administrator (**nxadmin**), you can add local users and/or group accounts to the system, and then configure Site and Storage Pool administrators, as needed. For more information about adding local users and/or group accounts to the system, see [Managing users and groups with Nexsan Unity](#) on page 90.

Troubleshooting site-level warning and error conditions

Unity provides enhanced reporting of hardware-specific events—including disk and component failures and sensor readings—for both Unity and for Nexsan storage connected to Unity. Unity reports on these events:

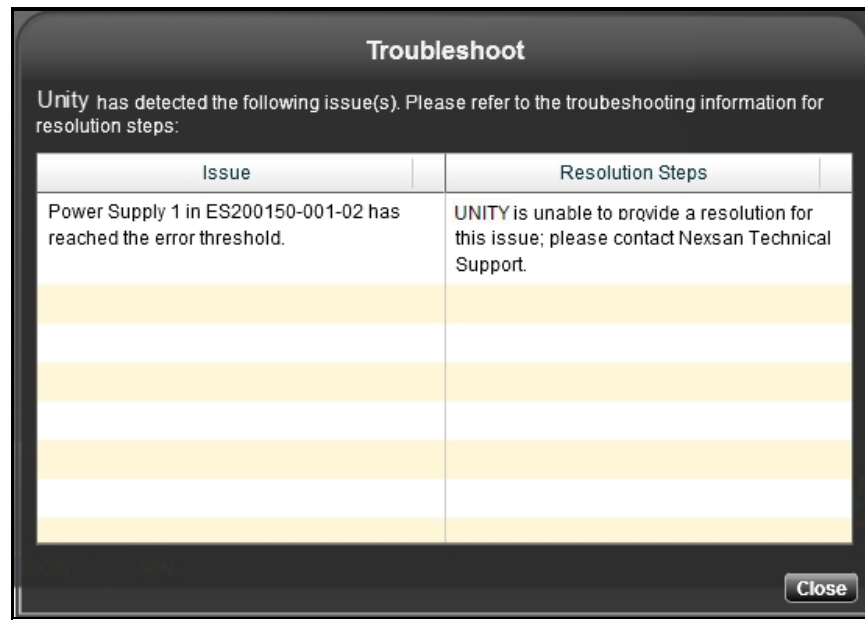
- Sensor readings (overheat thresholds, fan failures, etc.)
- SAS/Fibre Channel cabling/multi-pathing issues (for Nexsan storage)
- Disk failures
- Disk removal and insertion
- Network cable disconnect issues or port failures
- Power supply failures

When a hardware event occurs, Unity superimposes an error or warning indicator on the corresponding site node, as well as on the node affected by the error or warning condition—for example, on the specific storage system's node and/or on the Clusters node—in Unity's tree view to notify you of the event. You then click the site node to display more details about the event. Events are also recorded in the system's event logs, which you can then access from Unity's Event Viewer and receive as alerts via email.

► **To view more details about error or warning conditions:**

1. In Unity's tree view, click the Site node with the error or warning condition; the node should have either an error or warning indicator superimposed over it.
2. Expand the Site node's Properties panel.
3. Click the **Troubleshoot** button on the Properties panel. This opens the Troubleshoot pop-up, which details the source of the error or warning condition affecting the site, or a component on a storage system (s) connected to the site; the Troubleshoot popup also provides resolution steps for rectifying the condition, if applicable.

Figure 11-29: Troubleshoot popup



4. Review the information carefully and resolve any issues if possible; contact Nexsan Technical Support for issues that you are unable to resolve without assistance, or for any serious error conditions.

Configuring NFS settings

This section describes how to enable an NFSv4 domain and how to modify NFS general settings.

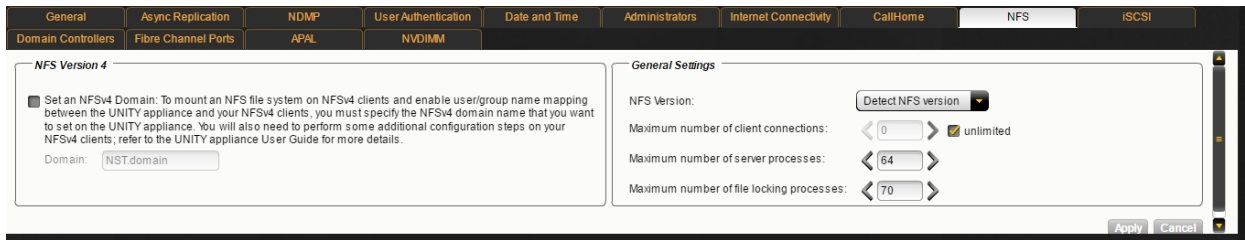
For further details on NFS support for file systems, see:

- [Using an NFS version 3 \(NFSv3\) client to access an NFS share with Microsoft Active Directory on page 178](#)
- [Using an NFS version 4 \(NFSv4\) client to access an NFS share on page 179](#)

▶ **To configure NFS settings:**

1. In Nexsan Unity's tree view, click the Site node corresponding to Unity where the NFS share exists; this displays its child nodes.
2. Expand the Site node's Properties panel.
3. Select the **NFS** tab.

Figure 11-30: Site's properties panel—NFS tab



4. Specify a domain name to enable user mapping between Unity and your NFSv4 clients:
 - a. Select the check box to enable the domain.
 - b. In the **Domain** text box, type a domain name for NFSv4 support. You will be required to specify this domain name on all NFSv4 client systems where you intend to mount the NFS share. You can use the default domain name, **NST.domain**, or specify a new name; the domain name must contain a period (.).

5. On the **General Settings** panel, define these settings:
 - a. In the **NFS Version** drop-down list, select the global NFS version control:
 - **Detect NFS version:** By default, Unity supports both NFSv3 and NFSv4. Choose this option if your environment is composed of mixed client versions. Unity will detect the version and use the same as the client automatically.
 - **NFSv3 only:** Choose this option for Unity to only use NFSv3.
 - b. Enter the maximum number of **client connections** in the corresponding field. Enter a value between **0** and **512** or select the **unlimited** option.
 - c. Enter the maximum number of **server processes** in the corresponding field. This setting allows you to tune NFS for better performance. When a request is made for an NFS service, the Services for UNIX NFS server generates a thread to handle the request. Each thread can process one NFS request. A large pool of threads can allow a server to handle more NFS requests in parallel.
 To determine the number of threads to make available, use the following formula:

$$16 + (4 \text{ processors })$$
 where *processors* is the number of additional processors on the NFS server. Enter a value between 0 and 512.
 - d. Enter the maximum number of **file locking processes** in the corresponding field. This setting defines the number of threads that can be used for NFS file locking. Enter a value between 0 and 512.
6. Click **Apply** to save your settings.

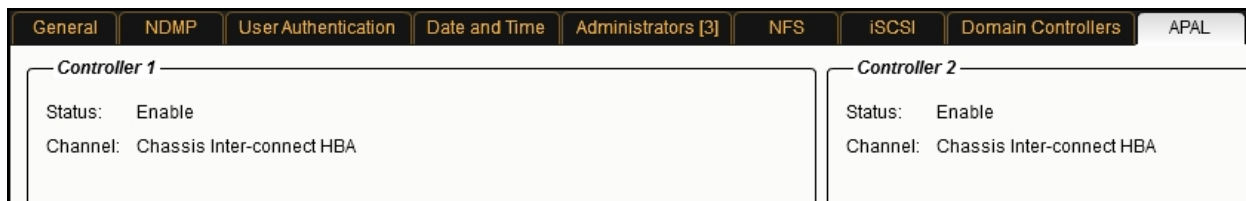
Viewing APAL status

All Ports / All LUNs is a feature used in a dual-controller, active-active cluster to provide high-availability during failover. Chassis inter-connectivity provides uninterrupted access to the LUNs hosted by each controller. The direct connection between the controller managing the LUNs and the Fibre Channel host is referred to as the *Optimized Path*. The *All Ports / All LUNs* feature creates an additional access path from one controller to the set of LUNs hosted by the other controller; this is referred to as the *Non-Optimized Path*.

► To view APAL status:

1. In Unity's tree view, click the **Site** node.
2. Expand the Site node's properties panel.
3. Select the **APAL** tab.

Figure 11-31: Site's properties panel—APAL tab



For each controller, you can view the status of the connection and the channel used. For the Unity 6000, the channel is the chassis inter-connect HBA card located on the back on each controller, and connected to the other card with two cables. For all other systems the channel is the inter-connect HBA card located internally in the chassis.

Note The chassis inter-connect card status can be viewed on the cluster **Status** tab; see [Viewing cluster health status and controller information](#) on page 300.

Viewing the Unity Vault Protection Module status

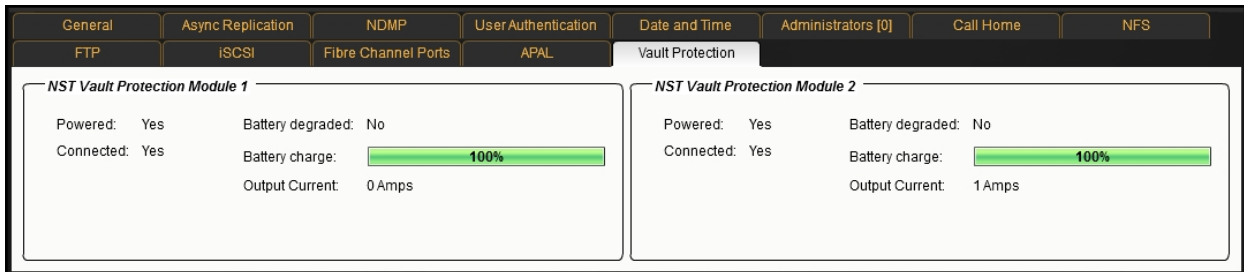
The Unity Vault Protection Module (Unity VPM) provides battery backup and protection to the Unity 4000 or Unity 6000 in case of power outage. Both controllers are connected to two Unity VPM units for power redundancy.

The Unity VPM units will provide power to Unity for five minutes so that all I/O operations saved on the FASTier™ write cache, since the power interruption, can be written to the SSD. Under normal conditions, each Unity VPM powers its own controller, and thus does not require to share the power load with the other Unity VPM.

► **To view the Unity VPM status:**

1. In the tree view, click the **Site** node.
2. Expand the Site node's properties panel.
3. Select the **Vault Protection** tab.

Figure 11-32: Site's properties panel—Vault Protection tab



For each Unity VPM, the tab provides this information:

- Power status
- Connection status with Unity
- Battery status: degradation, charge, and output current.

Viewing NVDIMM status

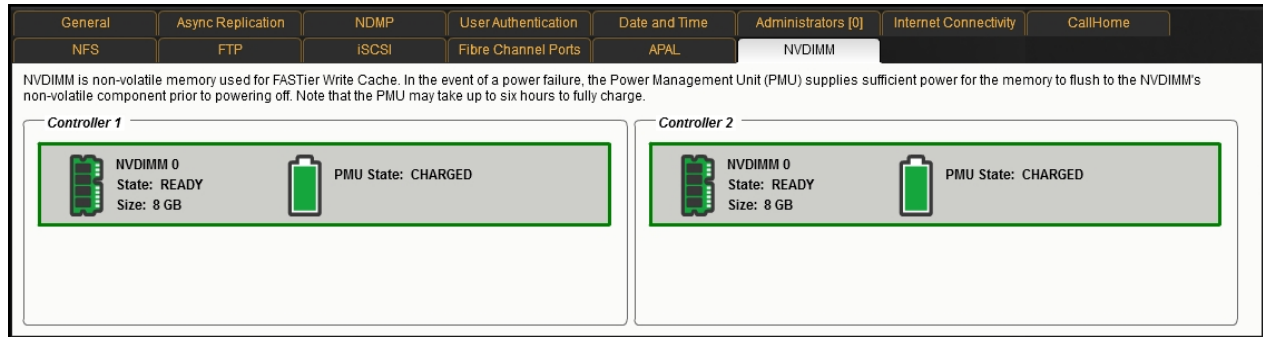
The Non-Volatile Dual In-line Memory Module (NVDIMM) provides the memory used for FASTier write cache. In the event of a power failure, the NVDIMM's Power Management Unit (PMU) supplies sufficient power for the in-memory data to flush to the NVDIMM's non-volatile internal flash prior to powering off.

► **To view the NVDIMM status:**

1. In the tree view, click the **Site** node.
2. Expand the Site node's properties panel.

3. Select the **NVDIMM** tab.

Figure 11-33: Site's properties panel — NVDIMM tab



For each NVDIMM, the tab provides this information:

- NVDIMM state: READY or NOT READY
- NVDIMM size
- PMU state:
 - **Charged:** PMU is functioning normally.
 - **Charged and nearing end-of-life:** PMU is functioning normally but is nearing the end of its life cycle and must be replaced.
 - **Charging:** PMU is charging (can take up to 6 hours)—NVDIMM is temporarily inactive.
 - **End-of-life:** PMU has reached the end of its life cycle and must be replaced before the NVDIMM can return to an active state.
 - **Error:** no status for PMU due to error with NVDIMM.

Enabling FTP support

A file system that you expose using the FTP sharing method can be accessed by UNIX/Linux-based and Windows-based systems using the FTP protocol. It must be enabled at the site level before you can expose file systems over FTP. Enabling FTP support opens port 21 by default.

If a user has access (either via anonymous access or explicit permission), that user can access the file system via FTP.

Note Enabling FTP support will create additional folders in the `/var/opt/nest/users/` directory. It is recommended to leave these folders untouched for proper FTP behavior.

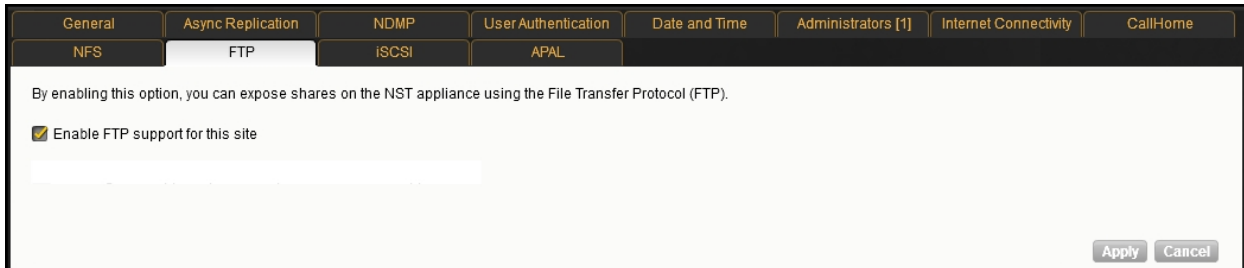
▶ Limitations of FTP sharing:

- FTP sharing is only supported for Nexsan Unity authentication in the user interface.
- Only nxadmin and site administrators can enable FTP at the site level. Pool administrators can enable FTP at the file system level if FTP is enabled at the site level.
- FTP support is not supported for IP restrictions.
- You cannot browse a replicated file system over FTP.
- FTP support is enabled for the primary site only; it is not replicated to the remote site. You must enable it manually on the remote site.

► **To enable FTP support for the site:**

1. In Unity's tree view, click the **Site** node.
2. Expand the Site node's properties panel.
3. Select the **FTP** tab.

Figure 11-34: Site properties panel: FTP tab



4. Select the **Enable FTP support for this site** option.
5. Click **Apply**.

► **Related topics:**

[Modifying a file system's sharing method on page 136](#)

[Step 2: Configuring the access method on page 126](#)

Understanding the CallHome feature

The CallHome feature allows Nexsan Technical Support personnel to monitor the state of Unity using the collected system logs, without customer notification. If you enable SSH connectivity, this feature also allows Nexsan Technical Support personnel to connect to Unity and troubleshoot issues remotely.

Log collection is disabled by default. You can enable CallHome log collection settings during site setup, or you can enable them later in Unity using the **CallHome** tab of the Site's properties panel; see [Enabling CallHome log collection settings on page 413](#).

The CallHome feature is disabled automatically during a firmware upgrade. This avoids triggering a critical event and sending system logs unnecessarily because the system is down. The CallHome feature is re-enabled when the Unity is back online.

Note The CallHome feature can also be configured from the nxadmin Command-Line Interface, using the `callhome` and `autolog` commands.

The CallHome feature offers these services:

1. Automatic collection and transfer of system logs: Unity collects and encrypts system logs (using 256-bit AES encryption) and transfers them to the Nexsan CallHome server for health checks and diagnostics.
 - If logs cannot be sent, the CallHome feature will try to send them again every hour until it succeeds. If the log transfer keeps failing, Unity triggers an event, which you can view in the Event Viewer, and sends you a notification by email (if you configured email notifications).
 - Autolog schedule: The CallHome feature packages and sends all system logs based on a pre-defined schedule. These system logs include both critical and non-critical events. The autolog schedule is not configurable in Unity; to modify it, use the `autolog` command in the nxadmin CLI.

- **Event-driven system logs based on critical events:** This function sends system logs when major issues are detected, based on events and diagnostics. For complete details on these events, see [How CallHome is triggered](#) below.

The sending of event-driven logs gets suspended for 24 hours for events that have the same security level. However, if an event of higher severity level occurs, the CallHome feature will send system logs for that event.

Note Maintenance tasks on Unity will trigger events that will send system logs. As such, we recommend that you suspend the sending of logs before performing maintenance tasks; you can use the `callhome suspend` command in the nxadmin CLI.

2. **Secure remote connectivity:** This service establishes a Secure Shell connection (SSH), which allows Nexsan Support to remotely connect to Unity and perform diagnostic and troubleshooting when technical support is required. If an SSH connection goes down, the CallHome feature will automatically try to reconnect up to ten times. If the ten attempts failed, the CallHome feature will send a signal to the Event Viewer.

This feature is disabled by default. To enable SSH connectivity, see [Enabling SSH connectivity for CallHome](#) on page 413. You can disable it at any time.

How CallHome is triggered

The CallHome feature will send system logs to the Nexsan CallHome server based on two factors:

- **Events:** Some critical and error events will immediately send system logs to Unity; see [Event-driven CallHome](#) below.
- **Diagnostics:** System and event logs are regularly scanned (every hour). The CallHome feature will send system logs when persistent errors are detected in the logs; see [Diagnostics-based CallHome](#) on page 411.

Event-driven CallHome

The CallHome feature will send system logs immediately when these events occur. Some of these events may require Nexsan Support assistance.

Table 11-2: Immediate events

Event ID	Severity Level	Description	Resolution
011010	Warning	Unity was unable to add spare drives because there are not enough free devices.	If a member of our technical support team has not contacted you, please reach out to us as soon as possible.
011011	Warning	A storage pool contains more spare drives than its configuration settings.	If a member of our technical support team has not contacted you, please reach out to us as soon as possible.
011014	Critical	A disk drive on the storage enclosure has failed or is missing.	If a member of our technical support team has not contacted you, please reach out to us as soon as possible.
012018	Critical	One of the controller nodes is down.	If a member of our technical support team has not contacted you, please

Event ID	Severity Level	Description	Resolution
			reach out to us as soon as possible.
012164	Critical	The system encountered an issue assigning spare drives.	If a member of our technical support team has not contacted you, please reach out to us as soon as possible.
012179	Warning	Unity failed to update the list of spare drives for a storage pool.	If a member of our technical support team has not contacted you, please reach out to us as soon as possible.
016045	Critical	A storage enclosure is either not connected or is malfunctioning.	If a member of our technical support team has not contacted you, please reach out to us as soon as possible.
016047	Critical	Sensor Warning events regarding voltage, temperature, fan, and power supply.	If a member of our technical support team has not contacted you, please reach out to us as soon as possible.
016048	Critical	Sensor Severe events regarding voltage, temperature, fan, and power supply.	If a member of our technical support team has not contacted you, please reach out to us as soon as possible.
024005	Critical	One of the SATADOMs or SSDs used for the operating system is running out of space. The warnings occur at 90% of disk space used.	If a member of our technical support team has not contacted you, please reach out to us as soon as possible.
024006	Warning	One of the SATADOMs or SSDs used for the operating system is running out of space. The warnings occur at 80% of disk space used.	If a member of our technical support team has not contacted you, please reach out to us as soon as possible.
031003	Warning	A spare drive on the storage enclosure is being used to replace a drive used by a storage pool.	Please wait for the process to complete. If the warning persists, please contact Nexsan Technical Support.
031005	Warning	A drive on the storage enclosure has failed and was replaced with a hot spare.	Although not critical, you should replace the failed drive as described in the <i>Nexsan Unity Hardware Maintenance Guide</i> .
042003	Critical	A storage pool cannot be imported after a storage enclosure was powered up. Unity is unable to	If a member of our technical support team has not contacted you, please reach out to us as soon as possible.

Event ID	Severity Level	Description	Resolution
		locate all volumes required to access the storage pool.	
042004	Critical	Unity is unable to import a storage pool after an enclosure is powered up again, subsequent to an enclosure shut down or reboot. This is because Unity is unable to determine if the storage pool is using volumes from other enclosures which are still offline.	If a member of our technical support team has not contacted you, please reach out to us as soon as possible.
042021	Critical	After a storage enclosure is back online, volumes appear to be missing. The storage pools associated with the storage enclosure might not be brought online.	If a member of our technical support team has not contacted you, please reach out to us as soon as possible.
042022	Critical	The storage device log query service cannot be started.	If a member of our technical support team has not contacted you, please reach out to us as soon as possible.
042037	Critical	A DIMM on Nexsan E-Series is failing and likely needs to be replaced.	Replace the DIMM as described in the <i>Nexsan Unity Hardware Maintenance Guide</i> .
042042	Critical	A Nexsan E-Series storage enclosure is encountering an issue, such as a failed drive or a failed controller.	If a member of our technical support team has not contacted you, please reach out to us as soon as possible.
042044	Critical	A DIMM on Nexsan E-Series is failing and likely needs to be replaced.	Replace the DIMM as described in the <i>Nexsan Unity Hardware Maintenance Guide</i> .
048013	Critical	The internal SSD device used for backing up FASTier write cache is not connected properly, or it may be experiencing a hardware failure.	If a member of our technical support team has not contacted you, please reach out to us as soon as possible.
048025	Critical	The battery on the Unity Vault Protection Module has degraded. You must replace it as soon as possible.	If a member of our technical support team has not contacted you, please reach out to us as soon as possible.
048029	Critical	The Power Management Unit for	If a member of our technical support

Event ID	Severity Level	Description	Resolution
		one of the NVDIMMs is failing.	team has not contacted you, please reach out to us as soon as possible.
048033	Critical	The Power Management Unit for one of the NVDIMMs has failed.	If a member of our technical support team has not contacted you, please reach out to us as soon as possible.
048034	Critical	Unity has detected an issue with an NVDIMM.	If a member of our technical support team has not contacted you, please reach out to us as soon as possible.
048035	Critical	A FASTier cache devive has been down for several hours.	If a member of our technical support team has not contacted you, please reach out to us as soon as possible.

Diagnostics-based CallHome

Diagnostics are based on pre-defined rules that verify system logs, event logs, cluster configuration, service states, and storage pool state logs. The CallHome feature will send logs when persistent errors occur.

Table 11-3: Scheduled rules

Rule ID	Severity level	Description	Resolution
140001	Warning	The cluster contains duplicate heartbeats.	<p>Perform these steps:</p> <ul style="list-style-type: none"> • Verify the cluster configuration using the <code>clustering</code> command. • Verify the cabling to the storage enclosure. <p>If the problem persists, please contact Nexsan Technical Support.</p>
140002	Critical	<p>Fault management has fault with the following classes:</p> <ul style="list-style-type: none"> • <code>fault.io.pciex.device-interr-corr</code> • <code>fault.io.pciex.bus-linkerr-corr</code> • <code>defect.sunos.smf.svc.maintenance</code> • <code>defect.sunos.kernel.panic</code> • <code>ereport.sensor.failure</code> • <code>fault.io.disk.predictive-failure</code> 	<p>If a member of our technical support team has not contacted you, please reach out to us as soon as possible.</p>
140003	Critical	<p>System logs:</p> <ul style="list-style-type: none"> • There is no space left on a device. • A hard disk drive is experiencing severe performance issues. • Unity has rebooted after a kernel panic. • The system pool cannot recover I/O operations. • The replacement of a device failed. • There is no hot spare to replace a failed device. 	<p>If a member of our technical support team has not contacted you, please reach out to us as soon as possible.</p>
140004	Critical	<p>Unity sends logs for services that are in these modes:</p> <ul style="list-style-type: none"> • <i>Panicking</i> 	<p>If a member of our technical support team has not contacted you, please reach out to us as soon as possible.</p>

Rule ID	Severity level	Description	Resolution
		<ul style="list-style-type: none"> ● <i>Panicked</i> ● <i>Broken(unsafe)</i> ● <i>Broken(safe)</i> ● <i>Aborting</i> 	
140005	Critical	<p>Any service that is in one of these states:</p> <ul style="list-style-type: none"> ● Any cluster service that is in <i>Manual</i> mode for at least an hour ● Any service that is in <i>Maintenance</i> state 	If a member of our technical support team has not contacted you, please reach out to us as soon as possible.
140006	Critical	The number of physical storage pools on the system is different from the number of configured pools.	If a member of our technical support team has not contacted you, please reach out to us as soon as possible.
140007	Critical	The event log contains a message about a bad DIMM.	If a member of our technical support team has not contacted you, please reach out to us as soon as possible.
140008	Critical	<p>Storage pools errors, including:</p> <ul style="list-style-type: none"> ● Any storage pool that is not <i>Online</i>. ● Any storage pool device that has more than 5 write, read, or checksum errors. 	<p>Perform these steps:</p> <ul style="list-style-type: none"> ● Verify the storage pool status by running the <code>nstpool status</code> command. ● Clear the pool errors by running the <code>nstpool clear</code> command or using Unity. <p>If the problem persists, please contact Nexsan Technical Support.</p>
140009	Warning	<p>Unity sends warning logs about the following:</p> <ul style="list-style-type: none"> ● A device was replaced successfully. ● A device was removed and detached from the storage pool. 	If a member of our technical support team has not contacted you, please reach out to us as soon as possible.
140013	Warning	One of the controller nodes has been in <i>Manual</i> mode for longer than an hour.	If a member of our technical support team has not contacted you, please reach out to us as soon as possible.

Enabling CallHome log collection settings

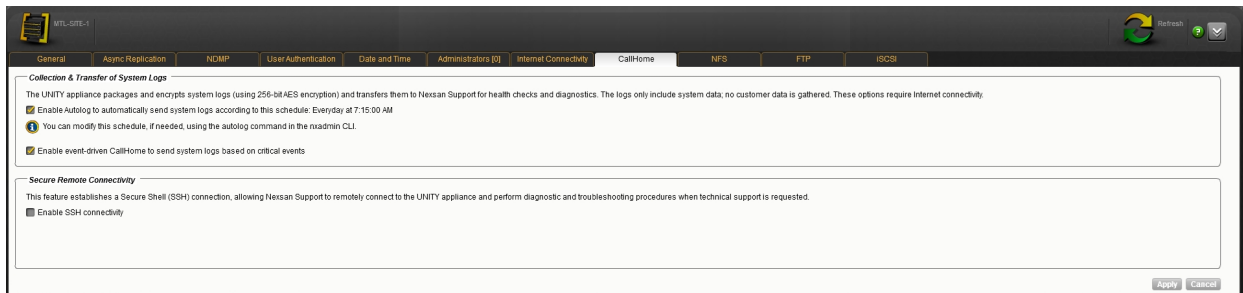
► Before you begin:

1. Unity must have Internet access; see [Enabling Internet Connectivity](#) on the next page.
2. At least one of these ports must be open and allowed between Unity and the network firewall:
 - 20022
 - 80

► To enable the CallHome log collection settings:

1. In Unity's tree view, click the **Site** node.
2. Expand the Site node's properties panel.
3. Select the **CallHome** tab.

Figure 11-35: Site properties panel: CallHome tab



4. Select one or two of these options:
 - **Enable Autolog to automatically send system logs according to a schedule**
 - **Enable event-driven CallHome to send system logs based on critical events**
5. Click **Apply**.

► Related topics:

[Understanding the CallHome feature](#) on page 406

[How CallHome is triggered](#) on page 407

[Enabling SSH connectivity for CallHome](#) below

Enabling SSH connectivity for CallHome

You can enable Secure Shell (SSH) connectivity even if you did not enable the CallHome collection of system logs. If you encounter a problem, this function allows Nexsan Technical Support personnel to connect to Unity and troubleshoot issues remotely.

If an SSH connection goes down, the CallHome feature will automatically try to reconnect up to ten times. If the ten attempts failed, the CallHome feature will send a signal to the Event Viewer.

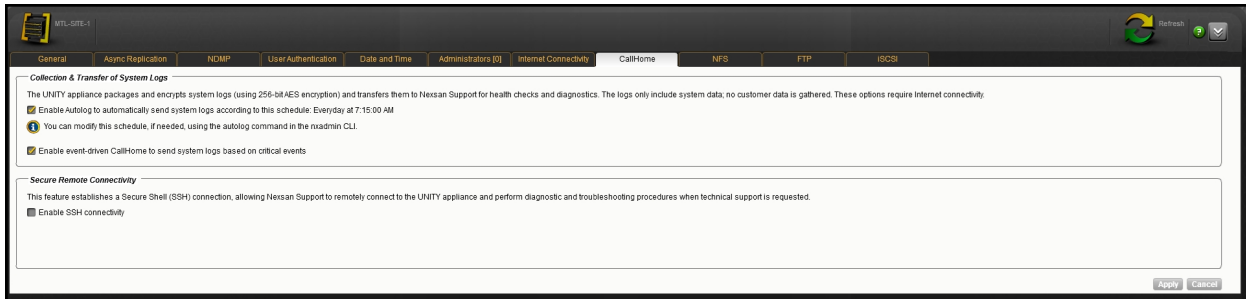
► Before you begin:

1. Unity must have Internet access; see [Enabling Internet Connectivity](#) on the next page.
2. At least one of these ports must be open and allowed between Unity and the network firewall:
 - 20022
 - 80

► **To enable SSH connectivity:**

1. In Unity's tree view, click the **Site** node.
2. Expand the Site node's properties panel.
3. Select the **CallHome** tab.

Figure 11-36: Site properties panel: CallHome tab



4. Select the **Enable SSH connectivity** option.
5. Click **Apply**.

You can disable SSH connectivity at any time by clearing the option.

► **Related topics:**

[Understanding the CallHome feature](#) on page 406

[How CallHome is triggered](#) on page 407

[Enabling CallHome log collection settings](#) on the previous page

Enabling Internet Connectivity

Internet connectivity is required for many features on Unity, such as firmware upgrade and Call Home. You can specify the method by which Unity connects to the Internet:

- **Direct LAN link:** This method uses the system default settings to establish a connection.
- **HTTP Proxy server:** This method connects to the Internet through a proxy present on your network. This is useful if Unity does have direct access to the Internet.
- **Workstation:** This method connects to the Internet using a Windows or Mac OS workstation, configured as a port-forwarding proxy on your network.

Note This method is only supported for the Call Home feature. For details on Call Home, see [Understanding the CallHome feature](#) on page 406. For all other features, you must use a direct LAN or proxy connection.

Once Unity is connected to the Internet using one of these methods, you cannot disable the connection from Unity.

This section covers these topics:

- [Connecting to the Internet using a Direct LAN link](#) on the facing page
- [Connecting to the Internet using an HTTP proxy server](#) on the facing page
- [Connecting to the Internet using a workstation](#) on page 416

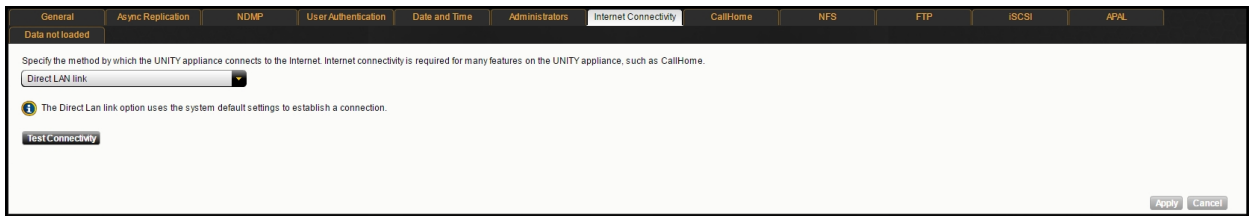
Connecting to the Internet using a Direct LAN link

This method uses the system default settings to establish a connection to the Internet.

► **To configure the direct LAN connection:**

1. In Unity's tree view, click the **Site** node.
2. Expand the Site node's properties panel.
3. Select the **Internet Connectivity** tab.
4. Select **Direct LAN link** from the drop-down list.

Figure 11-37: Site's properties panel—Internet Connectivity tab: Direct LAN link



5. Click **Test Connectivity**.
6. A confirmation message displays the result of the connection test. Click **OK**.
7. Perform one of these actions:
 - If the connection could not be established, verify and update your connection settings.
 - If the connection was successful, click **Apply** to finalize the configuration.

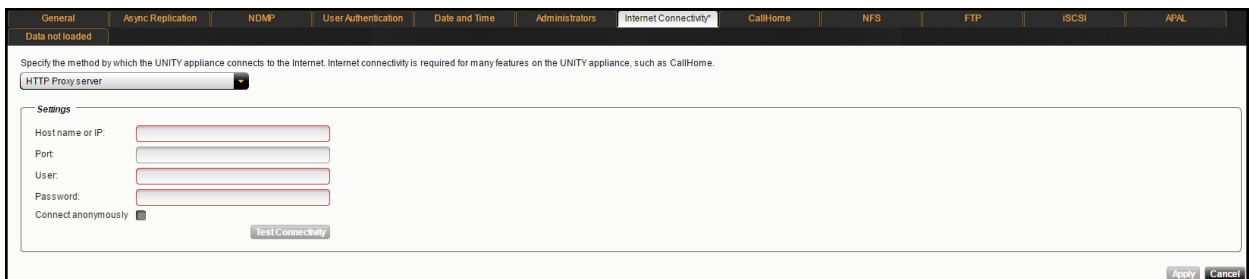
Connecting to the Internet using an HTTP proxy server

This method connects to the Internet through a proxy configured on your network.

► **To configure the connection to an HTTP proxy server:**

1. In Unity's tree view, click the **Site** node.
2. Expand the Site node's properties panel.
3. Select the **Internet Connectivity** tab.
4. Select **HTTP Proxy server** from the drop-down list.

Figure 11-38: Site's properties panel—Internet Connectivity tab: HTTP Proxy server



5. Enter the host name or IP address of the proxy server.
6. Enter the port number.
7. Enter the user name.

8. Enter the user password.
9. (Optional) Select **Connect anonymously**.
10. Click **Test Connectivity**.
11. A confirmation message displays the result of the connection test. Click **OK**.
12. Perform one of these actions:
 - If the connection could not be established, verify and update your connection settings.
 - If the connection was successful, click **Apply** to finalize the configuration.

Connecting to the Internet using a workstation

This method connects to the Internet using a Windows workstation, configured as a port-forwarding proxy on your network.

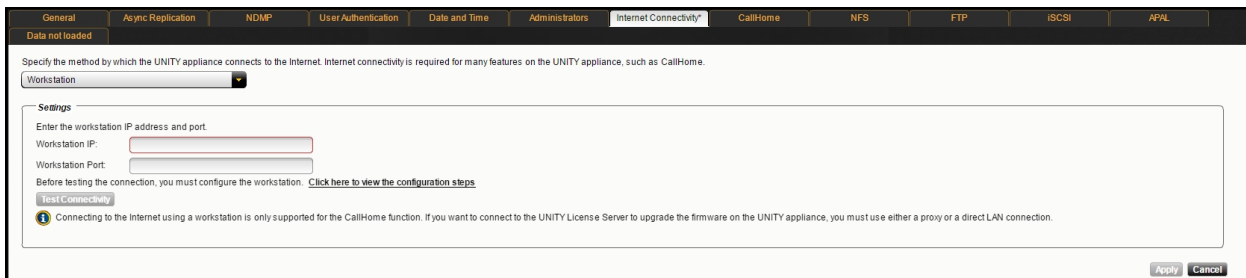
This method is only supported for the Call Home feature. For details on Call Home, see [Understanding the CallHome feature](#) on page 406. For all other features, you must use a direct LAN or proxy connection; see [Connecting to the Internet using a Direct LAN link](#) on the previous page or [Connecting to the Internet using an HTTP proxy server](#) on the previous page.

Note You must use a different workstation for each Unity in your storage infrastructure.

▶ **To configure the Internet connection using a workstation:**

1. In Unity's tree view, click the **Site** node.
2. Expand the Site node's properties panel.
3. Select the **Internet Connectivity** tab.
4. Select **Workstation** from the drop-down list.

Figure 11-39: Site's properties panel—Internet Connectivity tab: workstation



5. Enter the workstation IP address.
6. Enter the workstation port number.
7. Before testing the connection, you must configure the Windows workstation:
 - a. Open port **508** on the workstation firewall for both incoming and outgoing traffic.
 - b. Open the command prompt.
 - c. Run this command (one line):


```
netsh interface portproxy add v4tov4 listenport=508
listenaddress=xxx.xx.12.950 connectport=22
connectaddress=callhome.nexsan.ca
```
8. Back on the **Internet Connectivity** tab, click **Test Connectivity**.

9. A confirmation message displays the result of the connection test. Click **OK**.
10. Perform one of these actions:
 - If the connection could not be established, verify and update your connection settings.
 - If the connection was successful, click **Apply** to finalize the configuration.

Chapter 12

Data replication

Unity provides comprehensive data protection for your Unity deployment, including off-site disaster recovery and remote redundancy, through its asynchronous and synchronous data replication functions.

This section provides an overview of Unity's asynchronous and synchronous data replication functions, and describes how to set up and manage data replications for your Unity storage infrastructure.

It includes these topics:

Data replication concepts and terminology	420
Asynchronous data replication	421
Synchronous data replication	465

Data replication concepts and terminology

This table describes replication concepts and terminology used in Unity.

Table 12-1: Replication concepts and terminology

Replication Terminology	Description
primary , primary site, primary system, or primary Unity	<p>In asynchronous replication, a primary site refers to an Unity that contains the data to be replicated (to a secondary Unity).</p> <p>An Unity can be the primary site in a replicated environment and also perform double-duty as the secondary data replication site for another Unity.</p>
secondary site, replication site, or remote Unity	<p>In asynchronous replication, a secondary site represents the system to which data from the primary Unity is replicated.</p> <p>In a deployment where asynchronous replication is not implemented, a secondary Unity represents a site that is being managed remotely from another Unity or site.</p>
source , source storage system	In synchronous replication, the source storage system represents a Nexsan E18™ or Nexsan E60™ storage system that contains the source data to be mirrored on a target Nexsan E18™ or Nexsan E60™ storage system.
source storage pool	In both asynchronous and synchronous replication, source storage pool refers to the storage pool that contains the data to be replicated to a <i>target</i> .
target , target storage system	In synchronous replication, the target storage system represents the Nexsan E18™ or Nexsan E60™ storage system that mirrors the data on a source Nexsan E18™ or Nexsan E60™ storage system.
target storage pool	In both asynchronous and synchronous replication, target storage pool refers to the replica of the source storage pool on the target system.
peer , peer site, peer system, or replication peer	In asynchronous replication, a peer site represents an Unity that you set up data replication to/from.
replica , pool's replica or storage pool replica	In asynchronous replication, a replica, or a storage pool's replica, refers to the target storage pool that is created on the secondary Unity. The replica is an exact copy of its source storage pool on the primary Unity.
full replication	<p>In asynchronous replication, full replication refers to a replication operation that sends all the data on the primary Unity to the secondary Unity.</p> <p>Only the initial replication, when you first set up asynchronous data replication between two systems, is a full replication. All successive replications are incremental.</p>
incremental replication, or incremental update	In asynchronous replication, incremental replication refers to a replication operation that sends only the data that changed since the last replication (whether that one was full or incremental).
scheduled or automatic replication	In asynchronous replication, a scheduled replication refers to an automatic replication that occurs according to a schedule you define. You can configure a separate replication schedule for each storage pool on Unity.

Replication Terminology	Description
offline or manual replication	In asynchronous replication, an offline, or manual, replication is a replication process that you start manually on a storage pool. With offline replication, you can replicate the data in the storage pool to the secondary Unity, or to a USB storage device attached to the primary Unity.
scrubbing	<p>Unity provides a disk scrubbing mechanism that checks the physical hard disks, which comprise the volumes in a storage pool on Unity, for read or write errors.</p> <p>The storage pool scrubbing mechanism scans a storage pool to identify data integrity problems. It sequentially reads all the data on the hard disks, as well as the data's corresponding parity information, and rebuilds parity wherever needed. Performing routine scrubbing on a storage pool prevents parity errors and data corruption.</p> <p>You can enable/disable a pool scrub schedule on both the primary storage pool and on its replica on the secondary Unity. By default, the scrub schedule is enabled on the replica.</p> <p>See Setting a scrub schedule for a storage pool's replica on page 435.</p>

Asynchronous data replication

The asynchronous data replication feature allows you to designate a secondary Unity as the replication site for a storage pool. Once you set up data replication, Unity automatically creates a replica of the storage pool on the remote Unity. Later, when you add shares to the storage pool on the primary site, you can enable or disable replication for each dataset (shares and/or iSCSI LUNs) to the remote site, as needed.

This section includes these topics:

[Before you begin](#) on page 423

[Setting up asynchronous data replication](#) on page 424

[Modifying asynchronous replication properties and configuration settings](#) on page 432

[Configuring Asynchronous Replication settings for the site](#) on page 436

[Browsing replicated datasets and snapshots](#) on page 439

[Performing an offline replication](#) on page 442

[Configuring replication bandwidth settings for a storage pool](#) on page 446

[Failing over to the remote site for disaster recovery](#) on page 450

[Removing asynchronous data replication for a storage pool](#) on page 463

Asynchronous data replication features

The asynchronous data replication function includes these features:

- **Incremental updates:** Unity's asynchronous data replication function only replicates the data that changed since the last replication. This significantly reduces replication time and also reduces network bandwidth requirements for the replication process.
- **Scheduled automatic updates:** you can flexibly manage and automate data replication between two sites. You can automate replication updates based on a user-defined schedule, or perform manual replications of your data to either the secondary site Unity or to a USB-attached storage device (for offline replications).

- **Failover mechanism:** the asynchronous data replication function provides a failover mechanism that seamlessly transitions all system operations to the secondary site in case of system maintenance, or in the event of a disaster.
- **Replication of storage pool and dataset configuration settings and access permissions:** the asynchronous data replication replicates all share- and file-level access permissions, as well as administrative role assignments for storage pools. It also replicates configuration settings for both storage pools and datasets (shares and/or iSCSI LUNs).
- **Remote access to replicated data:** you can access read-only copies of replicated data on the secondary site Unity for off-site backup or data distribution.
- **Security:** the asynchronous data replication feature uses a secure file transfer protocol to transmit data streams between sites. This ensures that all your data, including share- and file-level access permissions, are transferred securely to the secondary site Unity. In addition, a Unity can only replicate to/from another Unity that you manually add to its list of peer sites.

Note The streams take additional space on Unity before they are replicated. That amount of space does not apply to the secondary site.

- **Flexible configuration:** you have the flexibility to replicate all the datasets (shares and/or iSCSI LUNs) in a storage pool on Unity, or only a subset of datasets. Replication of compressed datasets is also supported.
- **One-to-one topology:** one source is copied to one destination. On Unity, you set up asynchronous data replication separately for each storage pool; the result being that the one-to-one configuration allows you to replicate one or more storage pools on the primary Unity to a single secondary Unity. Alternately, you can replicate each storage pool on Unity to a different secondary site system.

Usage implementations

You can use the asynchronous data replication for:

- **Disaster recovery:** you can set up data replication between two sites—a primary and a secondary system—for disaster recovery. In the event of a disaster that impacts user access to the primary site, you can activate the disaster recovery site—by *promoting* it to primary status; the disaster recovery site automatically takes over using the most recently replicated data. Once you restore the primary site, you can then *demote* the disaster recovery site back to secondary status. During the demotion process, the asynchronous data replication function automatically preserves any data that changed while the secondary site was in service, and creates a *difference* file on the secondary site listing the changes. This process is explained in detail in [Failing over to the remote site for disaster recovery](#) on page 450.
- **Data distribution:** you can use the asynchronous data replication's offline replication function to distribute data (for example, virtual machine images or media) to a secondary site in a different geographic location. This feature is useful in situations where clients of the secondary site system do not ordinarily have access to the primary Unity, or such a setup has prohibitively high latency. To distribute data to a secondary site, you simply use the offline replication function to replicate the data to a USB storage device connected to the primary system; you then transport or ship the USB storage device to the secondary site and import the data. This process is explained in detail in [Performing an offline replication](#) on page 442.
- **Data backup:** you can use the asynchronous data replication function as a backup solution in environments where tape backups are not feasible (for example, where the available bandwidth is insufficient or because the latency for recovery is too high).
- **Data migration:** you can use the asynchronous data replication function to migrate data and system configurations between sites when upgrading hardware or re-balancing storage.

Before you begin

Before you set up asynchronous data replication for your Unity deployment, consider these points.

Element	What to do before creating a replication process
Network	<p>These ports must remain open across the WAN (and/or LAN) links:</p> <ul style="list-style-type: none"> ● TCP ports 22 and 873 ● UDP port 873 <p>All switches, routers, and firewalls between each source site and the remote/DR site must be configured accordingly to allow the source and destination Unities to communicate. The network should also be secured using firewalls, VPN, encryption, or other means.</p> <p>Consider network bandwidth requirements for data replications and allocate bandwidth based on the amount of data that you intend to replicate, as well as the replication frequency.</p> <p>Also, since Unity uses port aggregates, you cannot connect systems directly. You must use a switch between systems.</p>
Remote site	<ul style="list-style-type: none"> ● Make sure the site is properly configured using Unity. ● The remote site must have the Data Replication feature installed. ● Make sure the secondary Unity is connected to the network and powered on. It should be accessible from the primary Unity. ● If the remote Unity has any Nexsan storage enclosure (s) connected to it, and you intend to allocate volumes on the storage system(s) to the replicated data, make sure the system(s) is cabled properly and connected to the secondary Unity, and that it is powered on and online. The Nexsan storage system(s) must also be configured properly with Unity and added to the secondary site as a storage system.
Disaster recovery	<ul style="list-style-type: none"> ● Make sure to develop, document, and implement a clearly defined disaster recovery plan for your storage infrastructure. If you already have a disaster recovery plan in place, make sure you update the plan to include policies and procedures for recovering your Unity storage infrastructure.
Storage capacity	<p>Unity that you intend to use as your remote site should have adequate storage capacity to match the capacity on the primary site—although this is not a requirement for setting up asynchronous data replication for your Unity.</p> <p>For example, if the total disk space of the volumes allocated to the storage pool on the primary site is 100 TB, the remote site should also have a minimum of 100 TB of disk (volume) space available for the storage pool's replica.</p> <p>If the remote site does not have adequate disk space capacity, the replication process will fail. If you intend to only replicate a subset of the data or if you intend to add additional disk space capacity at a later time, you can continue with configuring data replication for the storage pool.</p> <p>For additional details on storage capacity, see Understanding disk space consumption on page 214.</p>

Element	What to do before creating a replication process
Authentication	Make sure that you have the nxadmin password, or if applicable, the user name and password for a Site Administrator on the remote site. When setting up data replication, if the user account you are currently logged on with on the primary site does not exist on the remote site, you will need the nxadmin password for the remote site, or optionally, the user name and password of a Site Administrator configured on the remote system.
USB storage device	If you replicate the datasets to a USB storage device attached to the primary site, you will need to connect the USB device to one of the USB ports on the <i>active</i> node. To determine which node is <i>active</i> prior to starting the procedure, see Viewing cluster health status and controller information on page 300.
Thick LUNs	If you intend to replicate thick LUNs, follow the recommendations mentioned in Understanding disk space consumption on page 214.
Data compression on file systems	<p>If you turn on data compression for a file system, and then you turn it off, before you set up replication for the file system, part of the data is compressed and the other part is not. Since the file system has not been replicated yet, the compression settings are not inherited and data compression is off at the remote site.</p> <p>If you set a space quota on the file system and that quota is almost full, the file system on the remote site will not have enough space to accommodate data coming from the primary file system. As a result, replication will fail.</p> <p>Perform ONE of these actions before replication:</p> <ul style="list-style-type: none"> ● Increase the quota to match the actual space used by data on the file system. ● Set the quota to <i>Unlimited</i>. ● Enable data compression on both sites.
Data compression on LUNs	<p>If you turn on data compression for a LUN, and then you turn it off before you set up replication for the LUN, part of the data will be compressed and the other part will not. Since the LUN has not been replicated yet, the compression settings are not inherited and data compression is off at the remote site.</p> <p>This means that data is taking less space on the primary LUN than it will on the replica. As a result, replication may fail if the LUN on the remote site does not have enough space. In this instance, it is recommended to enable data compression on both sites before replication. For procedural steps, see .</p>

Setting up asynchronous data replication

This section describes the process for setting up data replication for a storage pool on the primary Unity. Before you begin the data replication setup process, you must have, at least, one storage pool defined on the primary Unity; for information about creating a storage pool, see [Adding a storage pool](#) on page 100. Replication of compressed pools is also supported.

A storage pool can have both asynchronous and synchronous data replication configured for it. For more information about synchronous data replication, see [Setting up synchronous data replication for a storage pool](#) on page 466.

► **To start the Asynchronous Data Replication Setup Wizard:**

1. In Unity's tree view, under the site node, click the **Storage Pools** node. This displays its child nodes.
2. Click the node corresponding to the storage pool that you want to set up asynchronous data replication for.
3. Click the **Replications** node.
4. Click the **Properties** tab at the bottom of the screen to expand the Replications Properties panel.
5. Click **Add Asynchronous**.

The Asynchronous Data Replication Setup Wizard starts.

Note [Step 3: Selecting datasets to replicate on page 429](#) is only displayed if you already have shares and/or LUNs defined in the storage pool.

This section includes these steps:

Step 1: Add a remote site for asynchronous data replication	425
Step 2: Configuring a data replication schedule	428
Step 3: Selecting datasets to replicate	429
Step 4: Allocating FASTier cache devices to the storage pool's replica	430
Step 5: Verifying settings	431
Step 6: Viewing results	432

Step 1: Add a remote site for asynchronous data replication

In *step 1* of the Data Replication Wizard, you add or select a remote site where you want Unity to create a replica of the storage pool, and then you select the volumes on the remote site that you want to allocate to the replica.

Figure 12-1: Asynchronous Data Replication Setup Wizard, step 1

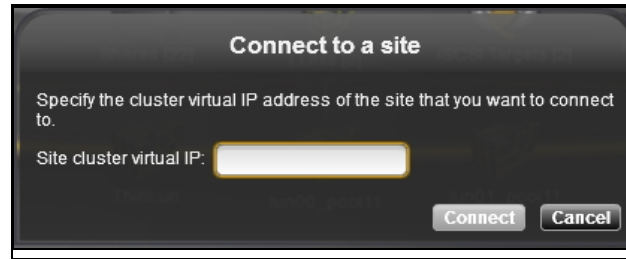


Step 1 of the Data Replication Wizard displays 3 list boxes:

- The first list box, **Storage on Remote System**, on the left-hand side of the panel, displays the storage enclosure(s) connected to the remote Unity currently selected in the site drop-down list above the list box. To expand a storage enclosure and display its volumes, click the arrow preceding the device name.
 - The **Remote Volumes** list box, in the middle of the panel, displays the volumes on the remote Unity that you allocate to the replica of the storage pool by dragging the volumes from the first list box. You can also allow Unity to suggest a suitable volume allocation for the replica by clicking the **Suggest Allocation** button.
 - The **Local Volumes** list box, on the right-hand side of the panel, displays the volumes on the primary site currently allocated to the storage pool that you are setting up data replication for.
- ▶ **To add a remote site as the data replication site:**
1. Click the plus (+) sign next to the site drop-down list. Unity displays the Connect to a remote site dialog box.

- Specify the IP address of the remote Unity to establish a connection with the remote Unity.

Figure 12-2: Asynchronous Data Replication Setup Wizard, step 1: Connecting to a remote site



- Type the **Intersite virtual IP address** of the remote Unity in the IP address field. This IP address enables connectivity between two or more sites for data replication and inter-site communication. This IP address is required even in single-site implementations.
- Click **Connect** to establish a connection to the remote Unity. Depending on the speed of your network connection, this process can take some time to complete. If the user account you are currently logged on with on the primary Unity does not exist on the secondary Unity, or the user account is not assigned the Site Administrator role on the secondary system, Unity prompts you for user credentials to connect to the secondary system. You must either provide the Unity Administrator (**nxadmin**) credentials for the secondary Unity, or the user name and password of a Site Administrator configured on the secondary system.
- Click the **Close** button.

▶ **To select a previously added Unity as the remote site for data replication:**

- From the site drop-down list (above the **Storage on secondary System** list box), select a secondary Unity that you previously added to the primary site—for data replication or for remote site management.

The site drop-down list is disabled if you did not previously add a remote Unity to the primary site.

Unity automatically displays the storage system(s) connected to the remote site, along with the storage system's available volumes. If no volumes display, this means the remote site does not have any free volume; they are all used by one or more storage pools.

Tip To expand a storage system and display its available volumes, click the arrow preceding the device name.

The next step is to allocate available volumes on the remote Unity to the replica of the storage pool.

▶ **To allocate volumes on the remote site:**

- Choose one of these options:

To allow Unity to suggest volume allocation:

- Click the **Suggest Allocation** button below the **Storage on Remote System** list box. Unity automatically allocates volumes to the replica of the storage pool, based on the size of the volume that you allocated to the storage pool—or based on the total combined size of the volumes, if the storage pool has multiple volumes allocated to it.

To manually allocate volumes:

- In the **Storage on Remote System** list box on the left-hand side of the panel, highlight the corresponding storage system on the remote site—where the volume(s) that you want to allocate to the replica of the storage pool exists—by selecting the storage system in the list.

- b. Expand the storage system to display its available volumes, by clicking the arrow preceding the device name.
- c. Drag the volume(s) that you want to allocate to the replica of the storage pool to the **secondary Volumes** list box.

The bars below the **secondary Volumes** and **Local Volumes** list boxes on the panel provides a graphical view of the storage pool's total volume space, as well as the amount of disk space that you assign to the replica of the storage pool. The value for the replica's assigned disk space changes as you allocate volumes. The Data Replication Wizard does not allow you to move forward to the next step until you allocate some disk space to the replica.

Depending on its configuration, if the secondary Unity has multiple storage systems, including externally attached Nexsan storage, you may not be able to combine volumes from different storage systems to allocate to the replica.

Figure 12-3: Asynchronous Data Replication Setup Wizard, step 1: allocating volumes to the replica

Add a Remote Site for Data Replication

Add or select the remote site where you want to replicate 'FinanceMTL' to, and select the volume(s) on the remote site that will be allocated to 'FinanceMTL'. Click the Suggest Allocation button if you want UNITY to automatically suggest volume allocation on the remote system, based on the total size of the volume(s) in 'FinanceMTL'.

2. When you finish allocating volumes on the remote system to the replica of the storage pool, click the right arrow on the panel to continue to [Step 2: Configuring a data replication schedule](#) below.

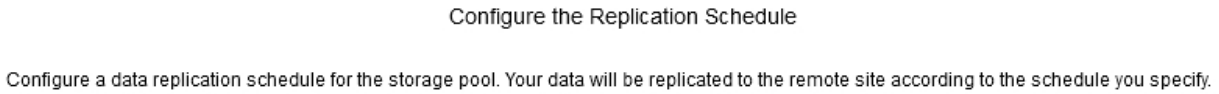
Step 2: Configuring a data replication schedule

In *step 2* of the Asynchronous Data Replication Setup Wizard, you configure the data replication schedule for the storage pool.

The default schedule for data replication is once a day at 10 PM, with the start date set to the current date on Unity. The default schedule assumes that 10 PM is an off-peak business hour. If you change the default

schedule, we recommend that you schedule data replications during off-peak business hours to prevent network congestion, and to ensure Unity has sufficient access to network bandwidth to perform the replications.

Figure 12-4: Asynchronous Data Replication Setup Wizard, step 2: Configuring a data replication schedule



Start date:

Recur every:

► **To configure the data replication schedule for the storage pool:**

1. Specify the start date for the schedule by clicking the **Start date** field and selecting a date from the calendar.
2. Specify the time when you want Unity to perform data replications. The default time is 10 PM.
3. Specify a recurrence pattern for the schedule by typing a value in the **Recur every** field.
4. Select the recurrence type from the drop-down list: **Minutes(s)**, **Hour(s)**, **Day(s)**, **Week(s)**, or **Month(s)**.
5. When you finish configuring the data replication schedule for the storage pool, click the right arrow button on the panel to continue to [Step 3: Selecting datasets to replicate](#) below.

Step 3: Selecting datasets to replicate

In *step 3* is only displayed if you already have datasets (shares and/or iSCSI LUNs) defined in the storage pool. Consider the dataset (shares and/or LUNs) that you intend to replicate to the remote site. Some dataset may contain non-critical user data that does not need to be replicated for off-site disaster recovery. You can exclude these dataset from data replication by disabling replication individually for each share.

You can bypass this step if you do not want to replicate your datasets immediately after configuring data replication for the storage pool: simply click the right arrow button on the panel to continue to [Step 4: Allocating FASTier cache devices to the storage pool's replica](#) on the next page.

You can enable data replication for your datasets later; see [Enabling or disabling asynchronous data replication for a dataset](#) on page 434.

Figure 12-5: Asynchronous Data Replication Setup Wizard, step 3: Selecting datasets to replicate

Enable Replication for datasets

Select the datasets in the storage pool that you want to replicate to the remote site.

Name	Type	Used space	Date of last replication	<input checked="" type="checkbox"/> Replication
FinanceLUN	LUN	16.71 KB		<input checked="" type="checkbox"/>

► **To select the datasets for replication to the remote site:**

1. In the grid, click the check box corresponding to the dataset(s) that you want to replicate to the secondary Unity.

You can search for a specific dataset by entering its name in the text box above the **Name** column heading. The grid automatically filters the list as you type.

If you want to replicate all the datasets in the storage pool, click the **All** check box.

2. Click the right arrow button on the panel to continue to [Step 4: Allocating FASTier cache devices to the storage pool's replica](#) below.

Step 4: Allocating FASTier cache devices to the storage pool's replica

Step 4 is displayed even if the remote Unity has no FASTier cache devices installed.

► **General guidelines for assigning FASTier cache devices:**


- You assign a read/write cache device as either read cache OR write cache.
- Unity only uses read cache devices once the RAM cache on the system is full. Read cache devices are filled only as files are read. This means that Unity uses read caching only on the second file access.
- Write-only cache devices aggregate smaller writes in one large write. They are particularly useful for many small, synchronous writes. Asynchronous writes will see no improvement.

Figure 12-6: Asynchronous Data Replication Setup Wizard, step 4: configure FASTier cache on the storage pool's replica

Configure FASTier Cache: Temp

Assign Nexsan FASTier cache devices to the storage pool's replica on the remote NST appliance. Nexsan's FASTier SSD cache devices enhance the performance of the NST appliance by caching data during read or write operations on the system.

FASTier Devices

There are 3 FASTier devices: 

3 FASTier Read	Use	0	▲▼	FASTier device(s) for read
0 FASTier Write	Use	0	▲▼	FASTier device(s) for write
0 FASTier Read or Write	Use	0	▲▼	FASTier device(s) for write

Summary

Read Devices Assigned: 0 FASTier Read

Write Devices Assigned: 0 FASTier Write, 0 FASTier Read or Write

► **To allocate FASTier cache devices to the storage pool's replica:**

1. Specify the number of read cache devices that you want to allocate to the storage pool's replica by typing or selecting a value in the **Use FASTier device(s) for read** ▲▼ box.

2. Specify the number of write cache devices that you want to allocate to the storage pool's replica by typing or selecting a value in the **Use FASTier device(s) for write** box.
For example, on an Unity with 2 FASTier read cache devices and 2 FASTier read/write cache devices, you can allocate one of these:
 - 4 cache devices as read cache.
 - 3 cache devices as read cache, and
 - 1 cache device as write cache.
 As you select the number of read and write cache devices to allocate to the storage pool's replica, the **Summary** section on the wizard panel automatically updates to display how your selections impact cache assignment on the remote site.
3. When you finish allocating FASTier cache devices to the storage pool's replica, click the right arrow on the wizard panel to continue to [Step 5: Verifying settings](#) below.

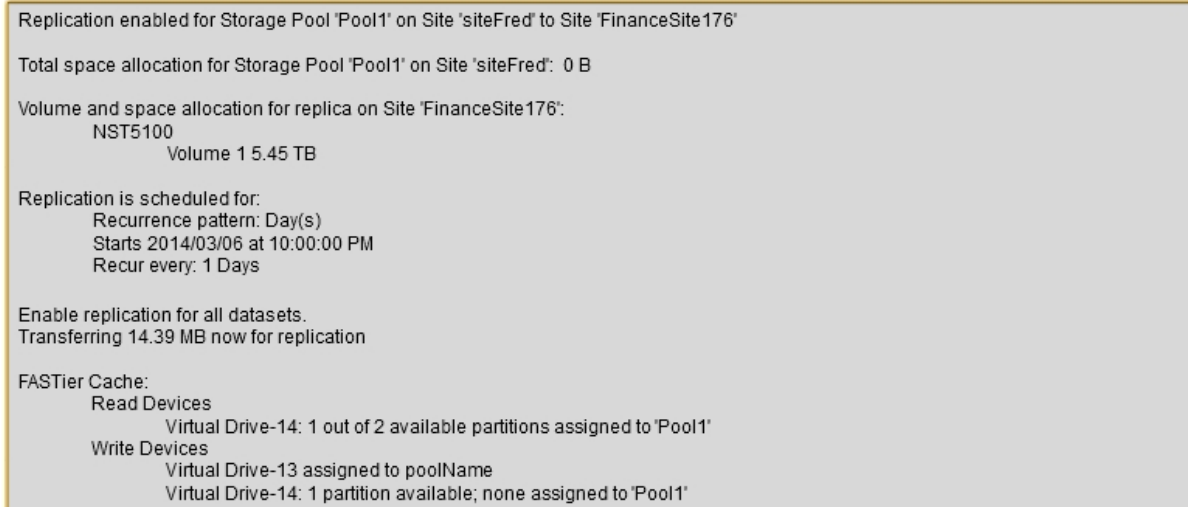
Step 5: Verifying settings

Step 5 of the Asynchronous Data Replication Setup Wizard summarizes the settings you selected for data replication and applies the settings when you click **Start**. Review the summary carefully before applying the data replication settings.

Figure 12-7: Asynchronous Data Replication Setup Wizard, step 5: verifying data replication settings

Verify Settings

Please verify your configuration settings. If you want to change a setting, click the back arrow to navigate to the relevant configuration panel. Or, click the step identifier at the top of the wizard panel to go back to a specific step.



► To change a configuration setting:

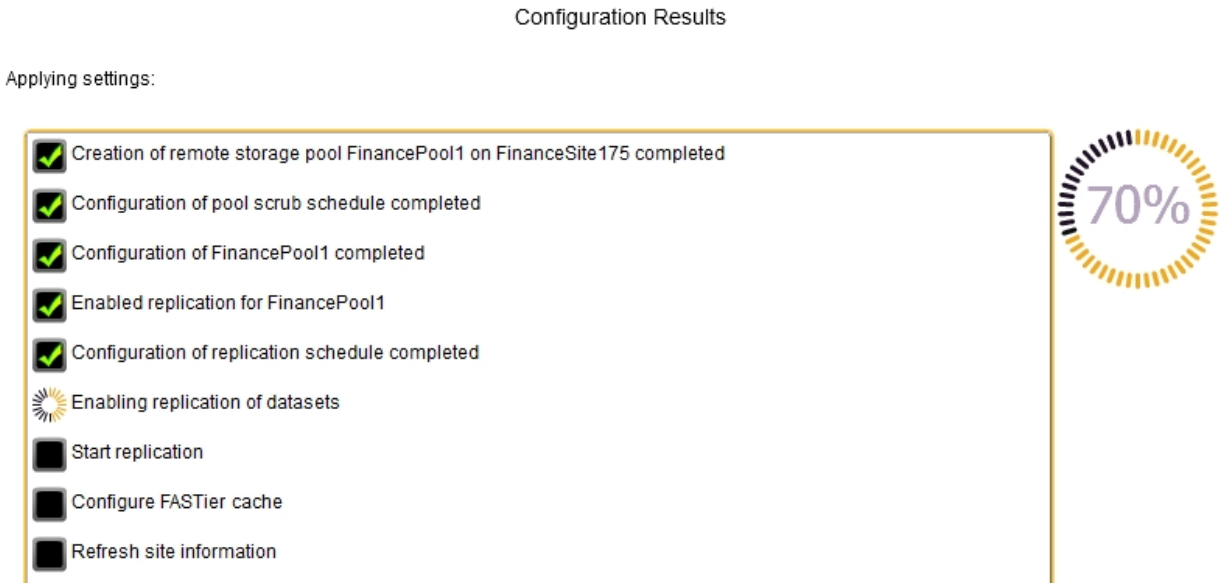
- Click the back arrow to navigate back to the corresponding configuration step.
Or
- Click the corresponding step identifier at the top of the Asynchronous Data Replication Setup Wizard panel. For example, if you want to modify the data replication schedule, click **Step 2**.

If you are satisfied with the configuration settings, click the **Start** button at the bottom of the panel. The Asynchronous Data Replication Setup Wizard automatically proceeds to [Step 6: Viewing results](#) on the next page.

Step 6: Viewing results

Step 6 of the Asynchronous Data Replication Setup Wizard displays progress as Unity applies your replication configuration to the primary and secondary systems.

Figure 12-8: Asynchronous Data Replication Setup Wizard, step 6: viewing results



The Asynchronous Data Replication Setup Wizard displays error events that the system encounters during the configuration process. You can view more details about an error event by expanding the corresponding entry.

► **To view more details for an error event:**

- Click the plus (+) sign corresponding to the error event.

Click **Close** to close the Asynchronous Data Replication Setup Wizard.

The replication will start at the new replication schedule. To change the schedule, see [Modifying a storage pool's replication schedule](#) on the facing page.

Modifying asynchronous replication properties and configuration settings

This section describes how to view and modify asynchronous data replication properties and configuration settings for a storage pool.

Note Any configuration change of a replicated share does not affect its replica immediately; the new configuration will be applied at the next replication. For example, if the primary share is CIFS-only, the replica will be available to browse in CIFS mode only. When you change the sharing method to both NFS and CIFS, the replica will not be browsable in NFS until the next replication.

This section includes these topics:

Modifying a storage pool's replication schedule	433
Disabling a storage pool's replication schedule	434
Enabling or disabling asynchronous data replication for a dataset	434

Setting a scrub schedule for a storage pool's replica 435

Modifying a storage pool's replication schedule

When you configure asynchronous data replication for a storage pool, you set a replication schedule for the pool. Unity then automatically replicates the data in the pool according to the schedule you define.

► To modify a storage pool's replication schedule:

1. In Unity's tree view, click the Site node representing the primary site.
In a multi-site environment, the Site node for the primary, or local, site—that is, the site from where you

access Unity—is identified by this node icon:



2. Click the **Storage Pools** node.
3. Click the node representing the storage pool that you want to modify the replication schedule for. The storage pool you select must have asynchronous data replication configured.
4. When the storage pool's child nodes are displayed, click its **Replications** node.
5. Click the node representing the secondary Unity, and expand its Properties panel.

Figure 12-9: Pool's properties panel—Settings tab



6. Select the **Settings** tab and modify the replication schedule for the storage pool.



CAUTION: The default schedule for data replication is once a day at 10 PM, with the start date set to the current date on Unity. This means that Unity will replicate the data in the storage pool every day at 10 PM, starting on the current date. The default schedule assumes that 10 PM is an off-peak business hour. If you change the default schedule, we recommend that you schedule data replications during off-peak business hours to prevent network congestion, and to ensure Unity has sufficient access to network bandwidth to perform the replications.

- a. Modify the start date for the schedule by clicking the **Start date** field and selecting a date from the calendar.
- b. Modify the time when you want Unity to perform data replications. The default time is 10 PM.
- c. Select a new recurrence pattern for the schedule by typing a value in the **Recur every** field.
- d. Select the recurrence type from the drop-down list: **Minutes(s)**, **Hour(s)**, **Day(s)**, **Week(s)**, or **Month(s)**.

- When you finish modifying the data replication schedule for the storage pool, click **Apply** to save the new schedule.

Disabling a storage pool's replication schedule

If needed, you can temporarily disable the replication schedule for a storage pool. If you disable the replication schedule, Unity will not replicate the storage pool and its data at the next scheduled replication cycle.

Note If replication is currently in progress for the storage pool, disabling the schedule will NOT stop the replication.

► **To disable a storage pool's replication schedule:**

- In Unity's tree view, click the Site node representing the primary Unity; this displays the primary site's child nodes.
- Click the **Storage Pools** node.
- Click the node representing the storage pool that you want to pause the replication schedule for. The storage pool you select must have asynchronous data replication configured.
- When the storage pool's child nodes are displayed, click its **Replications** node.

To...	Do this
use the Replications node's Properties panel	<ol style="list-style-type: none"> Expand the Replications node's Properties panel. On the Replications node's Properties panel, select the node representing the secondary Unity in the grid. Clear the Enable scheduling option.
use the secondary site node's Properties panel	<ol style="list-style-type: none"> Click the node representing the secondary Unity, and expand its Properties panel. On the secondary Unity node's Properties panel, clear the Enable scheduling option.

- Click **Apply**.

Enabling or disabling asynchronous data replication for a dataset

Unity allows you to enable or disable asynchronous data replication for individual datasets (shares and/or iSCSI LUNs) in a storage pool. This gives you the flexibility to choose the data that you want to replicate to the secondary Unity for disaster recovery. For example, if the storage pool on your primary Unity contains some datasets with non-critical data, such as test data, you may want to exclude those datasets from the data replication process. This will help you minimize network bandwidth consumption during data replications, and also save on storage capacity on the remote site.

► **To enable or disable asynchronous data replication for a dataset:**

- In Unity's tree view, click the Site node representing the primary site.
- Click the **Storage Pools** node.
- Click the node representing the storage pool that contains the datasets you want to enable or disable data replication for. The storage pool you select must have asynchronous data replication configured.
- When the storage pool's child nodes are displayed, click its **Replications** node.
- Click the node representing the secondary Unity, and expand its Properties panel.

- Click the **Datasets** tab.

Figure 12-10: Pool's properties panel—Datasets tab

Name	Type	Used space	Date of last replication	Select
lun162	LUN	115.81 GB	2014/10/31 11:26:59 AM	<input checked="" type="checkbox"/>
lun162lun2	LUN	151.44 MB	2014/10/31 11:26:58 AM	<input checked="" type="checkbox"/>
lunwithmaskandC	LUN	16 KB	2014/10/31 11:26:58 AM	<input checked="" type="checkbox"/>
lunwithmaskdiff	LUN	16 KB	2014/10/31 11:26:59 AM	<input checked="" type="checkbox"/>
share162	Share	1.06 MB	2014/10/31 11:26:59 AM	<input checked="" type="checkbox"/>

- In the grid, under the **Select** column, click the check box corresponding to the dataset(s) that you want to enable or disable data replication for. A check mark indicates that replication is enabled for the dataset. You can search for a specific dataset by entering its name in the text box above the **Name** column heading. The grid automatically filters the list as you type. You can also filter the list by datasets that have replication enabled or disabled; open the drop-down list above the **Select** column and select one of the available options: **All**, **Enabled**, or **Disabled**. The grid filters the list of datasets according to your selection. If you want to enable or disable replication for all the datasets in the storage pool, click the top-level check box in the **Select** column.
- Click **Apply** to save your settings.

Setting a scrub schedule for a storage pool's replica

You can enable/disable a pool scrub schedule on both the primary storage pool and on its replica on the secondary Unity. By default, the scrub schedule is enabled on the replica.



CAUTION: The default schedule for pool scrubbing is set to 12 AM, once every 4 weeks, on Saturdays. The default schedule assumes that this is an off-peak business hour. If you change the default schedule, we recommend that you schedule pool scrubs during off-peak business hours since a scrubbing operation may degrade the performance of Unity.

▶ To enable the pool scrub schedule for a storage pool's replica:

- In Unity's tree view, click the Site node representing the remote Unity where the storage pool that you want to enable and configure the pool scrub schedule for is replicated.
- Click the **Incoming Replications** node.
- If you have multiple incoming replications to this secondary Unity, click the Site node representing the site where the replicated storage pool that you want to enable and configure the pool scrub schedule for exists.
- Click the storage pool that you want to enable and configure the pool scrub schedule for, and expand its Properties panel.
- Select the **Scrub Schedule** tab on the Properties panel.
- Select the **Enable scrub scheduling** option to enable the scrub schedule for the storage pool's replica.

7. Set the scrub schedule for the storage pool's replica:
 - a. Specify the start date for the schedule by clicking the **Start date** field and selecting a date from the calendar.
 - b. Specify the time when you want Unity to perform pool scrubs. The default time is 12 AM.
 - c. Specify a recurrence pattern for the schedule by typing a value in the **Recur every** field.
 - d. Select the recurrence type from the drop-down list: **Minutes(s)**, **Hour(s)**, **Day(s)**, **Week(s)**, or **Month(s)**.
8. Click the **Apply** button to save your configuration settings.

During the pool scrub operation, Unity displays progress in the Tasks in progress panel.

Performing a manual pool scrub on a storage pool's replica

You can also manually start a scrub operation on a storage pool's replica, if needed.

► **To perform a manual pool scrub:**

1. In Unity's tree view, click the Site node representing the secondary Unity where the storage pool that you want to perform a manual pool scrub on; this displays its child nodes.
2. Click the **Incoming Replications** node.
3. If you have multiple incoming replications to this secondary Unity, click the Site node representing the site where the replicated storage pool that you want to perform a scrub operation on exists.
4. Select the storage pool replica that you want to perform a scrub operation on and expand its Properties panel.
5. Click the **Scrub** button.

During the pool scrub operation, Unity displays progress in the Tasks in progress panel.

Configuring Asynchronous Replication settings for the site

You can configure the general settings for Asynchronous Replication at the site level before or after configuring replication. The new settings are applied at the next replication if replication is already configured.

The **Async Replication** tab on the Site node's properties panel allows you to configure:

- Network settings
- Compression settings
- Encryption settings

This section includes these topics:

[Configuring network settings for Asynchronous Replication](#) below

[Configuring compression settings for Asynchronous Replication](#) on page 438

[Configuring encryption settings for Asynchronous Replication](#) on page 438

Configuring network settings for Asynchronous Replication

You configure network settings for Asynchronous Replication at the site level. All replication processes that will be created for that site will inherit the same settings. You can specify the type of network connection between the primary and remote sites, as well as the network interface for the replication stream.

Note If you change a network setting while replication is in progress, the setting will take effect in the next replication process. For the setting to take effect immediately, you can use the `services` command in the `nxadmin` CLI and restart the `system.filesystem.nstfs.nest-async-replication` service; for details, see the *Nexsan Unity nxadmin Command-line Reference Guide*.

► **Network type for data replication:**

Unity may terminate a replication session if the network response time falls below the acceptable threshold. Unity provides a configuration setting that allows you to specify the network connection: either a LAN or WAN connection.

Setting the network type to **WAN** increases the threshold for network response tolerance on slow WAN links. This setting also enables a checksum mechanism to ensure data integrity over the WAN link, on both the outbound data stream (at the source site) and on the inbound data stream (at the remote or DR site).

► **Network interface for data replication:**

By default, Unity uses the primary data network interface (nx0) to replicate data, that is, for the outgoing replication stream. You can change this setting and choose the Management interface (nx99) instead, or choose another data network interface (for example, nx1).



CAUTION:

- The network interface that you set on the primary site (for the outgoing replication stream) must be the same as the one on the remote site (for the incoming replication stream).
- If you select nx99 for replication, nx0 still needs to be configured and reachable on your network. Using nx99 offers the advantage to separate the traffic, in which nx0 is used for the control flow and x99 is used for the data flow.

To configure nx0, see *Modifying IP configuration settings in the Unity Snapshots and Replications Guide*.

► **To configure network settings:**

1. In Unity's tree view, click the Site node for the selected site.
2. Expand the Site's properties panel.
3. Select the **Async Replication** tab.

Figure 12-11: Site's properties panel—Async Replication tab: Network Settings

The screenshot shows the 'Async Replication' tab in the Unity management interface. The 'Network Settings' section includes a 'Type' dropdown set to 'LAN' (with 'WAN' also available) and an 'Interface' dropdown set to 'Data network interface (nx0)' (with 'Management interface (nx99)' also available). A note below states: 'Note: You can specify a different data network interface (other than nx0) if one exists. Use the nxadmin CLI to create additional data network interfaces.' The 'Compression Settings' section has an unchecked 'Enable Compression' checkbox. The 'Encryption Settings' section has a checked 'Enable Encryption' checkbox. 'Apply' and 'Cancel' buttons are at the bottom right.

4. Under **Network Settings**, perform one or more of these actions:

To change the...	Do this
type of network connection between the primary and replication sites	Select LAN or WAN .
network interface for the replication stream	Select the desired network interface.

5. Click **Apply**.

► **What's next:**

If you changed the network interface, you must make the same change on the remote site.

Configuring compression settings for Asynchronous Replication

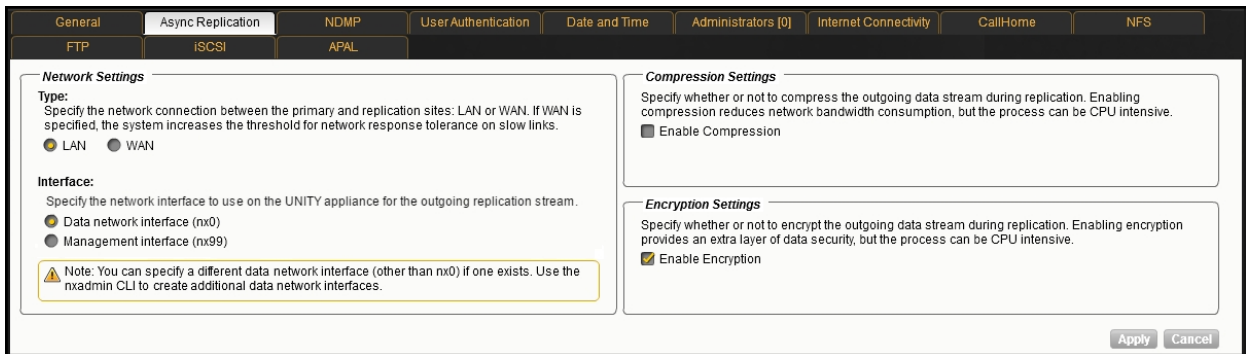
You configure compression settings for Asynchronous Replication at the site level. All replication processes that will be created for that site will inherit the same settings.

By default, data compression is disabled. If you enable this setting, the outgoing data stream will be compressed during replication to reduce network bandwidth consumption. This process can be CPU intensive. This compression setting only affects the outgoing data stream for replication; it does not affect local data on the storage pool and datasets.

► **To configure data compression for asynchronous replication:**

1. In Unity's tree view, click the Site node for the selected site.
2. Expand the Site's properties panel.
3. Select the **Async Replication** tab.

Figure 12-12: Site's properties panel—Async Replication tab: Compression Settings



4. Under **Compression Settings**:
 - To enable data compression, select the **Enable Compression** option.
 - To disable data compression, clear the **Enable Compression** option.
5. Click **Apply**.

Configuring encryption settings for Asynchronous Replication

You configure encryption settings for Asynchronous Replication at the site level. All replication processes that will be created for that site will inherit the same settings. By default, data encryption is enabled. This allows

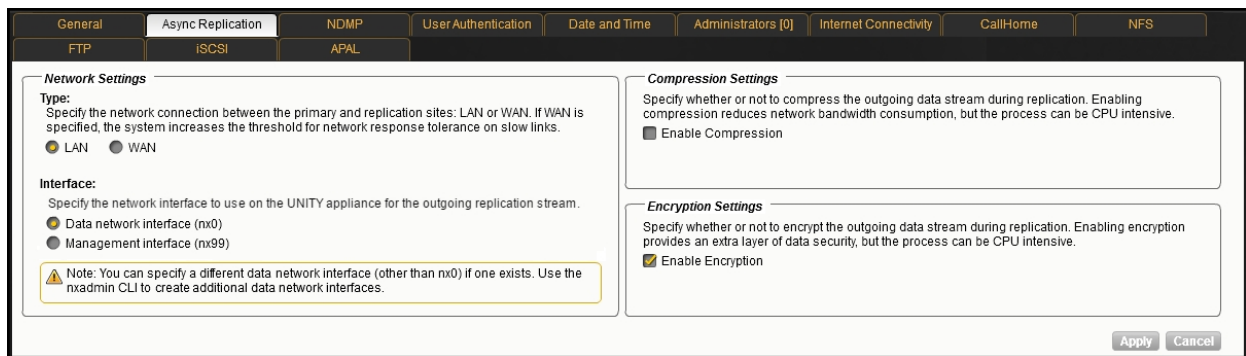
the outgoing data stream to be encrypted during replication to provide an extra layer of data security. This process can be CPU intensive.

Note If one site has encryption enabled, the data will be encrypted. If both sites have encryption disabled, the data will not be encrypted.

► **To configure encryption settings:**

1. In Unity's tree view, click the Site node for the selected site.
2. Expand the Site's properties panel.
3. Select the **Async Replication** tab.

Figure 12-13: Site's properties panel—Async Replication tab: Encryption Settings



4. Under **Encryption Settings**:
 - To enable data encryption, select the **Enable Encryption** option.
 - To disable data encryption, clear the **Enable Encryption** option.
5. Click **Apply**.

Browsing replicated datasets and snapshots

Once you set up data replication for a storage pool on the primary Unity, you can view and [browse](#) the storage pool's replicated datasets (file systems and/or LUNs) and snapshots on the remote site Unity, under the storage pool's replica.

This section includes these topics:

- [Viewing and browsing replicated datasets below](#)
- [Viewing and browsing replicated snapshots on the remote site on page 441](#)

Viewing and browsing replicated datasets

When you replicate a file system, Unity automatically enables sharing for the replicated dataset (file system or LUN) on the remote site.

Notes:

- To access and browse a replicated LUN, the replicated storage pool where the LUN resides must be the primary pool.
- You must configure LUN masking/host connectivity settings for the replicated LUN.
- You cannot browse a replicated file system using FTP sharing.

► **To view replicated datasets:**

1. In Unity's tree view, click the Site node representing the remote site where the storage pool for which you want to enable and configure the pool scrub schedule is.
2. Click the **Incoming Replications** node.
3. If you have multiple incoming replications to this remote site, click the Site node representing the site where the replicated storage pool hosting the datasets exists.
4. Click the storage pool containing the replicated dataset that you want to view.
5. Click the **Replicated File Systems** or **Replicated LUNs** node and expand its Properties panel.

Figure 12-14: Pool's properties panel—Replicated Shares tab

Name	Used space	Replication status	Date of last replication
PayRollData1	147.85 KB	Ok	2012/09/13 1:58:29 PM
PayRollData2	195.80 KB	Ok	2012/09/13 1:58:28 PM
PayRollData4	171.83 KB	Ok	2012/09/13 1:58:29 PM
PayRollData5	199.13 KB	Ok	2012/09/13 1:58:29 PM

The **Replicated File Systems** or **Replicated LUNs** node Properties panels display the File Systems/LUNs that are replicated to the remote site. It contains a grid displaying the replication status for each datasets, as well as the date and time of the last successful replication.

You can search for a specific File System/LUN in the grid by typing its name in the text box above the **Replicated File System** column. Unity automatically filters the grid as you type.

You can sort the list of File Systems displayed in the grid in either ascending or descending (alphabetical) order by clicking the sort pointer in the **Replicated File System** column heading.



► **To sort the list in descending order:**

- Click the sort pointer until the arrow points down.

► **To sort the list in ascending order:**

- Click the sort pointer until the arrow points up.

You can filter the File Systems displayed in the grid by **Browsing status**, and you can also use the filter to only display File Systems replicated within a specific time period.

► **To only display File Systems/LUNs replicated within a specific time period:**

1. Open the drop-down list above the **Date of last replication** column heading in the grid.
2. Select the time period (**This Hour**, **Today**, **Yesterday**, or **This Week**) that you want to display replicated File Systems fro. The default filter setting is **All**.

► **To browse the contents of a replicated dataset:**

You browse a replicated dataset in the same way that you browse the source dataset on the primary Unity, except that the replicated dataset is a read-only copy of the source File System (but with the same access permissions as the source dataset). Since the replicated dataset exists only on the remote site, you must set up a CIFS or NFS mapping to the remote site from the Windows-based (CIFS) system and/or UNIX/Linux-based (NFS) system from which you want to access the replicated dataset .

The process for accessing a File System and browsing its contents is described in detail in [Accessing an NFS file system from UNIX/Linux](#) on page 177.

Viewing and browsing replicated snapshots on the remote site

When you replicate a dataset, Unity also replicates the snapshots for the dataset and displays the snapshots on the secondary site. You can then enable browsing for the replicated snapshots to view their contents.

This mechanism allows you to access replicated snapshots on the remote site in the event that you do not have access to the primary Unity where the snapshots originate. In general, you would enable browsing for a replicated snapshot and view its contents on the remote site to:

- recover individual files, or an entire file system, in case the files are accidentally deleted or overwritten, or corrupted, in the source dataset, or
- back up the contents of the snapshot to tape, or to other media, for disaster recovery.

The process for viewing and browsing replicated snapshots on the remote site is the same as viewing and browsing snapshots for the source dataset on the primary site.

Note Snapshot auto-deletion settings are configured from the primary site only. When the share or LUN is replicated, snapshots are automatically deleted from its replica using the same threshold, during a subsequent replication session.

Tip You can also browse the snapshot of a replicated LUN using the mgmt target.

► **To view replicated snapshots on the remote site:**

1. In Unity's tree view, click the Site node representing the remote site Unity where the storage pool for which you want to enable and configure the pool scrub schedule is.
2. Click the **Incoming Replications** node.
3. If you have multiple incoming replications to this remote site, click the Site node representing the site where the replica for which you want to enable and configure the pool scrub schedule exists.
4. Click the storage pool containing the replicated datasets that you want to view.
5. Click the **Replicated File Systems** or **Replicated LUNs** node.
6. Click the node representing the replicated share or replicated LUN that you want to view replicated snapshots for; this displays its child nodes.
7. Click the **Snapshots** tab.

The **Snapshots** tab displays the replicated snapshots for the corresponding dataset. The functionality of the Replicated Snapshots node Properties panel is the same as the Snapshots Properties panel on the primary Unity (see [Using the File Systems properties panel](#) on page 194).

► **To browse the contents of a replicated share on the remote site:**

You use the **Replicated Snapshots** node Properties panel to enable browsing for replicated snapshots. You browse a replicated snapshot in the same way that you browse its source snapshot on the primary site, except that the replicated snapshot exists only on the remote site. As a result, to browse the contents of a

replicated snapshot, the Windows-based (CIFS) and/or UNIX/Linux-based (NFS) clients that will access the replicated share snapshot, or the iSCSI clients that will connect to the replicated LUN snapshot, must connect to the secondary site Unity.

The process for enabling browsing for a snapshot and viewing its contents from a Windows-based (CIFS) system and/or UNIX/Linux-based (NFS) system is described in detail in .

Performing an offline replication

Unity provides an offline data replication mechanism that allows you to initiate a manual replication of the data contained in a storage pool to either:

- the remote site configured as the data replication site for the storage pool, or
- a USB storage device attached to Unity. Once Unity copies the data to the USB storage device, you can transport or ship the USB storage device to the secondary site and import the data from the device to the corresponding storage pool replica on the secondary site system. This mechanism allows you to distribute data (for example, virtual machine images or media) to a secondary site in a different geographic location. This feature is useful in situations where clients of the secondary site system do not ordinarily have access to the primary site, or such a setup has prohibitively high latency

Typically, you initiate an offline replication to the remote site when you want to immediately update the copy of your data on the secondary site to create a specific point-in-time image of the data.

This section includes these steps:

Performing a manual replication to a remote site	442
Performing an offline replication to a USB storage device	443
Importing data from the primary Unity	444
Importing data from a USB storage device	445

Performing a manual replication to a remote site

This section explains how to perform a manual replication of the data in a storage pool to the remote site configured as the data replication site for the storage pool. To perform this operation, you must have configured a data replication for the storage pool, and added at least a share or a LUN to the storage pool.

▶ **To start the Replicate Data panel:**

1. In Unity's tree view, click the Site node representing the primary Unity.
2. Click the **Storage Pools** node.
3. Click the node representing the storage pool that contains the data you want to replicate.

4. Click its **Replications** node.
5. Perform one of these actions:

To...	Do this
use the Replications node's Properties panel	<ol style="list-style-type: none"> 1. Expand the Replications node's Properties panel. 2. On the Replications node's Properties panel, select the node representing the secondary site Unity in the grid. 3. Click the Replicate button at the bottom of the panel.
use the secondary site node's context menu	<ol style="list-style-type: none"> 1. Click the node representing the secondary site Unity, and then click the context menu button on the node. 2. When the node context menu opens, select Replicate.
use the secondary site node's Properties panel	<ol style="list-style-type: none"> 1. Click the node representing the secondary site Unity, and expand its Properties panel. 2. On the secondary site Unity node's Properties panel, click the Replicate button at the top of the panel.

This starts the Replicate Data panel, which displays all the datasets in the storage pool.

► **To perform a manual replication:**

1. In the grid, click the check box corresponding to the dataset(s) that you want to disable or enabled replication to the secondary Unity for. Only datasets that have replication enabled are displayed in the grid, and they are automatically selected for replication.
2. If you want to replicate additional datasets for replication, you must enable replication for the datasets. You can search for a specific dataset by entering its name in the text box above the **Name** column heading. The grid automatically filters the list as you type. If you want to replicate all the datasets in the storage pool, click the **All** check box.
3. For the destination for manual replication, select the **Replicate data to the secondary site** option.
4. Click **Calculate** to compute the amount of disk space required for the selected datasets on the remote site. The system calculates disk space requirements based on incremental changes to the data. Depending on the size and number of datasets selected, the calculation process may take some time.
5. Click the **Replicate** button.

Unity starts the replication process. The progress of the replication is displayed in the Tasks in progress panel.

Performing an offline replication to a USB storage device

To perform this operation, you must have configured a data replication for the storage pool, and added at least a share or a LUN to the storage pool. You must also connect a USB storage device to a USB port on the *active* node; to determine which node is *active*, see [Viewing cluster health status and controller information on page 300](#)). Unity automatically detects USB storage devices connected to the system, and assigns each device a unique device ID that includes the device's storage capacity; for example: **210 GB - c2t0d0**.

► **To perform an offline data replication to a USB storage device:**

1. Start the Replicate Data panel; see the steps in [Performing a manual replication to a remote site on page 442](#).
2. In the grid, click the check box corresponding to the dataset(s) that you want to replicate. Only datasets that have replication enabled are displayed in the grid, and they are automatically selected for replication. To replicate additional datasets for replication, you must enable replication for these datasets.
You can search for a specific dataset by entering its name in the text box above the **Name** column heading. The grid automatically filters the list as you type.
If you want to replicate all the datasets in the storage pool, click the **All** check box.
3. For the destination for offline replication, select the **Export data to:** option.
4. Select the USB storage device from the drop-down list. The USB storage device must be connected to one of the USB ports on the controller where the storage pool, that you want to replicate data from, is hosted.

If the USB storage device is not displayed in the drop-down list, make sure the device is connected properly, and if applicable, powered on; then, click the refresh icon next to the drop-down list to force a device discovery.



CAUTION: To replicate to a USB storage device, Unity requires the device to be formatted for compatibility with its operating system. If the device is not formatted properly, Unity automatically formats the device, and erases any existing data stored on the device.

5. Once you select the USB storage device to replicate the datasets to, select the **Delete all the existing data on device** option if you want Nexsan Unity to format the device and delete any existing data on it. If you select this option, Nexsan Unity prompts you to confirm the action. Click **Yes** to continue.
6. Click the **Calculate** button to compute the amount of disk space required for the selected datasets on the USB device. Replicating to a USB device entails a full replication, and thus, disk space requirements are calculated accordingly. Depending on the size and number of datasets selected, the calculation process may take some time.
7. Click the **Replicate** button

The progress of the replication is displayed in the Tasks in progress panel.

Importing data from the primary Unity

This section explains how to import data on the secondary site Unity from the primary Unity (configured as the data replication source for the secondary site system).

Unity provides the Import Data utility to guide you through the process of importing data.

► **To start the Import Data utility:**

1. In Unity's tree view, click the Site node representing the remote site.
2. Click the **Incoming Replications** node.
3. Click the node representing the primary site that you want to import data from.

4. Select the storage pool for which you want to import data.
5. Perform of these actions:

To...	Do this
use the storage pool's node context menu	<ol style="list-style-type: none"> a. Click the node representing the storage pool that contains the data you want to import, and then click the context menu button on the node to open the node context menu. b. When the node context menu opens, select Import Data.
use the storage pool's Properties panel	<ol style="list-style-type: none"> a. Click the node representing the secondary site Unity, and expand its Properties panel. b. On the secondary site Unity node's Properties panel, click the Replicate button at the top of the panel. c. Click the node representing the storage pool that contains the data you want to import, and expand its Properties panel. d. On the storage pool node's Properties panel, click the Import Data button at the top of the panel.

This starts the Import Data utility.

► **To import data from the remote site:**

1. Select the **Replicate data to the primary site** option. The Import Data utility retrieves the list of shares from the corresponding storage pool on the primary Unity and displays them in the grid; only those shares/LUNs that have replication enabled on the primary site are displayed in the grid.
2. In the grid, click the check box corresponding to the dataset(s) that you want to import.
You can search for a specific dataset by entering its name in the text box above the **Name** column heading. The grid automatically filters the list as you type.
If you want to import data from all the dataset in the storage pool, click the **All** check box.
3. Click **Calculate** to display the disk space required on the secondary site to replicate the selected datasets.
4. Click the **Import** button.

The progress of the data import is displayed in the Tasks in progress panel.

Importing data from a USB storage device

This section explains how to import data from a USB storage device to a storage pool's replica on the remote site.

To perform this operation, you must have previously replicated data to the USB storage device from the source storage pool on the primary Unity. You must also connect the USB storage device containing the data to one of the USB ports on the back of the *active* node; to determine which node is *active*, see [Viewing cluster health status and controller information](#) on page 300).

Unity automatically detects USB storage devices connected to the system, and assigns each device a unique device ID that includes the device's storage capacity; for example: **210 GB - c2t0d0**.

Unity provides the Import Data utility to guide you through the process of performing an offline replication.

► **To import data from a USB storage device on the remote site:**

1. Start the Import Data Utility; see the steps in [Importing data from the primary Unity](#) on page 444
2. Select the **Export data from:** option.
3. Select the USB storage device from the drop-down list. The USB storage device must be connected to one of the USB ports on the controller where the storage pool, that you want to import data from, is hosted.

If the USB storage device is not displayed in the drop-down list, make sure the device is connected properly, and if applicable, powered on; then, click the refresh icon next to the drop-down list to force a device discovery. The Import Data utility retrieves the list of shares on the USB storage device and displays them in the grid.

4. In the grid, click the check box corresponding to the dataset(s) that you want to import from the USB storage device.

You can search for a specific dataset by entering its name in the text box above the **Name** column heading. The grid automatically filters the list as you type.

If you want to import all the dataset on the USB storage device, click the **All** check box.

5. Click the **Import** button.

The progress of the data import is displayed in the Tasks in progress panel.

Configuring replication bandwidth settings for a storage pool

This feature allows you to configure and enable schedules to throttle network bandwidth usage for the replication stream during peak hours. This allows you to control bandwidth usage and prevents network congestion.

Before you can use this feature, asynchronous replication must be set up for the site; see [Setting up asynchronous data replication](#) on page 424.

This section covers these topics:

[Enabling bandwidth throttling](#) below

[Creating a bandwidth throttling schedule](#) on the facing page

[Modifying a bandwidth throttling schedule](#) on page 448

[Disabling a bandwidth throttling schedule](#) on page 449

[Deleting a bandwidth throttling schedule](#) on page 449

[Disabling bandwidth throttling](#) on page 450

Enabling bandwidth throttling

You can enable bandwidth throttling for the data network interface for the selected storage pool. Bandwidth throttling controls bandwidth usage on the data network interface configured on Unity and prevents network congestion during asynchronous data replication.

Before you can use this feature, asynchronous replication must be set up for the site; see [Setting up asynchronous data replication](#) on page 424.

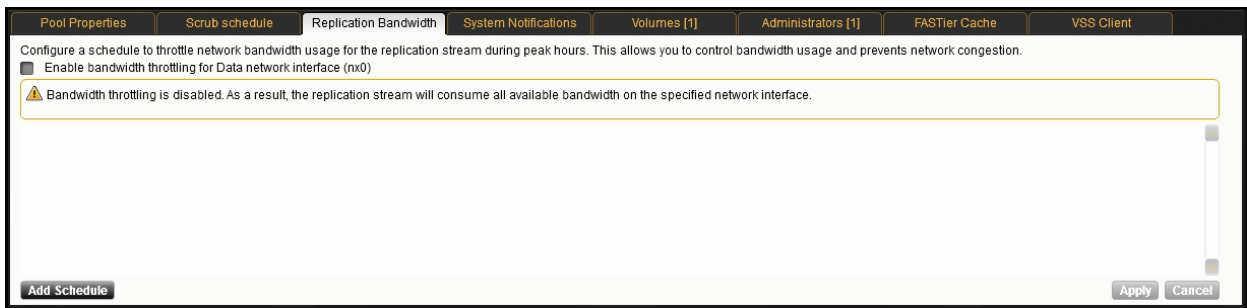
By default, the data network interface is `nx0`. You can select another network interface for the outgoing replication stream using the **Async Replication** tab under the **Site** node in Unity, as described in [Configuring network settings for Asynchronous Replication](#) on page 436.

You must enable bandwidth throttling to be able to create throttling schedules.

► **To enable bandwidth throttling:**

1. In Unity's tree view, click the Site node representing the site where the storage pool for which you want to enable bandwidth throttling is.
2. Click the **Storage Pools** node.
3. Click the applicable storage pool and expand its Properties panel.
4. Select the **Replication Bandwidth** tab.

Figure 12-15: Storage pool's properties panel—Replication Bandwidth tab



5. Check the **Enable bandwidth throttling for the Data network interface** option.
6. Click **Apply**.

► **What's next:**

You can now [create](#) a bandwidth throttling schedule.

Creating a bandwidth throttling schedule

This feature allows you to configure a schedule to throttle network bandwidth usage for the replication stream during peak hours. This allows you to control bandwidth usage and prevents network congestion.

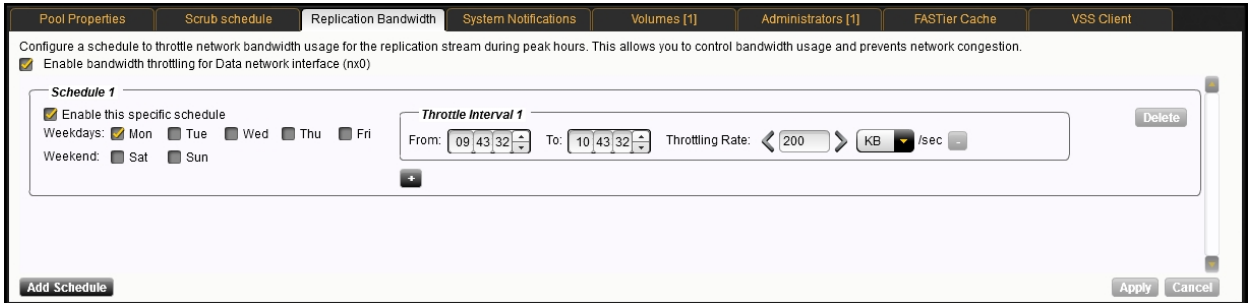
If you have a large amount of data to replicate, you can add a bandwidth throttling schedule that will run at the same time as your [replication schedule](#), in order to minimize network bandwidth congestion during data replication.

You can create multiple schedules and decide which ones to enable later, without having to recreate the schedules again. You can also have one schedule with several throttle intervals defined, with several intervals for the same day or for multiple days.

► **To add a specific schedule:**

1. You must first [enable bandwidth throttling](#) for the network interface.
2. **Schedule 1** becomes available and is enabled by default.

Figure 12-16: Storage pool's properties panel—Replication Bandwidth tab



3. Select one or more days to run this schedule.
As you create new schedules, you cannot use the same days selected in existing schedules, even if these schedules are not enabled. For example, if you configured *Schedule 1* to run on Mondays, you cannot select Monday for the subsequent schedules. The reverse is also true. For example, if you create a second schedule using Tuesday, you will notice that Tuesday is no longer available in *Schedule 1*.
4. Configure the throttle interval:
 - a. Select the **From** time by clicking in the hour text box and using the up and down arrows, or by typing the hours directly. Repeat this operation for the minutes and seconds.
 - b. Select the **To** time by clicking in the hour text box and using the up and down arrows, or by typing the hours directly. Repeat this operation for the minutes and seconds.
 - c. Configure the throttling rate in kilobytes or megabytes, per second. The minimum rate is 200 KB per second and the maximum rate is 1073741824 MB per second.
5. Optionally, add one or more throttle intervals to the schedule by clicking the + button and repeat step 4 for each interval.
6. Optionally, add one or more schedules by clicking the **Add Schedule** button, and repeat steps 3 and 4 for each schedule.
7. When you are done configuring schedules, click **Apply**.

Modifying a bandwidth throttling schedule

Bandwidth throttling schedules can be modified at any time.

► **To modify a specific schedule:**

1. In Unity's tree view, click the Site node representing the site where the storage pool for which you want to modify a bandwidth throttling schedule is.
2. Click the **Storage Pools** node.
3. Click the applicable storage pool and expand its Properties panel.
4. Select the **Replication Bandwidth** tab.

5. In the Schedule to modify, perform one or more of these actions:

To...	Do this
change the days during which the schedule will run	Remove or add specific days among the available days. If another schedule is using a day you would like to select, you need to remove that day from that schedule first.
change throttle intervals	<ol style="list-style-type: none"> Select the From time by clicking in the hour text box and using the up and down arrows, or by typing the hours directly. Repeat this operation for the minutes and seconds, as applicable. Select the To time by clicking in the hour text box and using the up and down arrows, or by typing the hours directly. Repeat this operation for the minutes and seconds, as applicable. Enter a new throttling rate in kilobytes or megabytes, per second. The minimum rate is 200 KB per second and the maximum rate is 1073741824 MB per second.
remove a throttle interval	Click the - button next to the throttle.
add a throttle interval	Click the + button and perform the steps to change throttle intervals.

6. When you are done modifying the schedule, click **Apply**.

Disabling a bandwidth throttling schedule

Bandwidth throttling schedules can be disabled at any time. Their configuration settings are saved, so if you decide to re-enable a schedule, it will automatically run again according to its configuration settings.

► **To disable a specific schedule:**

- In Unity's tree view, click the Site node representing the site where the storage pool for which you want to disable a bandwidth throttling schedule is.
- Click the **Storage Pools** node.
- Click the applicable storage pool and expand its Properties panel.
- Select the **Replication Bandwidth** tab.
- Clear the **Enable this specific schedule** option for the selected schedule.
- Click **Apply**.

Deleting a bandwidth throttling schedule

You can delete bandwidth throttling schedules at any time, whether they are enabled or not.

► **To delete a schedule:**

- In Unity's tree view, click the Site node representing the site where the storage pool for which you want to delete a bandwidth throttling schedule is.
- Click the **Storage Pools** node.
- Click the applicable storage pool and expand its Properties panel.
- Select the **Replication Bandwidth** tab.

5. Click the **Delete** button next to the schedule. The schedule disappears from the **Replication Bandwidth** tab.
6. Click **Apply**.

Disabling bandwidth throttling

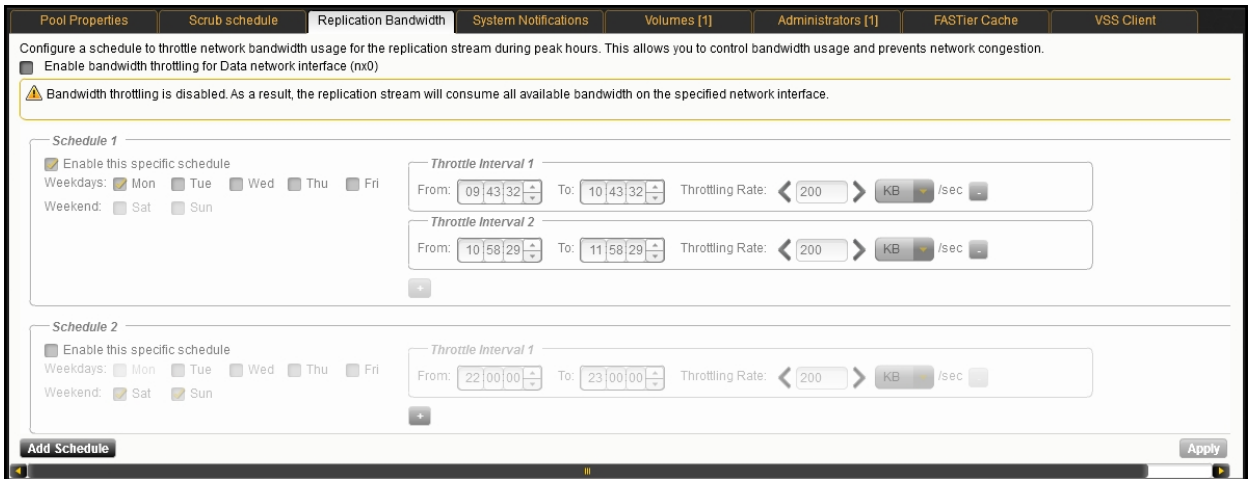
When you disable bandwidth throttling for a storage pool, all enabled schedules will stop running. Data replication will use the full network bandwidth.

Since the schedules are saved, if you decide to re-enable bandwidth throttling, the schedules will revert back to their original state, which means the schedules that were enabled will automatically run again, according to their configuration settings.

► **To disable bandwidth throttling:**

1. In Unity's tree view, click the Site node representing the site where the storage pool for which you want to disable bandwidth throttling is.
2. Click the **Storage Pools** node.
3. Click the applicable storage pool and expand its Properties panel.
4. Select the **Replication Bandwidth** tab.
5. Clear the **Enable bandwidth throttling for the Data network interface** option.
6. Click **Apply**.

Figure 12-17: Storage pool's properties panel—Replication Bandwidth tab



Failing over to the remote site for disaster recovery

Unity data replication function provides a failover mechanism for your Unity deployment that allows you to gracefully failover all your data and system operations on the primary Unity to the corresponding remote Unity (s).

This section includes these topics:

Failover vs. promote.....	451
Performing a failover of the entire site.....	452
Performing a failover of a storage pool.....	453
Promoting the remote site.....	454
Promoting a storage pool's replica.....	454

Demoting a site	455
Demoting a storage pool	456
Managing file system replication conflicts	457

Failover vs. promote

This table identifies the scenarios in which you should use the failover and promote functions, and it also describes what each function entails:

Function	When to use it...	What it does...
Failover	<ul style="list-style-type: none"> System maintenance on the primary system, including hardware component upgrade or replacement Imminent system failure Data migration Load balancing 	<p>When you start the failover function, it first performs an incremental replication to update the data on the remote site. It then promotes the remote site to primary status in your deployment, and demotes the primary site to secondary status.</p> <p>If you only failover a storage pool, or a subset of pools on the primary site, the failover function promotes the storage pool's replica on the remote site to primary status, and demotes the storage pool on the primary site to secondary status.</p> <p>After the failover completes, all storage pools that you failed over and their datasets are now accessible on the remote site.</p> <p>If the primary site has only one storage pool, failing over the storage pool has the same result as failing over the entire site.</p> <p>Note Only datasets that have replication enabled are failed over to the remote site. Datasets that do not have replication enabled remain on the primary site.</p>
Promote	<ul style="list-style-type: none"> Complete system failure on the primary site (primary system is non-responsive) 	<p>When you promote the remote site, the promote function changes the status of the secondary site to primary. The promote function does not replicate data from the primary system to the remote site.</p> <p>If you only promote a storage pool, or a subset of pools on the remote site, the promote function changes the status of the secondary storage pool to primary.</p> <p>After the promote completes, all storage pools that you promoted and their datasets are now accessible on the remote system.</p> <p>If the remote site has only one storage pool, promoting the storage pool to primary status has the same result as promoting the entire site.</p> <p>Note Only datasets that are replicated to the remote system are available after a promotion.</p> <p>When you restore the primary site, your deployment will have 2 primary systems or storage pools; you must then <i>demote</i> one of the systems or pools to secondary status.</p>

Site failover vs. pool failover

The failover functionality allows you to failover a single storage pool, or only a subset of the storage pools, to the corresponding remote site(s). Alternately, you can failover the entire site to the remote site(s). Pool or Site failover of a pool that has a compressed dataset is supported.

For example, on a primary Unity—Site A—with two storage pools, Pool 1 and Pool 2:

- Pool 1 is replicated to secondary site B
- Pool 2 is replicated to secondary site C

You can:

1. failover each pool separately to its corresponding remote site;
2. failover the entire site. Each storage pool is failed over to the remote site where the pool is replicated

Similarly, if both Pool 1 and Pool 2 on Site A are replicated to the same remote site, Site B, you can:

1. failover each pool separately to Site B;
2. failover the entire site. Both storage pools are failed over to Site B.

On a system with only one storage pool, failing over the storage pool has the same result as failing over the entire site.

Performing a failover of the entire site

This section describes the process for performing a [failover](#) of a primary Unity to the corresponding remote site(s) where the storage pool(s) from the primary site are replicated.



CAUTION: The failover process can take from several minutes to several hours, depending on the number of datasets and the amount of data to transition to the replicated site. During this time, all LUNs to be transitioned will be inaccessible and shares will be accessible in read-only mode. In addition, you will be unable to perform any other operation in Nexsan Unity. You can expedite the process by performing a [manual replication](#) prior to failing over.

Note Datasets that do not have replication enabled remain on the primary site, and are only accessible from that site.



CAUTION: Both the primary and remote sites are unavailable during the failover process. To prevent data loss, close any applications that access data on the primary site and also terminate any active connections to the system.

▶ **To failover the primary site to the remote site(s):**

1. In Unity's tree view, click the Site node representing the primary Unity.
2. Perform one of these actions:
 - Click the context menu button on the Site node to open the node context menu. Select **Failover Site**.
 - Open the Site nodes Properties panel, and then click the **Failover Site** button at the top of the panel.
3. Unity prompts you to confirm the action. Click **Yes** to continue.

Unity starts the failover process. If the primary system has multiple storage pools replicated to different remote sites, the failover function fails over each pool to its corresponding remote site.

In Unity's tree view on the remote site, Unity moves all replicated storage pools from under the **Incoming Replications** node to the **Storage Pools** node. On the primary site, Unity moves the replicated pools from under the **Storage Pools** node to the **Incoming Replications** node. Any dataset that was not included in the replication remains under the **Storage Pools** node on the primary site.

If the failover of the primary site is unsuccessful, you will be prompted to retry the failover or cancel it. Click **Retry** to try the failover again or **Cancel** to abort the failover. If you retried the failover and it is still unsuccessful, you can either:

- fail over the storage pools on the primary site individually, or
- promote the remote site, or
- promote the storage pools on the remote site individually.

► **What's next:**

You will need to update all relevant DNS mappings on the DNS server. This will allow your users and applications to access their data without the need to remap their connections to the datasets on Unity.

Performing a failover of a storage pool

This section describes the process for performing a [failover](#) of a storage pool from the primary Unity to the corresponding remote site where the storage pool is replicated.

If you fail over a storage pool the failover function promotes the storage pool's replica on the remote site to primary status, and demotes the storage pool on the primary site to secondary status.

Datasets that do not have replication enabled remain on the primary site, and are only accessible from that site.

Note You cannot perform a failover of a storage pool if the pool is in a degraded state.

► **To start the failover process:**

1. In Unity's tree view, click the Site node representing the primary Unity.
2. Click the **Storage Pools** node.
3. Perform of these actions:

To...	Do this
use the Storage Pools node	<ol style="list-style-type: none"> a. Expand the Storage Pools node's Properties panel. b. Select the storage pool that you want to fail over to its corresponding secondary site.
use the storage pool's node context menu	<ol style="list-style-type: none"> a. Click the node representing the storage pool that you want to fail over to its corresponding secondary site. b. Click the context menu button on the node to open the node context menu.
use the storage pool's Properties panel	<ol style="list-style-type: none"> a. Click the node representing the storage pool that you want to fail over to its corresponding secondary site b. Expand its Properties panel.

4. Click **Failover Pool**.
5. Once the failover process starts, Unity prompts you to confirm the action. Click **Yes** to continue.

In Unity's tree view on the remote site, Unity moves the storage pool that you failed over from under the **Incoming Replications** node to the **Storage Pools** node. On the primary site, Unity moves the storage pool from under the **Storage Pools** node to the **Incoming Replications** node. Any dataset that was not included in the replication remains under the **Storage Pools** node on the primary site.

► **What's next:**

You will need to update all relevant DNS mappings on the DNS server. This will allow your users and applications to access their data without the need to remap their connections to the datasets on Unity.

Promoting the remote site

This section describes the process for [promoting](#) the remote site. To promote a storage pool on the remote site, see [Promoting a storage pool's replica](#) below.

Note The promote function is only available on the remote site in the event of a complete system failure on the primary site—where the primary system (or a source storage pool on the primary site) becomes non-responsive.

When you promote the remote site, or a storage pool on the remoter site, it takes over system operations using the most recently replicated data. Once you restore the primary site, you must then *demote* the remote site back to secondary status, as only one primary system, or storage pool, should exist in your Unity deployment. For more information, see [Demoting a site](#) on the facing page.

Note Datasets that do not have replication enabled remain on the primary site, and are only accessible from that site.



CAUTION: The remote site is unavailable during the promote process. To prevent data loss, close any applications that access data on the system and also terminate any active connections to the system.

► **To promote the remote Unity to primary status:**

1. In Unity's tree view, click the Site node representing the remote site.
2. Perform one of these actions:

To...	Do this
use the Site's node context menu	<ol style="list-style-type: none"> a. Click the context menu button on the Site node. b. Select Promote Site.
use the Site's Properties panel	<ol style="list-style-type: none"> a. Expand its Properties panel. b. Click the Promote Site button at the top of the panel.

3. Unity prompts you to confirm the action. Click **Yes** to continue.

In Unity's tree view on the remote site, Unity moves all storage pools from under the **Incoming Replications** node to the **Storage Pools** node. Any dataset that was not included in the replication, remains on the primary system.

► **What's next:**

You will need to update all relevant DNS mappings on the DNS server. This will allow your users and applications to access their data without the need to remap their connections to the datasets on Unity.

Promoting a storage pool's replica

This section describes the process for [promoting](#) a storage pool's replica on the remote site to primary status in your Unity deployment.

Once you restore the primary storage pool, you must then *demote* the storage pool's replica back to secondary status, as only one primary copy of a storage pool can exist in your Unity deployment. For more information, see [Demoting a storage pool](#) on the next page.

Note Datasets that do not have replication enabled remain on the primary site, and are only accessible from that site.



The remote site is unavailable during the promote process. To prevent data loss, close any applications that access data on the system and also terminate any active connections to the system.

► **To promote the storage pool's replica:**

1. In Unity's tree view, click the Site node representing the remote site.
2. Click the **Incoming Replications** node.
3. Click the site node corresponding to the site where the source storage pool for the replica that you want to promote exists.
4. Click the **Storage Pools** node.
5. Perform one of these actions:

To...	Do this
use the Storage Pools node	<ol style="list-style-type: none"> a. Expand the Storage Pools node's Properties panel. b. Select the storage pool that you want to fail over to its corresponding secondary site.
use the storage pool's node context menu	<ol style="list-style-type: none"> a. Click the node representing the storage pool that you want to fail over to its corresponding secondary site, b. Click the context menu button on the node.
use the storage pool's Properties panel	<ol style="list-style-type: none"> a. Click the node representing the storage pool that you want to fail over to its corresponding secondary site, b. Expand its Properties panel.

6. Click **Promote Pool**.

In Unity's tree view on the remote site, Unity moves the storage pool that you promoted from under the **Incoming Replications** node to the **Storage Pools** node. Any dataset that was not included in the replication remains on the primary site.

► **What's next:**

You will need to update all relevant DNS mappings on the DNS server. This will allow your users and applications to access their data without the need to remap their connections to the datasets on Unity.

Demoting a site

This section explains how to demote a site in your Unity deployment. To demote a storage pool, see [Demoting a storage pool](#) on the next page.

This function is only available if you previously promoted a site, and you now have two primary sites in your Unity deployment.

The demote process transitions a primary site to secondary status. The demote function makes the corresponding Unity a remote site in your deployment. The demote function rolls back each share/LUN on Unity site that you are demoting to its previous replication baseline.

Before rolling back, the demote function compares the current contents of each share with its replication baseline. If it finds any differences—new data was added, removed, or updated in the share—the demote function takes a snapshot of the share and preserves the snapshot in a *difference* share on the site that you are demoting (this is known as Replication Conflicts in Unity).

The demote function also creates a text file with the *.diff* extension that it saves in each corresponding *difference* share on the system. The *.diff* file lists the changes between the *difference* share and the replication baseline that the demote function rolls the share back to during the demote process. For more information, see [Managing file system replication conflicts](#) on the facing page.

Note The Replication Conflicts function is only available for shares. Because of the nature of block-level storage, this mechanism is not available for LUNs.



CAUTION: The site is unavailable during the demote process. To prevent data loss, close any applications that access data on the system and also terminate any active connections to the system.

► **To demote a site:**

1. In Unity's tree view, click the Site node representing Unity site that you want to demote.
2. Perform one of these actions:

To...	Do this
use the Site's node context menu	<ol style="list-style-type: none"> a. Click the context menu button on the Site node. b. Select Demote Site.
use the Site's Properties panel	<ol style="list-style-type: none"> a. Expand its Properties panel. b. Click the Demote Site button at the top of the panel.

3. Unity prompts you to confirm the action. Click **Yes** to continue.

After the demote process completes, the demoted site and all its storage pools become secondary in your deployment. In Unity's tree view on the demoted system, Unity moves all storage pools from under the **Storage Pools** node to the **Incoming Replications** node.

► **What's next:**

- Update all relevant DNS mappings on the DNS server. This will allow your users and applications to access their data without the need to remap their connections to the datasets on Unity.
- Verify the **Replication Conflicts** tab for each share on the demoted system to see the differences in share contents, if any. For information, see [Managing file system replication conflicts](#) on the facing page.

Demoting a storage pool

This section explains how to demote a storage pool in your Unity deployment. When you demote a storage pool, the demote function makes the storage pool a secondary pool in your deployment. This essentially makes the storage pool a replica of its corresponding source storage pool.

This function is only available if the source, or primary, storage pool and its target, or remote, storage pool are currently both primary storage pools in your deployment.



CAUTION: The site is unavailable during the demote process. To prevent data loss, close any applications that access data on the system and also terminate any active connections to the system.

► **To demote a storage pool:**

1. In Unity's tree view, click the Site node for the site that contains the storage pool you want to demote; this displays the site's child nodes.
2. Click the **Storage Pools** node.
3. Perform one of these actions:

To...	Do this
use the Storage Pools node	<ol style="list-style-type: none"> a. Expand the Storage Pools node's Properties panel. b. Select the storage pool that you want to demote.
use the storage pool's node context menu	<ol style="list-style-type: none"> a. Click the node representing the storage pool that you want to fail over to its corresponding secondary site. b. Click the context menu button on the node.
use the storage pool's Properties panel	<ol style="list-style-type: none"> a. Click the node representing the storage pool that you want to demote. b. Expand its Properties panel.

4. Click **Demote Pool**.

In Unity's tree view on the demoted system, Unity moves the demoted storage pool from under the **Storage Pools** node to the **Incoming Replications** node.

► **What's next:**

- Update all relevant DNS mappings on the DNS server. This will allow your users and applications to access their data without the need to remap their connections to the datasets on Unity.
- Verify the **Replication Conflicts** tab for each share in the demoted storage pool to see the differences in share contents, if any. For information, see [Managing file system replication conflicts](#) below.

Managing file system replication conflicts

The **Replication Conflicts** function is only available for file systems. Because of the nature of block-level storage, this mechanism is not available for LUNs.

During the demote process, the demote function rolls back each file system on Unity site that you are demoting to its previous replication baseline. Before rolling back, the demote function compares the current contents of each file system with its replication baseline; if it finds any differences—data was added, removed, or updated in the file system—the demote function takes a snapshot of the file system and preserves the snapshot in a *difference* file system on the site that you are demoting (this is known as a Replication Conflict in Unity).

The demote function also creates a text file with the *.diff* extension that it saves in each corresponding *difference* file system on the site. The *.diff* file lists the changes between the *difference* file system and the replication baseline that the demote function rolls the file system back to during the demote process. You can later access the *difference* file system from a Windows-based (CIFS) system and/or a UNIX/Linux-based

(NFS) system and browse its contents—in the same way that you access a file system or a snapshot for which you enable browsing; you can also then view the contents of the *.diff* file.

Once you enable browsing for a *difference* file system, you can consult its *.diff* file, and if needed, recover individual files from the *difference* file system and add/update the files in the parent file system on the primary site. Unity maintains all of the parent file system's access-level attributes with its *difference* file systems to ensure any recovery is authorized. This means that you can safely authorize all users—that have access to the parent file system—to browse one of its *difference* file systems and recover their own data.

Note A *difference* file system is a read-only copy of its parent file system.

This section includes these steps:

Viewing a file system's replication conflicts.....	458
Enabling browsing for a difference share.....	460
Disabling browsing for a difference file system.....	461
Viewing the contents of a <i>.diff</i> file.....	462
Deleting a share's replication conflict.....	462

Viewing a file system's replication conflicts

This section explains how to view a file system's replication conflicts on a demoted Unity:

► **To view a file system's replication conflicts:**

1. In Unity's tree view, click the Site node representing Unity that you previously demoted to secondary status.
2. Click the **Incoming Replications** node.
3. If you have multiple incoming replications to this secondary site, click the Site node representing the site where the file system that you want to view replication conflicts for exists.
4. Click the storage pool that contains the file system you want to view replication conflicts.
5. Click the node representing the relevant file system, and expand its Properties panel

6. Select the **Replication Conflicts** tab.

The grid shows this information for each *difference* file system:

- **Browsing status:** this column indicates whether or not browsing is enabled for the *difference* file system; it displays one of these icons:



Browsing is enabled



Browsing is disabled

- **Name:** this column displays the *difference* file system's name assigned to it by Unity; the name includes the parent file system's name followed by the underscore character (`_`) and a value representing the increment count for the file system; for example, **payrolldata2_0** indicates that this is the *difference* file system for the **payrolldata2** file system, and it is the first *difference* file system currently on the system for **payrolldata2**.
- **Change count:** this column identifies the number of differences, or replication conflicts, for the parent file system; for example; if you added 4 new files to the file system between the time that it was a member of a primary site, or storage pool, and when you demoted the file system to secondary status, the change count displays **4**.
- **Creation date:** this column displays the date and time the *difference* file system was created.
- **Diff file name:** this column displays the name of the `.diff` file for the *difference* file system; the `.diff` file's name includes the file's creation date and a unique ID assigned to it by Unity.

Unity converts the date and time to local format; that is, the date and time on the system where Unity is currently running.

You can sort the list of *difference* file systems displayed in the grid in either ascending or descending (alphabetical) order by clicking the sort pointer in the **Name** column heading:



▶ **To sort the list in descending order:**

- Click the sort pointer until the arrow points down.

▶ **To sort the list in ascending order:**

- Click the sort pointer until the arrow points up.

You can also sort by **Browsing status**, **Change count**, **Creation date**, and **Diff file name**; or a combination of **Name**, **Browsing status**, **Change count**, **Creation date**, and **Diff file name**, in any particular sort order that you want: 1, 2, and 3.

For example, to sort by **Creation date** first, and **Name** second:

1. Click the sort pointer in the **Creation date** column heading until **1** is displayed (with the arrow pointing either up for ascending order, or down for descending order).
2. Click the sort pointer in the **Name** column heading until **2** is displayed (with the arrow pointing either up for ascending order, or down for descending order).

▶ **To filter the list:**

You can filter the *difference* file systems displayed in the grid by **Name**, **Browsing status**, **Change count**, **Creation date**, and **Diff file name**, and you can also filter the *difference* file system to only display *difference* file system created within a specific time period.

To...	Do this
only display <i>difference</i> file system created within a specific time period	<ol style="list-style-type: none"> Open the drop down list above the Creation date column. Select This Hour, Today, Yesterday, This Week, This Month, This Year, or Custom. If you select Custom, you must select a From and To date in the popup that display. <div style="border: 1px solid #ccc; padding: 2px; display: inline-block;">From <input type="text" value="2011/06/07"/> To <input type="text" value="2011/06/08"/> </div> Click the To date field, and select an end date for the time period.
only display <i>difference</i> file systems with a specific Browsing status	<ol style="list-style-type: none"> Open the drop-down list above the Browsing status column heading in the grid. Select the browsing status (Browsing enabled or Browsing disabled) that you want to display snapshots for in the grid. The default filter setting is All.
only display <i>difference</i> file systems with a specific change count	Enter a value in the text box above the Change count column.

Tip To reset filter settings in the grid, click another node in Unity's tree view and then return to the Replication Conflicts Properties panel by clicking the corresponding share node. All filter options in the grid revert to their default settings.

► **To search for a specific *difference* file system in the grid:**

- Type a search string in the text boxes above the **Name, Creation date, or Diff file name** column headings.

For example, if you want to search for all *difference* file systems that have the current date in the diff file name, type the date value in the text box above the **Diff file name** column heading.

Enabling browsing for a difference share

This section explains how to enable browsing for a share's *difference* share.

► **To enable browsing for a *difference* share:**

- In Unity's tree view, click the Site node representing Unity the that you previously demoted to secondary status.
- Click the **Incoming Replications** node.
- If you have multiple incoming replications to this remote Unity, click the Site node representing the site where the share containing the *difference* share that you want to enable browsing for exists.
- Click the storage pool where the share containing the *difference* share that you want to enable browsing for exists.
- Click the node representing the corresponding share, and expand its Properties panel.

6. Highlight the *difference* share that you want enable browsing for by selecting the *difference* share in the grid.
7. Click the **Browse** button. Unity displays the Browse Difference File System dialog box where you specify the sharing method for the *difference* share.
8. Select the sharing method that you want to use to expose the *difference* share to client computers on the network:

Note To enable the Read-only anonymous access options, you must first select either the CIFS sharing, NFS sharing, or both the CIFS and NFS sharing options.

To...	Do this
expose the <i>difference</i> share to Windows-based systems over the CIFS protocol	Select the Use the CIFS protocol to make this share accessible from Windows-based systems option.
expose the <i>difference</i> share to UNIX/Linux-based systems over the NFS protocol	Select the Use the NFS protocol to make this share accessible from UNIX/Linux-based systems option.
expose the <i>difference</i> share to both Windows and UNIX/Linux-based systems (mixed-mode operation)	Select both the CIFS and NFS options.
gives all users on the network Read access to the <i>difference</i> share, including the ability to display and traverse folders and read the contents of files in the <i>difference</i> share	Select the Give everyone on the network Read-access to the share (Read-only anonymous access) option.

9. Click **Apply** to save your settings and close the Browse Difference File System dialog box.

Once Unity completes this process, the **Browsing status** column in the grid displays the browsing enabled icon for the *difference* share.

Depending on the sharing method you configure for the *difference* share, you can now access the *difference* share in the same way that you access a share. For more information, see .

When you select a *difference* share that has browsing enabled in the grid, the **Browse** button changes to **Stop browsing**.

Disabling browsing for a difference file system

This section explains how to disable browsing for a file system's *difference* file system.

► **To disable browsing for a file system's *difference* file system:**

1. In Unity's tree view, click the Site node representing Unity site that you previously demoted to secondary status.
2. Click the **Incoming Replications** node.
3. If you have multiple incoming replications to this secondary Unity, click the Site node representing the site where the file system containing the *difference* file system that you want to disable browsing for exists.

4. Click the storage pool where the file system containing the *difference* file system that you want to disable browsing for exists.
5. Click the node representing the corresponding share, and expand its Properties panel.
6. Highlight the *difference* file system that you want disable browsing for by selecting the *difference* file system in the grid.
7. Click the **Stop browsing** button.

The **Stop browsing** button is only displayed if you select a *difference* file system in the grid that has browsing enabled.

Once Unity completes this process, the **Browsing status** column in the grid displays the browsing disabled icon for the *difference* file system.

Viewing the contents of a .diff file

Once you enable browsing for a *difference* file system, you can open the *.diff* file contained in the *difference* file system to view the changes between the *difference* file system and the replication baseline that the demote operation rolled its parent file system back to during the demote process.

The *.diff* file is a basic text file that you can open in any text editor. It identifies each object (file, folder, or permission setting) that changed in the file system before the demote operation, including how the object changed; for example, if you remove the **payrolldata2.dat** file from the file system before the demote operation, the *.diff* file includes this information:

```
- / payrolldata2.dat
```

► To view the contents of a .diff file:

1. Enable browsing for the *difference* file system that contains the *.diff* file you want to view; see [Enabling browsing for a difference share](#) on page 460.
2. Depending on the sharing method you selected for the *difference* file system, access the *difference* file system from a Windows-based (CIFS) system and/or a UNIX/Linux-based (NFS) system and browse its contents.
3. Locate the *.diff* file contained in the *difference* file system.
4. Open the file in a text editor, such as Microsoft WordPad, to view its contents.

Deleting a share's replication conflict



CAUTION: When you delete a replication conflict, you also delete its *difference* file system, and the *.diff* file contained in the *difference* file system. This operation cannot be undone.

► To delete a file system's replication conflict:

1. In Unity's tree view, click the Site node representing Unity that you previously demoted to secondary status.
2. Click the **Incoming Replications** node.
3. If you have multiple incoming replications to this secondary Unity, click the Site node representing the site where the file system containing the *difference* file system that you want to delete exists.

4. Click the storage pool where the file system containing the *difference* file system that you want to delete exists.
5. Click the node representing the corresponding file system, and expand its Properties panel.
6. Highlight the *difference* file system that you want delete by selecting the *difference* file system in the grid.
7. Click the **Delete** button.
8. Unity prompts you to confirm the action. Click **Yes** to delete the replication conflict.

Removing asynchronous data replication for a storage pool

This process terminates replication for a storage pool. You may want to remove asynchronous data replication for a storage pool to (temporarily or permanently) migrate the data on the primary system to the remote system, or for load balancing, where each system manages a specific set of storage pools in your deployment.



CAUTION: The remove operation does not replicate data before terminating asynchronous replication between the primary storage pool and its replica. Prior to terminating asynchronous data replication for a storage pool, perform a manual data replication to the pool's replica. This ensures that the replica contains the most recent data when the remove operation promotes it to primary status. For more information, see [Performing an offline replication on page 442](#).

When removing asynchronous replication, you can choose to promote or delete the storage pool's replica:

- Promoting the replica on the remote site makes it a primary storage pool in your deployment. Your deployment will then have two primary storage pools containing exactly the same data.
- Deleting the replica will keep data on the primary storage pool only.



CAUTION: If you [promote the replica](#) first and THEN remove asynchronous data replication, deleting the replica deletes the former primary pool. All datasets belonging to the replica (former primary pool) will be deleted. Any LUNs or shares in the replica that were NOT previously replicated to the remote site will be deleted, resulting in data loss.

▶ **To terminate asynchronous data replication for a storage pool:**

1. In Unity's tree view, click the Site node representing the primary site.
2. Click the **Storage Pools** node.
3. Click the node representing the storage pool for which you want to terminate asynchronous data replication. The storage pool you select must have asynchronous data replication configured.
4. Click its **Replications** node.
5. Click the node representing the remote Unity, and expand its Properties panel.
6. Perform one of these actions:
 - Click the **Remove** button on the Properties panel, or
 - Click the context menu button on the remote site node and select **Remove**.

7. Unity displays a pop-up asking you whether you want to promote or delete the replica.

Figure 12-18: Removing asynchronous replication



- Select **Promote replica** to promote the replica to be a primary pool.
 - Select **Delete replica** to remove the replicated pool from the remote Unity.
8. Type **Yes** where indicated to confirm the action, then click the **Yes** button.
 9. If you chose to promote the replica, another pop-up displays to ask you to provide new names for the replica and any replicated datasets. Enter the names and click **OK**.

Synchronous data replication

Use the synchronous data replication feature to simultaneously replicate a storage pool between two Nexsan E-Series storage systems that are connected in a standard fashion to one Nexsan Unity Storage System. The feature mirrors all the data contained in a storage pool between a *source* and a *target* Unity Storage System—both of which are connected to Nexsan E-Series storage expansions via SAS (or Fibre Channel). You can also use synchronous data replication to migrate data when upgrading hardware or re-balancing storage. You designate the storage system to use as the *source*—that is, the system on which you create the storage pool and store your data—and the *target*, where the source data is mirrored.

If either the source or target system fails for any reason, your users and applications can continue to access their data on the storage system that is currently online. When you restore the second system, Unity automatically reestablishes the synchronous link between the two systems.

In addition, you can later promote the mirror (storage pool) on the target system to an independent storage pool in your Unity deployment. Promoting the mirror (storage pool) severs the synchronous link between the source and mirror, and creates a second, independent copy of the storage pool—with both copies containing exactly the same data.

This feature enables you to create an exact copy of your production data for testing and validation, or to migrate data when upgrading hardware or re-balancing storage.

Note Synchronous data replication is available ONLY:

- from the Unity classic interface and `nxcmd` command-line interface.
- for systems configured with the appropriate hardware.

► To configure Synchronous data replication:

- Using the Unity classic interface, click the **Site node**, then the **Synchronous** tab, or
- Using the `nxcmd` command-line interface, for command information enter

```
nxcmd syncreplication
```

For detailed instructions, see

- [Setting up synchronous data replication for a storage pool](#) on the next page
- "SyncReplication" in the *nxcmd Command-Line Interface Reference Guide*.

This section includes these topics:

[Before you begin](#) on the next page

[Setting up synchronous data replication for a storage pool](#) on the next page

[Promoting the mirrored storage pool](#) on page 470

[Removing synchronous replication for a storage pool](#) on page 471

Synchronous data replication features

The synchronous data replication function includes these features:

- **Zero data loss and downtime:** the synchronous data replication function ensures that the data on Unity is always current. If the source E-Series system experiences a disruption in operation, client access to data on Unity automatically reverts to the target, or mirror, E-Series system. When you restore access to the source E-Series system, the synchronous data replication function synchronizes the source system's data with the target system, thereby ensuring that both the source and target E-Series systems contain accurate and consistent data at all times.

- **Mirror promotion to create a current and accurate copy of production data for non-disruptive testing:** the synchronous data replication feature allows you to promote the mirrored storage pool on the target E-Series system to an independent pool in your Unity deployment. The promote process terminates synchronous replication between the source and target E-Series systems, and creates two independent storage pools containing identical copies of your data. You can then use the copy for testing and validation.

Usage implementations

You can use synchronous data replication for:

- **Data backup for disaster recovery:** in environments where tape backups are not feasible (for example, where the available bandwidth is insufficient or because the latency for recovery is too high), you can use the synchronous data replication function as a backup solution to mirror the data between a source and target Nexsan E-Series system. Once the mirror is created and the data between the source and target E-Series systems is synchronized, you can terminate synchronous replication and move the target system off site for disaster recovery.
- **Testing on non-production E-Series systems:** you can use the synchronous data replication function to create an exact copy of production data for testing and validation. You simply mirror production data from a source Nexsan E-Series system to a target Nexsan E-Series system. Once the mirror is created and the data between the source and target E-Series systems is synchronized, you can promote the mirror storage pool, which terminates the link between the source and the target, and then perform any tests with the copy of your production data.
- **Data migration:** you can use the synchronous data replication function to migrate data from one E-Series system to another when upgrading hardware or re-balancing storage.

Before you begin

Before you set up synchronous data replication for a storage pool, consider these points:

- You must have two Nexsan E-Series systems connected to Unity via SAS (or Fibre Channel); both systems must also be configured with Unity and allocated to the site.
- The target system, where the storage pool from the source system will be mirrored, must have a matching set of volumes, both in quantity and size, to match the volumes on the source system. For synchronous data replication, Unity requires one-to-one volume matching between the source and the target. This means that for every volume you allocate to the source storage pool, there must be a volume of equal or greater size on the target system.
- You must have, at least, one storage pool configured on the source E-Series system.
- Consider future capacity requirements on both the source and target E-Series systems. Specifically, if you allocate more volumes to the storage pool on the source system, you must likewise increase storage capacity on the target system.

Setting up synchronous data replication for a storage pool

Before you begin the data replication setup process, you must have, at least, one storage pool defined on the source storage system connected to Unity. Replication of compressed pools is also supported.

Note A storage pool can have both asynchronous and synchronous data replication configured for it. For more information about asynchronous data replication, see [Setting up asynchronous data replication on page 424](#).

▶ **To start the Synchronous Data Replication Setup Wizard:**

1. In Unity's tree view, under the site node, click the Storage Pool node to select it.
2. Click the node corresponding to the storage pool that you want to set up synchronous data replication for.

- 3. Click the **Replications** node.
- 4. Click the **Properties** tab to expand the Replications Properties panel.
- 5. Select **Add Synchronous**.

The **Add Synchronous** option is only available if you have Nexsan storage systems connected to Unity via SAS; both systems must also be configured with Unity and allocated to the site.

The Synchronous Data Replication Setup Wizard starts. The wizard includes 3 steps that you must complete in the order presented to successfully set up data replication.

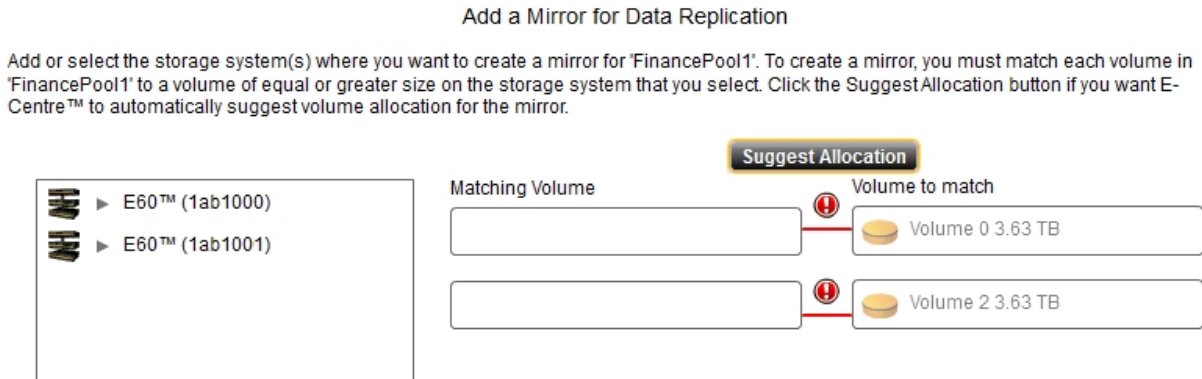
This section includes these steps:

- Step 1: Add mirror volumes468
- Step 2: Verifying settings.....469
- Step 3: Viewing configuration results.....470

Step 1: Add mirror volumes

In *step 1* of the Synchronous Data Replication Wizard, you designate the target storage system where you want Unity to mirror the storage pool on the source system, and you also select the volumes on the target storage system to allocate to the mirror.

Figure 12-19: Synchronous Data Replication Setup Wizard, step 1: select mirror volumes



Step 1 of the Synchronous Data Replication Wizard displays a list box containing the Nexsan storage systems connected to Unity via SAS (or Fibre Channel). You can expand each storage system to display its available volumes; to expand a storage system and display its volumes: click the arrow preceding the device name.

On the far right of panel, under **Volume to match**, the Synchronous Data Replication Wizard displays the volumes on the source storage system that are currently allocated to the storage pool. Under **Matching volume**, the Synchronous Data Replication Wizard displays the volumes that you allocate to the storage pool's mirror on the target storage system. As you match volumes between the target and the source storage systems, by either dragging the volumes from the storage systems list box to the volume boxes under **Matching volume**, or by allowing Unity to automatically suggest suitable volume allocations for the mirror, the **Xs** between the volume boxes change to check marks—if a suitable volume is matched.

There are two ways to allocate volumes on the target storage system to the storage pool's mirror:

- Manually allocate volumes
- Allow Unity to suggest volume allocation (*recommended*)

► To manually allocate volumes on the target storage system to the storage pool's mirror:

1. In the list box on the left-hand side of the panel, highlight the target storage system—where the volume(s) that you want to allocate to the storage pool's mirror exists—by selecting the storage system in the list.
2. Expand the target storage system to display its available volumes, by clicking the arrow preceding the device name.
3. Match each volume on the source storage system with a volume on the target system by dragging individual volumes from the target storage system in the list box to a corresponding box under **Matching volume**. A check mark appears between volumes as you match them.

The size (disk space) of the volume(s) that you select must be equal to or greater than the volume(s) that you allocated to the storage pool on the source storage system. For example, if you allocated two 5 TB volumes to the storage pool on the source system, then you must also allocate two 5 TB, or greater, volumes to the storage pool's mirror on the target system.

4. When you finish allocating volumes to the mirror, click the right arrow button on the panel to continue to 2.

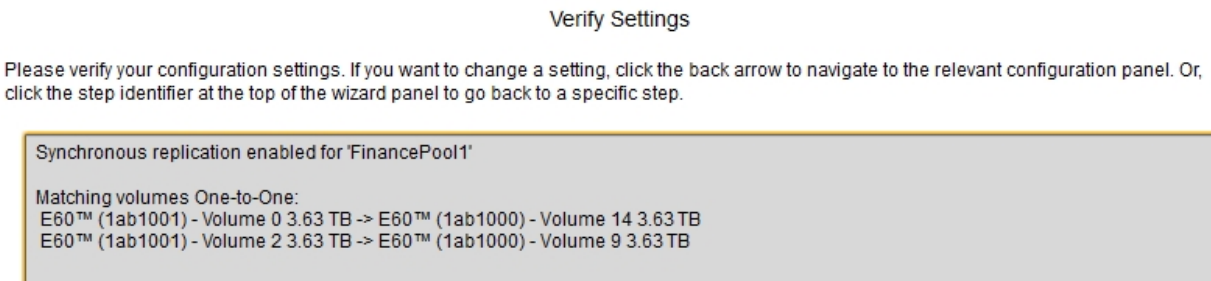
► **To allow Unity to suggest volume allocation:**

1. Click the **Suggest Allocation** button. Unity automatically allocates volumes to the mirror.
2. When Unity finishes allocating volumes to the mirror, click the right arrow button on the panel to continue to [Step 2: Verifying settings](#) below.

Step 2: Verifying settings

Step 2 of the Synchronous Data Replication Setup Wizard summarizes the settings you selected for synchronous data replication and applies the settings when you click **Start**. Review the summary carefully before applying settings.

Figure 12-20: Synchronous Data Replication Setup Wizard, step 2: verify settings



► **To change a configuration setting:**

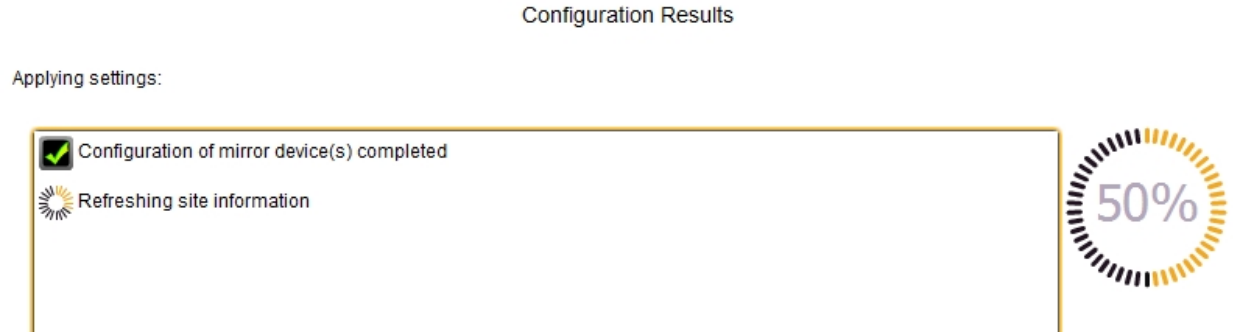
- Click the back arrow to navigate back to the corresponding configuration step.
Or
- Click the corresponding step identifier at the top of the Synchronous Data Replication Setup Wizard panel. For example, if you want to modify volume allocations for the mirror, click **Step 1**.

If you are satisfied with the configuration settings, click the **Start** button at the bottom of the panel. The Synchronous Data Replication Setup Wizard automatically proceeds to [Step 3: Viewing configuration results](#) on the next page.

Step 3: Viewing configuration results

Step 3 of the Synchronous Data Replication Setup Wizard displays progress as Unity applies your replication configuration to the system.

Figure 12-21: Synchronous Data Replication Setup Wizard, step 3: viewing configuration results



The Synchronous Data Replication Setup Wizard displays error events that the system encounters during the configuration process. You can view more details about an error event by expanding the corresponding entry.

► **To view more details for an error event:**

- Click the plus (+) sign corresponding to the error event.

When Unity informs you that it successfully configured synchronous data replication for the storage pool, click **Close** to exit the wizard.

Unity automatically synchronizes data and property settings between the storage pool on the source storage enclosure and the mirror on the target storage enclosure. During the synchronization process, Unity performs a resilvering operation and displays the progress of this operation in the Tasks in progress panel; resilvering is essentially the process of copying data from one pair of a mirror to the other.

A mirror of the storage pool now exists on the target storage enclosure. If either the source or target system fails for any reason, your users and applications can continue to access their data on the storage system that is currently online. When you restore the second system, Unity automatically reestablishes the mirrored link between the two systems.

► **What's next:**

- To view details and properties about the mirror configuration for the storage pool, navigate down to the **Replications** node for the storage pool in Unity's tree view.
- To view the volumes allocated to the storage pool on the source storage enclosure, as well as to the mirror on the target storage enclosure, open the **Mirror** node's Properties panel.

Promoting the mirrored storage pool

This process promotes the mirrored storage pool to an independent storage pool in your Unity deployment. Promoting a mirrored storage pool removes the synchronous link between the source and target systems and creates a second, independent copy of the storage pool—with both copies containing exactly the same data.

This feature allows you to create an exact copy of your production data for testing and validation; or for data migration—in order to move data from one storage enclosure to another, when upgrading hardware or rebalancing storage.

► **To promote a storage pool's mirror on the target system:**

1. In Unity's tree view, click the Site node representing Unity where the storage pool that you want to perform a mirror promote on exists.
2. Click the **Storage Pools** node.
3. Click the node representing the storage pool that you want to perform a mirror promote on. The storage pool must have synchronous data replication configured.
4. Click its **Replications** node
5. Click the **Mirror** node and expand its Properties panel.
6. Perform one of these actions:
 - Click the **Promote** button on the Properties panel, or
 - Click the context menu button on the Mirror node and select **Promote**.
7. Unity displays the Promote Mirrored Storage Pool popup, where you must specify a new name for the mirrored storage pool and for each of its shares. Type a new name for the storage pool, and for each of its shares/LUNs.
8. Click the **Promote** button.

Removing synchronous replication for a storage pool

This process removes the synchronous link between the source and target systems, and deletes the mirrored storage pool and shares, including all their underlying data, on the target system.

► **To remove synchronous replication for a storage pool:**

1. In Unity's tree view, click the Site node representing Unity where the storage pool that you want to remove synchronous replication for exists.
2. Click the **Storage Pools** node.
3. Click the node representing the storage pool that you want to remove synchronous replication for. The storage pool you select must have synchronous data replication configured.
4. Click its **Replications** node.
5. Click the **Mirror** node, and expand its Properties panel.
6. Perform one of these actions:
 - Click the **Remove** button on the Properties panel, or
 - Click the context menu button on the Mirror node and select **Remove**.
7. Unity prompts you to confirm removal. Type **yes** in the text box.
8. Click the **Yes** button.

Chapter 13

System monitoring

There are three ways to monitor system performance on Unity:

- Viewing performance metrics with the Dashboard
- Viewing performance metrics with the Performance Monitor
- Generating and viewing reports

Unity displays real-time performance information for Unity in graphical format in Unity's Dashboard and Performance Monitor.

The Performance Monitor provides a visual display of built-in performance counters on Unity. It features multiple graph views that enable you to visually examine real-time performance metrics for Unity.

The Dashboard provides a visual display of performance data for the entire site, in addition to space usage, site health, and reports for shares, LUNs, pools, and storage devices on Unity.

The Nexsan Unity Reports feature allows you to generate dashboard-type, graphical reports detailing storage capacity across Unity storage infrastructure.

This section includes these topics:

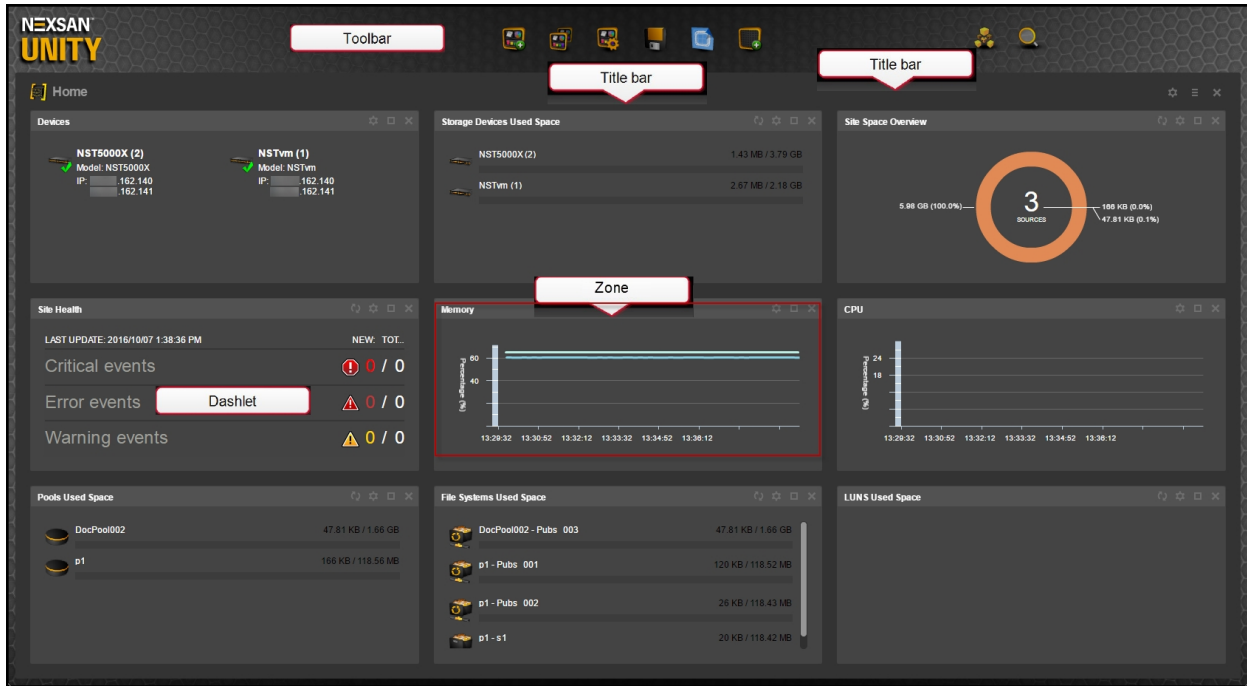
Viewing performance metrics with the Dashboard view	474
Viewing and recording performance metrics with the Performance Monitor	499
Creating and viewing reports	507

Viewing performance metrics with the Dashboard view

The [dashboard](#) consists of:

- a toolbar at the top
- a title bar
- zones that contain one or more dashlets

Figure 13-1: Dashboard view



To switch to Tree view, click the Tree view icon  on the top right corner of the screen; for a description of tree nodes, see [Tree view and nodes](#) on page 52.



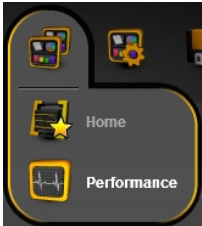




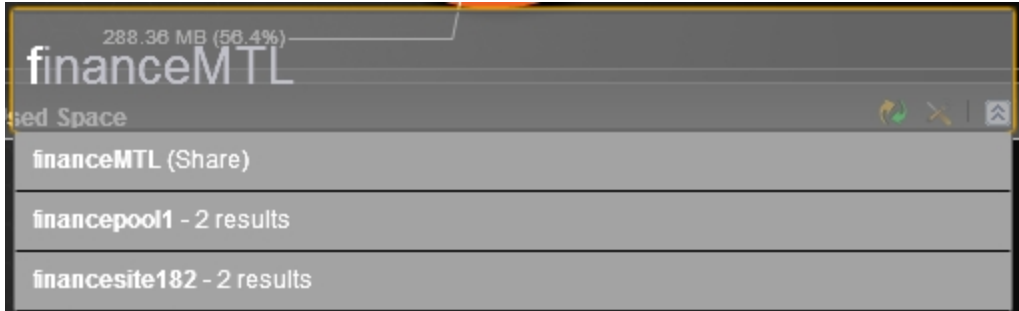
This section includes these topics:

Dashboard toolbar	475
Dashboard title bars	476
Home dashboard	477
Performance dashboard	478
Adding and configuring dashlets	486
Managing dashboards	479

Dashboard toolbar

The dashboard toolbar includes these icons. This toolbar offers general options for managing dashboards, and remains visible in all dashboard views.







Table 13-1: Dashboard toolbar icons

Icon	Description	
	Adds a new dashboard; see Configuring dashboard settings on page 479.	
	Switches dashboards. By default, the list displays the Home and Performance dashboards; see Home dashboard on page 477 and Performance dashboard on page 478. If you create new dashboards, they will be listed as well.	
	Opens the Manage Dashboard Templates dialog box, which enables you to add, delete, copy, rename, edit, and use templates. For more information, see Managing dashboard templates on page 480. Dashboards are only visible to the user who created them. If you want all users to view the same dashboards, the nxadmin or Site Admin user creates templates that regular users will be able to select in their own view.	
	Adds a new dashlet to the current dashboard displayed. For more information, see Adding and configuring dashlets on page 486 . If the dashboard display space is full, you will be prompted to remove a dashlet before adding a new one.	
	Toggles the view to show the Tree view; see Tree view and nodes on page 52.	
	Opens a text field to search for a specific item on Unity. This function is useful to find a share, pool, or LUN very quickly and take action if there is an issue, instead of having to switch views and drilling down the nodes manually to find the item. For example, if you see a pool that is running out of space, entering the pool name will take you directly to the pool in the tree view, where you can provision more space using the pool's property panel. Tip To open and close the Quick Access search, use this shortcut key, Ctrl + f. This example shows the Find function returning results after just entering one letter, f:	

Dashboard title bars

All dashboards have a title bar, from which you can perform these actions using the icons on the right-end side of the toolbar.




Table 13-2: Dashboard title bar icons



Icon	Description
	Resets watchers. This icon indicates that new events happened in a Site Health dashlet. Click this icon to clear new events.
	Shows legend details for all dashlets in the current dashboard.
	Hides legend details for all dashlets in the current dashboard.
	Opens the Configure Dashboard Settings window, from which you can modify the dashboard name, icon, layout, and the number of zones. For more information, see Configuring dashboard settings on page 479.
	Hides title bars for all dashlets in the current dashboard. When clicked again, it toggles to show back all dashlet title bars.
	Deletes the current dashboard. Note You must have at least one dashboard in Unity. You will not be able to delete the dashboard if it is the only one remaining.

Dashlet title bars

Each dashlet also has a title bar. The icons displayed on the title bar may differ from one dashlet to the other. This table lists all existing icons.

Table 13-3: Dashlet title bar icons

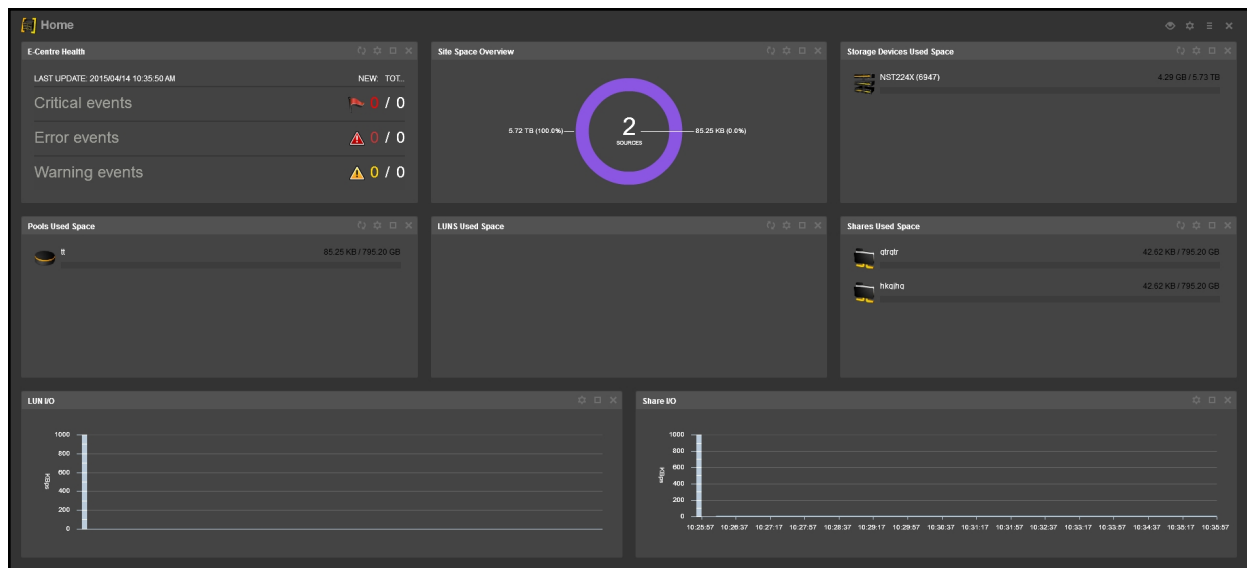
Icon	Description
	Refreshes the information displayed in the current dashlet.
	Opens the configuration panel for the specific dashlet. For more information, see: <ul style="list-style-type: none"> • Configuring a Site Health dashlet on page 488 • Configuring a Space Usage dashlet on page 490 • Configuring a Site Space Overview dashlet on page 492 • Configuring a Performance Metrics dashlet on page 493 • Configuring a Report dashlet on page 495 • Configuring a Device List dashlet on page 496 • Configuring an I/O Operations Per Second dashlet on page 497
	Shows the current dashlet in full view. The dashlet will display across the entire dashboard view.

Icon	Description
	Shows the current dashlet back to normal view.
	Deletes the current dashlet. Click Yes when prompted to confirm the action. The dashboard will automatically adjust the view by expanding other dashlets present in that zone.

Home dashboard

When you first log in to Unity, the Home dashboard is the dashboard that gets displayed if there are storage pools with LUNs or shares created (otherwise, the Unity's Tree view gets displayed). If you want another dashboard to be displayed as default view, see [Configuring dashboard settings](#) on page 479.

Figure 13-2: Home Dashboard



By default, the Home dashboard comprises the following dashlets, from left to right, per zone:

- Unity Health
 - Site Space Overview
 - Storage Devices Used Space
 - Pools Used Space
 - LUNs Used Space
 - File Systems Used Space
 - Report; if no reports have been created, none will display. To create a report, see [Generating reports](#) on page 509.
- ▶ **Related topics:**
- For details on icons located on the title bars, see [Dashboard title bars](#) on the previous page.
 - To add and configure dashlets, see [Adding and configuring dashlets](#) on page 486.
 - To change the Home dashboard layout, see [Configuring dashboard settings](#) on page 479.

Performance dashboard

The Performance dashboard displays performance metrics, similarly to the Performance Monitor. For details on the Performance Monitor, see [Viewing and recording performance metrics with the Performance Monitor on page 499](#).

Figure 13-3: Performance dashboard



By default, the Performance dashboard comprises these dashlets (from left to right, per zone), which display performance statistics for:

- CPU
- Device I/O
- Memory
- Network

▶ **Related topics:**

- To know more about performance metrics and to add a Performance Metrics dashlet, see [Configuring a Performance Metrics dashlet on page 493](#).
- For details on icons located on the title bars, see [Dashboard title bars on page 476](#).
- To change the Performance dashboard layout, see [Configuring dashboard settings on the facing page](#).

Managing dashboards

Refer to these sections to update and modify your dashboards:

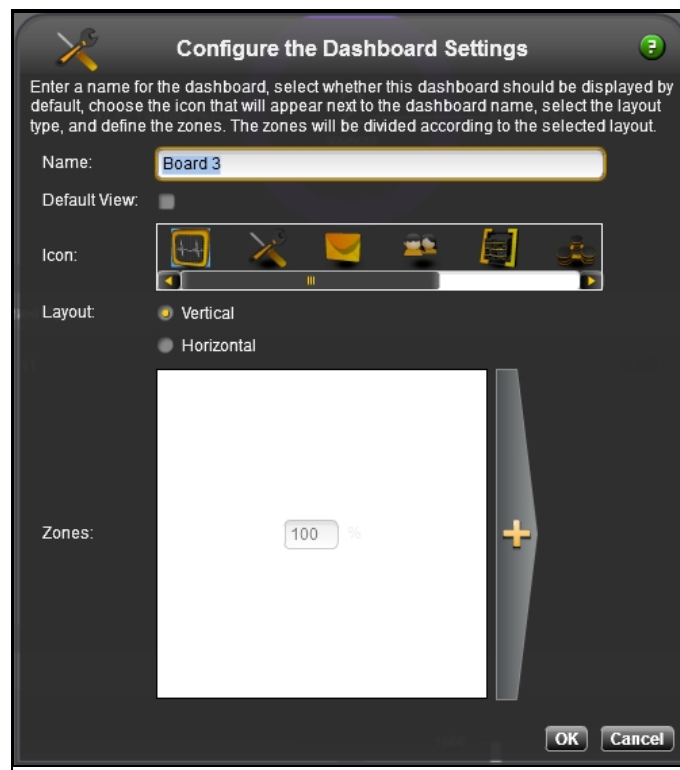
- [Configuring dashboard settings](#) below
- [Managing dashboard templates](#) on the next page
- [Configuring autosave settings](#) on page 485
- [Saving dashboard settings](#) on page 485
- [Adding and configuring dashlets](#) on page 486

Configuring dashboard settings

The Configure the Dashboard Settings dialog box allows you to define the appearance of a new dashboard, or modify the appearance of the currently showing dashboard. You can define the name, default view status, icon, layout, and/or the number of zones.

The new dashboard can be only viewed by the current user.

Figure 13-4: Configuring the new dashboard settings



► To configure dashboard settings:

1. In the **Name** field, enter a new name.
2. Check or uncheck the **Default View** option. When selected, this option will display the current dashboard as the main view when you log in to Unity.
3. In the **Icon** slide bar, select the icon that will identify this dashboard.
4. Select whether you want the layout to be **Vertical** or **Horizontal**.

5. Zones will be presented as columns if you chose **Vertical**, or rows if you chose **Horizontal**. Perform one of these actions:

- To add a zone, click the + icon.
- To remove a zone, click the red x icon.

Notes:

- You can have a maximum of four zones in your dashboard.
- The maximum number of dashlets in a zone depends on the dashlet content. Unity will even out the zones (rows or columns) as space permits. You can move the dashlets around by dragging them.
- If you remove a zone that contains dashlets, Unity will reorganize the layout by moving those dashlets in space available in the remaining zones. However, if Unity runs out of space, the dashlets that could not be moved to other zones will be placed in the first zone and will be partially hidden from view. A warning message will prompt you to create a new zone to place these dashlets or to create a new dashboard and recreate the same dashlets in that dashboard.

6. Click **OK**.

If you modified an existing dashboard, it will appear according to the new settings. If you created a new dashboard, it will display in your current view, and its icon will appear beside the other dashboard icons when you click **Switch Dashboards** on the toolbar.

Note We recommend that you do not exceed five dashboards in Unity. Having more dashboards may cause memory issues and you may need to delay the refresh interval.

▶ **What's Next:**

The autosave feature is disabled by default. After making changes, a dialog box will appear to provide you the steps to enable the Autosave function; see [Configuring autosave settings on page 485](#).

Managing dashboard templates

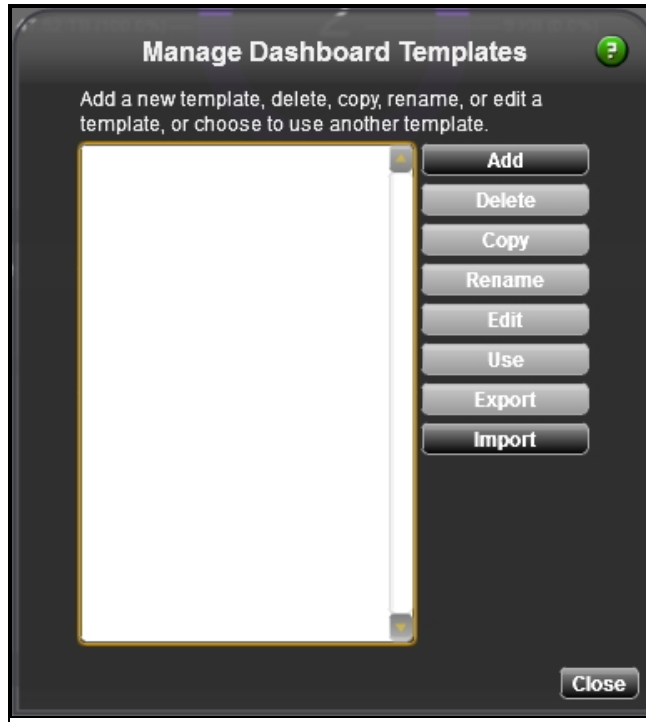
Dashboard templates allow users to use the same dashboards across the site. Only the nxadmin user or Site Administrator can create and edit templates. When users log in to Unity, they can view the list of available templates created by nxadmin or the Site Administrator, and choose to use the same template without affecting other users. Templates allow storage administrators to share a consistent look and feel of Unity performance. Templates are saved at the site level.

Home and **Performance** are default templates in Unity.

Note The nxadmin and the Site Admin users will see all option buttons on the Manage Dashboard Templates dialog box. Regular users will only see the **Use** button.

► **To manage dashboard templates:**

1. Click **Manage Templates**  from the dashboard title bar.
2. The Manage Dashboard Templates dialog box appears.

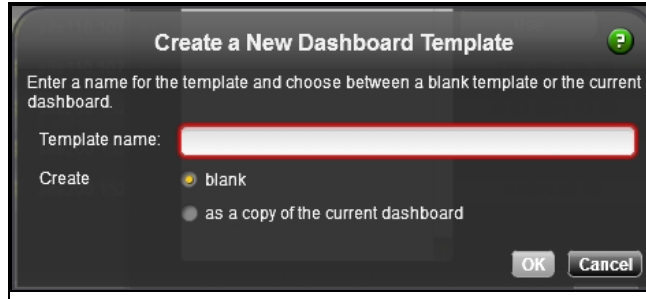


Perform one or more of these actions:

- [Add a dashboard template](#)
 - [Delete a dashboard template](#)
 - [Copy a dashboard template](#)
 - [Rename a dashboard template](#)
 - [Edit a dashboard template](#)
 - [Use a dashboard template](#)
 - [Export a dashboard template](#): This option allows you to copy the configuration of a dashboard template to another Unity.
 - [Import a dashboard template](#): This option allows you to paste the configuration of a dashboard template on an Unity that you previously copied from another system.
3. Click **Close** when you are done.

► **To create a template:**

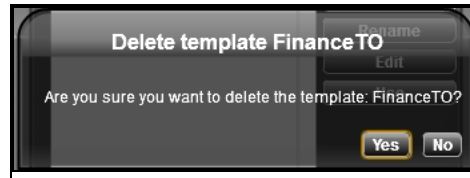
1. Click **Add**.



2. Enter a name for the template. The name must start with an (upper-case or lower-case) alphabetic or numeric character; and, with the exception of the hyphen (-), and period (.), the name can only contain alphanumeric characters, without spaces. These characters are NOT allowed: " / \ [] : ; | = , + * ? < >
3. Create a brand-new template or use your current dashboard as a base for the template.
4. Click **OK**.

► **To delete a template:**

1. Select the desired template.
2. Click **Delete**.



3. When prompted to confirm the deletion, click **Yes**.

► **To copy a template:**

1. Select the desired template.
2. Click **Copy**.



3. Enter a name for the template. The name must start with an (upper-case or lower-case) alphabetic or numeric character; and, with the exception of the hyphen (-), and period (.), the name can only contain alphanumeric characters, without spaces. These characters are NOT allowed: " / \ [] : ; | = , + * ? < >
4. Click **OK**.


▶ **To rename a template:**

1. Select the desired template.
2. Click **Rename**.



3. Enter a new name for the template. The name must start with an (upper-case or lower-case) alphabetic or numeric character; and, with the exception of the hyphen (-), and period (.), the name can only contain alphanumeric characters, without spaces. These characters are NOT allowed: "/\ [] ; | = , + * ? < >
4. Click **OK**.

▶ **To modify a template:**

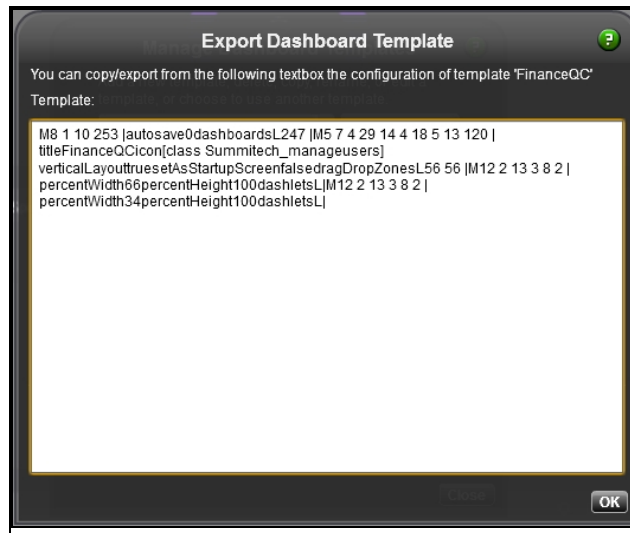
1. Select the desired template.
2. Click **Edit**.
3. Perform one or more of these actions:
 - Add dashlets; see [Adding and configuring dashlets](#) on page 486.
 - Delete dashlets; click to delete and click **Yes** to confirm.
 - Modify the dashboard settings; see [Configuring dashboard settings](#) on page 479.
 - Delete dashboard; click to delete and click **Yes** to confirm. If there is only one dashboard, you will not be able to delete it.
4. When finished, save your settings, unless the auto-save feature is enabled.
5. Click next to "*Editing template...*" message on the right-end side corner on the title bar to close the template editor .
6. When prompted to confirm the closure, click **Yes**. The template will be saved with your changes.

▶ **To choose a template for use:**

1. Select the desired template.
2. Click **Use**. The dashboard view changes to the selected template settings.

► **To export a template:**

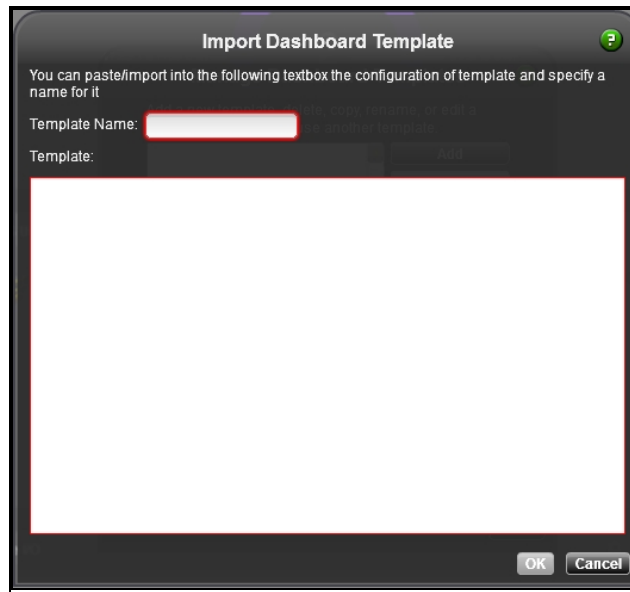
1. Select the template from which you want to copy the configuration.
2. Click **Export**. The Export Dashboard Template displays.



3. Copy the text inside the box.
4. Click **OK** to close the dialog box.

► **To import a template:**

1. Click **Import**. The Import Dashboard Template displays.



2. Enter a name for the template. The name must start with an (upper-case or lower-case) alphabetic or numeric character; and, with the exception of the hyphen (-), and period (.), the name can only contain alphanumeric characters, without spaces. These characters are NOT allowed: " / \ [] : ; | = , + * ? < >
3. Paste the template configuration into the text box.
4. Click **OK**.

Configuring autosave settings

This feature allows you to save all your existing dashboards automatically without having to worry about losing your changes. You do not need to manually save the settings using the Save Settings function (see [Saving dashboard settings](#) below). The Autosave feature is disabled by default.

After making a change in a dashboard (or a dashlet), the Save Settings icon changes and displays a blue

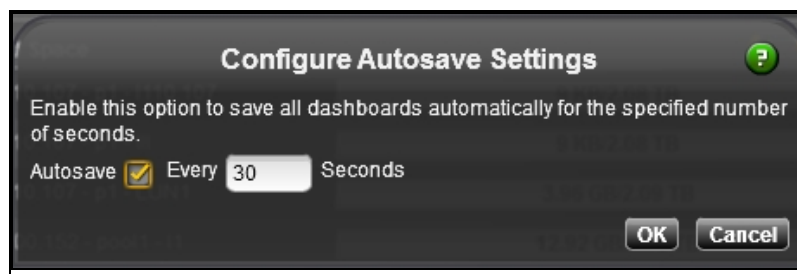
arrow . This icon goes back to its original look  when you save your changes (using the procedure in [Saving dashboard settings](#) below), or when the Autosave feature saves the settings.

Note If you made extensive changes to your dashboard, you cannot revert back to an older version since this autosave feature will have already overwritten your previous settings.

► **To save changes to dashboards automatically:**

1. Click the Set Up Dashboards icon .

Figure 13-5: Configuring dashboard autosave settings



2. Select the **Autosave** option.
3. Enter the number of seconds. The minimum value is 10 seconds and there is no maximum.
4. Click **OK**.

Saving dashboard settings

If you added or deleted dashlets, or if you rearranged your dashlet layout, and you wish to keep those changes, you can save the current settings for the next time you log in to Unity. Since dashboards are only visible to the user who created and/or changed them, Unity will confirm the save operation under your current user credentials. For example, if user Bob made changes to the Performance dashboard, other users will not see those changes in their Performance dashboard, unless they log in to Unity using Bob's user credentials. Users who log in to Unity with nxadmin credentials will see all changes.

After making a change in a dashboard (or a dashlet), the Save Settings icon changes and displays a blue

arrow . This icon goes back to its original look  when you save your changes (using the procedure in this section), or when the Autosave feature saves the settings (see [Configuring autosave settings](#) above).

Note This function only applies to the dashboard you are currently viewing.

► **To save dashboard view changes:**


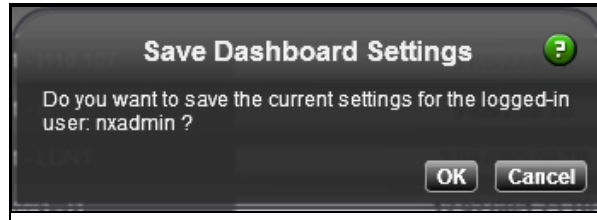
1. Click the Save Settings icon .
2. When prompted to confirm the save operation, click **OK**.

Figure 13-6: Saving dashboard settings





Adding and configuring dashlets



You can add dashlets to the default Home or Performance dashboard, or to a brand-new dashboard. As you add dashlets, the view gets reorganized according to your dashboard layout settings, as long as there is enough space on the screen. Unity will even out the zones (rows or columns) as space permits. You can move the dashlets around by dragging them.




Note When you run out of space, Nexsan Unity prompts you to delete a dashlet before you can add a new one. The number of dashlets you can have in a zone depends on how much space is taken by the information displayed in the dashlet.

To change the dashboard layout, see [Configuring dashboard settings](#) on page 479. For a description of dashlet icons, see [Dashboard title bars](#) on page 476.

Table 13-4: Dashboard dashlets

Dashlet	Description
Events 	<p>This dashlet displays the system health in graphical format, based on events that are recorded in the event logs. Unity records events from these source components:</p> <ul style="list-style-type: none"> ● Unity ● Storage system ● File system ● System <p>You can choose one or more of these source components for the dashlet. Event data displayed in this dashlet is the same as event data displayed in Event Viewer—for details, see Event logging and notification on page 517.</p> <p>To add or configure an event dashlet, see Configuring a Site Health dashlet on page 488.</p>
Space Usage 	<p>This dashlet displays the amount of space used for one of these source components:</p> <ul style="list-style-type: none"> ● Devices ● Pools ● File Systems ● LUNs

Dashlet	Description
	<ul style="list-style-type: none"> • Sites • Volumes <p>You must create a dashlet for each component. By default, the Home dashboard displays Space Usage dashlets for storage devices, LUNs, pools, and file systems. To add or configure a space usage dashlet, see Configuring a Space Usage dashlet on page 490.</p>
<p>Space Overview</p> 	<p>This dashlet displays a general view of used and free space for one of these source components:</p> <ul style="list-style-type: none"> • Devices • Pools • File Systems • Sites • Volumes <p>You must create a dashlet for each component. By default, the Home dashboard displays the Site Space Overview dashlet. To add or configure a space overview dashlet, see Configuring a Site Space Overview dashlet on page 492.</p>
<p>Performance Metrics</p> 	<p>This dashlet displays displays real-time performance information for Unity in graphical format, for one of these performance metrics:</p> <ul style="list-style-type: none"> • CPU • Device I/O • Device latency • FASTier I/O • FASTier IOPS • FASTier Read access • FASTier Write access • LUN I/O • LUN IOPS • Memory • Network • File System I/O • File System IOPS <p>By default, the Performance dashboard displays all these dashlets for the primary site. If you have multiple sites, you can add performance metrics dashlets for another site. For example, you could create a new dashboard containing all these dashlets for the secondary site.</p> <p>Performance data displayed in these dashlets is the same as performance data seen in the Performance Monitor; for details, see Viewing and recording performance metrics with the Performance Monitor on page 499</p> <p>To add or configure a performance metrics dashlet, see Configuring a Performance Metrics dashlet on page 493.</p>
<p>Report</p>	<p>This dashlet displays the selected report in the dashboard. Unity reports provide</p>

Dashlet	Description
	<p>detailed information about the storage resources in your environment, including space usage consumption for each file system and/or iSCSI LUN on Unity, space usage consumption on a per user basis, and overall storage pool capacity and used space.</p> <p>Note Reports must be created beforehand in the Unity's Tools menu; see Generating reports on page 509.</p> <p>You can select any of your reports, and choose to sort data per used space, user name, or percentage of space consumption to customize the appearance of the dashlet.</p> <p>To add or configure a report dashlet, see Configuring a Report dashlet on page 495.</p>
Device List 	<p>This dashlet displays the health all storage devices on Unity, per site. If you have multiple sites, you must create a dashlet for each site. Clicking the a device in the dashlet takes you directly to the device in the tree view.</p> <p>To add or configure a device list dashlet, see Configuring a Device List dashlet on page 496.</p>
IOPS 	<p>This dashlet displays I/O operations per second in graphical format, for these I/O types, per site:</p> <ul style="list-style-type: none"> • LUN IOPS • File System IOPS • Pool I/O <p>I/O operations refers to all read and write I/O operations sent to the storage pool(s), device(s) , or on the network, per second. This dashlet allows you to view Read and Write I/O performance and track potential I/O bottlenecks. The higher the number of input/ouput operations that can be done in a second, the more performant the system.</p> <p>To add or configure a IOPS dashlet, see Configuring an I/O Operations Per Second dashlet on page 497.</p>

Configuring a Site Health dashlet

This dashlet displays the system health in graphical format, based on events that are recorded in the event logs. Unity records events from these source components:

- **Nexsan Unity:** these events are generated by Unity and its software components, including Unity Clustering, Data Replication, and Snapshots functions.
- **Storage System:** these events are generated by Nexsan storage systems attached externally to Unity (via SAS or Fibre Channel), if available, and logged to the event logs.
- **File System:** these events are generated by the Unity operating system.
- **System:** these events are generated by Unity for hardware faults on the system, such as fan, power supply, or disk failures.



Event data displayed in this dashlet is the same as event data displayed in Event Viewer—for details, see [Event logging and notification](#) on page 517.

Figure 13-7: Site Health dashlet

E-Centre Health		NEW	TOTAL
LAST UPDATE: 2015/04/10 3:20:53 PM			
Critical events		0	0
Error events		0	0
Warning events		0	25

To view the list of events, click anywhere in the category row (critical, error, or warning). Unity will open the Event Viewer dialog box for the selected category.

► **To add or configure a Site Health dashlet:**

1. From the toolbar, click **Add Dashlet** .
2. Select **Events** .
3. The configuration dialog box for the selected dashlet displays.

Configure the Site Health Dashlet

Change the dashlet's name, site, source(s) for which you want to view events, event time line, and/or refresh frequency.

Name:

Site:

Source(s):

View events from the: last 24 hours
 last 7 days

Refresh every: Minutes

Enter this information:

- a. Enter a meaningful name in the **Name** field.
 - b. Choose a site from the **Site** drop-down list. If there is only one site, it is selected by default.
 - c. From the **Source(s)** drop-down list, select one or more sources:
 - Unity
 - Storage system
 - File system
 - System
 - d. Select the duration for the events you want to see, either the last 24 hours, or the last 7 days.
 - e. Enter a number for the refresh frequency, in minutes.
4. Click **OK** to save your settings. The dashlet appears in the current dashboard view.

Configuring a Space Usage dashlet

This dashlet displays the amount of space used by specific Unity components. You must create a dashlet for each component type. By default, the Home dashboard displays Space Usage dashlets for storage devices, LUNs, pools, and shares.

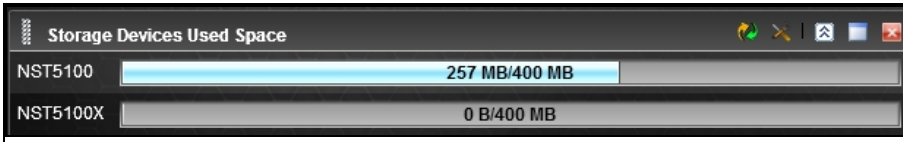
As a component uses more and more space, the progress bar changes color accordingly, and the amount of space gets updated. This allows you to view the space situation quickly and take action accordingly. For pools, shares, and LUNs, the colors displayed are based on the space usage notification thresholds set at 75% by default.

To modify the space usage thresholds, see:

- [Setting space usage notification thresholds for a storage pool](#) on page 115
- [Setting space usage notification thresholds for file systems](#) on page 139
- [Enabling client-side space usage notifications for a LUN](#) on page 228

► Color scheme:

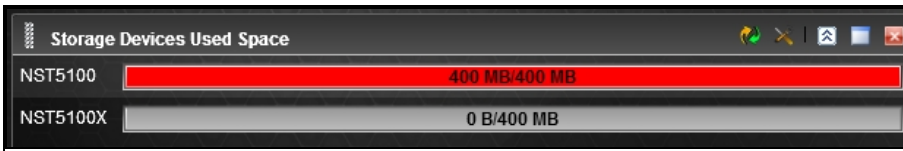
- Gray: all or most space is available
- Blue: some space is used




- Orange: most space is used



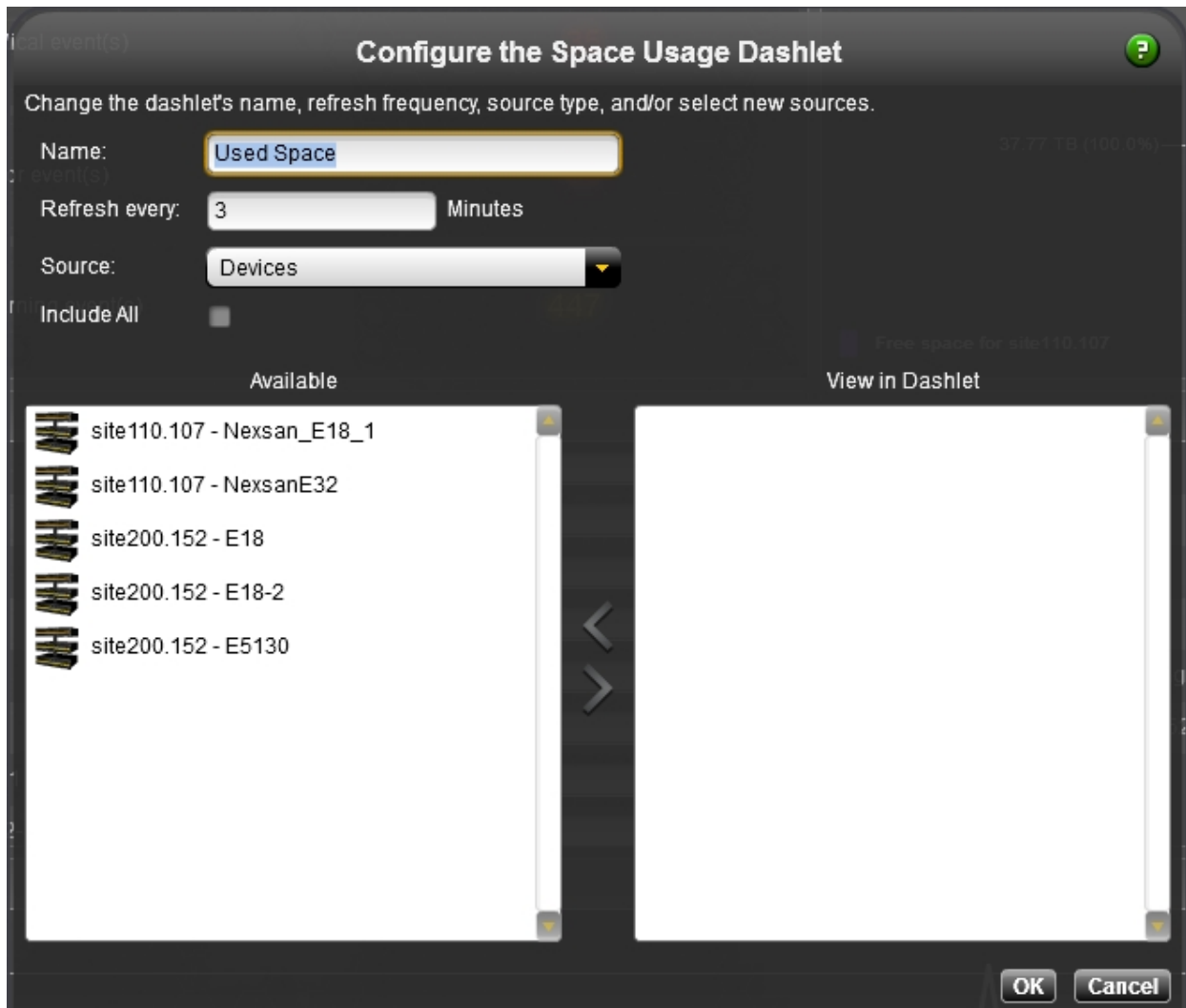
- Red: almost or all space is used



► To add or configure a Space Usage dashlet:

1. From the toolbar, click **Add Dashlet** .
2. Select **Space Usage** .

3. The configuration dialog box for the selected dashlet displays.



Enter this information:

- a. Enter a meaningful name in the **Name** field.
- b. Enter a number for the refresh frequency, in minutes.
- c. From the **Source** drop-down list, select one of the component types present in your environment:
 - Devices
 - LUNs
 - Pools
 - FASTier Read (cache)
 - File Systems
 - Sites
 - Volumes

- d. (Optionally) Select the **Include All** option. When this option is selected, any component that you add to Unity afterwards will automatically be added to the dashlet, so you will not need to update the dashlet configuration settings again.
- e. Select the components to be viewed in the dashlet. From the **Available** panel on the left, drag the component to the **View in Dashlet** panel on the right, or select the component and click the arrow button to move it.

The list of available components will vary according to the selection you made in the **Source** drop-down list.

4. Click **OK** to save your settings.

► **What's next:**

If the dashlet displays space issues for a component, refer to these topics to take action:

- To modify share space settings, see [Modifying a file system's space usage settings](#) on page 137.
- To modify LUN space settings, see [Modifying LUN space settings](#) on page 229.
- To add storage devices to the site, see [Allocating new storage to the site](#) on page 328.
- To add drives to a storage device, see [Adding new drives to a Nexsan storage enclosure](#) on page 333.

Configuring a Site Space Overview dashlet

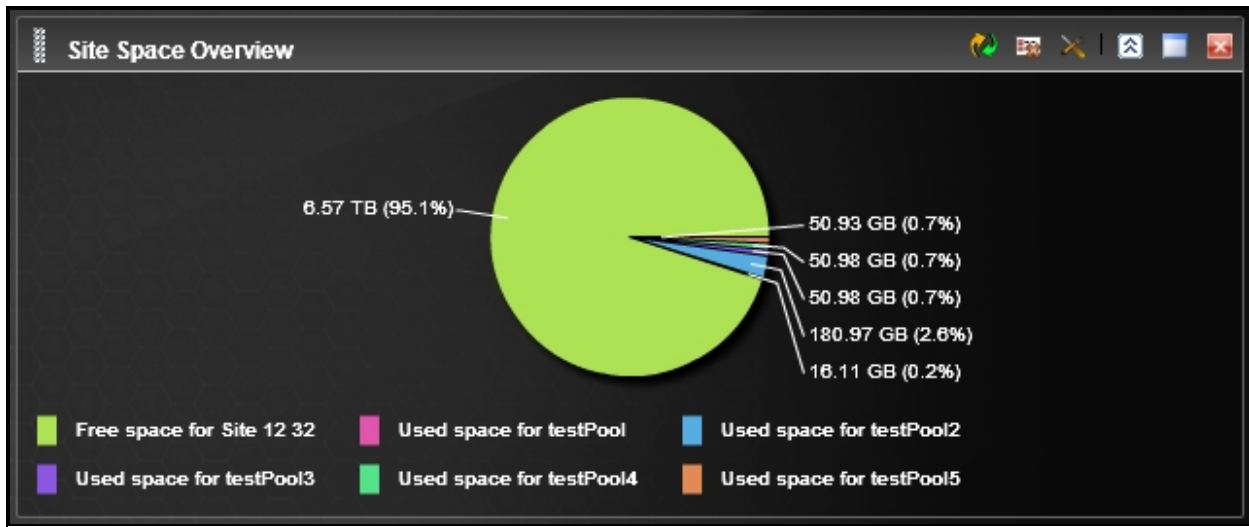
This dashlet displays the amount of free space and the amount of space used by Unity components, in the shape of a pie chart. As a component uses more and more space, the slices of the pie chart gets updated. You must create a dashlet for each component.

By default, the Home dashboard displays the Site Space Overview dashlet, which allows you to view the overall space usage for the site at a glance.

► **Color scheme:**

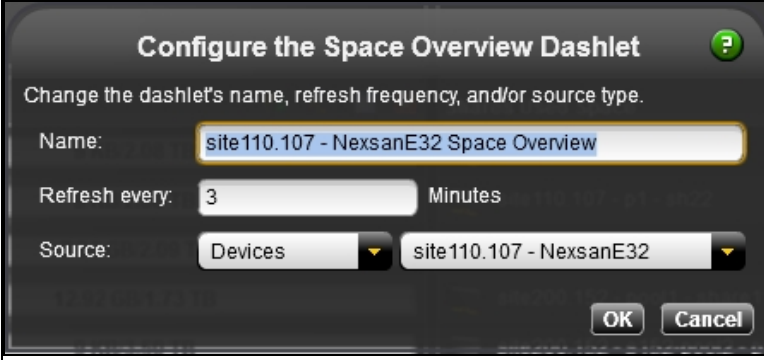
Unity automatically assigns colors according to the number of pools in the site, and assigns another color for free space.

Figure 13-8: Dashboard's color scheme



► **To add or configure a Space Overview dashlet:**

1. From the toolbar, click **Add Dashlet** .
2. Select **Space Overview** .
3. The configuration dialog box for the selected dashlet displays.



Enter this information:

- a. Enter a meaningful name in the **Name** field.
 - b. Enter a number for the refresh frequency, in minutes.
 - c. From the **Source(s)** drop-down list, select one or more categories:
 - Devices
 - LUNs
 - Pools
 - File Systems
 - Volumes
 - d. Depending on your selection in the first drop-down list, the second drop-down list displays the components pertaining to the selected category.
For example, selecting **Devices** will display Unity currently used in your site; selecting **Pools** will display the list of existing pools, etc.
4. Click **OK** to save your settings. The dashlet appears in the current dashboard view.

Configuring a Performance Metrics dashlet

This dashlet provides a visual display of built-in performance counters used on Unity. You must create a dashlet for each site and each metric. By default, the **Performance** dashboard displays all these dashlets for the primary site.



Unity collects current (real-time) performance data for these metrics:

- **CPU**: gathers CPU usage for each controller at the specified time interval, and then displays the data as percentage values in graphical format.

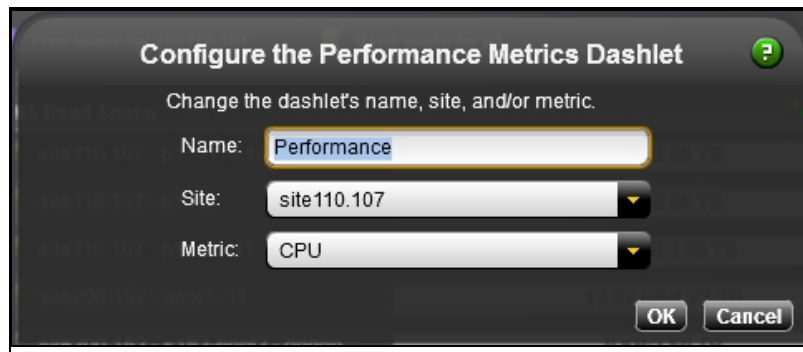
- **Device I/O**: gathers device I/O at the specified time interval. This includes read and write I/O statistics for all disks and storage systems connected to Unity.
Each slot of Unity storage device and each volume of Nexsan E-Series storage device is represented in a different color.
- **Device Latency**: storage pools latency (delay of response time) displayed in microseconds at the specified time interval.
- **FASTier I/O**: I/O operations for FASTier Read cache and FASTier Write cache.
- **FASTier IOPS**: number of operations per second (OPS) for FASTier Read cache and FASTier Write cache.
- **FASTier Read access**: hit and miss access operations for FASTier Read cache.
- **FASTier Write access**: if write cache devices are present, displays values for hit and miss access operations for FASTier Write cache.
- **LUN I/O**: gathers LUN I/O at the specified time interval. This includes read and write I/O statistics. You can filter the graphical representation to only show I/O statistics for a specific LUN.
- **LUN IOPS**: input/output operations per second (IOPS) displayed at the specified time interval. This includes read and write operations.
- **Memory**: gathers memory usage for each controller at the specified time interval, and then displays the data as percentage values.
- **Network**: performance counter values for the site network I/O at the specified time interval. This includes read and write I/O statistics for each controller. Unity aggregates the network performance statistics and displays them as percentage values.
- **File System I/O**: share I/O displayed at the specified time interval. This includes read and write I/O statistics. You can filter the graphical representation to only show I/O statistics for a specific share.
- **File System IOPS**: share input/output operations per second (IOPS) displayed at the specified time interval. This includes read/write CIFS and/or NFS operations per second, depending on the type of share.

Note To modify the sampling interval at which performance data is collected, see [Changing the duration to keep sampling data](#) on page 505.

► **To add or configure a Performance Metrics dashlet:**

1. From the toolbar, click **Add Dashlet** .
2. Select **Performance Metrics** .

3. The configuration dialog box for the selected dashlet displays.



Enter this information:

- a. Enter a meaningful name in the **Name** field.
 - b. Choose a site from the **Site** drop-down list. If there is only one site, it is selected by default.
 - c. From the **Metric** drop-down list, select one of the metrics.
4. Click **OK** to save your settings. The dashlet appears in the current dashboard view.

This image provides an example of the CPU usage in Full View, where Controller 1 is represented in yellow and Controller 2 is represented in orange.

Figure 13-9: Example of CPU dashlet



► **Related topics:**

- [Performance dashboard](#) on page 478
- [Viewing and recording performance metrics with the Performance Monitor](#) on page 499

Configuring a Report dashlet

Report dashlets provide a graphical representation detailing storage capacity across the Unity storage infrastructure. You can create a report dashlet from any report that you created beforehand. You can create one dashlet per report.

► **To add or configure a Report dashlet:**

1. From the toolbar, click **Add Dashlet** .
2. Select **Report** .

3. The configuration dialog box for the selected dashlet displays.

Figure 13-10: Configuring the Report dashlet

Enter this information:

- a. Enter a meaningful name in the **Name** field.
 - b. Choose a site from the **Site** drop-down list. If there is only one site, it is selected by default.
 - c. From the **Report** drop-down list, select one of the available reports.
 - d. In the **Sort** area, select the order in which you want to view the data.
 - e. Enter a number for the refresh frequency, in minutes or hours.
4. Click **OK** to save your settings. The dashlet appears in the current dashboard view.



► **Related topics:**

- [Creating and viewing reports](#) on page 507
- [Report types](#) on page 507
- [Generating reports](#) on page 509

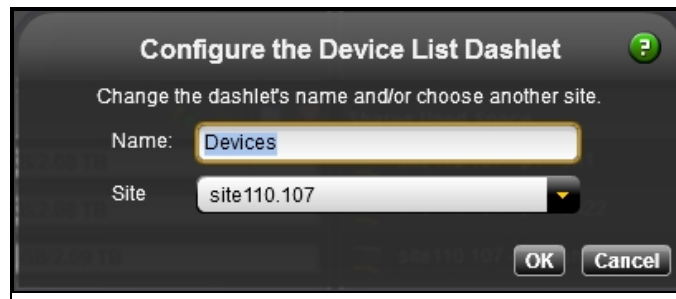
Configuring a Device List dashlet

This dashlet provides a list of all disks and storage systems connected to Unity. It also provides their status with a corresponding icon and a tool tip when hovering your mouse over the device.

► **To add or configure a Device List dashlet:**

1. From the toolbar, click **Add Dashlet** .
2. Select **Device List** .

3. The configuration dialog box for the selected dashlet displays.



Enter this information:



- a. Enter a meaningful name in the **Name** field.
 - b. Choose a site from the **Site** drop-down list. If there is only one site, it is selected by default.
4. Click **OK** to save your settings. The dashlet appears in the current dashboard view.

Configuring an I/O Operations Per Second dashlet

This dashlet displays IOPS statistics for shares. The IOPS dashlet allows you to view performance bottlenecks for the selected IOP type. By default, Unity displays the output in 10-second samples.

Note To modify the sampling interval at which performance data is collected, see [Changing the duration to keep sampling data](#) on page 505.

- ▶ **To add or configure an I/O Operations Per Second dashlet:**

1. From the toolbar, click **Add Dashlet** .
2. Select **IOPS** .

- The configuration dialog box for the selected dashlet displays.

Enter this information:

- Enter a meaningful name in the **Name** field.
 - Choose a site from the **Site** drop-down list. If there is only one site, it is selected by default.
 - From the **IOP type** drop-down list, select the **File System IOPS** or LUN IOPS.
 - Set the maximum value:
 - Select **Adaptive**: Unity will automatically display the maximum values.
 - Select **Preset to** and enter a number in the field, in megabytes. There is no maximum value.
 - Enter a maximum number for the columns. This dashlet is going to display many columns. Keep in mind that if you already have many dashlets in the zones, the columns may appear thin.
- Click **OK** to save your settings. The dashlet appears in the current dashboard view.

► **To view data in an IOPS dashlet:**

- You can sort the view by clicking **Write** to view only write I/O statistics or **Read** to view only read I/O statistics. By default, the total I/O statistics are displayed.
- To view data specific to a column, hover the mouse over the column. Its color will change to black and a tool tip will display to provide more information.
- To view data for a specific dataset, click the desired column. The **Select a dataset** dialog box appears. Select the dataset from the drop-down list and click **OK**.

Figure 13-11: Selecting a dataset

Viewing and recording performance metrics with the Performance Monitor

Unity displays real-time performance information for Unity in graphical format in Unity's Performance Monitor. The Performance Monitor provides a visual display of built-in performance counters on Unity. It features multiple graph views that enable you to visually examine real-time performance metrics for Unity.

The Performance Monitor collects and displays this performance data and then displays the data it collects in graphical and tabular formats:

- **Site CPU usage:** current (real-time) performance counter values for CPU usage for each controller at the specified time interval, and then displays the data as percentage values in graphical format.
- **Site Memory usage :** current (real-time) performance counter values for memory usage for each controller at the specified time interval, and then displays the data as percentage values.
- **Network statistics:** current (real-time) performance counter values for the site network I/O at the specified time interval. This includes read and write I/O statistics for each controller. Unity aggregates the network performance statistics and displays them as percentage values.
- **Device I/O statistics:** current (real-time) performance counter values for device I/O at the specified time interval. This includes read and write I/O statistics for all disks and storage systems connected to Unity. You can filter the graphical representation to only show I/O statistics for the disks/devices currently allocated to a specific storage pool on the system, including the devices reserved for the Unity's operating system pool, and the system pool (on Clustered systems).

Each slot of Unity storage device and each storage device volume is represented in a different color.

- **File System I/O and IOPS statistics:** current (real-time) performance counter values for share I/O at the specified time interval. This includes read and write I/O statistics. You can filter the graphical representation to only show I/O statistics for a specific share.

The counter values for input/output operations per second (IOPS) are displayed at the specified time interval. This includes read/write CIFS operations per second.

Note Monitoring of NFS performance metrics is disabled, by default. You can enable this function using the `perfmon` command in the `nxadmin` CLI, as follows: `perfmon -c enable -a nfs`. Please note that the process for collecting NFS performance metrics may significantly impact system performance.

- **LUN I/O and IOPS statistics:** current (real-time) performance counter values for LUN I/O at the specified time interval. This includes read and write I/O statistics. You can filter the graphical representation to only show I/O statistics for a specific LUN.

The counter values for LUN input/output operations per second (IOPS) are displayed at the specified time interval. This includes read and write operations.

- **FASTier I/O, IOPS, and access statistics:** current (real-time) performance counter values for FASTier cache devices installed on Unity.

Performance data can be I/O statistics for FASTier Read cache and FASTier Write cache at the specified time interval, the number of input/output operations per second (OPS) for FASTier Read cache and FASTier Write cache at the specified time interval, as well as hit and miss access operations for FASTier Read cache.

Notes:

- Read I/O refers to the bandwidth of all read I/O operations sent to the storage pool(s) or device(s) (including metadata requests), expressed as kilobytes per second (KB/s).

- Write I/O refers to the bandwidth of all write I/O operations sent to the storage pool(s) or device(s) (including metadata requests), expressed as kilobytes per second (KB/s).
- For historical performance data, the time interval is 10 seconds by default and then data is aggregated for display in the historical view.

This section includes these topics:

Starting the Performance Monitor	500
Filtering live performance metrics	501
Taking performance snapshots	502

Starting the Performance Monitor

This section explains how to start the Performance Monitor to display real-time performance information for Unity.

► To start the Performance Monitor:

- In the Unity toolbar, select the **Performance Monitor** option from the **Tools** menu.

The Performance Monitor opens in a new browser tab or window, depending on your internet browser's configuration settings. The Performance Monitor includes a graphical chart and a table for each of these performance metrics and component types:

Table 13-5: Performance metrics and types

Metric	Type
LUN	I/O IOPS
File System	I/O IOPS
Pool	Latency
Site	CPU Usage Memory Usage Network
Devices	I/O
FASTier	I/O (read and write cache) IOPS (read and write cache) Access (read cache)

In the Dashboard interface, you can also view the same performance metrics in the Performance Dashboard—see [Performance dashboard](#) on page 478.

Figure 13-12: Performance Monitor—Live view



When the Performance Monitor opens, only the graphical chart for CPU performance is expanded. You can open, or expand, the graphical chart for another performance metric by clicking its corresponding title bar. Similarly, click the title bar of an expanded graphical chart to close, or collapse, it.

By default, the sampling interval is set to every 10 seconds. This means that the Performance Monitor collects performance statistics at 10 second intervals, and updates the graphical charts in real-time accordingly. The time line at the bottom of each graphical chart indicates the current sampling interval. You can modify the sampling interval for the Performance Monitor from the **Options** tab; see the [Changing the duration to keep sampling data](#) on page 505.

Filtering live performance metrics

The Performance Monitor allows you to filter the graphical charts to display only metrics for a specific storage pool, LUN, share, device, or controller (depending on the performance metric selected).

This procedure provides an example on how to filter I/O performance metrics for a specific pool.

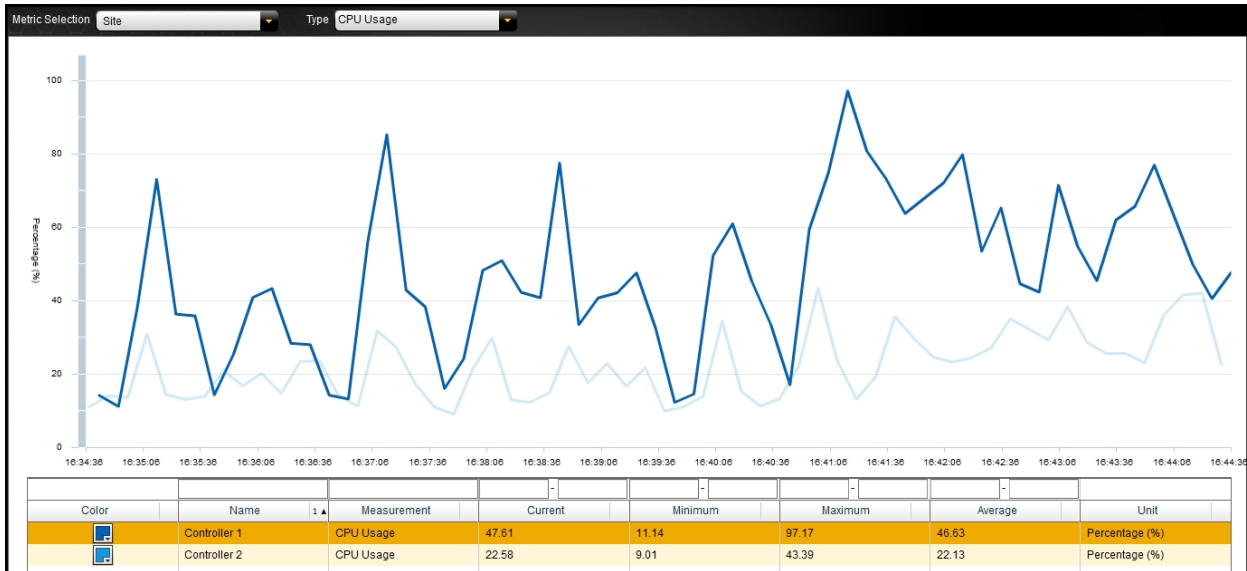
► To filter performance information:

1. Start the Performance Monitor; see [Starting the Performance Monitor](#) on the previous page.
2. Select the **Live** tab (opened by default).
3. From the **Metric Selection** drop-down list, select a component type. In our example, we select **Site**.

- From the **Type** drop-down list, select the Performance Metrics type available (according to your previous selection). In our example, we select **CPU Usage**.

Tip Depending on the metric you selected, for example, if there are many shares, you can sort the column by alphabetical order by clicking the small arrow beside **Name**.

Figure 13-13: Filtering performance metrics



The graphical chart automatically adjusts to display performance statistics for the selected component.

Taking performance snapshots

The Performance Monitor allows you to take performance snapshots for Unity. You can record performance metrics during a specific time period, and then review the snapshots later for analysis. This mechanism can help you diagnose system bottlenecks.

This section includes these topics:

- [Taking a performance snapshot below](#)
- [Viewing a performance snapshot on page 504](#)
- [Deleting a performance snapshot on page 504](#)

Taking a performance snapshot

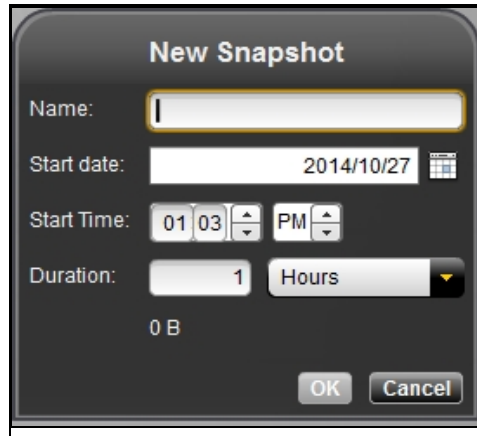
Unity records all performance data metrics by default.

► To create a new snapshot:

- Start the Performance Monitor; see [Starting the Performance Monitor on page 500](#).
- Select the **Snapshots** tab. The Performance snapshots panel opens.

- Click the **New** button at the top. This displays the New Snapshot popup.

Figure 13-14: New Snapshot popup

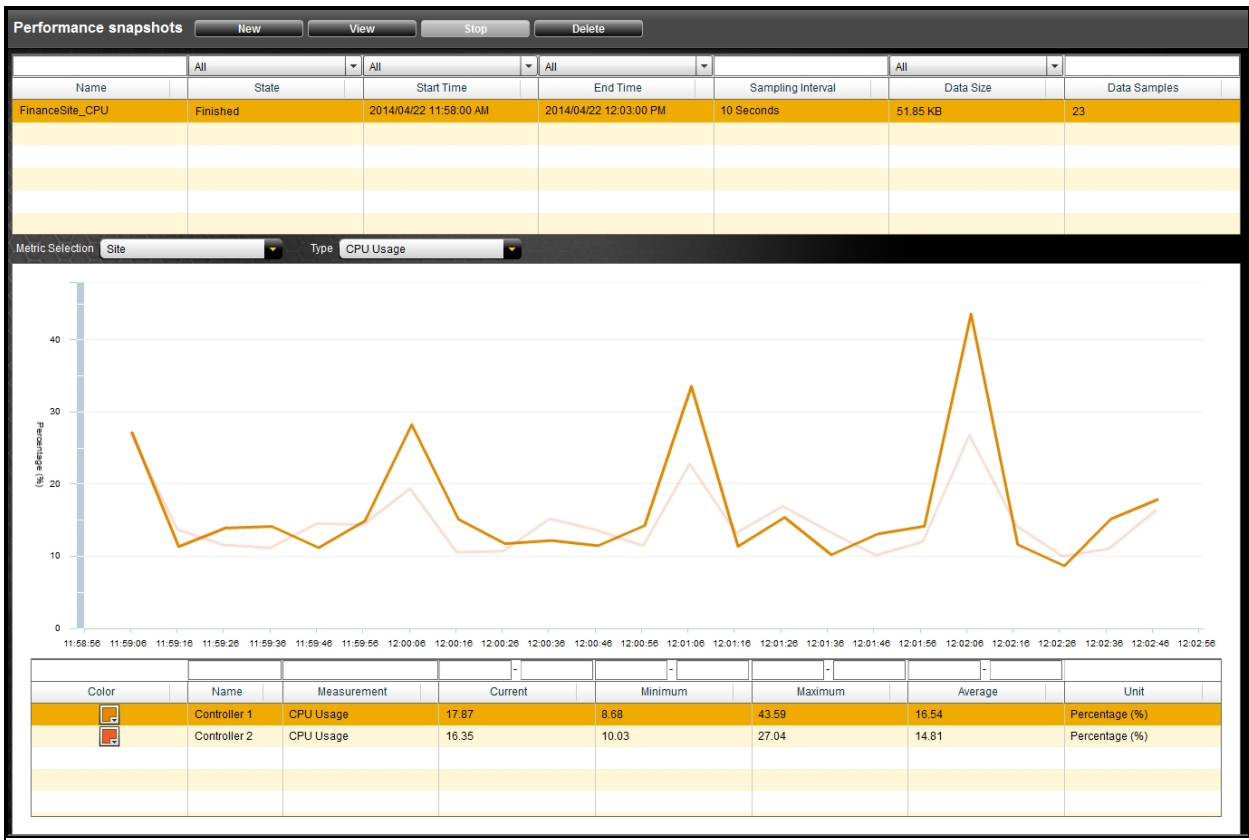


- Specify a name for the snapshot, and then specify its start date, start time, duration, and the sampling interval. The New Snapshot popup updates the total file size of the recording as you change the duration and interval.

Note The snapshot is saved to Unity—not to system disk drives.

- Click **OK**. The new snapshot appears in the grid on the Performance Snapshots panel with a status of *Running*.

Figure 13-15: Performance Monitor—Snapshots view



The **State** column in the grid indicates *Running* for a snapshot that is currently in process, and *Finished* for a snapshot that has completed.

▶ **To stop a snapshot that is currently in process:**

1. Select the snapshot in the grid.
2. Click the **Stop** button. The button changes to *Resume* for the selected snapshot and the state changes to *Stopped*.

▶ **To resume a snapshot that was stopped:**

1. Select the snapshot in the grid.
2. Click the **Resume** button.

Viewing a performance snapshot

You can view snapshots that are:

- currently in process (identified by the **Running** value under the **State** column in the grid on the Recordings panel) and
- completed (identified by the **Finished** value under the **State** column).

▶ **To view a recording:**

1. Start the Performance Monitor; see [Starting the Performance Monitor on page 500](#).
2. Select the Snapshots tab. The Performance snapshots panel opens.
3. In the grid, select the snapshot that you want to view.
4. Click the **View** button at the top. The snapshot opens with the CPU Usage graphical chart displayed.
5. Expand the graphical charts for the other metrics to view recorded data.

Deleting a performance snapshot

This section explains how to delete a performance snapshot.

▶ **To delete a snapshot:**

1. Start the Performance Monitor; see [Starting the Performance Monitor on page 500](#).
2. Select the **Snapshots** tab. The Performance snapshots panel opens.
3. In the grid, select the snapshot that you want to delete. This can be a snapshot currently in process or a previous snapshot.

Viewing historical performance data

The Performance Monitor allows you to keep and view performance data for up to the past 7 days. You can change the number of days during which to keep historical data; see [Changing the duration to keep sampling data on the facing page](#).

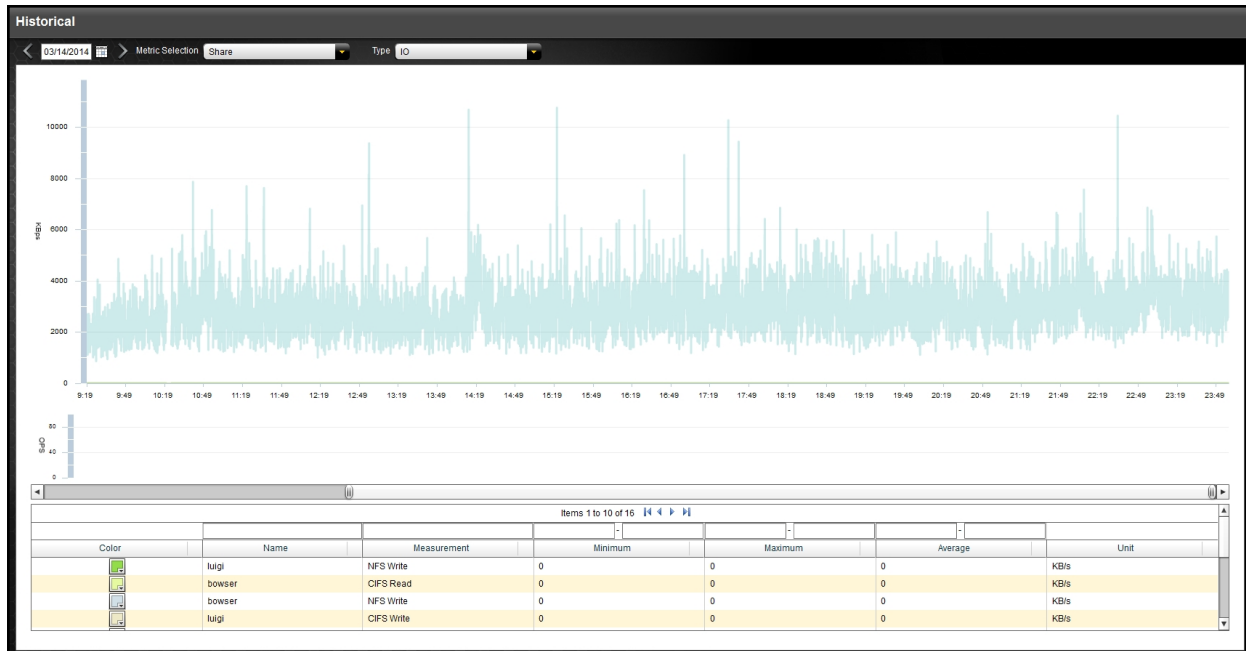
Similarly to the Live and Recordings views, you can filter performance metrics and sort all columns.

▶ **To view historical performance data:**

1. Start the Performance Monitor; see [Starting the Performance Monitor on page 500](#).
2. Select the **Historical** tab. The Historical panel opens.

3. Select a date by clicking the calendar or using the left arrow on the toolbar. By default, today's date is selected.
4. From the **Metric Selection** drop-down list, select the desired performance metric.
5. From the **Type** drop-down list, select one of the available component types.

Figure 13-16: Performance Monitor—Historical view



Changing the duration to keep sampling data

The **Options** tab of the Performance Monitor allows you to change the number of days during which Unity keeps performance sampling data. This data is saved on Unity, not on the system storage pools.

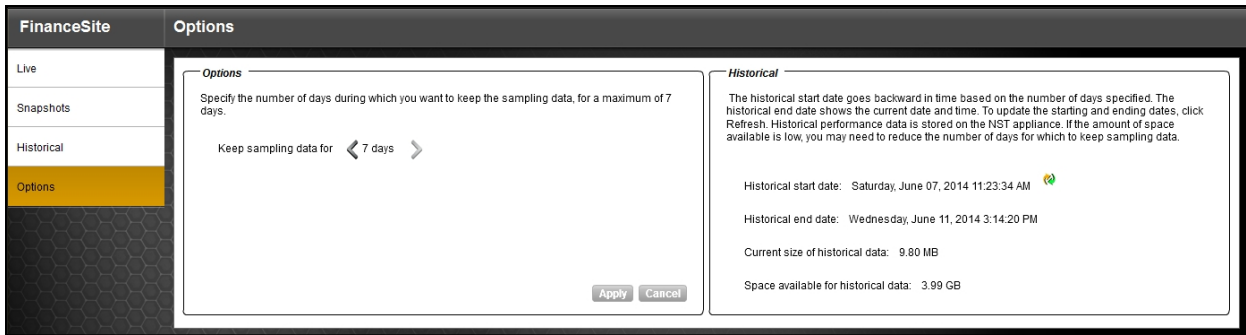
By default, the Performance Monitor keeps sampling data for 7 days. The historical start date goes backward in time based on the number of days specified. The historical end date shows today's date and time.

► To change the number of days:

1. Start the Performance Monitor; see [Starting the Performance Monitor](#) on page 500.
2. Select the **Options** tab. The Options panel opens.

3. In the **Historical** box, use one the left arrow to reduce or the right arrow to increase the number of days for which to keep sampling data. The maximum is 7 days.

Figure 13-17: Performance Monitor—Options view



4. Click **Save Changes**.

Note Once deleted, the sampling data cannot be recovered.

Creating and viewing reports

The Nexsan Unity Reports feature allows you to generate dashboard-type, graphical reports detailing storage capacity across the Unity storage infrastructure.

Reports are organized into six different types and provide detailed information about the storage resources in your environment, including space usage consumption for each file system and/or iSCSI LUN on Unity, space usage consumption on a per user basis, and overall storage pool capacity and used space. You can select the specific site, storage pool, file systems, iSCSI LUNs, and even users upon which you want to report.

Data in reports is based on statistical information accumulated by data collection schedules and stored in a database repository on Unity. Data is collected once a day at 1:00 a.m. at a fixed schedule. When you generate a report, the data displayed is the data obtained during the last data collection. To view the latest data, you must refresh data manually using the **Refresh Data Now** button.

The Nexsan Unity Reports feature can help you answer key questions about your Unity storage resources, including:

- How much storage space is being used?
- How much unused or unallocated storage space is available?
- Is there enough space available for snapshots, or for backups?
- Which user is consuming the most storage resources?
- How fast are storage resources being consumed?
- Where is disk space reaching a critical shortage?

This section includes these topics:

Report types.....	507
Configuring report settings.....	508
Generating reports.....	509
Sending reports by email.....	513
Exporting reports.....	515
Printing reports.....	515
Deleting reports.....	516

Report types

The Nexsan Unity Reports feature currently includes these report types:

Available Space

Available Space reports display overall available capacity on the system. You can also select specific storage pools, file systems, and/or iSCSI or Fibre Channel LUNs upon which you want to report.

Used Space

Used Space reports display the overall space consumption on the system. You can also select specific storage pools, file systems, and/or iSCSI or Fibre Channel LUNs upon which you want to report.

LUN Virtual Volume Size (Thin Provisioning)

These reports display the virtual volume size for each thin-provisioned iSCSI or Fibre Channel LUN, including both available and used space for the LUNs. You can select specific storage pools and iSCSI or Fibre Channel LUNs upon which you want to report.

When selecting this report type, LUNs that do not have Thin Provisioning enabled cannot be selected. Likewise, file systems are not available for selection.

User Quota(s): Space Consumption by User

The Space Consumption by User reports display space consumption on a per user basis for each file system on the system. You can select specific file systems and users upon which you want to report. Space quotas must be set for the selected user(s) to be able to view this report. To set space quotas, see *Setting a space usage quota on a file system for a user and/or group* in the *Using the menu-driven nxadmin CLI* chapter, of the *nxadmin CLI Reference Guide*.

User Quota(s): Critical Consumption

These reports display critical space consumption for selected file systems on a per user basis. Use these reports to display space consumption for users who have reached or exceeded set quota limits. By default, the quota threshold is set to 90%. If a user is still below 90% of his quota limit for the selected file system(s), no data will be displayed in the report.

To modify quota limits for users, see *Setting a space usage quota on a file system for a user and/or group* in the *Using the menu-driven nxadmin CLI* chapter, of the *nxadmin CLI Reference Guide*. To modify the quota threshold, see [Configuring report settings](#) below.

When selecting this report type, LUNs are not available for selection.

User Quota(s): Normal Consumption

These reports display normal space usage for selected file systems on a per user basis. Use these reports to view the overall space consumption for users who have usage quota limits configured. To modify quota limits for users, see *Setting a space usage quota on a file system for a user and/or group* in the *Using the menu-driven nxadmin CLI* chapter, of the *nxadmin CLI Reference Guide*.

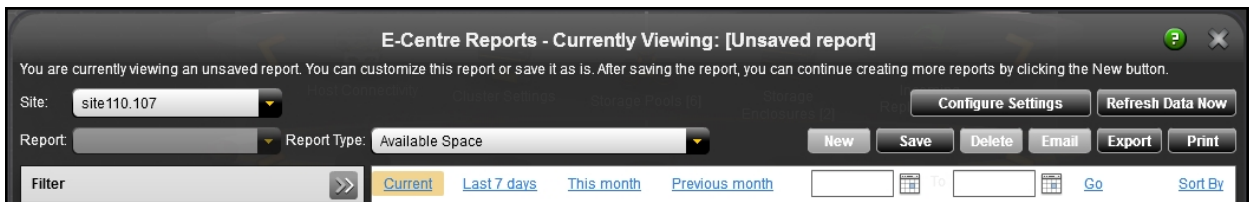
When selecting this report type, LUNs are not available for selection.

Configuring report settings

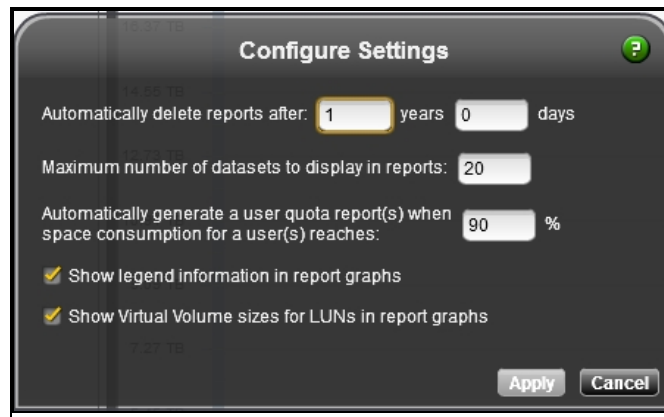
Before generating reports, you may want to modify some settings that will alter the information displayed. For example, you may want to generate a report showing the space consumption when user quotas reach a threshold of 80%. To generate this report, you must modify the space consumption threshold first.

► **To configure settings:**

1. Launch Nexsan Unity.
2. From the **Tools** menu, click the **Generate Reports**  icon. The Unity Reports window opens.
3. From the upper right corner of the Reports window, click the **Configure Settings** button.



4. The Configure Settings dialog box appears. This image displays the default configuration settings.



5. Perform one or more of the following actions:

To...	Do this
modify the time period during which reports are kept	Specify the value for the number of years and/or days in the relevant fields. You must set at least 1 day.
modify the maximum number of datasets to display in each report	Specify the value in the field.
modify a space consumption threshold for user quota reports	Specify the percentage value in the field.
remove legend information in report graphs	Clear the option.
remove the virtual volume size in report graphs for LUN reports	Clear the option.

6. Click **Apply**.

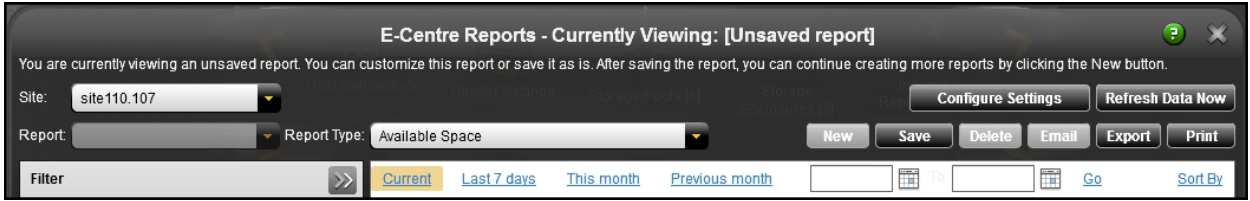
Generating reports

Follow this procedure to generate a report. After generating the report, you have the option to save it for later reference.

► **To generate a new report:**

1. Launch Nexsan Unity.
2. From the **Tools** menu, click the **Generate Reports**  icon. The Unity Reports window opens.

- From the **Site** drop-down list, select a site. If there is only one site, it is selected by default.



- From the **Report** tool bar, click **New**.

Note If this is the first time you are generating a report, you will see the default report and the **New** button will not be available. Customize this report as described in the following steps or save it as is. The **New** button will then become available and you will be able to create reports from scratch.
- From the Date Selection bar, select the time frame for which to generate the report:
 - **Current** (default)
 - **Last 7 days**
 - **This month**
 - **Previous month**
 - To view data older than the previous month, click the calendar icon and select the start and end dates. Click **Go**.
- From the **Filter** panel, select the applicable child nodes(s) for the site. A check mark indicates that specific pools will be included in the report. A star indicates that all pools (including future pools) will be included.

To select all child nodes, click the site name, then click the **Select all child nodes** button on the **Filter** panel.
- From the **Report Type** drop-down list, select the report type; see [Report types](#) on page 507 for details. If you selected a report type that does not include users, the reports gets generated; skip to **step 13**. Otherwise, if you selected a report type that includes users, the **Add Users** button becomes visible next to the **Report Type** drop-down list. Click this button to choose one or more users.

8. From the Select Users to Display in Report dialog box, enter the user name in the **Name** field. By default, the **Name** field has **Starts with** selected. You can modify this to **Ends with** or **Is exactly**.

Figure 13-18: Reports - Select Users to Display in Report

Select the user(s) that you want to generate a space usage report(s) for; the user(s) you specify must have access permissions to, at least, one share on the system. To select a user, first open the Domain drop-down list and select the domain where the user(s) exists. Then, drag the relevant user(s) to the Selected Users list; if needed, use the Search function to display specific users.

Name: Starts with Find Now

Advanced search options ▼

Search results:

Name	Type
Bob	User

Selected Users:

Name	Type

Apply Cancel

9. Click **Find Now**. The **Search Results** lists gets updated accordingly.
10. Select the user name by doing one of these actions:
 - Drag and drop the name to the **Selected Users** list, or
 - Click the arrow pointing to the right
11. Click **Apply**. The reports gets generated.
12. (Optional) To sort data in the report, click **Sort By** from the Date Selection bar. Depending on the report type you generated, one or more of these options will be available:
 - Used Space (Descending)
 - Used Space (Ascending)
 - User Name (Ascending)
 - % Space Consumption (Descending)
13. To save the report, click the **Save** button from the Report tool bar.
14. Enter a name for the report and click **Save**. The saved report now appears in the **Report** drop-down list.

Tip To view more detailed information on data displayed, rest the mouse on a bar.

▶ **To view a saved report:**

- From the **Report** drop-down list, select the desired report.

▶ **To modify a report:**

1. After a report is generated, whether new or saved, you can modify these settings:

- Add or remove users, if this report involves users
- Change the time duration
- Add or remove child nodes from the current selection
- Modify the report configuration settings; see [Configuring report settings](#) on page 508.

2. Apply the modifications to regenerate the report.

If data does not display right away, click the **Refresh Data Now** button from the right-end corner of the window.

3. To save the report, click the **Save button** from the Report tool bar.

4. If this report was previously saved:

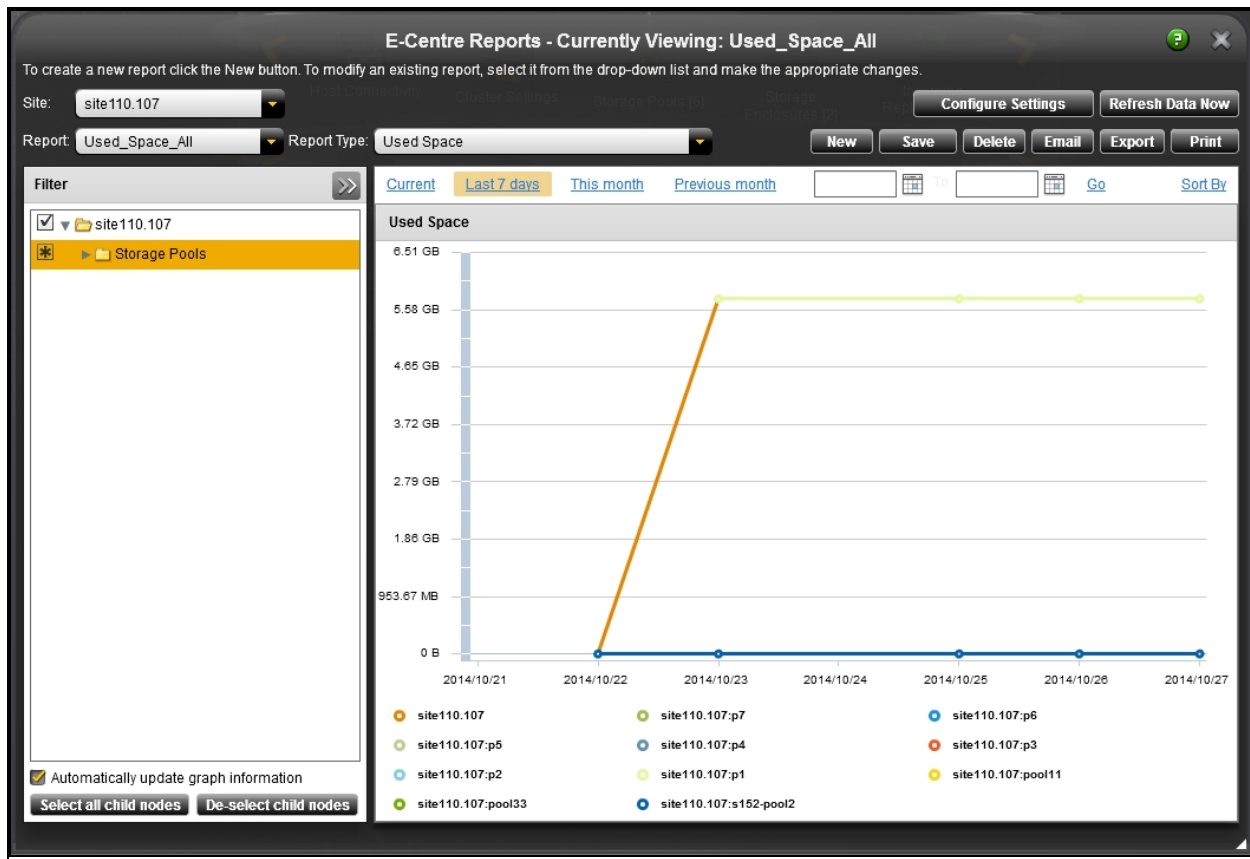
- Click **Yes** if you want to overwrite the existing report.
- Click **No** if you want to create a new report.

If the report was new:

- a. Enter a name for the report when prompted.
- b. Click **Save**. The saved report now appears in the **Report** drop-down list. The view reverts back to the default view.

This image provides an example of the space used in the selected site.

Figure 13-19: Example of report



13

Sending reports by email

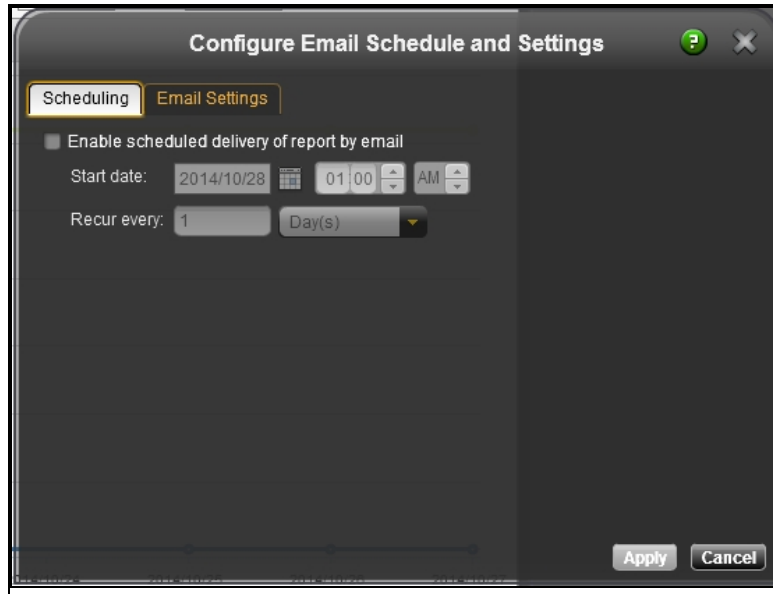
Reports can be sent by email automatically to storage administrators to notify them of critical information regarding space usage and consumption. Reports must be generated and saved, as described in [Generating reports](#) on page 509.

► To send reports automatically by email:

1. Configure SMTP notifications for the site. For the procedure steps, see [Configuring SMTP server settings for the site](#) on page 535.
2. From the **Report** drop-down list, select a saved report.
3. Click the **Email** button.

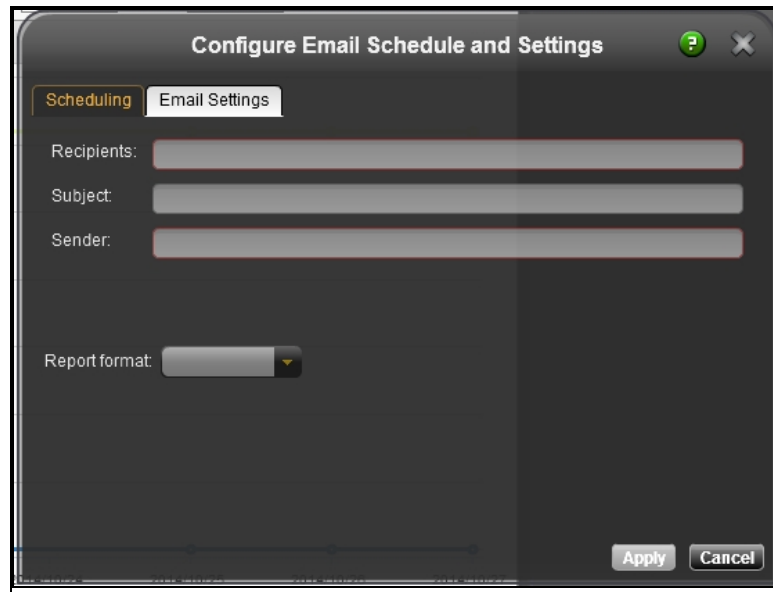
4. On the **Scheduling** tab, select the **Enable scheduled delivery of report by email** option.

Figure 13-20: Reports - Email Scheduling



5. Set the start date.
6. Set the recurrence frequency.
7. Click the **Email Settings** tab.

Figure 13-21: Reports - Email Settings



8. Enter an email address in the **Recipients** field.
9. Enter the report name in the **Subject** field.
10. Enter your email address in the **Sender** field.
11. Select the report format, either sent as HTML in the email or in a CSV file as attachment.

- Click **Apply**. The selected report will be regenerated and sent at the specified time.

Exporting reports

Reports can be exported to external files in HTML or CSV formats. Reports can be exported without being saved.

► To export a report:

- Generate a report as described in [Generating reports on page 509](#).
- From the Report tool bar, click the **Export** button.

Figure 13-22: Reports - Exporting



- Select the file format.
- Click **Save**.
- In the Save As dialog box, enter the file name and choose the folder.
- Click **Save**.

This example shows a user quota report for user Bob, who is exceeding the 90% quota limit of space consumption.

Figure 13-23: Reports - Sample of exported report in HTML format

Critical space usage Bob				
Critical User Quota Report				03/28/2013
Date range: 03/28/2013				
Jump to: <input type="text" value="Share: FinanceSite176/ FinancePool1/ PayRollData1"/>				
Share: FinanceSite176/ FinancePool1/ PayRollData1				
User Name	Used Space	Available Space	Quota	Date
bob	92.21 GB	7.79 GB	100.00 GB	03/28/2013

Printing reports

Reports can be printed on a printer connected to your network or in a file. Reports can be printed without being saved.

► To print a report:

- Generate a report as described in [Generating reports on page 509](#).
- From the Report tool bar, click the **Print** button.

3. In the Print dialog box, leave the default printer or select a new one and click **Print**.

Deleting reports

This task provides steps to delete a saved report.

▶ **To delete a report:**

1. From the **Report** drop-down list, select the report.
2. From the Report tool bar, click the **Delete** button.
3. When prompted to confirm, click **Yes**.

Chapter 14

Event logging and notification

All event messages generated by Unity (including those issued by a Nexsan storage device connected externally to the system) are logged to the [event logs](#), which you can then retrieve and display in Unity's Event Viewer. The event logs provide a record of past events that have occurred on the system to help you monitor Unity and its software and hardware components.

This section includes these topics:

Viewing events	518
Using the Event Viewer	519
Configuring logging options	529
Setting up notification	530

Viewing events

Unity continuously monitors both its software components (for example, the Clustering, Data Replication, and Snapshots functions) and hardware components (such as, fans, power supply units, and disk drives). This also includes the remote sites to which the primary site is connected, in a multi-site environment. When an event occurs (for example, a disk failure or a possible breach of security), Unity records the event in the event logs.

By default, Unity keeps events in the event logs for up to one year, after which the system automatically clears the event logs; you can change this default setting if needed. For more information, see [Configuring logging options](#) on page 529.

You view and filter events contained in the event logs in Unity Event Viewer. The Event Viewer also allows you to save events to disk (in either Microsoft Excel, Microsoft Word, HTML, or text format), or email a specific set of events to recipients that you specify.

▶ **To access Unity Event Viewer:**

- Select the **View Events** option from the **System Events** menu in the Unity toolbar.

Using the Event Viewer

Unity's Event Viewer allows you to view and filter events in the event logs, save events in the logs to disk (in either Microsoft Excel, Microsoft Word, HTML, or text format), and email a specific set of events to recipients that you specify.

This section includes these topics:

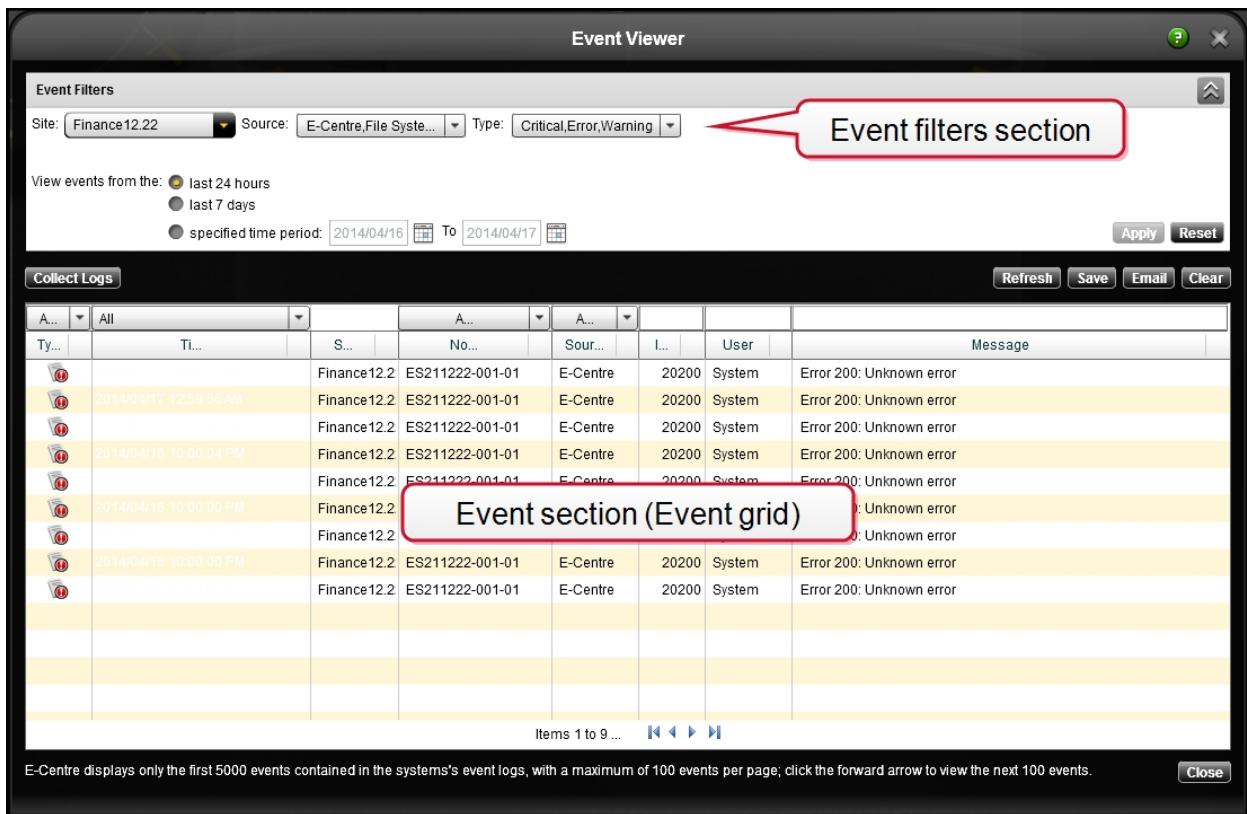
Layout of the Event Viewer.....	519
Filtering events in the Event Viewer.....	522
Saving events.....	526
Emailing events.....	527
Clearing event logs.....	527
Collecting logs.....	528

Layout of the Event Viewer

When you initially open the Event Viewer, it displays the first 200 events in the event logs that were generated in the last 24 hours. By default, it displays events for all source components (Unity, Storage Device, File System, and System) and for all severity levels or types (Critical, Error, Warning, and Information). The site you are connected to is selected by default; you can choose another site from the drop-down menu.

The Event Viewer includes these sections.

Figure 14-1: Event Viewer



Event Filters section





This section contains options and settings for filtering events displayed in the Event Viewer. You can filter events by site, source, and type; you can also filter events by a specific date or time period. For more information about filtering events, see [Filtering events in the Event Viewer on page 522](#).

Events section

This section contains the following items.

Table 14-1: Event Viewer—Events section

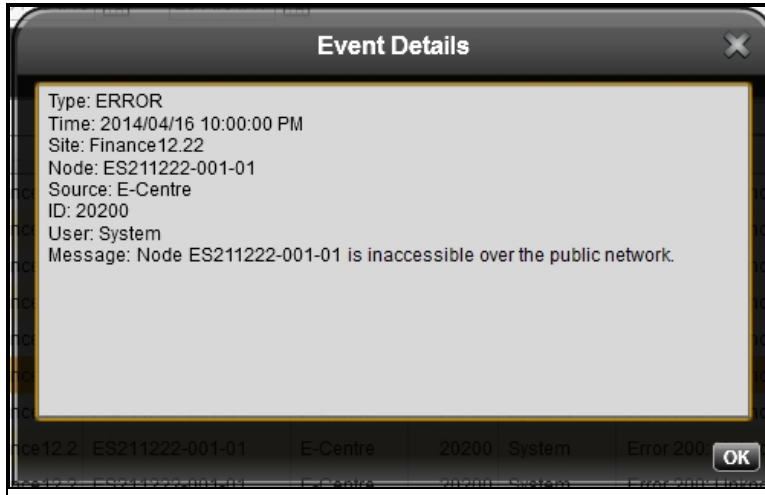
Item	Description
Collect Logs button	Click the Collect Logs button to collect all system log files on Unity and create an encrypted package. After downloading the encrypted package, you can send it to Nexsan Technical Support for analysis. This command is similar to the <code>createlogpackage</code> command in the <code>nxadmin</code> command-line interface (CLI) and the <code>nxcmd Event CollectLogs</code> command in the Unity ADM command-line interface (CLI).
Refresh button	Click the Refresh button to retrieve new events from the event logs and display them in the Event grid. Unity periodically checks the event logs for new events, and if it finds new entries in the logs, it displays a message instructing you to refresh the grid.
Save button	Click the Save button to save the events currently displayed in the Event grid to disk (in either Microsoft Excel, Microsoft Word, HTML, or text format); for more information, see Saving events on page 526 .
Email button	Click the Email button to send the events currently displayed in the Event grid to an email recipient. Unity prompts you to specify email settings, including the email address of your recipient(s) and the IP address of the SMTP server from where the email will be routed; For more information, see Emailing events on page 527 .
Clear button	Click the Clear button to erase all the events in the event logs.
Event grid	The Event grid displays the first 200 events in the event logs. The logs are displayed on two separate pages, with each page displaying 100 events; use the left and right arrows below the grid to scroll through the pages. The Event grid includes these columns:

Item	Description
	<ul style="list-style-type: none"> ● Type: this column displays an icon identifying the event's severity level, or type. The icons that are displayed in the Type column include: <ul style="list-style-type: none"> ● : identifies a critical event. A critical event indicates a severe error that prevents a system component(s) from running. A critical event may lead the system to an abort situation. ● : identifies an error event. An error event may still allow any affected system component(s) to continue running. However, if left unattended, an error event may lead the system to an abort situation. ● : identifies a warning event. A warning event indicates a potentially harmful situation. ● : identifies an informational event. Informational events highlight the progress of Unity's software components, such as the Clustering, Data Replication, and Snapshots functions. ● Time: this column displays the date and time when the event occurred. ● Site: this column identifies the Unity site where the event occurred. This is particularly useful in multi-site environments where you use a single Unity running Unity to manage multiple systems installed in disparate geographic locations. ● Source: this column identifies the source component of Unity that generated the event; source components include: <ul style="list-style-type: none"> ● Unity: events logged by Unity and its software components, including Unity Clustering, Data Replication, and Snapshots functions. ● Storage System: events generated by Nexsan storage systems attached externally to Unity (via SAS or Fibre Channel), if available, and logged to the event logs. ● File System: events generated by the Unity operating system. ● System: events generated by Unity for hardware faults on the system, such as fan, power supply, or disk failures. ● ID: this column displays each event's event ID. ● User: this column displays the service id of the service that logged the event. ● Message: this column displays a description of the event. <p>▶ Viewing the event message and details for an event: You can view the full error message and all the details for an event by double-clicking the event in the Event grid. The Event Viewer displays the Event Details dialog box.</p>

Filtering events in the Event Viewer

The Event Viewer provides event filters that allow you to retrieve events from the event logs that match a certain criteria and display only those events in the Event grid. The Event Viewer displays the Event Details dialog box.

Figure 14-2: Event Details



You can use the event filters for:

- [Filtering events by site, source, and/or severity type](#) below
- [Filtering events according to a time period or a date](#) on the facing page

You can also filter the events displayed in the Event grid, or search for specific types of events:

- [Filtering events in the Event grid](#) on page 524
- [Searching for a specific event in the Event grid](#) on page 525

Filtering events by site, source, and/or severity type

This section describes how to filter events in the event logs by site, source, and/or event type.

► To only display events from a specific site:

Note Use this filter if your Unity implementation includes multiple systems that you manage from a single Unity running Unity. By default, the Event Viewer displays events from the site that you are currently managing.

1. In the Event filters section, open the **Site** pick list.
2. Select the site that you want to display events for.
3. Click **Apply**; the Event Viewer retrieves events from the event logs on the selected site and it displays the events in the Event grid.

► **To only display events from a specific source component of the system:**

1. In the Event filters section, open the **Source:** pick list.
2. Select the source components that you want to display events for. By default, the Event Viewer displays events from all source components. If you do not want to display events from a specific source, clear its check box:
 - **Unity**
 - **Storage Device**
 - **File System**
 - **System**
3. Click **Apply**; the Event Viewer retrieves events that match the selected source component(s) from the event logs and it displays the events in the Event grid.

► **To only display events of a specific severity or type:**

1. In the Event filters section, open the **Type:** pick list.
2. Select the severity level that you want to display events for. By default, the Event Viewer displays events for all severity levels; if you do not want to display events of a specific type, clear its check box:
 - **Critical**
 - **Error**
 - **Warning**
 - **Information**
3. Click **Apply**; the Event Viewer retrieves events that match the selected severity type(s) from the event logs and it displays the events in the Event grid.

► **To further filter events:**

You can further filter events in the event logs by combining filter settings; for example, if you only want to display all *critical* events for the *Unity* source component from *site176* that were generated in the last 24 hours, set these filter settings:

1. Open the **Site:** pick list and select *site176*.
2. Open the **Source:** pick list and select **Unity**; if all the source components are selected in the pick list (default setting), clear the corresponding check boxes to deselect them.
3. Open the **Type:** pick list and select **Critical**; if all the severity types are selected in the pick list (default setting), clear the corresponding check boxes to deselect them.
4. Select the **last 24 hours** option (default setting).
5. Click **Apply**; the Event Viewer retrieves all the events that match the specified filter criteria and it displays the events in the Event grid.

Notes:

- The Event Viewer maintains the settings that you configure for event filters, even after you log out of Unity.
- You can manually reset event filters to their default settings by clicking the **Reset** button.

Filtering events according to a time period or a date

This section describes how to filter events that were generated on a specific date or within a specified time period in the event logs, and display the events in the Event Viewer.

► **To only display events generated in the last 24 hours or in the last 7 days:**

1. In the Event filters section, select the **last 24 hours** option (default setting) or **last 7 days** option.
2. Click **Apply**; the Event Viewer retrieves all the events from the event logs that were generated in the last 24 hours or the last 7 days, depending on your selection, and it displays the events in the Event grid.

► **To only display events generated on a specific date or within a specified time period:**

1. In the Event filters section, select the **specified time period** option.
2. Click the relevant calendar icons to specify the *from* and *to* date that you want to display events for. For example, if you want to display events from May 26, 2013 to May 29, 2013, select May 26, 2013 in the first (or *from*) calendar and select May 29, 2013 in the **To** calendar. If you want to display events that were generated on a specific date, specify the same date for both the *from* and *to* calendar entries. For example, if you want to display events that were generated on May 29, 2013, select May 29, 2013 in both the first (or *from*) calendar and the **To** calendar.
3. Click **Apply**; the Event Viewer retrieves all the events from the event logs that were generated within the time period or on the date that you specified, and it displays the events in the Event grid.

Notes:

- The Event Viewer maintains the settings that you configure for event filters, even after you log out of Unity.
- You can manually reset event filters to their default settings by clicking the **Reset** button.

Filtering events in the Event grid

Once you filter the events in the event logs by configuring the filters in the Event filters section, you can further filter the events displayed in the Event grid by site, source, event type, and/or time period.

► **To only display events from a specific site in the Event grid:**

Note Use this filter if your Unity implementation includes multiple systems that you manage from a single Unity running Unity. By default, the Event Viewer displays events from the site that you are currently managing.

- In the text box above the **Site** column heading in the Event grid, type the site name for the site that you want to display events for. For example, if you want to display events for *site176*, type *site176* (or another variation of the site name—for example, *176*) in the text box.

The Event Viewer searches for the relevant site in the grid and only displays the events for the specified site.

► **To only display events from a specific source component of the system in the Event grid:**

1. Open the pick list above the **Source** column heading in the Event grid.
2. Select the source components (**Unity**, **Storage Device**, **File System**, and **System**) that you want to display events for in the grid. By default, the Event Viewer displays events from all source components; if you do not want to display events from a specific source, clear its check box.

The Event Viewer displays all events for the source component(s) you specified.

▶ **To only display events of a specific severity or type in the Event grid:**

1. Open the pick list above the **Type** column heading in the Event grid.
2. Select the severity type (**Critical**, **Error**, **Warning**, and **Information**) that you want to display events for in the grid. By default, the Event Viewer displays events for all severity levels; if you do not want to display events of a specific type, clear its check box.

The Event Viewer displays all events for the severity type(s) you specified.

▶ **To only display events from a specific time period:**

1. Open the pick list above the **Time** column heading in the Event grid.
2. Select the time period (**This Hour**, **Today**, **Yesterday**, **This Week**, **This Month**, **This Year**, or **Custom**) that you want to display events for in the grid. You must specify a date range for the **Custom** time period.

The Event Viewer displays all events for the time period you specified.

▶ **To further filter events:**

You can further filter events in the Event grid by combining filter settings; for example, if you only want to display all *critical* events for the *Unity* source component from *site176* that were generated *yesterday*, set these filter settings in the Event grid:

1. In the text box above the **Site** column heading in the Event grid, type *site176* (or another variation of the site name—for example, *176*).
2. Open the pick list above the **Source** column heading in the Event grid and select *Unity*; if all the source components are selected in the pick list (default setting), clear the corresponding check boxes to deselect them.
3. Open the pick list above the **Type** column heading in the Event grid and select **Critical**; if all the severity types are selected in the pick list (default setting), clear the corresponding check boxes to deselect them.
4. Open the pick list above the **Time** column heading in the Event grid and select **Yesterday**.

The Event Viewer filters the events in the Event grid according to the filter settings you specified.

Notes:

- The Event Viewer maintains the settings that you configure for event filters, even after you log out of Unity.
- You can manually reset event filters to their default settings by clicking the **Reset** button.

Searching for a specific event in the Event grid

You can search for a specific event or events in the grid by site name, event ID, or user, or by looking for a specific search string in the event messages.

▶ **To search for a specific event or events in the grid:**

- Enter a search string in the text boxes above the **Site**, **User**, and or **Message** column headings.
For example, if you want to search for all events related to storage pools on *site176*, type *site176*, *176*, or another variation of the site name in the text box above the **Site** column heading; and type *pool* in the text box above the **Message** column heading.

Figure 14-3: Searching for an event in the Event grid

Type	Time	Site	Node	Source	ID	User	Message
	2014/06/11 10:47:39 AM	Finance12.2	ES211222-001-01	E-Centre	20200	System	Error 200: Unknown error
	2014/06/11 10:33:04 AM	Finance12.2	ES211222-001-01	E-Centre	20200	System	Error 200: Unknown error
	2014/06/11 10:32:57 AM	Finance12.2	ES211222-001-01	E-Centre	20200	System	Error 200: Unknown error
	2014/06/11 10:30:48 AM	Finance12.2	ES211222-001-01	E-Centre	20200	System	Error 200: Unknown error
	2014/06/11 9:47:37 AM	Finance12.2	ES211222-001-01	E-Centre	1271	System	Network communication error occurred attempting to communicate
	2014/06/11 9:44:19 AM	Finance12.2	ES211222-001-01	E-Centre	1271	System	Network communication error occurred attempting to communicate
	2014/06/11 8:27:50 AM	Finance12.2	ES211222-001-01	E-Centre	1271	System	Network communication error occurred attempting to communicate
	2014/06/11 8:24:32 AM	Finance12.2	ES211222-001-01	E-Centre	1271	System	Network communication error occurred attempting to communicate
	2014/06/11 7:08:04 AM	Finance12.2	ES211222-001-01	E-Centre	1271	System	Network communication error occurred attempting to communicate
	2014/06/11 7:04:46 AM	Finance12.2	ES211222-001-01	E-Centre	1271	System	Network communication error occurred attempting to communicate
	2014/06/11 5:48:17 AM	Finance12.2	ES211222-001-01	E-Centre	1271	System	Network communication error occurred attempting to communicate
	2014/06/11 5:44:59 AM	Finance12.2	ES211222-001-01	E-Centre	1271	System	Network communication error occurred attempting to communicate
	2014/06/11 4:28:30 AM	Finance12.2	ES211222-001-01	E-Centre	1271	System	Network communication error occurred attempting to communicate

Items 1 to 21 of 21

E-Centre displays only the first 5000 events contained in the system's event logs, with a maximum of 100 events per page; click the forward arrow to view the next 100 events.

The Event Viewer displays all events matching your search criteria.

Saving events

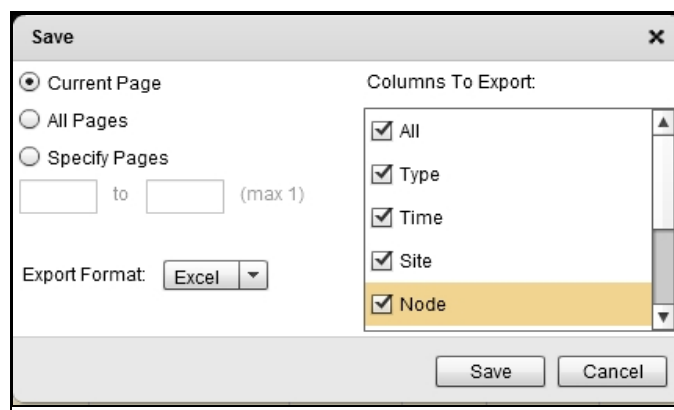
The Event Viewer allows you to save the events displayed in the Event grid to disk, as a permanent record. You can save events in one of these formats:

- Microsoft Excel (CSV)
- Microsoft Word
- HTML
- Text

► To save all the events currently displayed in the Event Viewer to disk:

1. Click the **Save** button in the Event filters section. This displays the Save dialog box.

Figure 14-4: Event Viewer, Save dialog box



2. Select the page range containing the events that you want to save to disk:
 - **Current Page:** select this option if you want to display the events on the page that is currently displayed in the Event grid. For example, if the Event grid is currently displaying events on page 2, Unity saves all events on that page to disk.
 - **All Pages:** select this option if you want to save the events on both pages 1 and 2 to disk.
 - **Specify Pages:** select this option if you only want to save the events on a specific page to disk. You must enter the relevant page number(s) in the text boxes.
3. Select the format that you want to save the events to in the **Export Format:** pick list.
4. Click the **Save** button. Unity prompts you to specify the location where you want to save the file. Unity provides a default file name; you can change the file name, if needed.

Emailing events

The Event Viewer allows you to email the events displayed in the Event grid to any valid email address. To email events, you need to provide a valid SMTP server IP address through which Unity will send the email.

► To email all events currently displayed in the Event Viewer:

1. Click the **Email** button in the Event filters section. This displays the Email Events dialog box.

Figure 14-5: Event Viewer, Email Events dialog box

2. Enter a subject for the email in the **Subject** field.
3. Enter a valid sender's email address in the **From** field.
4. Enter a valid recipient address in the **To** field. If you want to send the email to more than one recipient, use the semi-colon (;) to separate recipient email addresses; for example:
bob@abc.com;jack@abc.com;jill@abc.com.
5. Enter a valid SMTP server IP address in the **SMTP Server** field. If you configured email notification for the site and have already provided a valid SMTP Server IP address, Unity automatically sets that IP address in the **SMTP Server** field.
6. Click **Email** to send the events to the email recipient(s).

Clearing event logs

If needed, you can clear the event logs on Unity. This permanently deletes all log entries in the event logs.

Note Before clearing the logs, we recommend that you save the logs to disk using the **Save** function; see [Searching for a specific event in the Event grid on page 525](#).

► **To clear the event logs:**

1. In the Event filters section, open the **Site:** pick list.
2. Select the site that you want to clear logs from.
3. Click the **Clear** button.
4. Unity prompts you to confirm the clear operation; click **Yes** to clear the event logs.

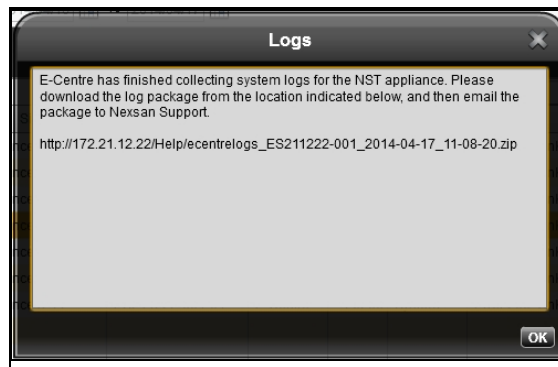
Collecting logs

This function collects all system log files on Unity and creates an encrypted package that you download from Unity. This function is similar to the `createlogpackage` command in the `nxadmin` command-line interface (CLI). After downloading the encrypted package, you can send it to Nexsan Technical Support for analysis.

► **To collect logs:**

1. Click the **Collect Logs** button in the Event filters section. Unity begins the log collection process and generates a log package.
2. Once this process completes, the Logs dialog box displays the URL location on the Management virtual IP address from where you can download the log package. Click **OK** to close the Logs dialog box.

Figure 14-6: Event Viewer, Logs dialog box

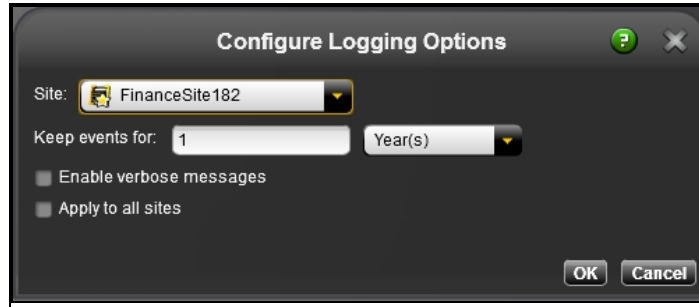


3. Copy the URL to your browser and download the log package.
4. Send the log package to Nexsan Technical Support.

Configuring logging options

Unity provides the Configure Logging Options dialog box to let you customize logging options for your Unity site(s).

Figure 14-7: Configure Logging Options dialog box



You can specify a duration after which event logs are automatically deleted from the system. In general, Unity periodically rotates event logs to prevent system log files from rapidly increasing in size and affecting performance.

Unity does not delete log entries during log rotation; it only clears the log files if:

- you manually invoke the **Clear** option to delete event logs;
- the duration that you set for keeping logs on the system has elapsed; or,
- the disk space reserved for the log files is at over 80% used capacity.

You can enable the verbose logging mode records more information than the usual logging mode. Use this option to help troubleshoot technical problems.

► To configure the Configure Logging Options:

1. From the **System Events** menu in the Unity toolbar, select the **Configure** option.
2. Select the site using one of these options:
 - For one site only, select the site that you want to configure from the **Site** pick list.
 - For all sites, select the **Apply to all sites** option.
3. To configure how long to keep event logs:
 - a. Select a duration—**Day(s)**, **Weeks(s)**, **Month(s)**, or **Year(s)**—from the pick list.
 - b. Enter the desired value for the **Keep events for** field. The default setting is 1 year.
4. To enable verbose logging, select the **Enable verbose messages** option.
5. Click **OK** to save your settings and close the Configure Logging Options dialog box.

Setting up notification

You can configure Unity to send automated notifications to selected personnel when an event is generated, based on the level of severity of the event. For example, if your Unity runs out of disk space, you can configure Unity to send a notification email to the system administrator. Or, you can configure Unity to send a Simple Network Management Protocol (SNMP) trap to a Network Management Station (NMS), which could in turn be configured to send an SMS text message to the administrator's cellular phone.

This allows you to proactively monitor the health of Unity and address any issues that may arise.

In Unity, event notification can take two forms:

- An Email message, which Unity sends through an SMTP server that you specify.
- An SNMP (Simple Network Management Protocol) trap, to notify a central Network Management Station (NMS)—such as, HP OpenView or CA Unicenter—of any events generated by Unity.

You set up event notification in the Configure Email and SNMP Notification dialog box.

Note Before you set up email notification for system events and space usage threshold violations on storage pools and shares, you must configure SMTP server settings for the site.

▶ **To access the Configure Email and SNMP Notification dialog box:**

- Select the **Configure Notification Settings** option from the **Tools** menu in the Unity toolbar.

This section includes these topics:

Setting up email notification for system events	531
Setting up system notifications	533
Configuring SMTP server settings for the site	535
Setting up SNMP notification	537

Setting up email notification for system events

You can configure Unity to send email notifications to selected personnel when an event is generated on the system. Unity allows you to send separate email notifications for each event type or severity level—Critical, Error, Warning, and Information; and Unity also allows you to configure the notification frequency for each event type. For more information about event types, see [Viewing events](#) on page 518.

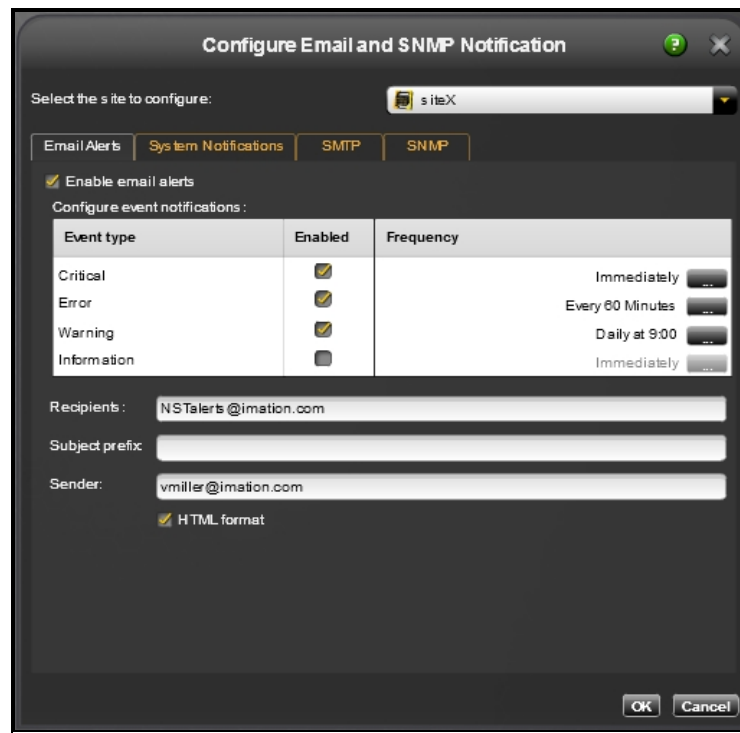
To configure email notification, you need:

- valid email addresses for notification recipients;
- a subject prefix for email notifications;
- a sender email address.

► To set up email notification for system events:

1. Select the **Notifications** option from the **Tools** menu in the Nexsan Unity toolbar.
2. Select the **Email Alerts** tab.

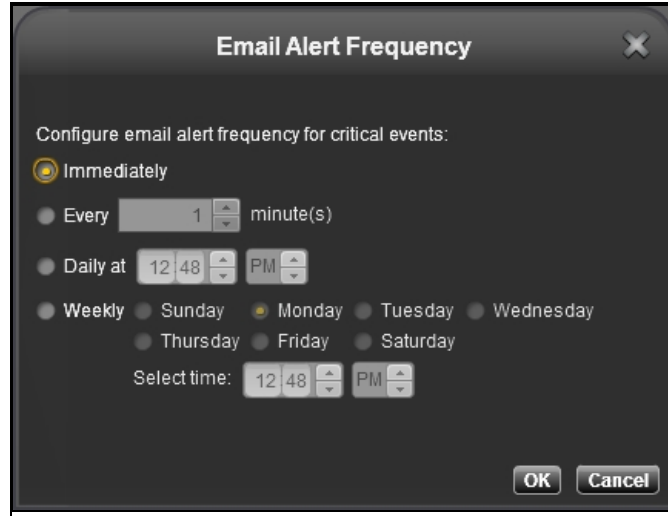
Figure 14-8: Configure Email and SNMP Notification dialog box—Email Alerts tab



3. From the **Select the site to configure:** list, select the site that you want to configure email notifications for.
4. Select the **Enable email alerts** option to enable email notification.
5. In the **Configure event notifications:** grid, click the corresponding check box in the **Enabled** column for each event type that you want to enable email notifications for. For example, if you want to enable email notifications for Critical and Error events, select the corresponding check boxes in the **Enabled** column.

6. Set the notification frequency for each event type that you enabled email notifications for:
 - a. Click the corresponding button in the **Frequency** column; this displays the Email Alert Frequency dialog box.

Figure 14-9: Setting up email notification, Email Alert Frequency dialog box



- b. Set the frequency at which you want Unity to send email notifications for the selected event type. For Critical events, we recommend that you set the frequency to **Immediately**, in order to be notified as soon as possible of a critical system event. For Error events, we recommend that you set the frequency to at least once every 60 minutes.
 - c. Click **OK** to save your settings and close the Email Alert Frequency dialog box.
7. In the **Recipients:** field, enter a valid list of recipient email addresses that you want to send email notifications to. Use the semi-colon (;) to separate recipient email addresses; for example: **bob@abc.com;jack@abc.com;jill@abc.com**.
8. In the **Subject prefix** field, type a subject prefix that you want Nexsan Unity to automatically prefix to each email notification. For example: *Event notifications for the Unity 5100 in Mtl.*
9. In the **Sender:** field, type a valid sender's email address from which email notifications are sent.

Note To prevent your SMTP server from filtering out notification emails from Nexsan Unity, we recommend that you create a specific email account for Nexsan Unity notifications, or use an existing corporate account.
10. Select the HTML format option (default setting) if you want User name: to send email notifications in HTML format. If you clear this option, Unity sends email notifications in text format.
11. Click **OK** to save your settings and close the Configure Email and SNMP Notification dialog box.

Setting up system notifications

You can configure Nexsan Unity to send email notifications to selected personnel when space consumption reaches or exceeds space usage threshold settings that you configure for storage pools and/or for shares on Unity.

Nexsan Unity allows you to configure the frequency of email notifications for each threshold setting that you enable and configure for storage pools and/or for shares on the system—Critical, Error, Warning.

In order for Nexsan Unity to send system notifications for space usage threshold violations, you must first enable and configure space usage thresholds for storage pools and/or shares on the system.

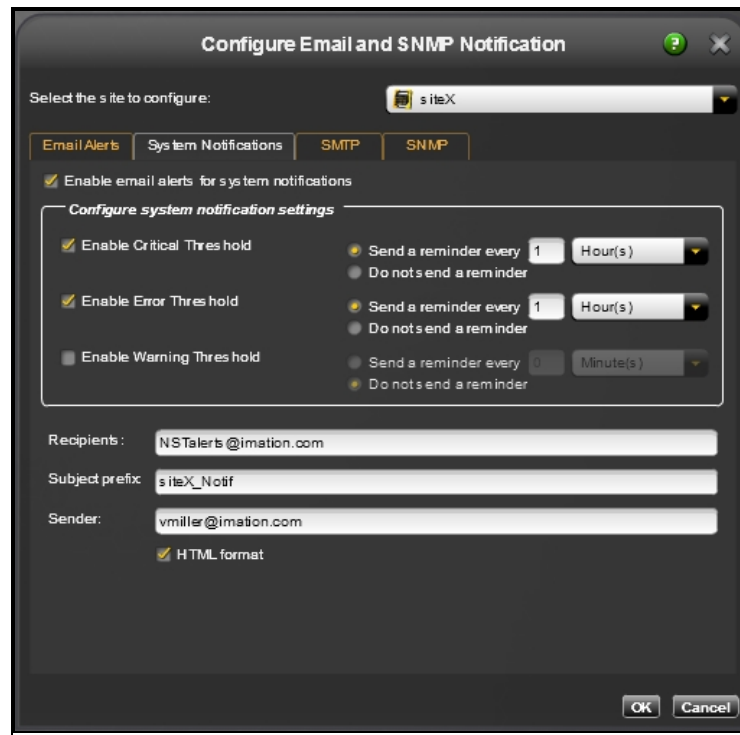
To configure email notification for space usage threshold violations, you need:

- valid email addresses for notification recipients;
- a subject prefix for email notifications;
- a sender email address.

► To set up email notification for space usage threshold violations:

1. Select the **Notifications** option from the **Tools** menu in the Nexsan Unity toolbar.
2. Select the **System Notifications** tab.

Figure 14-10: Configure Email and SNMP Notification dialog box—System Notifications tab



3. From the **Select the site to configure:** list, select the site that you want to configure email notifications for.
4. Select the **Enable email alerts for system notifications** option to enable email notification.

5. Under **Configure system notifications settings**, select the space usage threshold that you want to enable email notifications for. For example, if you want to enable email notifications for Critical thresholds, select the **Enable Critical Thresholds** option.

Note By default, email notifications are enabled for all space usage thresholds. To disable email notifications for a particular threshold, clear its check box.

6. Specify whether or not to enable email reminders for each space usage threshold that you enable email notifications for; and also specify the frequency (if you enable reminders); for example:

- To enable email reminders for Critical thresholds:
 - a. Select the **Send a reminder every** option.
 - b. Enter a value for the reminder frequency in the text box.
 - c. Select the recurrence type from the drop-down list: Minutes(s), Hour(s), or Day(s).
- To disable email reminders for Critical thresholds, select the **Do not send a reminder** option.

7. In the **Recipients:** field, type a valid list of recipient email addresses that you want to send email notifications to. Use the semi-colon (;) to separate recipient email addresses; for example:
`bob@abc.com; jack@abc.com; jill@abc.com.`

8. In the **Subject prefix** field, type a subject prefix that you want Nexsan Unity to automatically prefix to each email notification. For example: `Event notifications for the Unity 5100 in Mt1.`

9. In the **Sender:** field, type a valid sender's email address from which email notifications are sent.

Note To prevent your SMTP server from filtering out notification emails from Nexsan Unity, we recommend that you create a specific email account for Nexsan Unity notifications, or use an existing corporate account.

10. Select the **HTML format** option (default setting) if you want to send email notifications in HTML format. If you clear this option, Nexsan Unity sends email notifications in text format.
11. Click the **OK** button to save your settings and close the Configure Email and SNMP Notification dialog box.

Configuring SMTP server settings for the site

Before you set up email notification for system events and space usage threshold violations on storage pools and shares, you must configure [SMTP](#) server settings for the site. Nexsan Unity sends email notifications to the SMTP server, which then routes the email notifications to the recipients that you specify.

To configure SMTP server settings, you need:

- the IP address of the SMTP server on your network;
- the user name and password of a user account to authenticate with the SMTP server (if the SMTP server does not allow anonymous access);
- a valid recipient email address to test the connection between Unity and the SMTP server;
- a valid sender's email address to test the connection between Unity and the SMTP server.

Figure 14-11: Configure Email and SNMP Notification dialog box—SMTP tab



► To set up the SMTP server settings for the site:

1. Select the **Notifications** option from the **Tools** menu in the Nexsan Unity toolbar.
2. Select the **SMTP** tab.
3. From the **Select the site to configure:** drop-down list, select the site that you want to configure SMTP settings for.
4. Type a valid SMTP server IP address in the **SMTP server:** field.
5. Type a valid user name and password in the **User name:** and **Password:** fields to authenticate with the specified SMTP server.

Or, select the **Use anonymous credentials to connect to the SMTP server** option, if your SMTP server supports anonymous authentication.

6. In the **Specify email address to test with:** field, type a valid recipient email address to test the connection between Unity and the SMTP server.
7. In the **Specify sender email address:** field, type a valid sender's email address to test the connection between Unity and the SMTP server.
8. Click the **Test** button to validate the connection between Unity and the SMTP server that you specify.
9. Click **OK** to save SMTP settings.

Setting up SNMP notification

Unity includes an [SNMP](#) agent that you can configure to send SNMP traps to a Network Management Station when a Critical, Error, and/or Warning event is generated by a source component of Unity. For information on event types and Unity source components, see [Viewing events](#) on page 518 .

► Before you begin, you need:

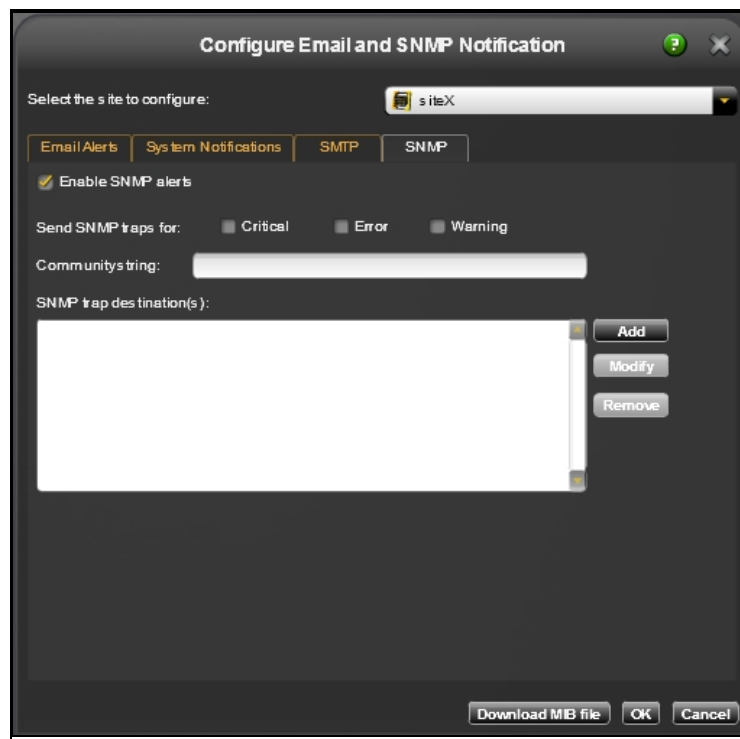
- The IP address of the Network Management Station where Unity will send SNMP traps.
- The community string used by the Network Management Station. The community string is a text string that acts as a password. It is used to authenticate messages that are sent between the Network Management Station and SNMP agents and it is included in every packet that is transmitted between the SNMP agent and the Network Management Station.
- The Unity Management Information Base (MIB). Once you configure SNMP notification on Unity, you must import the Unity MIB to the Network Management Station. You can download the Unity MIB from the Configure Email and SNMP Notification dialog box.

Note Depending on the network interface cards used in your environment, SNMP traps are sent over the Management Interface (nx99) for 10GigE network interfaces, and the Primary data network interface (nx0) for Fibre channel interfaces.

► To set up SNMP notification:

1. Select the **Notifications** option from the **Tools** menu in the Nexsan Unity toolbar.
2. Select the **SNMP** tab.

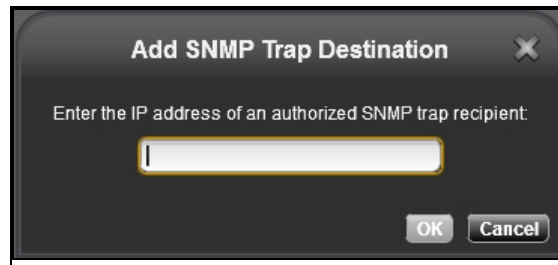
Figure 14-12: Configure Email and SNMP Notification dialog box—SNMP tab



3. From the **Select the site to configure:** pick list, select the site that you want to configure SNMP notifications for.

4. Select the **Enable SNMP alerts** option to enable SNMP notification.
5. Select the event types that you want Unity to send SNMP traps for. For example, if you want to SNMP traps for Critical and Error events, select the corresponding check boxes.
6. In the **Community string** field, enter the community string that the Network Management Station uses to authenticate messages from SNMP agents on the network. The default is public. You can leave the **Community string** field set to *public*, or specify a private name if you have a more segregated monitoring scheme.
7. Click the **Add** button to specify a Network Management Station where you want Unity to send SNMP traps. The Add SNMP Trap Destination dialog box displays.

Figure 14-13: Add SNMP Trap Destination dialog box



- a. Enter the IP address of the Network Management Station where you want Unity to send SNMP traps.
 - b. Click **OK** once you finish entering the IP address. Unity adds the Network Management Station to the list of **SNMP trap destinations** in the Configure Email and SNMP Notification dialog box.
 - c. Click the **Add** button again to add additional Network Management Stations to send SNMP traps to. Or, click the **Modify** button to change the IP address of a Network Management Station; click **Remove** to delete a Network Management Station from the list.
8. Click the **Download MIB file** button to save the Unity MIB on Unity to disk. Once you download the MIB, you need to import it to the Network Management Station(s).
 9. Click the **OK** button to save your settings and close the Configure Email and SNMP Notification dialog box.

Chapter 15

Operating in mixed mode environments

This section explains how changing the mode (permission settings) for files (and folders) under NFS affects ACL entries for the files (and folders) under CIFS, in mixed mode environments. This document discusses file permissions as seen from the UNIX (NFS) and Windows (CIFS) perspective.

This section also explains user and/or group identity mapping functionality available with Unity, which gives domain administrators the ability to map UNIX user and/or group accounts, from an LDAP Directory server, to corresponding accounts in a Microsoft Active Directory domain—for environments that use both Microsoft Active Directory and LDAP for user authentication.

This section covers these topics:

Understanding how changing the mode of a file in NFS affects permission settings in CIFS	540
Understanding how using chmod in NFS creates allow and deny entries in CIFS ACLs	542
Examples of CIFS permissions after applying chmod in NFS	543
Mapping UNIX accounts on Unity to corresponding Microsoft Active Directory accounts	548

Understanding how changing the mode of a file in NFS affects permission settings in CIFS

NFS (NFSv3 or NFSv4) permission settings follow the traditional UNIX owner, group, and other combination of Read (r), Write (w), and Execute (x) access permissions. Windows (CIFS) has a much richer set of access attributes; as a result, no one-to-one mapping occurs between NFS and CIFS.

In NFS, you set the mode of a file using `chmod`. This sets the user, group, and other permissions for the file. When you change the mode of a file in NFS, the following changes are made in the access control list (ACL) for the file in CIFS:

- all CIFS ACL entries are reset or cleared (except for user and group entries, which, if they exist, are preserved);
- **allow** and/or **deny** access control entries may get added for both owner and group (or for group only), depending on the mode that you set for the file in NFS (see [Understanding how using chmod in NFS creates allow and deny entries in CIFS ACLs on page 542](#));
- the **default** access control entries for owner, group, and everyone are set in CIFS according to the mode that you set for the file in NFS.

Table 15-1: Default access control entries

Default entries always set in CIFS	Entries set in CIFS only if the corresponding permission is set in NFS3
Owner	
<ul style="list-style-type: none"> • Write attributes • Take ownership • Change permissions • Write extended attributes • Read permissions • Read attributes • Read extended attributes 	<ul style="list-style-type: none"> • List folder / read data file access control entry is added for <i>owner</i> in CIFS if Read (r) access is set for user in NFS • Create files / write data access control entry is added for <i>owner</i> in CIFS if Write (w) access is set for user in NFS • Traverse folder / execute file access control entry is added for <i>owner</i> in CIFS if Execute (x) access is set for user in NFS
Group	
<ul style="list-style-type: none"> • Read permissions • Read attributes • Read extended attributes 	<ul style="list-style-type: none"> • List folder / read data file access control entry is added for <i>group</i> in CIFS if Read (r) access is set for group in NFS • Create files / write data access control entry is added for <i>group</i> in CIFS if Write (w) access is set for group in NFS • Traverse folder / execute file access control entry is added for <i>group</i> in CIFS if Execute (x) access is set for group in NFS
Everyone	
<ul style="list-style-type: none"> • Read permissions 	<ul style="list-style-type: none"> • List folder / read data file access control entry is added for <i>everyone</i> in CIFS if Read (r) access is set for <i>others</i> in NFS

Default entries always set in CIFS	Entries set in CIFS only if the corresponding permission is set in NFS3
<ul style="list-style-type: none">● Read attributes● Read extended attributes	<ul style="list-style-type: none">● Create files / write data access control entry is added for <i>everyone</i> in CIFS if Write (w) access is set for <i>others</i> in NFS● Traverse folder / execute file access control entry is added for <i>everyone</i> in CIFS if Execute (x) access is set for <i>others</i> in NFS

Understanding how using chmod in NFS creates allow and deny entries in CIFS ACLs

If you set Read (r), Write (w), **or** Execute (x) permissions on a file for *user* and/or *others* in NFSv3, there will be a corresponding access control **allow** entry added for *owner* to the file's CIFS access control list.

Table 15-2: Example of Allow entry

NFSv3 permissions set for <i>user</i>	allow access control entry added for <i>owner</i> in CIFS
Read (r)	List folder / read data file
Write (w)	Create files / write data
Execute (x)	Traverse folder / execute file

Deny access control entry added for *owner* and *group*

There may be a **deny** access control entry added for *owner* and *group* in CIFS if:

- you do **not** set Read (r), Write (w), **or** Execute (x) permissions on a file for *user* in NFSv3,
- but you grant *group* or *others* Read (r), Write (w), **or** Execute (x) permissions on the file.

Table 15-3: Deny entry added for *owner* and *group*

NFS permissions set for <i>user</i>	NFS permissions set for <i>group</i> or <i>others</i>	allow access control entry added for <i>owner</i> in CIFS
Read (r) not set	Read (r)	List folder / read data file
Write (w) not set	Write (w)	Create files / write data
Execute (x) not set	Execute (x)	Traverse folder / execute file

Deny access control entry added for *group* only

There may be a **deny** access control entry added for *group* in CIFS if:

- you do not set Read (r), Write (w), or Execute (x) permissions on a file for *group* in NFSv3,
- but you grant *others* Read (r), Write (w), or Execute (x) permissions on the file.

Table 15-4: Deny entry added for *group*

NFS permissions set for <i>user</i>	NFS permissions set for <i>others</i>	allow access control entry added for <i>group</i> in CIFS
Read (r) not set	Read (r)	List folder / read data file
Write (w) not set	Write (w)	Create files / write data
Execute (x) not set	Execute (x)	Traverse folder / execute file

Examples of CIFS permissions after applying chmod in NFS

This section contains several examples that demonstrate how using the chmod command in NFS affects CIFS ACLs.

Example 1

This command grants all permissions to file owner, and Read (r) and Execute (x) to everyone else.

```
chmod u=rwx,g=rx,o=rx <file>
```

In this example, the chmod command results in standard entries added for *owner*, *group*, and *everyone* in CIFS.

CIFS ACL entries	Permissions
<i>owner</i> allow entry	<ul style="list-style-type: none"> ● List folder / read data ● Create files / write data ● Create folders / append data ● Read extended attributes ● Write extended attributes ● Traverse folder / execute file ● Read attributes ● Write attributes ● Read permissions ● Change permissions ● Take ownership
<i>group</i> allow entry	<ul style="list-style-type: none"> ● List folder / read data ● Read extended attributes ● Traverse folder / execute file ● Read attributes ● Read permissions
<i>everyone</i> allow entry	<ul style="list-style-type: none"> ● List folder / read data ● Read extended attributes ● Traverse folder / execute file ● Read attributes ● Read permissions

Example 2

This command grants Read (r) and Write (w) access to file *owner* and *others* only.

```
chmod u=rw,g=,o=rw <file>
```

In this example, the `chmod` command results in **allow** entries added for *owner* and a **deny** entry added for *group* in CIFS.

CIFS ACL entries	Permissions
<i>owner</i> allow entry 1	<ul style="list-style-type: none"> ● List folder / read data ● Create files / write data ● Create folders / append data
<i>group</i> deny entry	<ul style="list-style-type: none"> ● List folder / read data ● Create files / write data ● Create folders / append data
<i>owner</i> allow entry 2	<ul style="list-style-type: none"> ● List folder / read data ● Create files / write data ● Create folders / append data ● Read extended attributes ● Write extended attributes ● Read attributes ● Write attributes ● Read permissions ● Change permissions ● Take ownership
<i>group</i> allow entry	<ul style="list-style-type: none"> ● Read extended attributes ● Read attributes ● Read permissions
<i>everyone</i> allow entry	<ul style="list-style-type: none"> ● List folder / read data ● Create files / write data ● Create folders / append data ● Read extended attributes ● Write extended attributes ● Read permissions

Example 3

This command grants Read (r) and Write (w) access to *group* only.

```
chmod u=,g=rwx,o= <file>
```

In this example, the `chmod` command results in a **deny** entry added for owner to the CIFS ACL, since the file *owner* (user) does not have Read (r), Write (w), or Execute (x) permissions set on NFS.

CIFS ACL entries	Permissions
<i>group deny</i> entry	<ul style="list-style-type: none"> ● List folder / read data ● Create files / write data ● Create folders / append data
<i>owner allow</i> entry	<ul style="list-style-type: none"> ● Read extended attributes ● Write extended attributes ● Read attributes ● Write attributes ● Read permissions ● Change permissions ● Take ownership
<i>group allow</i> entry	<ul style="list-style-type: none"> ● List folder / read data ● Create files / write data ● Create folders / append data ● Read extended attributes ● Traverse folder / execute file ● Read attributes ● Read permissions
<i>everyone allow</i> entry	<ul style="list-style-type: none"> ● Read extended attributes ● Read attributes ● Read permissions

Example 4

This example demonstrates how user and group entries, which exist for a file in its original CIFS ACL, are preserved after the chmod command is executed on the file in NFS.

Original CIFS ACL entries:

- *lily@win.domain* is a Microsoft Active Directory domain user
- *bob* is an LDAP user

This command grants Read (r) and Write (w) access to *group* only:

```
chmod u=rwx,g=rx,o=rx <file>
```

In this example, standard entries for *owner*, *group*, and *everyone* are created.

Original entries		New entries	
CIFS ACL entries	Permissions	CIFS ACL entries	Permissions
<i>owner allow</i> entry	<ul style="list-style-type: none"> • List folder / read data • Create files / write data • Create folders / append data • Read extended attributes • Write extended attributes • Traverse folder / execute file • Delete subfolders and files • Read attributes • Write attributes • Delete • Read permissions • Change permissions • Take ownership 	<i>lily@win.domain allow</i> entry	<ul style="list-style-type: none"> • List folder / read data • Read extended attributes • Traverse folder / execute file • Read attributes • Read permissions
<i>group allow</i> entry	<ul style="list-style-type: none"> • List folder / read data • Read extended attributes • Traverse folder / execute file • Read attributes • Read permissions 	<i>bob allow</i> entry	<ul style="list-style-type: none"> • List folder / read data • Read extended attributes • Traverse folder / execute file • Read attributes • Read permissions
<i>everyone allow</i> entry	None	<i>owner allow</i> entry	<ul style="list-style-type: none"> • List folder / read data • Create files / write data

Original entries		New entries	
CIFS ACL entries	Permissions	CIFS ACL entries	Permissions
			<ul style="list-style-type: none"> ● Create folders / append data ● Read extended attributes ● Write extended attributes ● Traverse folder / execute file ● Read attributes ● Write attributes ● Read permissions ● Change permissions ● Take ownership
<i>lily@win.domain</i> allow entry	<ul style="list-style-type: none"> ● List folder / read data ● Read extended attributes ● Traverse folder / execute file ● Read attributes ● Read permissions 	<i>group</i> allow entry	<ul style="list-style-type: none"> ● List folder / read data ● Read extended attributes ● Traverse folder / execute file ● Read attributes ● Read permissions
<i>bob</i> allow entry	<ul style="list-style-type: none"> ● List folder / read data ● Read extended attributes ● Traverse folder / execute file ● Read attributes ● Read permissions 	<i>everyone</i> allow entry	<ul style="list-style-type: none"> ● List folder / read data ● Read extended attributes ● Traverse folder / execute file ● Read attributes ● Read permissions

Mapping UNIX accounts on Unity to corresponding Microsoft Active Directory accounts

Unity provides a user and/or group identity mapping mechanism for environments that implement both Microsoft Active Directory and LDAP for user authentication. The identity mapping mechanism gives domain administrators the ability to map LDAP/UNIX accounts from an LDAP Directory server to corresponding accounts in a Microsoft Active Directory domain.

You map user and/or group account with the Nexsan Unity `nxadmin` CLI using the `nstusermaps` command. This command is available both from the `nxadmin` CLI menu and the `nxadmin` CLI command shell. Before using this command, you need to access the `nxadmin` CLI as described in the *Nexsan Unity nxadmin CLI Reference Guide*.

nstusermaps

The `nstusermaps` command is provided to allow the user to map local accounts to UNIX accounts for NFS. The `nstusermaps` command is identical to the `nstusermaps` command in the `nxadmin` CLI command shell.

To support NFS access of an NFS share on Unity, you must map the user or group accounts that you add to Unity to their corresponding user or group account names in the Microsoft Active Directory domain.

▶ **To set identify mapping for a user and/or group account:**

1. In the NestOS Admin Menu, type **4 (Run a Command)**.
2. Press Enter.

3. At the `command:` prompt, type one of these commands:

To...	Type this
create a mapping	<code>nstusermaps add winuser:<useraccount@AD.net> unixuser:<username></code>
remove a mapping	<code>nstusermaps remove winuser:<user_account@domain.xxx> unixuser:<user_name></code>
map multiple user and/or group accounts	<p>The <code>nstusermaps</code> command includes a wildcard (*) option that allows you to map multiple user and/or group accounts on Unity with their corresponding domain accounts in the Microsoft Active Directory.</p> <p>To map a user account, type:</p> <pre>nstusermaps add winuser:*@AD.net unixuser:*</pre> <p>To map a group account, type:</p> <pre>nstusermaps add wingroup:*@AD.net unixgroup:*</pre> <p>where <code>@AD.net</code> represents the Microsoft Active Directory domain containing the user or group accounts that you want to specify mapping for.</p>
exclude a user or group from identity mapping	<p>When mapping user or group accounts between Microsoft Active Directory and Unity, Unity processes name-based mappings in this order of precedence:</p> <ol style="list-style-type: none"> 1. Exclusions: <code>cwindows-name@domain to " ", or unix-name to " "</code> 2. Name-to-name mappings: <code>windows-name@domain to unix-name</code> 3. Wild-card mappings: <code>*@domain to *</code> <p>Type one of these variations of the <code>nstusermaps</code> command:</p> <pre>nstusermaps add unixuser:<user> " " nstusermaps add unixgroup:<group> " "</pre> <p>Where <code><user/group></code> represents the user or group account on Unity that you do not want to map to its corresponding account in the Microsoft Active Directory domain.</p> <p>You can also set exclusions in reverse by specifying the Microsoft Active Directory domain account that you do not want to map to its corresponding user or group account on Unity. For example, type one of these variations:</p> <pre>nstusermaps add winuser:*@AD.net " " nstusermaps add wingroup:*@AD.net " "</pre> <p>Where <code>@AD.net</code> represents the Microsoft Active Directory domain containing the user or group account you do not want to map to its corresponding account on Unity.</p>

To...	Type this
display identity mapping information for a specific user and/or group	<p>Type one of these commands:</p> <pre>nstusermaps show -c winuser:<user> nstusermaps show -c unixuser:<user> nstusermaps show -c wingroup:<group> nstusermaps show -c unixgroup:<group></pre> <p>Where <user/group> represents the user or group account in Microsoft Active Directory domain and/or on Unity.</p>

4. Press Enter.

Tip To exit the `command:` prompt and return to the NestOS Admin Menu, type `Exit`, and then press Enter.

▶ **Example: create a mapping to the corresponding user account in Active Directory**

We map Bob Summer's Microsoft Active Directory domain account to the account created for Bob on Unity.

```
nstusermaps add winuser:<bob.summers@AD.net> unixuser:<bsummers>
```


Terminology

10

10Gb Ethernet

A 10 gigabit per second (Gb/s) Ethernet connection using either fiber-optic cables or twisted-pair copper wires.

10Gb iSCSI

An iSCSI connection that runs on a 10Gb Ethernet network.

A

Access methods

Unity supports both Read-only anonymous access and Read/Write anonymous access to file systems:

- Read-only anonymous access gives all users on the network Read access to the data contained in a file system, including the ability to display and traverse folders and read the contents of files.
- Read/Write anonymous access gives all users on the network Write access to the data contained in a file system, including the ability to delete and create folders and files and change the contents of files.

From the perspective of a Window-based (CIFS) system, if you enable Read-only anonymous access and/or Read/Write anonymous access to a file system, the *Everyone* account in Windows is granted access to the file system; this means that all users on

the network have either Read or Read/Write access to the file system, depending on the setting you specify in Unity.

From the perspective of a UNIX/Linux-based (NFS) system, if you enable Read-only anonymous access and/or Read/Write anonymous access to a file system, all user accounts on the UNIX/Linux system are granted access to the file system.

See [Step 2: Configuring the access method on page 126](#) and [Modifying a file system's sharing method on page 136](#).

Active/Active Clustering

The Unity has built-in Active/Active Clustering capability, whereby both controller nodes on the Unity operate in active mode—that is, both controllers can actively serve data in parallel—in addition to providing full redundancy in the event that one of the controller nodes fails. The Unity's Active/Active Clustering configuration provides both high-availability and load balancing for your Nexsan storage infrastructure.

For details and examples of Active/Active clustering, see [Clustering on page 293](#).

Active Directory

Microsoft Active Directory® is a directory service that stores directory information on a network and makes this information available to network users and administrators. AD stores information about user accounts, such as names, passwords, phone numbers, and so on, and enables other authorized users on the same network to access this information.

See [Joining an Active Directory domain using Unity on page 380](#).

Active node

This refers to the controller node currently hosting the [System Management](#) component, which includes cluster- and system-related services on Unity. In reality, both controller nodes on Unity operate in active mode, but only one controller can host cluster- and system-related services at any given time.

For example, when you need to perform routine or emergency maintenance on the *active* controller node—you can transition, or move, the System Management component to the *passive* controller node in Unity, making it *active*.

See [Clustering overview](#) on page 294.

Anti-static wrist-strap

An antistatic device used to prevent electrostatic discharge (ESD) by safely grounding a person working on electronic equipment. Also called an ESD strap or a grounding bracelet.

APAL

(All Ports / All LUNs) Feature used in a dual-controller, active-active cluster to provide high-availability during failover on Unity. All LUNs can be accessed through all Fibre Channel ports. This feature also provides load balancing across the two controllers, thus improving the overall performance of the cluster.

Each controller hosts a set of LUNs, which can be accessed through the controller's Fibre Channel ports and iSCSI connections. The direct connection between the controller managing the LUNs and the host is referred to as the *Optimized Path*.

Chassis inter-connectivity provides uninterrupted access to the LUNs hosted by each controller. The direct connection between the controller managing the LUNs and the Fibre Channel host is referred to as the *Optimized Path*.

The *All Ports / All LUNs* feature creates an additional access path from one controller to the set of LUNs hosted by the other controller; this is referred to as the *Non-Optimized Path*. As a result, this feature provides uninterrupted access to the LUNs by using multipathing.

APAL is supported on Unity 2000, Unity 4000, and Unity 6000. To view examples of *All ports / All LUNs* clustering, see [Clustering](#) on page 293.

Asynchronous data replication

The asynchronous data replication function provides off-site disaster recovery protection for the Unity. It delivers high-performance asynchronous replication of your data over both LAN and WAN networks, providing protection from site-specific and regional disasters.

The Unity's asynchronous data replication function uses snapshot-based replication technology: when you initiate data replication, the asynchronous data replication function takes a snapshot of the data on the primary site and sends either the entire contents up to the snapshot to the secondary site—in the case of an initial data replication; or, only the changes since the last replication—in the case of an incremental update.

Because the asynchronous data replication function takes a snapshot of the source data (on the primary system), the data always remains accessible to clients during replication. Additionally, the asynchronous data replication function keeps track of data transfers during replication by checkpointing the data stream. If data replication is interrupted—due to a network disconnect issue—the asynchronous data replication function automatically restarts replication from the most recent checkpoint.

The asynchronous data replication function includes features that reduce bandwidth consumption during data replication, and consequently minimize the infrastructure cost of data replication and disaster recovery. Specifically, the asynchronous data replication function only replicates the data that changed since the last replication—which significantly reduces replication time and bandwidth requirements, particularly where only small parts of large files change or where only file system metadata has changed on the primary site.

Authentication mode

See [User authentication mode](#).

Automatic replication

In asynchronous replication, an automatic replication refers to a scheduled replication that occurs according to a schedule you define. You can configure a separate replication schedule for each storage pool on Unity.

B

Bit

The smallest unit of digital data, representing a 0 or a 1. Abbreviated “b”.

Boot Drive

The device from which a computer’s operating system is loaded. Typically, an internal hard disk drive (or one of several partitions on such a drive) is used for this purpose, but any attached storage device—such as an optical disc drive, a USB flash drive, a SATADom, or other attached storage—can be used.

Browsing snapshots

See [Snapshot browsing](#).

Browsing replicated datasets

You browse a replicated file system in the same way that you browse the source file system on the primary Unity, except that the replicated file system is a read-only copy of the source file system (but with the same file system-level access permissions as the source file system).

In addition, the replicated file system exists only on the secondary site Unity; as a result, to browse the contents of a replicated file system, you must set up a CIFS or NFS mapping to the remote site from the Windows-based (CIFS) system and/or UNIX/Linux-based (NFS) system that you want to access the replicated file system from; see [Accessing an NFS file system from UNIX/Linux](#) on page 177.

See the *Nexsan Unity Snapshots and Replication Guide*.

C

CHAP

iSCSI initiators and targets prove their identity to each other using the Challenge Handshake Authentication Protocol (CHAP). You can use CHAP authentication to restrict iSCSI access to LUNs on Unity; only servers (initiators) that provide the correct user name and password (or secret) combination can connect to LUNs on Unity.

Unity’s iSCSI implementation provides several layers of CHAP authentication. See [Configuring and managing CHAP authentication](#) on page 281.

In addition to CHAP authentication, Unity provides LUN masking for added security; see [Setting up host connectivity](#) on page 233.

CIFS

(Common Internet File System) The protocol used in Windows environments for shared folders.

CIFS sharing

See [Sharing methods](#).

CLI

(Command-line interface) A means of interaction between a human user and a computer program, or between two programs, where the user (or client) passes commands in the form of a line of text to a computer program.

The Nexsan Unity offers the nxadmin command-line interface. Abbreviated “CLI”.

Clustering

Clustering configurations provide both high-availability and load balancing, using the Unity Storage System’s redundancy features, including dual controllers and RAIDs. See also [Active/Active Clustering](#)

Cluster Resources

Cluster resources represents the components of a cluster; these include:

- Controller 1 and Controller 2
- Pool Resource Group 1 and Pool Resource Group 2
- System Management

See [Clustering overview](#) on page 294.

Controller

Can also be referred to as Controller Node or Node.

The controller in Unity acts as the interface between Unity and network clients. Unity has two controller nodes, for which you can configure both cluster and network settings.

Controllers host Pool Resource Groups, which, in turn, are assigned storage pools. Typically, for load balancing, a controller hosts a single Pool Resource Group, although one controller can host both Pool Resource Groups indefinitely, if needed. See [Clustering](#) on page 293.

D

Dashboard

Unity's dashboard view interface presents the same data as the property panels in the Unity's tree view, but for the entire site. The dashboard displays performance data, site health, I/O statistics, and space usage information in graphical format, using a dashlet for each category. Data shown in the dashboard cannot be modified. You must use the tree view wizards and property panels to change data configuration settings.

See [Viewing performance metrics with the Dashboard view](#) on page 474.

DHCP

(Dynamic Host Configuration Protocol) A communication protocol that lets network administrators manage centrally and automate the assignment of Internet Protocol (IP) addresses in a network.

DIMM

Dual In-line Memory Module. The type of random-access memory (RAM) that the Nexsan Unity uses.

Directory Service

A directory service is the software system that stores, organizes and provides access to information in a directory. A directory service called a naming service, maps the names of network resources to their respective network addresses. With the name service type of directory, a user does not have to remember the physical address of a network resource; providing a name will locate the resource. Each resource on the network is considered an object on the directory server. Information about a particular resource is stored as attributes of that object. Information within objects can be made secure so that only users with the available permissions are able to access it.

In LDAP, the name is called the Distinguished Name (DN) and is used to refer to a collection of attributes (relative distinguished names) which make up the name of a directory entry. See [Connecting to an LDAP Directory service](#) on page 398.

DNS

(Domain Name System) A program or computer server that implements a name-service protocol. It maps a human-recognizable identifier to a system-internal, often numeric, identification or addressing component (usually an IP address).

DRAM

(Dynamic Random-Access Memory) type of random-access memory that stores each bit of data in a separate capacitor within an integrated circuit. The capacitor can be either charged or discharged; these two states are taken to represent the two values of a bit, conventionally called 0 and 1. Since even "nonconducting" transistors always leak a small amount, the capacitors will slowly discharge, and the information eventually fades unless the capacitor charge is refreshed periodically. Because of this refresh requirement, it is a dynamic memory as opposed to static random access memory (SRAM) and other static types of memory. See [FASTier](#).

E

Electrostatic discharge (ESD)

The sudden and momentary electric current that flows between two objects at different electrical potentials caused by direct contact or induced by an electrostatic field. Potentially harmful to electronic components.

Ethernet

A local area network (LAN) architecture using a bus or star topology and supporting data transfer rates of 10, 100, and 1000 Mbps. It is one of the most widely implemented LAN standards. The 802.11 protocols are often referred to as "wireless Ethernet."

Event log

All event messages generated by Unity (including those issued by a Nexsan storage device connected externally to the system) are logged to the event logs,

which you can then retrieve and display in Unity's Event Viewer.

The event logs provide a record of past events that have occurred on the system to help you monitor Unity and its software and hardware components.

The Unity records events in the event logs from these **source components**:

- **Nexsan Unity**: these events are generated by Unity and its software components, including Unity Clustering, Data Replication, and Snapshots functions.
- **Storage System**: these events are generated by Nexsan storage systems attached externally to Unity (via SAS or Fibre Channel), if available, and logged to the event logs.
- **File System**: these events are generated by the Unity operating system.
- **System**: these events are generated by Unity for hardware faults on the system, such as fan, power supply, or disk failures.

All events logged in the event logs are categorized according to four **severity levels** (or event types):

- **Critical**: designates a severe error that prevents a system component (s) from running. A critical event may lead the system to an abort situation.
- **Error**: designates an error event that may still allow any affected system component(s) to continue running. However, if left unattended, the error event may lead the system to an abort situation.
- **Warning**: designates potentially harmful situations.
- **Information**: designates informational messages that highlight the progress of Unity's software components, including Unity's Clustering, Data Replication, and Snapshots functions.

In addition to event logging, Unity also provides **automated event notification** in one of two forms:

- An Email message, which the system sends through an SMTP server that you specify.
- An SNMP trap, to notify a central Network Management Station (NMS) of any events generated by Unity.

See [Event logging and notification](#) on page 517.

Expandable storage

See [Storage](#).

Expansion controller

A module of Nexsan expansion units that connects via SAS to a Nexsan main Unity Storage Expansion's Controller Node. Expansion units can be the Unity 5100X, Unity 2000XC, Unity 2000XP, and US224X.

F

Failover

The capability of a system to switch over automatically to a redundant or standby system upon the failure or abnormal termination of the previously active system.

Cluster failover: This refers to the act of transitioning, or moving, Pool Resource Groups or the System Management component from one controller node to the other. This can be a manual process that you initiate if you want to shut down a controller for maintenance, or an automatic process initiated by Unity if a controller fails.

Site or pool failover: Typically, you use the failover function to transfer data and system operations to a remote site in the event of an imminent hardware-related failure on the primary system, or if you want to perform system maintenance—for example, a hardware component upgrade or replacement—on the primary system.

For disaster recovery, Unity data replication function provides a failover mechanism for your Unity deployment that allows you to gracefully failover all your data and system operations on the primary Unity to the corresponding remote Unity.

The failover mechanism also includes a promote function that allows you to forcefully promote the remote site to primary status in your Unity deployment in the event of a complete system failure—due to a catastrophic disaster—on the primary site.

See the *Nexsan Unity Snapshots and Replication Guide*.

FASTier

Nexsan's proprietary cache system that uses SSD and SDRAM technology to increase random I/O performance of SATA and SAS disk drives. Unity includes support for Nexsan's FASTier cache devices. The FASTier caching mechanism enhances the performance of Unity by caching data to FASTier read, write, or read/write [SSD](#) and [DRAM](#) cache devices during read or write operations on the system. Unity

FASTier cache devices accelerate read and/or write speeds for a storage pool:

- FASTier read cache stores frequently-read chunks of data to accelerate read operations on the system.
- FASTier write cache accelerates synchronous write operations to disk.
- FASTier read/write cache can be used for either read or write cache for the storage pool.

The Unity 5000 supports Read and Write cache. FASTier cache devices are available for purchase as optional components for the Unity 5000. For more information, please contact your Nexsan reseller or Nexsan Support Representative.

The Unity 4000 supports Read and Write cache devices, and also comes equipped with FASTier write cache—non-volatile high-speed cache memory.

The Unity 6000 supports Read cache devices, and also comes equipped with FASTier write cache—non-volatile high-speed cache memory.

In the event of a power failure, the Unity Vault Protection Module provides power to Unity; when this occurs, Unity transfers in-memory cached data to an internal SSD—in order to prevent data loss. Once power is restored, the system transfers data stored on

the SSD to disk. The system also mirrors in-memory cached data to the peer controller to protect against controller failure.

Depending on the configuration of the Unity 4000, there is a certain amount of physical memory reserved for FASTier write cache—where each controller is assigned an equal amount. The FASTier write cache is divided into chunks, which are seen as devices by the system. Each chunk is 512 MB. When you create a storage pool on the Unity 4000, the pool is assigned eight devices/chunks out of the sixteen devices. As you create more storage pools, the amount of FASTier write cache gets divided equally among the storage pools automatically. See [Disabling automatic FASTier write cache assignment](#) on page 348.

The Unity 6000 comes with a total of 64 GB of memory—32 GB per controller, by default. The FASTier write cache is divided into chunks, which are seen as devices by the system. On the Unity 6000, each chunk is 1 GB. When you create a storage pool, the pool is assigned 8 devices/chunks by default (so 8 GB in size). As you create more storage pools, the amount of FASTier write cache gets divided equally among the storage pools automatically. See [Disabling automatic FASTier write cache assignment](#) on page 348.

See [Step 2: Allocating FASTier cache devices to the storage pool](#) on page 103 and [Disabling Read caching](#) on page 231.

FCC

The Federal Communications Commission; the federal agency that regulates electromagnetic emissions.

Fibre Channel

A gigabit (Gb) speed network technology primarily used for storage networking and the current standard connection type for storage area networks (SANs). Despite its name, Fibre Channel signaling can run on both twisted-pair copper wire and fiber-optic cables.

Fibre Channel port

Any entity that actively communicates over a Fibre Channel network. Usually implemented in a device such as disk storage or a Fibre Channel switch. Depending on the system, the Fibre Channel ports on

Nexsan Unity Storage Expansions can support 2Gb/s, 4Gb/s, or 8Gb/s connections.

Fibre Channel switch

A network switch compatible with the Fibre Channel protocol. Allows the creation of a Fibre Channel network, which is currently the core component of most storage area networks (SANs).

Firmware

Software stored in read-only memory (ROM) or programmable ROM (PROM), therefore becoming a permanent part of a computing device.

Full Replication

In asynchronous replication, full replication refers to a replication operation that sends all the data on the primary Unity to the remote Unity.

Only the initial replication, when you first set up asynchronous data replication between two systems, is a full replication. All successive replications are incremental.

See the *Nexsan Unity Snapshots and Replication Guide*.

G

Gateway

An Internet working system that joins together the different subnets of a network or two networks that use different base protocols. A network gateway can be implemented completely in software, completely in hardware, or as a combination of both.

Gb

(Gigabit) Approximately one billion (1,000,000,000) bits.

Gb/s

(Gigabits (Gb) per second) Used to describe the speed of network data transmission.

Gigabit interface converter

A standard for transceivers, commonly used with Gigabit (Gb) Ethernet and Fibre Channel, with a hot-swappable electrical interface. Gigabit interface converter ports can support a wide range of physical

media, from copper to optical fiber, at lengths of hundreds of kilometers.

Group

Groups are logical expressions of organization, tying users together for a common purpose.

For example, if you add a user to a group that has Read/Write permissions to a file system on Unity, the user automatically inherits the group's Read/Write permissions to that file system. By adding a user account to a group, you can avoid having to grant the same access rights and file system-level permissions to multiple users one by one. Members of a group can make the same types of changes to settings in Unity and have the same access permissions to file systems.

Because maintaining permissions for a group is easier than maintaining permissions for many user accounts, you generally will want to use groups to manage access to resources in Unity. To assign access rights or file system-level permissions to a set of users, assign the permissions or access rights to a group and then grant membership in the group to each of the users.

Note Unity only supports Microsoft Active Directory domain Security Groups; Distribution groups are not supported because Microsoft Windows does not allow setting file system-level access permissions for Distribution groups.

In Unity, groups can be:

- Microsoft Windows Active Directory domain or LDAP Directory service groups: Unity uses existing Microsoft Windows Active Directory domain or LDAP Directory service group accounts, and saves supplemental authorization settings on Unity. This allows you to give access rights to log on to Unity and administer Unity to your Microsoft Windows Active Directory domain or LDAP Directory service groups.
- Local groups: All account information is created and saved locally on Unity.

You grant access rights to groups by assigning an administrative role to them in Unity; see [Nexsan Unity roles and access rights](#) on page 67 and [Setting access rights](#) on page 82.

GUI

(Graphical user interface) A type of user interface that allows users to interact with electronic devices using images rather than text commands. Nexsan Unity Storage Expansions use a graphical user interface for system configuration.

H

HBA port WWN

HBA ports use a unique World Wide Name (WWN), which is an 8-byte (64-bit) identifier in Fibre Channel, similar to that of MAC Addresses on a Network Interface Card (NIC).

Unity automatically configures the Fibre Channel HBA ports in target mode. See [Fibre Channel initiator](#) and [Adding a LUN mask](#) on page 237.

Hot spare

Disks that you assign to the storage enclosure with the Storage Configurator. If a disk on the system fails, Unity automatically replaces the failed disk with the hot spare, allowing the system to continue operating. Depending on your [RAID](#) level and RAID sets selections, and the number of disks available on the system, you may only be able to assign one disk as a hot spare.

See [Allocating new storage to the site](#) on page 328 and [Resetting the RAID configuration for storage](#) on page 331.

Host

A computer, server, or other device which accesses the file systems in a Nexsan Unity storage enclosure. The host can be connected to the storage system with a Fibre Channel, iSCSI, or SAS connection.

HTTP

The Hypertext Transfer Protocol is an application protocol for distributed, collaborative, hypermedia information systems. HTTP is the foundation of data communication for the World Wide Web. Hypertext is structured text that uses logical links (hyperlinks)

between nodes containing text. HTTP is the protocol to exchange or transfer hypertext.

HTTPS

(HTTP Secure) Communications protocol for secure communication over a computer network, with especially wide deployment on the Internet. Technically, it is not a protocol in itself; rather, it is the result of simply layering the Hypertext Transfer Protocol (HTTP) on top of the SSL/TLS protocol, thus adding the security capabilities of SSL/TLS to standard HTTP communications.

I

I/O

(Input/Output) The communication between an information processing system (such as a computer or a Nexsan storage system's Controller Node), and the outside world (either an operator or another information processing system).

Inputs are the signals or data received by the system, and outputs are the signals or data sent from it.

IDMU

(Microsoft Identity Management for UNIX) IDMU makes it easy to integrate users of Windows operating systems into existing UNIX environments. It provides manageability components that simplify network administration and account management across both platforms. IDMU allows you to manage user accounts and passwords on Windows and UNIX systems using Network Information Service (NIS). IDMU also allows you to automatically synchronize passwords between Windows and UNIX operating systems.

Incremental replication

In asynchronous replication, incremental replication refers to a replication operation that sends only the data that changed since the last replication (whether that one was full or incremental).

See the *Nexsan Unity Snapshots and Replication Guide*.

Initiator

An application or production system end-point that is capable of initiating an iSCSI session with an iSCSI target, sending iSCSI commands and I/O requests. Initiators are also identified by unique addressing methods. See also [iSCSI target](#).

IP

(Internet Protocol) The network layer for the TCP/IP protocol suite widely used on Ethernet networks.

IPMI

(Intelligent Platform Management Interface) The IPMI interface allows you to perform administrative tasks to remotely manage Unity in the event that you are unable to connect to Unity using a conventional method: through Nexsan Unity or from the nxadmin CLI.

Administrative tasks that you can perform through the IPMI interface include:

- setting network settings for Unity;
- viewing hardware-related error conditions;
- launching a remote console session to Unity; and
- performing other maintenance tasks on the system.

The Unity IPMI interface is provided as a web-used utility that you can access from a browser using the IPMI IP address. Before you can access Unity's web-based IPMI interface, you must first set an IPMI IP address, subnet mask, and a default gateway IP address for Unity in Unity; on a clustered system, you must set a separate IPMI IP address for each controller node.

See [Setting or modifying IPMI settings](#) on page 316.

IQN

An IQN (iSCSI qualified name) is the unique identifier of a device in an iSCSI network. iSCSI uses the form `iqn.date.authority:uniqueid` for IQNs. For example, the Unity uses this IQN to identify iSCSI targets:

```
iqn.1999-02.com.nexsan:<site name>:<pool name>:<unique ID>
```

This name indicates that this is an iSCSI device from Nexsan, which was registered as a company in February of 1999. The naming authority is simply the DNS name of the company reversed; in this case, **com.nexsan**. Following this is the site name, the storage pool name where the target exists, and a user-defined unique ID to identify the target.

iSCSI

An abbreviation for Internet Small Computer System Interface, is an Internet Protocol (IP)-based storage networking standard that facilitates SCSI-based storage commands to be sent over network structures, such as a LAN or VPN.

iSCSI target

A storage system end-point on Unity that processes iSCSI commands and I/O requests from an initiator. Each storage pool on Unity can have one, or multiple, iSCSI targets, with a maximum of 256 targets per storage pool (0 to 255). In turn, each target can have a maximum of 256 LUNs (0 to 255). Each target on Unity is identified by a unique addressing method (IQN).

A LUN is essentially a block of storage that you add to a storage pool on Unity, and then present to client systems (initiators) on the network through a target. For example, using Microsoft's iSCSI Software Initiator, a Windows-based client system on the network sees a LUN, presented through an iSCSI target on Unity, as a locally attached hard disk. In reality, the hard disk that the Windows client sees is a block of storage—or, more specifically, a LUN—which exists on Unity.

Because the disk space is virtual, there is no need to add additional hardware to the (Windows) client system as the LUN is administered through a common network infrastructure. The (Windows) client can then create a file system on the iSCSI target—reading and writing data as if it were on a local disk. In addition, Windows server applications, such as Microsoft Exchange and Microsoft SQL Server, can operate using iSCSI targets on Unity as data repositories. See [LUNs](#) on page 213 and [iSCSI Functions](#) on page 280.

iSCSI target public alias

This is a symbolic name that you can assign to a iSCSI target on Unity. The public alias is seen by

some iSCSI initiators; it can help you identify the target.

The public alias for a storage pool's default target—that is, the target that Unity creates for a storage pool when you first add a LUN to the storage pool—is the pool name. You can change a target's public alias at any time.

iSNS

The Internet Storage Name Service (iSNS) protocol is designed to facilitate the automated discovery, management, and configuration of iSCSI devices on a TCP/IP network. You can configure iSCSI targets on Unity to use an iSNS server. An iSNS server provides a central management point for LUNs on Unity by dynamically maintaining up-to-date information about their corresponding iSCSI target names. An iSNS server must already be set up and available on the network in order for Unity to access it.

For steps to add an iSNS server, see [Adding an iSNS server](#) on page 244.

J

Jumbo Frames

A jumbo frame is essentially an Ethernet frame that is larger than 1,518 bytes. When the frame is 1,518 bytes, the MTU (or payload—not frames) on the Unity is actually 1500 bytes. For the Unity, gigabit Ethernet supports a maximum MTU (payload) of 9,000 bytes. You will notice the greatest benefit from enabling jumbo frames when you transfer large files across your network: since fewer frames are needed to carry the same amount of data, transfer speeds go up and CPU utilization goes down.

Every device in the path of the file transfer—all your switches (starting with the one in the router), your clients that access data on Unity, and Unity, itself—must all have jumbo frames enabled. In addition, each device must be capable of passing the same size jumbo frames.

See [Enabling jumbo frames](#) on page 318 and [Enabling jumbo frames using the menu-driven nxadmin CLI](#) on page 319.

L

LACP

(Link Aggregation Control Protocol) allows multiple individual Ethernet links to be aggregated together to form a single logical channel. LACP allows a network device to negotiate an automatic bundling of links by sending LACP packets to the peer (directly connected device that also implements LACP).

See [Enabling LACP](#) on page 320.

LAN

(Local area network) A computer network that links devices within a small geographic area, such as a building or group of adjacent buildings.

LDAP

(Lightweight Directory Access Protocol) LDAP is a protocol used to communicate with a directory service. It defines operations to refer to an entity in the directory, to describe the attributes of an entity, and the security features that can be used to authenticate to the directory and control access to the entities within the directory. The protocol is carried directly over TCP for connection-oriented transport (receipt of data is acknowledged) and User Datagram Protocol (UDP) for connectionless transport (no acknowledgment upon sending or receiving data).

LED

(Light Emitting Diode) LEDs are used for indicator lights on the front and back of Nexsan Unity Storage Expansions.

LUN

A LUN is a term used to describe a block of storage on the Unity. Uniquely numbered, this creates what is referred to as a Logical Unit Number, or LUN.

Unity can contain up to a maximum of 255 LUNs per target with a per-system maximum of **255** LUNs for the Nexsan Unity 5100™ Storage System, and **1024** LUNs for the Nexsan Unity 5300™ Storage System/Nexsan Unity 5500, and **1024** LUNs for the Nexsan Unity 6000.

LUNs can be exposed over iSCSI. When associated with an iSCSI target on Unity, a LUN forms a unique

iSCSI block device that can be accessed by one or more iSCSI initiators.

See [LUNs](#) on page 213.

LUN ID

The LUN ID is a number used to identify a LUN—from 0 to 254. Each LUN associated to the same target and the same initiators must have a unique LUN ID.

However, if you associate each LUN to a different target or to different initiators (even if they are part of the same target), there is no need for the LUN IDs to be different. For LUN masking, the LUN ID has to be unique within the same mask.

See [Adding a LUN](#) on page 216 and [Adding a LUN mask](#) on page 237.

M

Management target (mgmt)

Each storage pool on Unity has a Management target (**mgmt**) assigned to it by the system, by default. The management target allows a [VSS](#) (Volume Snapshot Service or Volume Shadow Copy Service) host to create and manipulate shadow copies (point-in-time snapshots) of the data in LUNs on Unity.

The VSS host connects to a storage pool's Management target via iSCSI to view, create, and manage snapshots of the LUNs in the storage pool. You can assign a [CHAP](#) (Challenge Handshake Authentication Protocol) user to the Management target to restrict access to LUN snapshots in a storage pool, to specific VSS hosts.

Manual replication

In asynchronous replication, a manual, replication is a replication process that you start manually on a storage pool. With offline replication, you can replicate the data in the storage pool to the remote site, or to a USB storage device attached to the primary site.

Same as [Offline replication](#).

Mb

(Megabit) Approximately one million (1,000,000) bits.

Mb/s

(Megabits per second) Used to describe the speed of network data transmission.

Microsoft Volume Shadow Copy Service

Microsoft Volume Shadow Copy (also referred to as Volume Snapshot Service, Volume Shadow Copy Service, or VSS), is a technology included in Microsoft Windows that allows you to take manual or automatic backup copies or snapshots of data.

If the Unity is joined to a Microsoft Active Directory domain, Unity automatically exposes all the snapshots for each file system/LUN on the Unity to Microsoft Windows (CIFS) clients that access the file system/LUNs—provided the Windows client computers support Microsoft VSS.

You can then use Microsoft VSS on the Windows client computers to restore previous versions of files and folders from a snapshot of a file system/LUN, or roll back a file system/LUN to a specific point-in-time snapshot.

Move a storage pool

This refers to the act of moving, or transitioning, a storage pool from one [Pool Resource Group](#) to the other.

You should only perform this action if you need to rebalance the I/O load on the system, since this changes the virtual end point through which end users and client systems access the data in the storage pool.

When you move a storage pool from one Pool Resource Group to the other, the data sets (file systems and/or iSCSI LUNs) in the storage pool are no longer accessible through the virtual IP address of the Pool Resource Group that the storage pool was previously assigned to. You will need to change all file system and iSCSI LUN mappings on client systems to reflect the virtual IP address of the Pool Resource Group to which the storage pool is currently assigned.

See [Moving a storage pool](#) on page 116.

MPIO

Multipathing I/O is designed to provide multiple paths to SAN storage. It provides connection failover and load balancing benefits to strengthen the stability of a network storage environment.

Multi-site

Unity allows you to manage any number of sites within a single instance of Unity. Every Unity site has its own set of resources independent from other sites. This functionality provides a global point of control for managing your Nexsan storage infrastructure across multiple geographic locations.

When configuring a site that is the primary site of a replicated site, its replicated counterpart is automatically added as well. The same applies when the site is a secondary site.

Likewise, disconnecting a site that is part of a replicated pair also disconnects the replicated site.

See [Understanding multi-site implementation on page 28](#).

N

NAS

(Network-attached storage) File-level computer data storage connected to a computer network providing data access to clients on the network. Network-attached storage uses specialized hardware, software, or both, and is often a specialized device built from the ground up for storing and serving files.

NIS

(Network Information Service) One of the three UNIX directory services supported by Unity. NIS is a client-server directory service protocol for distributing system configuration data such as user and host names between computers in a UNIX network environment. It was originally called Yellow Pages or YP. A NIS/YP system maintains and distributes a central directory of user and group information, host names, e-mail aliases and other text-based tables of information in a computer network.

NDMP

(Network Data Management Protocol) Open standard protocol used to transport data between network attached storage (NAS) devices and backup devices. This removes the need for transporting the data through the backup server itself, thus enhancing speed and removing load from the backup server. It enables backup vendors and NAS storage vendors to work together without creating specific ports for each vendor and storage array in addition to allowing

storage array vendors to have their arrays *backup-ready* without installing extra backup client software.

Unitys include a NDMP plug-in that allows you to back up data from Unity to an industry-standard backup and restore solution that supports NDMP. The plug-in preserves all access rights for CIFS and NFS shares on Unity, and uses background snapshots for fast backups. See [Setting NDMP configuration options on page 349](#).

NetBIOS

(Network Basic Input/Output System) API that allows applications on separate computers to communicate over a local area network.

NetBIOS offers 3 services:

- Name service (UDP port 137)
- Datagram distribution service (UDP port 138)
- Session service (TCP port 139).

NestOS

NestOS is an optimized embedded operating system that runs on Unity. If you do not have access to Unity, you can run CLI commands against the NestOS command shell from any client machine with network access to Unity, or from a console connected directly to Unity via KVM.

NFS

(Network File System) A protocol allowing a user on a client computer to access files over a network in a manner similar to how local storage is accessed. Used in most UNIX environments for folder or device sharing. File Systems on Unity support NFS sharing.

NFS sharing

See [Sharing methods](#).

NFSv3

(Network File System version 3) In Microsoft Active Directory environments, if you want to give an Active Directory user and/or group access to an NFS share on Unity from a UNIX/Linux client machine, you must first add a corresponding user or group account to Unity, with the same UID (for user accounts) or GID (for group accounts) that the user/group account is assigned in the Microsoft Active Directory domain. Then, you must map the user or group account that

you add to Unity to its corresponding user or group account in the Microsoft Active Directory domain.

Unity's `nxdm` CLI (Command Line Interface) provides a set of commands for adding user and/or group accounts with specific UIDs/GIDs to Unity, and then mapping the accounts to their corresponding accounts in the Microsoft Active Directory domain. For more information, see `useradd`, `groupadd`, and `idmap` in the CLI. See also [Using an NFS version 3 \(NFSv3\) client to access an NFS share with Microsoft Active Directory](#) on page 178.

NFSv4

(Network File System version 4) NFSv4 uses name-based permissions mapping. This means users must have the same name on both the client and Unity. It also requires an NFSv4 Domain to be set. This must be identical on both Unity and the client. To access an NFS share from an NFS version 4 (NFSv4) client, you must perform specific configuration steps, see [Using an NFS version 4 \(NFSv4\) client to access an NFS share](#) on page 179.

NMP

(Network Management Protocol) Suite of network protocols that define the processes, procedures and policies for managing, monitoring and maintaining a computer network. NMP conveys and manages the operations and communications performed on a computer network.

Node

See [Controller](#).

NTP

(Network Time Protocol) A protocol designed to synchronize the clocks of devices over a network. See [Time server](#).

O

Offline replication

In asynchronous replication, an offline, or manual, replication is a replication process that you start manually on a storage pool. With offline replication, you can replicate the data in the storage pool to the remote Unity, or to a USB storage device attached to the primary Unity.

See the *Nexsan Unity Snapshots and Replication Guide*.

OU (Organizational Unit)

A useful type of directory object that is contained within domains is the organizational unit (OU). OUs are Active Directory containers into which you can place users, groups, computers, and other OUs. An OU cannot contain objects from other domains.

An OU is the smallest scope or unit to which you can assign Group Policy settings or delegate administrative authority. Using OUs, you can create containers within a domain that represent the hierarchical, logical structures in your organization. You can then manage the configuration and use of accounts and resources based on your organizational model.

OUs can contain other OUs. You can extend a hierarchy of OUs as necessary to model your organization's hierarchy within a domain. Using OUs helps you minimize the number of domains that are required for your network.

You can use OUs to create an administrative model that you can scale to any size. A user can have administrative authority for all OUs in a domain or for a single OU. An administrator of an OU does not have to have administrative authority for any other OUs in the domain.

P

Passive node

This refers to the controller node that currently is NOT hosting the System Management component, which includes cluster- and system-related services on the Unity.

Although both controller nodes on Unity operate in active mode, only one controller can host cluster- and system-related services at any given time.

For example, when you need to perform routine or emergency maintenance on the *active* controller node—you can transition, or move, the System Management component to the *passive* controller node in Unity, making it *active*.

See [Clustering overview](#) on page 294.

PCIe

(Peripheral Component Interconnect Express) A computer expansion card standard designed to replace the older Peripheral Component Interconnect (PCI), PCI-eXtended (PCI-X), and Accelerated Graphics Port (AGP) standards.

Peer

Also referred to as peer site, peer system, or replication peer. In asynchronous replication, a peer site represents an Unity that you set up data replication to/from.

Pool

A storage pool is a user-defined virtual grouping of volumes available on the Unity. Pools allow you to organize your storage into logical groups; expose file systems as shares to Windows-based (CIFS) and/or UNIX/Linux-based (NFS) clients on the network; expose blocks of storage as LUNs to iSCSI initiators on the network; and replicate all the data in the pool, or just a subset of it, for disaster recovery.

Unity allows you to create as many storage pools as there are available volumes (RAID sets) on the system.

If Unity has both internal storage and Nexsan Unity expansion unit(s) connected externally via SAS, you can create storage pools by combining volumes from both the main unit and the expansion unit(s)—provided the RAID level configurations are the same on both storage systems (or, enclosures).

Pool Resource Group

When you create a storage pool on the Unity, you assign it to one of the two Pool Resource Groups in the cluster. In turn, each Pool Resource Group, along with the storage pools assigned to it, is hosted on one of the two controller nodes on the Unity. By default, each controller node hosts a single Pool Resource Group. This configuration ensures a balanced load on the system.

During the initial setup of Unity, you assign a virtual IP address to each Pool Resource Group. End users and client systems on the network access their data (through file systems and/or iSCSI LUNs) in the storage pools using the corresponding Pool Resource Group's virtual IP address. For more information about data accessibility through Pool Resource Groups, see

[Example of data access in a typical Unity cluster implementation on page 300.](#)

See [Clustering overview on page 294](#)

Primary site

See [Site](#).

PSU

(Power supply unit) A module that regulates electrical power to the components of Nexsan Unity Storage Expansions.

Public alias

This is a symbolic name that you can assign to a target on Unity. The public alias is seen by some iSCSI initiators; it can help you identify the iSCSI target. The public alias for a storage pool's default target is the pool name. You can change a target's public alias at any time.

R

RAID

(Redundant Array of Independent Disks) A storage method in which data, along with information used for error correction, such as parity bits or Hamming codes, is distributed among two or more hard disk drives in order to improve performance and reliability.

Unity supports RAID 5, RAID 6, and RAID 10. See [Allocating new storage to the site on page 328](#) and [Resetting the RAID configuration for storage on page 331](#).

RAID 5

RAID 5 provides redundancy by writing data and parity information across three or more drives, thereby increasing performance. You need at least 3 disk drives for a RAID 5 implementation.

RAID 5 can withstand a single disk failure without losing data or access to data. It is ideally suited for transaction processing, database applications, file and print servers.

RAID 6

RAID 6 is similar to RAID 5, but with better fault tolerance. RAID 6 stripes blocks of data and parity across an array of drives like RAID 5, except that it

calculates two sets of parity information for each parcel of data. This significantly improves fault tolerance: RAID 6 can withstand the failure of any two drives in the array without losing data or access to data.

You need at least 4 disk drives for a RAID 6 implementation. RAID 6 is ideally suited for the same applications as RAID 5, but in situations where additional fault tolerance is required. We recommend adding Nexsan FASTier cache devices to a RAID 6 implementation to improve write performance.

RAID 10

RAID 10 provides very high performance and redundancy. Data is simultaneously mirrored and striped. On Unity, you have the flexibility of creating a RAID 10 set with 2 drives, instead of 4, in order to create a mirrored pair. This is similar to a RAID 1 implementation, but with the added benefit that when you expand the RAID array on Unity, you can do so with only 2 drives and striping will automatically be applied across 2 mirrored pairs.

RAID 10 can, under certain circumstances, support multiple drive failures. It is ideally suited for situations where both high performance and redundancy are important. RAID 10 implementation on Unity has some unique requirements; see [Mixing volumes with different RAID levels](#) on page 98.

RAM

(Random-access memory) A memory chip that allows stored data to be accessed at any time in any order. Commonly used in computers as main operating memory. Values in random-access memory are often volatile; information is lost if power is removed from the module.

Remote

In asynchronous replication, a remote or secondary site represents the system to which data from the primary Unity is replicated.

In a deployment where asynchronous replication is not implemented, a remote Unity represents a site that is being managed remotely from another Unity or site. See [Site](#).

Replica

In asynchronous replication, a replica, or a storage pool's replica, refers to the target storage pool that is created on the secondary Unity. The replica is an exact copy of its source storage pool on the primary Unity. Replicas can be promoted to full file systems, after which replication between the two storage pools is no longer possible.

Replication

Replication can be asynchronous or synchronous.

Asynchronous data replication allows you to replicate data between two sites—a primary and a remote Unity—over a LAN or WAN connection. See [Asynchronous data replication](#).

The synchronous data replication feature allows you to synchronously replicate a storage pool between two Nexsan E-Series systems connected to an Unity via SAS (or Fibre Channel). See [Synchronous data replication](#).

Rollback function

Unity allows you to roll back all the data in a file system/LUN to a specific point-in-time [snapshot](#) of the file system/LUN. The rollback function reverts a file system/LUN's contents to what they were at the time the snapshot was taken, including all file- and folder-level permission settings and file system/LUN-level access attributes. This function also automatically deletes all snapshots that are newer than the snapshot that you roll back to, including snapshots that have browsing enabled.

Unity provides the rollback function for extreme circumstances: for example, if all the data in a file system/LUN is corrupted and can no longer be recovered. The rollback function overwrites all the existing data in the file system/LUN with the contents of the snapshot that you roll back to; any new data that was added after the snapshot is recorded, including updates to existing data, is lost during the rollback process.

See the *Nexsan Unity Snapshots and Replication Guide*.

ROM

(Read-only memory) A memory chip that stores values but cannot be changed by normal program

instructions. Values in read-only memory are nonvolatile; they are retained even when the unit is powered down.

S

SAN

(Storage area network) An architecture that provides for attachment of remote computer storage devices to servers in such a way that the devices appear as locally attached to the operating system.

SAS

(Serial Attached SCSI) A serial version of the SCSI interface. A point-to-point architecture that uses a disk controller with four or more channels that operate simultaneously. Each full-duplex channel, known as a SAS port, transfers data at 1.5Gb/s, 3Gb/s, or 6Gb/s in each direction. SAS also supports Serial ATA (SATA) drives, which can be mixed with SAS drives in a variety of configurations.

SATA

(Serial Advanced Technology Attachment) A connection standard for fixed and removable hard disk drives.

Scheduled replication

In asynchronous replication, a scheduled replication refers to an automatic replication that occurs according to a schedule you define. You can configure a separate replication schedule for each storage pool on Unity.

Scrubbing

The Unity provides a disk scrubbing mechanism that checks the physical hard disks, which comprise the volumes in a storage pool on the Unity, for read or write errors.

The storage pool scrubbing mechanism scans a storage pool to identify data integrity problems. It sequentially reads all the data on the hard disks, as well as the data's corresponding parity information, and rebuilds parity wherever needed. Performing routine scrubbing on a storage pool prevents parity errors and data corruption.

You can enable/disable a pool scrub schedule on both the primary storage pool and on its replica on the

secondary Unity. By default, the scrub schedule is enabled on the replica.

See [Scrubbing a storage pool](#) on page 105.

SCSI

Small Computer System Interface. A collection of standards and proposed standards for input/output (I/O) communication, primarily intended for connecting storage subsystems or devices to hosts.

Secondary

In asynchronous replication, a remote or secondary site represents the system to which data from the primary Unity is replicated.

In a deployment where asynchronous replication is not implemented, a remote Unity represents a site that is being managed remotely from another Unity or site.

SFP

(Small Form-factor Pluggable) A type of gigabit interface converter (GBIC) in a compact form factor. The Fibre Channel ports or 10Gb iSCSI ports on Nexsan storage devices are SFPs.

Shadow copy

See [Microsoft Volume Shadow Copy Service](#).

Sharing method

These sharing methods are available in Unity:

CIFS sharing

The CIFS sharing method uses the Common Internet File Service (CIFS) protocol to expose a file system. Most operating systems, including Windows, Linux, and OS X can connect via CIFS.

CIFS is also known as SMB. Unity supports CIFS (SMB) versions 1, 2, and 3.

When you expose a file system using the CIFS sharing method, Unity emulates the file-serving functions of a Windows file server, including:

- File manipulation (read, write, create, delete, move, and copy)
- File locking and byte-range locking

- File access control with support for the semantics of Windows NTFS ACLs; see [Windows and UNIX Access Control Lists \(ACLs\) on page 188](#)
- File and directory attributes (read-only and archive)

NFS sharing

The NFS sharing method uses the Network File System (NFS) protocol to expose a file system to UNIX/Linux-based systems. NFS is used by UNIX/Linux-based platforms to file system files across the network. Unity supports NFS version 3 (NFSv3) and NFS version 4 (NFSv4).

When you expose a file system using the NFS sharing method, the Unity implements the file-serving functions of an NFS server, including:

- File manipulation (read, write, link, create, and so on)
- Directory manipulation (mkdir, readdir, lookup, and so on)
- Byte-range file locking
- UNIX-style ACL attributes (such as, rwx) for owner, group owner, and other; for more information, see [Windows and UNIX Access Control Lists \(ACLs\) on page 188](#)
- File and directory attributes (sizes, access times, and so on)
- Hard links and symbolic (soft) links

CIFS and NFS sharing

Selecting both CIFS and NFS sharing methods allows you to expose a file system to Windows and UNIX/Linux-based systems over both the CIFS and NFS protocols. This is called mixed-mode operation.

Although Unity integrates seamlessly in mixed environments, the CIFS and NFS protocols are quite different and can present some challenges.

File and folder name representation:

- On Windows, individual components of a file name—specifically, each folder along the path, and the final file name—are limited to 255

characters, and the total path length is limited to approximately 32,000 characters.

- On UNIX/Linux, individual components of a file name—specifically, each subdirectory along the path, and the final file name—are limited to 255 characters.
- It is important to note that some Windows Applications, including Windows Explorer will not let you create a physical path (including folders and the final file name) greater than 255 characters. However, Windows Explorer is able to browse a physical path (including folders and the final file name) greater than 255 characters.
- File names may contain any Unicode character. Windows 2003, Windows Vista, Windows 2008, and Windows 7-based systems can make full use of Unicode, but Windows 9x and NFS clients support only the Latin-1 version of extended ASCII.

File Locks in mixed-mode operation:

- When a CIFS client reads or writes to a file in a file system on Unity, it respects the locks that both CIFS and/or NFS clients take out on the file.
- In contrast, an NFS client only respects the locks taken out on a file by a CIFS client. NFS clients must therefore check for existing NFS locks with the Network Lock Manager (NLM) protocol used in UNIX/Linux environments. Unity supports both monitored and non-monitored NFS file locks.

To configure or modify the sharing method, see [Step 2: Configuring the access method on page 126](#) and [Modifying a file system's sharing method on page 136](#).

To access an NFS share from an NFS version 4 (NFSv4) client, you must perform specific configuration steps, see [Using an NFS version 4 \(NFSv4\) client to access an NFS share on page 179](#).

To access an NFS share from NFS version 3, see [Using an NFS version 3 \(NFSv3\) client to access an NFS share with Microsoft Active Directory on page 178](#).

Site

A site—also referred to as the local site, active site, or primary site (in a replicated environment)—represents a geographic location that hosts a Unity. More specifically, a site can contain either:

- a Unity with no external storage;
- a Unity with one or multiple Nexsan storage systems connected to it (via Fibre Channel or SAS).

A remote site—also referred to as a secondary site or a replication site (in a replicated environment)—represents either:

- a site that is designated as the data replication site for the local site;
- a site that is being managed remotely from the local site.

A site can be the primary site in a replicated environment and also perform double-duty as the remote data replication site for another Unity.

See [Setting up the site on page 39](#) and [Understanding multi-site implementation on page 28](#).

Site name

A site name allows you to assign a unique label to an Unity on the network. This label can then help you identify the function and/or physical location of Unity. For example, **Finance3rd** can describe a Unity that is designated as a file server/data repository for financial and/or accounting data, and which is currently located on the 3rd floor.

The site name is particularly useful in identifying sites in multi-site environments, where a single Unity session manages multiple sites on the network (remote site management).

See [Step 2: Configuring the site information on page 40](#) and [Modifying the site name on page 348](#).

SMB

(Server Message Block) CIFS—also referred to as SMB—is used by Windows-based systems to share files and printers across the network. Use this sharing method if your environment consists mainly of Windows-based systems. See [CIFS sharing](#).

SNMP

(Simple Network Management Protocol) The SNMP agent included in Unity allows you to send SNMP traps to a Network Management Station—such as, HP OpenView or CA Unicenter—when a Critical, Error, and/or Warning event is generated by a source component of Unity.

See [Setting up SNMP notification on page 537](#).

SMTP

(Simple Mail Transfer Protocol) Nexsan Unity sends email notifications to the SMTP server, which then routes the email notifications to the recipients that you specify.

See [Configuring SMTP server settings for the site on page 535](#)

Snapshot

A snapshot is a read-only copy of a file system/LUN at a specific point in time. Think of a snapshot as a frozen image of the data in a file system/LUN at the time the snapshot is recorded. You can use snapshots to maintain a set of previous versions of all the files in a file system/LUN, which can serve as temporary backups of your data.

For example, if a set of files in a file system/LUN are accidentally (or maliciously) deleted or overwritten, you can easily restore individual files from a snapshot of the file system/LUN by browsing the snapshot (and accessing it from a Windows-based (CIFS) system and/or a UNIX/Linux-based (NFS) system). Or, if all the data in a file system/LUN becomes corrupted, you can restore the data to a specific point-in-time snapshot using the [rollback](#) function.

Unity allows you to take manual snapshots of a file system/LUN and also set a schedule for automatic snapshots. You can create a separate snapshots schedule for each file system/LUN on Unity.

The snapshot is created almost instantly, and initially consumes no additional disk space within the storage

pool where the file system/LUN resides. When data within the file system/LUN changes—new data is added or existing data is updated—the snapshot maintains a reference to the previous copy of the data, and Unity updates the snapshot size accordingly. Unity protects the file's original data blocks from being overwritten; it stores the new updates in a new location. Unity maintains records and pointers to keep track of the data and file changes.

This results in minimal disk space consumption and also allows for rapid recovery of data in case of a disk write error, a corrupted file, or a program malfunction.

See the *Nexsan Unity Snapshots and Replication Guide*.

Snapshots browsing

The Unity provides a mechanism that allows you to access a snapshot from a Windows-based system and/or a UNIX/Linux-based system and browse its contents—in the same way that you access a file system or a LUN. A snapshot that you browse is a read-only copy of its parent file system/LUN and its contents mirror the parent file system/LUN's contents at the time the snapshot is recorded.

You can use Unity's snapshot browsing mechanism to recover individual files from a snapshot in case the files are accidentally deleted or overwritten, or corrupted in the snapshot's parent file system/LUN. Unity maintains all of the parent file system/LUN's access-level attributes with the snapshots to ensure any recovery is authorized. This means that you can safely authorize all users—that have access to the file system/LUN—to browse a snapshot and recover their own lost data from the snapshot.

This also applies to replicated snapshots see the *Nexsan Unity Snapshots and Replication Guide*.

SSD

(Solid State Disk) A high-performance storage device that contains no moving parts.

See [FASTier](#).

SSL

(Secure Sockets Layer) A commonly used protocol for transmitting private documents via the Internet. SSL works by using a public key to encrypt data that is transferred over the SSL connection. The SSL protocol secures the following data: I/O, serial port,

and VSIP communication; it does not apply to audio and video transmission.

See [Logging on to Unity](#) on page 50.

Storage enclosure

On Unity, a storage enclosure can be a **Nexsan external storage system**: this refers to a Nexsan E-Series storage system connected externally to Unity via a SAS add-on card (optional).

- E18™ / E18V™ / E18VT™ (serial #)
- E32V™ (serial #)
- E48™ / E48V™ / E48VT™ (serial #)
- E60™ / E60V™ / E60VT™ (serial #)

Unity Storage Expansions that connect to the Nexsan E-Series:

- E18X™/E18XV™ (serial #)
- E32XV™ (serial #)
- E48X™/E48XV™ (serial #)
- E60X™/E60XV™ (serial #)

A storage enclosure can be **internal storage**: internal storage is composed of SAS disks drives installed in the front bay of the Unity5100. The NST5100 includes 16 slots by default, with one slot typically used for a FASTier write cache device. The remaining slots can be used for 15 direct-attached, hot-swappable SAS drives.

A storage enclosure can also be a **Nexsan Unity Storage Expansion connected to the Unity via SAS**:

- The Unity5100X™ unit connects to the Unity5100 using the NST5110's on-board SAS host bus adapters.
- The Nexsan US224X™ unit connects to the Unity5310™ or Nexsan Unity 6530™ via a SAS add-on card (optional).
- The Nexsan Unity 2000XC unit connects to the Nexsan Unity 2000C, using the Unity 2000C's on-board SAS host bus adapters. The Nexsan Unity 2000XP unit connects to the Nexsan Unity 2000P, using the Unity 2000C's on-board SAS host bus adapters.

All disk storage on Unity is represented as volumes.

Storage pool

See [Pool](#).

Subnet

A subnetwork, or subnet, is a logically visible subdivision of a TCP/IP network. All computers in a subnet have IP addresses with the same prefix. Addresses in the same subnet are reachable without going through a router, and thus can be reached by broadcast.

When connecting to Unity, the client computer must be on the same network and subnet as Unity.

Subnet mask

A means of restricting IP addresses on a subnet to a specific range.

Synchronous data replication

The synchronous data replication feature essentially mirrors all the data contained in a storage pool between a *source* Nexsan E-Series system and a *target* Nexsan E-Series system—both of which are connected to the same Unity via SAS (or Fibre Channel). You designate the storage system to use as the *source*—that is, the system on which you create the storage pool and store your data—and the *target*, where the source data is mirrored.

Synchronous replication ensures that a copy of the data, which is identical to the source copy, is created at the time the source copy is updated. An I/O-update operation is not considered done until completion is confirmed on both the source and the target. An incomplete operation is rolled back on both the source and target, ensuring that the target is always an exact mirror image of the source.

If either the source or target system fails for any reason, your users and applications can continue to access their data on the storage system that is currently online. When you restore the second system, Unity automatically reestablishes the synchronous link between the two systems.

In addition, you can later promote the mirror (storage pool) on the target system to an independent storage pool in your Unity deployment. Promoting the mirror (storage pool) severs the synchronous link between the source and mirror and creates a second,

independent copy of the storage pool—with both copies containing exactly the same data.

See the *Nexsan Unity Snapshots and Replication Guide*.

System Management

The System Management component includes all system- and cluster-related services on Unity. You assign the System Management component the management virtual IP address during the initial setup of the system.

Notes: You use the management virtual IP address to access Unity.

The System Management component is hosted only on one controller node in the cluster at any given time. This controller node is typically referred to as the *active* node, while the other controller is considered *passive*. In reality, both nodes are active, but only one controller node can host the cluster services.

In a failover situation, where the *active* controller node—that is, the node currently hosting the System Management component—fails, or needs to be shut down for maintenance, Unity automatically transitions the System Management component to the *passive* controller, making it *active*.

See [Moving cluster resources on page 304](#), [Restarting the cluster or individual controller nodes on page 306](#) and [Shutting down the cluster or individual controller nodes on page 307](#)

T

Target public alias

See [iSCSI target public alias](#).

TCP/IP

(Transmission Control Protocol/Internet Protocol) The set of communications protocols used for the Internet and other similar networks. TCP provides reliable delivery of messages between networked computers. IP uses numeric IP addresses to join network segments.

Time server

Unity uses a time server, or NTP (Network Time Protocol) server, to synchronize its date and time with. This ensures that the date and time settings on

Unity are synchronized with the Active Directory or LDAP server on the network—which, in turn, ensures accurate time for time stamps and log files, as well as network transactions, such as, user authentication.

If you do not specify a time server, Unity synchronizes its date and time with the Microsoft Active Directory server or the LDAP Directory Server that it is connected to; the corresponding domain server **MUST** support this implementation.

See [Modifying the time server](#) on page 348.

Thin Provisioning

Thin Provisioning allows you to dynamically allocate disk space to a client system (initiator) connected to the LUN on Unity. With Thin Provisioning, you can flexibly allocate disk space (on a LUN) to the client system (initiator), in order to expand the storage capacity available to the client system at anytime. Specifically, Thin Provisioning allows you to specify the size of the virtual volume that initiators on the network see when they connect to a LUN, irrespective of the actual space that you reserve for the LUN in the storage pool.

The size of a LUN's virtual volume is not constrained by the storage pool's physical capacity; you can set any *reasonable* value, provided you intend to fulfill the LUN's virtual capacity with physical space, some time in the near future. You can flexibly allocate disk space to the LUN, on an as needed basis, without the need to immediately allocate physical storage.

See [Setting the LUN name and block size](#) on page 217.

U

User

Users can be either people (meaning accounts tied to physical users) or accounts which exist for specific applications to use.

Each user can be associated with multiple groups and automatically inherits their access rights and share-level permissions. All access rights and permissions are additive, which means that a user inherits the sum of access rights and permissions of all groups that the user belongs to. For example, if group A grants a certain right, you cannot revoke it in group B.

In Unity, users can be:

- [Microsoft Windows Active Directory domain or LDAP Directory service users](#): Unity uses existing Microsoft Windows Active Directory domain or LDAP Directory service user accounts, and saves supplemental authorization settings on Unity. This allows you to give access rights to log on to Unity and administer Unity to your Microsoft Windows Active Directory domain or LDAP Directory service users.
- [Local users](#): All account information is created and saved locally on Unity.

You grant access rights to users by assigning an administrative role to them in Unity; see [Nexsan Unity roles and access rights](#) on page 67 and [Setting access rights](#) on page 82.

User authentication mode

Unity supports three modes for user authentication:

- Microsoft Windows Active Directory domain
- LDAP Directory service (in UNIX/Linux environments)
- Unity authentication

With Unity authentication, a user enters a user name and password to log on to Unity, and Unity verifies that they match a user name and password stored locally on the Unity. With authentication through a Microsoft Windows Active Directory domain or an LDAP Directory service, a user enters a user name and password in the same Unity login window and Unity checks the Microsoft Windows Active Directory server or LDAP Directory server for a matching user record.

Regardless of the type of authentication, Unity uses the information in your configuration to determine the type of access that a user has to Unity—site-level or pool-level access—as well as the file system-level access permissions that are granted to the user.

See [User authentication modes](#) on page 66 and [Role-based administration in Nexsan Unity](#) on page 66.

Benefits of Microsoft Windows Active Directory domain or an LDAP Directory service:

- **Convenient account setup:** Your users can use the same login credentials to log on to Unity that they use to log on to the Microsoft Windows Active Directory domain or LDAP Directory service. This saves you the time and effort involved in creating individual user accounts and groups in Unity.
- **Efficient access control:** Unity allows you to configure the access rights to the file systems on Unity for each of your Microsoft Windows Active Directory domain or LDAP Directory service users or groups.
- **Robust security:** Allows you to enforce the password management policies that are implemented in your corporate infrastructure.
- **Additional file system management features available with Microsoft Windows Active Directory:** When joining a Microsoft Windows Active Directory domain, you can use Microsoft's Volume Shadow Copy function on your Windows client machines to restore previous versions of files and folders from a snapshot of a file system, or roll back a file system to a specific point-in-time snapshot. Additionally, you can use Microsoft's Quota management function to limit the amount of disk space used by individual users on a file system.

V

VMware VAAI

Unity includes a built-in VAAI (vStorage APIs for Array Integration) plugin to provide hardware acceleration on Unity when integrated into a VMware ESX/ESXi environment. VAAI hardware acceleration functionality enables the VMware ESX/ESXi host to offload specific virtual machine and storage management operations to Unity. With storage hardware assistance, the VMware ESX/ESXi host performs these operations faster and consumes less CPU, memory, and storage fabric bandwidth.

The Unity supports these 4 VAAI primitives:

- Full Copy
- Block Zeroing
- Block Unmap
- Hardware assisted locking

See [Enabling VMware VAAI hardware acceleration for a LUN on page 228](#).

Volume

A volume represents a virtual subset of the aggregated disk space available on Unity, or on a Nexsan E-Series connected externally to Unity via Fibre Channel or SAS, or an Nexsan Expansion unit connected to Unity via SAS.

Nexsan Unity presents the disk space available on Unity, or on any Nexsan storage enclosure attached externally to Unity, as volumes. The total number of volumes available on Unity's internal disk storage, as well as on storage systems attached externally to Unity, depends on the [RAID level](#) (5, 6, or 10) and RAID sets that you specify during the site setup. All disk storage on Unity is represented as volumes.

See [Storage](#) and [Pool](#). See also [Mixing volumes with different RAID levels on page 98](#), and [Resetting the RAID configuration for storage on page 331](#).

VSS Hardware Provider

([Volume Shadow Service](#)) Unity's VSS Hardware Provider enables a VSS host to create and manipulate shadow copies (point-in-time snapshots) of the data in LUNs on Unity. The VSS Hardware Provider supports Windows Volume Snapshot Service (or Volume Shadow Copy Service). The VSS Hardware Provider serves as the interface between Windows Volume Shadow Copy Service running on a host system and Unity.

The Unity's VSS Hardware Provider serves as the interface between Windows Volume Shadow Copy Service running on a host system and the Unity. Upon receiving instructions from a VSS host to create, mount, and restore snapshots, the VSS Hardware Provider sends the appropriate commands to the Unity and returns the result of these commands to the host.

The VSS Hardware Provider supports snapshot management for any Windows Server applications,

such as Microsoft SQL Server and Microsoft Exchange, and also for LUNs hosted on external storage, such as Nexsan E-Series or a Nexsan Unity Storage Expansion.

The VSS Hardware Provider includes a Windows Shell extension that adds a Unity property page for managing shadow copies on the VSS host. .

You must install the VSS Hardware Provider on a Windows Server host, and then use the host's initiator to connect to a storage pool's management iSCSI target for viewing, creating, and managing snapshots of the LUNs in the storage pool.

See the *Nexsan Unity Snapshots and Replication Guide*.

W

WAN

(Wide Area Network) A computer network that spans a relatively large geographical area. Typically, a WAN consists of two or more local area networks (LANs).

Wizard

A graphical user interface type that presents a user with a sequence of dialog boxes that lead the user through a series of well-defined steps.

Index

A

- Access Control Lists (ACLs) 188
- Access permissions 66-67, 186
 - shares 170, 186
- Access Rights and Share Permissions window 78
- Access Rights tab 78-79
- Access Time mode 114, 142
- Accessing a CIFS share 173
- Accessing an hidden share 127
- Accessing an NSTshare 177
- Accessing the IPMI web-based interface 317
- ACLs 19-20, 188, 207, 380, 397, 400, 542-543, 569
- Active Directory 66, 423, 573
 - Configuring the host for Kerberos support 393
 - creating computer objects 373
 - domain requirements 371
 - time server 573
- Active mode 320
- Active/Active clustering 22, 293, 553
- Add a secondary site for asynchronous data replication 425
- Add dashlet icon 475
- Add mirror volumes 468
- Add synchronous 467
- Adding
 - users 90, 92
 - volumes 101
- Adding a CHAP user 281
- Adding a dashboard 479
- Adding a group 91
- Adding a host for each Resource Controller in DNS Manager 393
- Adding a LUN 216
- Adding a Reverse Lookup Zone in DNS Manager 387
- Adding a secondary site 357
- Adding a share 123, 168
- Adding a storage pool 100
- Adding a user account 90
- Adding a user to a group 92
- Adding an iSCSI target 288
- Adding an iSNS server 244-245
- Adding new drives 333
- Adding volumes to a pool 101, 107
- Adding volumes to a pool replica 109
- Adding volumes to a replicated pool 109
- Adding volumes to the primary pool 109
- Additional network interfaces 314
- Advanced search function 76
- All ports / All LUNs feature 22, 554
- Allocating cache devices to a pool 103
- Allocating FASTier cache devices 430
- Allocating new storage 328
- Allocating storage 44
- Allowing Unity to suggest volume allocation 110
- Alternate primary/secondary domain controllers 386
- Anonymous access 187
- APAL status 403
- Applications 218
- Asynchronous replication
 - Enabling bandwidth throttling 446
- Asynchronous Replication
 - before you begin 423
 - compression 438
 - Creating a bandwidth throttling schedule 447
 - Deleting a bandwidth throttling schedule 449
 - disabling 434
 - Disabling a bandwidth throttling schedule 449
 - enabling 434
 - encryption 438
 - features 421
 - Modifying a bandwidth throttling

- schedule 448
 - network settings 436
 - offline replication 442
 - one-to-one 422
 - removing 463
 - starting 424
 - step 1 425
 - step 2 428
 - step 3 429
 - step 4 430
 - step 5 431
 - step 6 432
 - terminology 247, 420
 - usage 422
- Authentication modes
 - LDAP 398
- Auto-deletion 127, 222
- Auto-deletion settings of snapshots 112
- Auto-refresh interval for the site 351
- Automatic collection and transfer of system logs 406
- Automatic replication 420
- Automatic snapshots 197, 252
- Automatically assing a name 199, 254
- Available Space report 507
- Available Volumes 109

B

- Bandwidth throttling
 - creating a schedule 447
 - deleting a schedule 449
 - disabling a schedule 449
 - enable 446
 - modifying a schedule 448
- Before adding LUNs 216
- Before creating pools 98
- Benefits of authenticating users 573
- Browsing a LUN snapshot 254
- Browsing a share snapshot 199
- Browsing contents of a replicated share 441
- Browsing disabled for a difference file system 461
- Browsing enabled for a difference share 460
- Browsing replicated snapshots 441
- Browsing snapshots 194-195, 199, 202, 247, 249-250, 254, 256, 273, 280, 439-440, 459, 461-462, 555

C

- Cache devices 103
- CallHome
 - understanding 406

- Change My Password 62
- Changing a user's password 94
- Changing the Unity Administrator (nxadmin) password 95
- CHAP 214
- CHAP authentication 281
 - Adding a CHAP user 281
 - Deleting a CHAP user 283
 - For a target 287
 - Setting the site-level CHAP user 286
- CHAP secret 283
 - Modifying 284
- Chassis inter-connect card status 301
- Check for updates 365
- Choosing a dashboard template 483
- CIFS 201, 461
- CIFS and NFS sharing 173
- CIFS Permissions tab 78
- CIFS sharing 19, 23, 32, 34, 36, 69, 78, 97-98, 121-123, 126, 133, 136, 143, 145, 153, 159, 168, 172-173, 175, 183, 186-188, 190, 193, 203, 207, 209-210, 246, 248, 300, 344, 349, 380, 386, 397, 400, 432, 441, 457, 462, 494, 499, 539-540, 542-546, 553, 568
- Clearing event logs 527
- Clearing pool errors 118
- Cluster
 - chassis inter-connect card status 300
 - Controller information 300
 - Health status 300
 - License information 300
 - Managing active/active clustering 293
 - Moving cluster resources 304
 - Restarting cluster nodes 306
 - Shutting down cluster nodes 307
 - Typical cluster implementation 300
 - When a node is down 302
- Cluster-level access rights 68
- Collecting logs 528
- Collection of system logs 406
- Complete system failure 451
- Compression settings 438
- Computer objects 373, 383
- Concepts and terminology
 - Replication 247, 420
- Configurable RAID 22
- Configure Event Logging 61
- Configuring a data replication schedule 428
- Configuring IPMI settings 316
- Configuring LACP 323
- Configuring logging options 529
- Configuring LUNs in Disk Management 268
- Configuring network settings with setip 316
- Configuring new drives 333
- Configuring RAID settings 328
- Configuring report settings 508

- Configuring SMTP server settings 535
- Configuring storage 43-44
- Configuring the host in Active Directory 393
- Connecting to a specific domain
 - controller 383
- Connecting to an iSCSI LUN from a
 - Windows-based initiator 290
- Connecting to the Internet
 - using a direct LAN link 415
 - using a workstation 416
 - using an HTTP proxy server 415
- Connectivity to the Internet 414
- Controller IP addresses 310
- Convention for a site name 348
- Copying a dashboard template 482
- CPU 493, 499
- createlogpackage 528
- Creating
 - snapshots 194, 245
 - storage pool 98
- Creating a bandwidth throttling
 - schedule 447
- Creating a dashboard 479
- Creating a dashboard template 482
- Creating a recording 502
- Creating a storage pool 100
- Creating an Initiator group 234
- Creating file systems for home
 - directories 152
- Critical 139
 - pool 115
- Critical event 521, 523
- Current and accurate copy of production
 - data 466

D

- Dashboard
 - Templates 480
 - toolbar 475
- Data backup 422, 466
- Data backups 214
- Data compression for Async
 - Replication 438
- Data distribution 422
- Data encryption 438
- Data import 444-445
- Data management functions on LUNs 214
- Data migration 422, 451, 466
- Data protection 214
- Data replication 127
 - access rights 71
 - LUN 220
- Data Replication 98, 122, 124, 155, 168, 214, 217, 220, 296, 423, 425, 428-432, 466, 468-470, 488, 518, 521, 557

- Data sharing disabled 135
- Data type 218
- Dataset replication 422, 429, 434
- Date and time formats 353
- DEGRADED 119
- Deleting a bandwidth throttling
 - schedule 449
- Deleting a CHAP user 283
- Deleting a dashboard template 482
- Deleting a recording 504
- Deleting a share's replication conflict 462
- Deleting a storage pool 120
- Deleting a user or a group 94
- Deleting an Initiator group 236
- Deleting LUN snapshots manually 257
- Deleting reports 516
- Deleting share snapshots manually 205
- Demoting a site 455
- Demoting a storage pool 456
- Device I/O 494, 499
- diff file 462
- Difference file system 461
- Difference share 458, 460, 462
- Direct LAN link 415
- Disabling a bandwidth throttling
 - schedule 449
- Disabling a storage pool's replication
 - schedule 434
- Disabling asynchronous data replication for
 - a dataset 434
- Disabling automatic FASTier write cache
 - assignment 348
- Disabling browsing for a difference file
 - system 461
- Disabling data sharing
 - shares 183
- Disabling data sharing for a share 135
- Disabling Read caching 231
- Disabling the Access Time mode 142
 - pool 114
- Disaster recovery 214, 422, 450, 466
- Disconnecting a site 360
- Discovering new domain controllers 385
- Discovering new storage 328
- Disk Management 268
- Disk properties 269
- Displaying events
 - based on severity type 523
 - for a site 522
 - for a specific date or time period 524
 - from a source component 523
 - in the last 24 hours or last 7 days 524
- distinguishedName 383
- DNS alias 371
- DNS Manager
 - Adding a host for each Resource
 - Controller 393
 - Adding a Reverse Lookup Zone 387
- DNS mappings 453-457

- dNSHostName 375
- Domain
 - Joining 380
 - Unjoining 396
- Domain controller
 - Alternate primary/secondary 386
- Domain controller discovery 385
- Domain controller management 385

E

- E-Series storage enclosures 332
- Emailing events 527, 531
 - Space usage threshold violations 533
- Emailing reports 513
- Enable auto-deletion of snapshots 205, 259
- Enable email alerts 531
- Enable NDMP 350
- Enable scheduled delivery of report by email 514
- Enable Scrub Scheduling option 107
- Enable snapshot scheduling 127, 221
- Enable SNMP alerts 538
- Enabling a scrub schedule for a replica 435
- Enabling asynchronous data replication for a dataset 434
- Enabling bandwidth throttling 446
- Enabling browsing for a difference share 460
- Enabling browsing of a replicated snapshot 441
- Enabling client-side space usage notifications for a LUN 228
- Enabling compression
 - LUN 230
 - share 141
 - storage pool 113
- Enabling FTP support 405
- Enabling Internet Connectivity 414
- Enabling IPMI 316
- Enabling jumbo frames 319
- Enabling jumbo frames using Unity 318
- Enabling Kerberos 386
- Enabling LACP 324
- Enabling LACP on the NST appliance 320
- Enabling Read caching 231
- Enabling the Access Time mode 142
- Enabling the security mode for NFS shares at the site level 180, 403
- Enabling verbose logging 529
- Enabling VMWare VAAI hardware acceleration 228
- Encryption settings 438
- Error 140
- Error event 521, 523
 - pool 116, 118
- Ethernet switches for LACP 321, 324

- Event logs 517
 - access rights 73
 - Clear 527
 - Collecting logs 528
 - Configuring logging options 529
 - Emailing events 527
 - Event grid 520, 524
 - Event Viewer 522
 - Filtering events 522
 - Messages 521
 - Searching for an event 525
 - Viewing events 518
- Event notification 517
 - Setting up emails 531
 - Setting up notifications 530
- Event Viewer 522
 - Layout 519
 - Saving events 526
- Example of cluster implementation 300
- Expandable storage 22
- Expanding capacity for a pool 107
- Exporting a template 484
- Exporting data 446
- Exporting reports 515

F

- Failover 422
 - Demoting a site 455
 - Demoting a storage pool 456
 - disaster recovery 450
 - of a storage pool 453
 - of the entire site 452
 - Promoting a storage pool's replica 454
 - Promoting the remote system 454
 - Site failover vs. pool failover 451
 - versus promote 451
- FASTier cache devices 103, 348, 430
- FASTier I/O 494
- FASTier I/O statistics 499
- FASTier Read access 494
- FASTier Read caching 231
- FASTier IOPS 494
- FAULTED 118
- Features by platform 26
- File locks 569
- File name representation 569
- File system 121
 - considerations 122
 - data management functions 122
 - renaming 134
 - viewing space usage 149
- Filtering events 522
 - by site, source, or severity type 522
 - by time period or date 523
 - Event grid 524
- Filtering live performance metrics 501
- Filtering snapshots in the grid 195, 250

- Find Domain Controllers 385
- Find function 76
- Find icon 475
- Firmware version of E-Series 332
- Folder name representation 569
- Frequency of email alerts 532
- FTP 405
- FTP Sharing 173
- Full-Duplex 321
- Full access
 - shares 188

G

- Generating reports 509
- GID 92, 179, 564
- Global catalog 371
- Global toolbar 61
- Group Members tab 79, 81
- groupadd 178
- GUID Partition Table 268
- Guidelines for LUNs 214

H

- Hidden CIFS share 136, 170
- Hidden share 127
- High availability 294
- home directories
 - adding 152
 - example in Windows 167
 - modifying 147, 151
 - Performing file system-level tasks 166
- home directories
 - Managing group assignments 165
- Hot spares 46, 329, 332
- How long to keep event logs 529
- HTTP proxy server 415

I

- IDMU 178-179, 383
- igb# 314
- Imminent system failure 451
- Importing a template 484
- Importing data from a USB storage
 - device 445
- Importing data from the primary site 444
- Incoming replications 440-441
- Incremental updates 420-421
- Informational event 521
- Initializing a LUN 291
- Initializing LUNs in Disk Management 268

- Initiator group
 - create 234
 - delete 236
 - modify 235
- Internet connection
 - with a direct LAN link 415
 - with a workstation 416
 - with an HTTP proxy server 415
- Intersite virtual IP address 427
- Intersite Virtual IP address 310, 358
- IP address requirements 309
- IPMI console 319-320, 323
- IPMI settings 316
- IPMI web-based interface 317
- IQN 288
- iSCCI target
 - Adding 288
 - Managing 280
 - mgmt target 259
 - Specifying IQN and public alias 288
- iSCSI initiators 281
- iSNS 244-245
- ixgbe# 314

J

- Joining
 - LDAP 398
- Joining a domain 380
- Jumbo frames 319

K

- Keep a limited number of auto-
 - snapshots 205, 258
- Keep auto-snapshots 205, 259
- Keeping event logs 529
- Kerberos
 - Adding a host for each Resource
 - Controller in DNS Manager 393
 - Adding a Reverse Lookup Zone in DNS
 - Manager 387
 - Configuring the host in Active
 - Directory 393
- Key features 22
- KVM console 323

L

- LACP 320
 - configuring 323
 - Requirements and guidelines 320
 - Understanding link aggregation 322
- Layout of Event Viewer 519

- Layout of the Manage Users and Groups panel 74
 - LDAP 24, 51, 62, 66, 74-75, 79-82, 84, 86, 88, 90, 126, 136, 159, 170, 175, 186-187, 189, 192-193, 348, 350, 359, 371-372, 381, 385, 398, 400, 423, 539, 546, 548, 573
 - LDAP catalog 371
 - LDAP Directory server 371
 - LDAP directory service 398
 - LDAP Domain 398
 - LDAP server 573
 - License status for the cluster 300
 - Link aggregation 322
 - Link layers 313
 - Linux 218
 - Live performance metrics 501
 - Load balancing 294, 320, 451
 - Local volumes 426
 - Logging options 529
 - Logical Unit Number (LUN) 217
 - Logs 406
 - LUN
 - Adding a target 288
 - Connecting to an iSCSI LUN from a Windows-based initiator 290
 - Data management functions 214
 - Deleting snapshots 257
 - Enabling client-side space usage notifications 228
 - Enabling VMWare VAAI hardware acceleration 228
 - guidelines 214
 - Initializing a LUN 291
 - LUN-level access rights 69
 - Managing 213
 - mgmt target 259
 - renaming 227
 - Snapshots 245
 - Snapshots Properties panel
 - Settings tab 251
 - Stopping snapshot browsing 256
 - viewing space usage 115, 232
 - LUN compression 230
 - LUN I/O 494
 - LUN name 218
 - LUN Virtual Volume Size report 507
- M**
- Maintenance update plan 364
 - Manage CHAP Users 62
 - Manage templates icon 475
 - Manage Users 62
 - access rights 72
 - Manage Users and Groups panel 74
 - Management interface IP addresses 310
 - Management network interface 22, 42-43
 - Management Virtual IP address 310
 - Managing
 - events 26
 - Managing snapshots for shares 194
 - using Properties panel 194
 - Managing Templates 481
 - Managing users and access rights 74
 - Manual pool scrub 106, 436
 - Manual replication 421
 - Manual snapshots 198, 253
 - Manually allocating volumes 110, 468
 - Manually deleting LUN snapshots 257
 - Manually deleting share snapshots 205
 - Manually refreshing site-level or share-level information 352
 - Mapping a CIFS share 175
 - Master Boot Record 268
 - Matching volume 468
 - Maximum number of targets per pool 280
 - Memory 494, 499
 - mgmt target 259
 - Microsoft Active Directory 51, 62, 74-75, 79, 90, 127, 152-153, 156, 158-159, 170, 178, 186, 203, 248, 348, 350, 359, 371, 373, 385, 396, 400, 539, 546, 548-549, 553
 - Microsoft Exchange 218
 - Microsoft Volume Shadow Copy Service 203, 248
 - Mirror pool 572
 - promoting 470
 - Mixed mode operation 569
 - Mixing of volumes 99
 - Modifying a bandwidth throttling schedule 448
 - Modifying a CHAP user's secret 284
 - Modifying a dashboard 479
 - Modifying a dashboard template 483
 - Modifying a storage pool's replication schedule 433
 - Modifying an Initiator group 235
 - Modifying data and time formats 353
 - Modifying network settings 309
 - Modifying sharing methods 136
 - Modifying site auto-refresh intervals 351
 - Modifying space usage settings 137
 - Modifying user authentication settings 371
 - Mount points
 - shares 178, 186
 - Moving a storage pool
 - from pool's properties panel 116
 - Moving cluster resources 304
 - msDS-SupportedEncryptionTypes 375
 - MTU 562
 - Multi-site management 357
 - Mutual CHAP authentication 281, 287

N

- NDMP configuration 349
- NDMP support for data backups 214
- NESTHOSTNAME 375
- NestOS Admin Menu
 - Shutdown and Reboot menu 320
- Network interfaces
 - IP addresses 311
 - link layers 313
 - naming convention 314-315
 - setting up a secondary interface 314
- Network performance 494, 499
- Network settings 42-43, 330
 - modifying 309
- Network settings for asynchronous replication 436
- Network Time Protocol (NTP) 371
- New drives 333
- New features and enhancements 20
- New Simple Volume 269, 291
- New storage allocation 328
- New storage discovery 328
- New user for E-Centre authentication 90
- Nexsan storage system 330
- NFS 201, 461
- NFS security mode
 - site 180, 403
- NFS sharing 16, 19, 21, 23, 32, 34, 36, 97-98, 121-123, 126, 133, 136, 143, 145, 153, 159, 169, 173, 177-179, 186-188, 207, 209-210, 246, 300, 344, 349, 380, 397, 400, 402, 432, 441, 457, 462, 494, 499, 539-540, 542-543, 545-546, 549, 553, 569
- NFS Version 180, 403
- NFSv3 178, 188
- NFSv4 188
- nic
 - create-aggr 315
 - modify-aggr 324
 - remove-aggr 314
 - set-linkprop 320
- nic show-link 313-314
- No access 143
- Node context menu 59
- Non-Administrator user account 373
- Non-Optimized Path 22, 32, 34, 36, 294, 296, 298-299, 403, 554
- Non-responsive 301
- Notification thresholds 139
- nstndmp 349
- nstusermaps 178, 549
- Number of RAID sets 46, 329, 332
- nx# 314
- nx0 42-43, 313, 324
 - IP addresses 309-310

O

- Network interface 311
- nx1 324
- nx99 42-43, 313-314
 - IP addresses 309-310
 - Network interface 311
- nxadmin access rights 66-67
- nxadmin credentials 359, 400

- OFFLINE 119
- Offline disks 268
- Offline replication 421, 442
 - to USB device 443
- on-board LAN1 port 311
- One-to-one replication 422
- One-way CHAP authentication 281, 287
- Opening the Manage Users and Groups panel 74
- Optimized path 22, 32, 34, 36, 294, 296, 298-299, 403, 554
- Oracle OLTP 218
- Order of precedence for pool and dataset properties 99
- Organizational Unit (OU) 383

P

- Passive mode 320
- password
 - Unity administrator 40
- Password change 94
- Peer site 420, 566
- Performance metrics 501
- Performance Monitor
 - Starting 500
- Performance snapshot 502
- Performing a failover 452
- Performing a failover of a storage pool 453
- Permissions 62, 74-75, 78-81, 96, 122, 145, 171, 188, 190, 192-193, 281, 543-546
- Pool
 - property settings order of precedence 99
- Pool Administrator access 66-67, 85
- Pool compression 113
- Pool resource group
 - Virtual IP address 311
- Pools
 - Adding volumes to a pool 107
 - Adding volumes to a pool replica 109
 - Adding volumes to a replicated pool 109
 - Adding volumes to the primary pool 109

- creating a storage pool 100
 - Deleting 120
 - Demoting a storage pool 456
 - Disabling a storage pool's replication schedule 434
 - Disabling the Access Time mode 114
 - Manual scrub 106
 - Modifying a storage pool's replication schedule 433
 - Performing a failover of a storage pool 453
 - pool level access rights 68
 - Promoting a storage pool's replica 454
 - Promoting the mirrored storage pool 470
 - Removing asynchronous data replication for a storage pool 463
 - Replacing a volume 110
 - replica 420
 - Setting the scrub schedule 106
 - Snapshot auto-deletion 112
 - Space usage notification thresholds 115
 - Powering down Unity storage enclosures 335
 - Powering on Unity 337
 - Powering Unity back on 337
 - Pre-defined computer objects 383
 - Primary pool 109
 - Primary site 420
 - Printing reports 515
 - private0 311, 313
 - Promote 451
 - Promoting a replica 454
 - Promoting the mirrored storage pool 470
 - Promoting the remote system 454
 - Properties panel 60
 - Proxy DN 398
 - Proxy server 415
 - Public alias 288
- Q**
- Quiesce the system 307
 - Quota 125, 137
- R**
- RAID configuration 328
 - Resetting 331
 - RAID level 46, 329, 332
 - Read-only access 143
 - Read-only anonymous access 201, 461, 553
 - Read-write access 143
 - Read access
 - shares 188
 - Read caching 231
 - Read/Write access
 - shares 188
 - Read/Write anonymous access 553
 - Rebalancing storage 470
 - Rebooting E-Series 339
 - Recording
 - Creating 502
 - Deleting 504
 - Stopping 502
 - Viewing 504
 - Recurrence 127
 - Redundancy 320
 - Refresh System Cache 62
 - Refreshing events 520
 - Refreshing site-level or share-level information 352
 - Remote access to replicated data 422
 - Remote connectivity 407
 - Remote site
 - access rights 72
 - adding 357
 - disconnecting 360
 - Remote volumes 426
 - Removing a storage enclosure 335
 - Removing a user from a group 93
 - Removing asynchronous data replication for a storage pool 463
 - Removing synchronous replication for a storage pool 471
 - Renaming a dashboard template 483
 - Renaming a file system 134
 - Renaming a LUN 227
 - Renaming a share 184
 - Renaming a storage enclosure 332
 - Replacing a volume in a pool 110
 - Replica 420
 - Replicated datasets 439
 - Replicated pool 109
 - Replicated share 441
 - Replicated snapshots 441
 - Replication
 - compression settings 438
 - encryption settings 438
 - network settings 436
 - Replication conflict 457-458, 462
 - Replication schedule
 - configuring 428
 - disabling 434
 - Modifying 433
 - Reports 507
 - Configuring settings 508
 - Deleting 516
 - Emailing 513
 - Exporting 515
 - Generating 509
 - Printing 515

- Types 507
 - Requirements and guidelines for implementing LACP 320
 - Reserved space 125, 137
 - Resetting RAID configuration 331
 - Resilvering operation 119, 470
 - Resolution of screen 352
 - Resource Group 102
 - Restarting cluster nodes 306
 - Restarting the NST after power failure 337
 - Restore previous versions 204
 - Reverse Lookup Zone 387
 - Revoking Pool Administrator access using the Manage Users and Groups panel 88
 - Revoking Site Administrator access using the Manage Users and Groups panel 84
 - Role-based administration in Unity 66
 - Rollback function 202-203, 256, 567
 - Run a command
 - nstusermaps 549
- S**
- Saving events 520, 526
 - Scaling the interface to the screen resolution 352
 - Scheduled automatic updates 421
 - Scheduled replication 420
 - Screen resolution 352
 - Scrub schedule for a replica 435
 - Scrubbing a pool
 - manual 106
 - scheduling 106
 - Searching for a snapshot 196, 251
 - Searching for a specific event 525
 - Secondary network interface 314
 - secondary site 442, 450-451, 455
 - Adding 357
 - definition of 420
 - offline replication 442
 - Promoting the remote system 454
 - Security and Permissions 74, 281
 - Security and Permissions menu 62
 - Selecting alternate primary/secondary domain controllers 386
 - Selecting datasets to replicate 429
 - Send critical notification when space usage reaches 141
 - Server time zone 40
 - servicePrincipalName 375
 - Set the Subnet Mask, Default Gateway, and DNS on all externally-attached Nexsan storage systems 309
 - setip 316
 - Setting
 - quota 149, 154, 508, 574
 - reservation 126, 137, 219
 - Setting a CHAP user for mgmt target 259
 - Setting a schedule for automatic snapshots 197, 252
 - Setting a scrub schedule for a replica 435
 - Setting auto-deletion settings for LUN snapshots 258
 - Setting auto-deletion settings for share snapshots 204
 - Setting Pool Administrator access 85
 - Setting Site Administrator access 82
 - Setting up a secondary network interface 314
 - Setting up asynchronous replication 424
 - Setting up SNMP notification 537
 - Setting up synchronous data replication for a storage pool 466
 - Settings tab, snapshots 197, 251
 - Share
 - adding 123
 - deleting a replication conflict 462
 - Deleting snapshots 205
 - disabling browsing for a difference share 461
 - Disabling data sharing for a share 135
 - enabling browsing for a difference share 460
 - Enabling the Access Time mode 142
 - Managing snapshots 194
 - mapping a CIFS share to a drive 175
 - replication conflict 457
 - Rollback function 567
 - point-in-time snapshot 202, 256
 - using VSS 203
 - searching for a snapshot 196, 251
 - Setting a schedule for automatic snapshots 197, 252
 - setting space usage 139
 - Snapshots Properties panel 194
 - Settings tab 197
 - Snapshots tab 194, 249
 - Sorting the list of snapshots 195, 250
 - Stopping snapshot browsing 201
 - viewing a replication conflict 458
 - viewing mount points 186
 - viewing permissions 79
 - Share-level refresh 352
 - Share compression 141
 - Share I/O 494
 - Share name and space usage 124
 - Share Permissions tab 80
 - Shares
 - access permissions 170
 - adding 168
 - disabling data sharing 183

- name 168
- Renaming 184
- Sharing method
 - FTP 405
 - modifying 136
- Shutting down cluster nodes 307
- Shutting down Unity storage
 - enclosures 335
- Site-level access rights 67
- Site-level CHAP authentication 281, 286
- Site-level refresh 352
- Site-level troubleshooting 401
- Site Administrator access 66-67, 82
- Site auto-refresh interval 351
- Site failover vs. pool failover 451
- Site name 348
- Site name and time zone 40
- Size of block 218
- SMTP 22, 31, 116, 139, 311, 513, 520, 527, 530, 532, 534-535, 557
- SMTP server settings 535
- Snapshot
 - access rights 70
 - Auto-deletion settings 112
 - browsing a LUN snapshot 254
 - browsing a share snapshot 199
 - filtering 195, 250
 - LUNs 245
 - Manually deleting LUN snapshots 257
 - Manually deleting share snapshots 205
 - Properties panel
- Settings tab 197, 251
- Snapshots tab 194, 249
 - Rollback function 567
- point-in-time snapshot 202, 256
- using VSS 203
 - searching for 196, 251
 - Setting a schedule for automatic snapshots 197, 252
 - Setting auto-deletion settings 204, 258
 - sorting 195, 250
 - Stopping LUN snapshot browsing 256
 - Stopping share snapshot browsing 201
 - Taking a snapshot 198, 253
 - Taking performance snapshots 502
- Snapshots
 - Properties panel 194
 - scheduling 127, 220
 - viewing replicated snapshots 439
- SNMP 22, 31, 61, 73, 311, 530-531, 533, 535, 537, 557
- SNMP notification 537
 - access rights 73
- Software upgrades 364
- Sorting the list of snapshots 195, 250
- Source storage system 420
- Space usage for a file system
 - viewing 149
- Space usage for a LUN 115, 214, 218, 228, 232
- Space usage for a share 125, 137
 - Modifying 137
 - notification thresholds 139
- Space usage notification thresholds 115
- Space usage threshold violations 533
- Specific domain controller 383
- SQL Server 218
- SSH 407
- Starting asynchronous replication 424
- Starting the Performance Monitor 500
- Starting Unity 337
- Static IP addresses 46
- Stopping a recording 502
- Stopping LUN snapshot browsing 256
- Stopping share snapshot browsing 201
- Storage allocation 328
- Storage by platform 27
- Storage configuration 43-44
- Storage Configurator 329
- Storage enclosures 99
 - remove 335
 - renaming 332
 - shutting down E-Series 335
- Storage on Remote Ssystem 426
- Storage on Remote System 110
- Storage pool
 - access rights 68
 - Adding volumes to a pool replica 109
 - Adding volumes to the primary pool 109
 - compression 113
 - creating a storage pool 100
 - deleting 120
 - Disabling a storage pool's replication schedule 434
 - Manual scrub 106
 - Modifying a storage pool's replication schedule 433
 - Moving a pool 116
 - Performing a failover of a storage pool 453
 - Promoting a storage pool's replica 454
 - Promoting the mirrored storage pool 470
 - property settings order of precedence 99
 - Removing asynchronous data replication for a storage pool 463
 - Replacing a volume 110
 - replica 420
 - Setting the scrub schedule 106
 - Space usage notification thresholds 115
- Suggest volume allocation 469

Supported features by platform 26
 Supported storage by platform 27
 Synchronous replication
 Add mirror volumes 468
 before you begin 466
 configuration results 470
 features 465
 promoting the mirrored pool 470
 removing 471
 setting up 466
 usage 466
 verifying settings 469
 System events 518
 System maintenance 451
 System notifications 533
 System Preferences 62

T

Taking a snapshot 198, 253
 Target CHAP authentication 287
 Target storage system 420
 Tasks and operations when a cluster node
 is down 302
 Tasks in progress panel 63
 Terminate asynchronous replication 463
 Testing Jumbo Frames 319
 Testing on non-production storage
 systems 466
 Thin Provisioning 214
 Time server 348
 Time Server 398
 Time server support 371
 Time zone 40
 Tools menu 61
 Transfer of system logs 406
 Trap destinations 538
 Tree view 52
 Tree view icon 475
 Troubleshooting site-level warnings and
 errors 401
 Types of reports 507
 Typical cluster implementation 300

U

UID 91, 179, 564
 Unallocated disk 291
 Unallocated disks 268
 UNAVAILABLE 119
 Understanding access rights 66
 Understanding link aggregation 322
 Understanding link layers 313
 Understanding the CallHome feature 406
 Unity authentication 66, 400, 573
 Adding a group 91

 Adding a user account 90
 Adding a user to a group 92
 Changing a user's password 94
 Changing the nxadmin password 95
 Deleting a user or a group 94
 Removing a user from a group 93
 Unity Authentication 398
 Unity Preferences 62
 Unity roles and access rights 67
 Unity UI
 Global toolbar 61
 node context menu 59
 tasks in progress panel 63
 tree view and nodes 52
 Unity, shutting down 335
 UNIX Access Control Lists (ACLs) 188
 Unjoining a domain 396
 Unlimited quota 125, 137
 Unshare 183
 Upgrading software 364
 USB 364, 442, 445
 offline replication 443
 Use FASTier device(s) for read 430
 Use FASTier device(s) for write 431
 Used Space report 507
 User authentication modes 66
 User authentication settings 371
 User Quota(s)-Critical Consumption
 report 508
 User Quota(s)-Normal Consumption
 report 508
 User Quota(s)-Space Consumption by User
 report 508
 userAccountControl 375
 useradd 178
 userPrincipalName 375
 Users and Groups permissions 66
 Users and Groups window 75
 Using an NFS version 3 (NFSv3) client to
 access an NFS share 178
 Using an NFS version 4 (NFSv4) client to
 access an NFS share 179

V

VAAI plug-in 228
 Vault Protection Module
 status 404
 Verbose logging 529
 Verifying
 settings 104, 110, 131, 163, 171, 224,
 330, 431, 469
 Verifying configuration settings 46
 Video Streaming 218
 View Events 61
 Viewing
 Events 61, 401, 407, 486, 489, 518,

- 520, 527, 529
- Viewing a recording 504
- Viewing a replication conflict 458
- Viewing APAL status 403
- Viewing cluster health status 300
- Viewing cluster license status 300
- Viewing controller information 300
- Viewing events 518
- Viewing file system usage
 - file system 149
- Viewing group members 81
- Viewing group memberships 80
- Viewing mount points 186
- Viewing pool errors 118
- Viewing replicated datasets 439
- Viewing replicated snapshots 441
- Viewing share permissions 79
- Viewing snapshots 439
- Viewing space usage
 - LUN 115, 232
- Viewing the contents of a .diff file 462
- Viewing user or group access rights 79
- Viewing Vault Protection Module status 404
- Virtual volume size 219
- VMWare VAAI hardware acceleration 228
- Volume mixing 99
- Volume replacement 110
- Volume Shadow Copy Service 203, 248
- VSS Hardware Provider 25, 246, 248, 279
- vStorage APIs for Array Integration 228, 574

W

- Warning 140
- Warning event 521, 523
 - pool 116
- When a cluster node is down 302
- Windows 218
- Windows-based initiator 290
- Windows Access Control Lists (ACLs) 188
- Workstation used to connect to the Internet 416

Z

- Zero data loss and downtime 465



Nexsan Headquarters

325 E. Hillcrest Drive, Suite #150
Thousand Oaks, CA 91360
United States of America

Nexsan Shipping

302 Enterprise Street , Suite A
Escondido, CA 92029
United States of America

Nexsan Unity Documents & Downloads page:

https://helper.nexsansupport.com/unt_support

Worldwide Web

www.nexsan.com

Copyright © 2010—2019 Nexsan Technologies, Inc.. All Rights Reserved.

Nexsan® is a trademark or registered trademark of Nexsan Technologies, Inc..

The Nexsan logo is a registered trademark of Nexsan Technologies, Inc..

All other trademarks and registered trademarks are the property of their respective owners.

Document Reference: 20190916PM034024

Nexsan Canada

1405 Trans Canada Highway, Suite 300
Dorval, QC H9P 2V9
Canada

Nexsan UK

Units 33–35, Parker Centre, Mansfield Road
Derby, DE21 4SZ
United Kingdom

Nexsan Unity support:

https://helper.nexsansupport.com/unt_support

This product is protected by one or more of the following patents, and other pending patent applications worldwide:

United States patents US8,191,841, US8,120,922;

United Kingdom patents GB2466535B, GB2467622B, GB2467404B, GB2296798B, GB2297636B