NEXSAN

HYPER-UNIFIED STORAGE

Nexsan Unity

Software User Guide

Firmware version: Unity v. 7.4

NEXSAN | 1287 Anvilwood Avenue | Sunnyvale, CA 94089 USA
Printed November 3, 2026 | www.nexsan.com

Copyright © 2010—2026 Nexsan, Inc. All rights reserved.

Regulatory Compliance

• United States Statement for FCC: Nexsan equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

• Electromagnetic Emissions: FCC Class A, EN 55022 Class A, EN 61000-3-2/-3-3, CISPR 22 Class A, ICES-003, UKCA

• Electromagnetic Immunity: EN 55024/CISPR 24, (EN 61000-4-2, EN 61000-4-3, EN 61000-4-4, EN 61000-4-5, EN 61000-4-6, EN 61000-4-8, EN 61000-4-11)

• Safety: CE , CSA/EN/IEC/UL 60950-1 Compliant, UL or CSA Listed (USA and Canada), CE Marking (Europe)

RoHS: RoHS2 (Global)

• Other international regulatory compliance: VCC (Japan)

• California Best Management Practices Regulations for Perchlorate Materials: This Perchlorate warning applies only to products containing CR (Manganese Dioxide) Lithium coin cells. Perchlorate Material-special handling may apply. See www.dtsc.ca.gov/hazardouswaste/perchlorate.

• Modifications disclaimer: Changes or modifications to Nexsan hardware not expressly approved by Nexsan could void the user's authority to operate the equipment and invalidate any active product warranties.

Trademarks

Nexsan® is a trademark or registered trademark of Nexsan, Inc. The Nexsan logo is a registered trademark of Nexsan, 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

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

Table of Contents

About this document ..... **xiii**

Audience xiii
Conventions xiii
Contacting Nexsan xiii
Notes, Tips, Cautions, and Warnings xiv
Related documentation xiv
Safety notices xiv

Chapter 1: Introducing Nexsan Unity **17**

New features and enhancements 18
Other important Unity features 22
Finding Unity features 26
The Dashboard panel 26
Unity wizards 27
Using the navigation bar and main menus 28
The main menus 28
The System menu 29
The Storage menu 30
The Data Protection menu 31
The Help menu 31
Unity panels and panel menus 32
Systems panels and menus 33
Unity Systems panels 33
Cluster Settings panels 34
Host Connectivity panels 34
User Management panels 35
Notifications panel 35
Storage panels and menus 35
Storage Systems panels 35
Storage Pools panels 36
File Systems panels 37
LUNs panels 38
iSCSI Targets panels 38
Object Store properties 39
Data Protection panels and menus 40
Active Archive panels 40

Replications panels ... 40
Snapshots panel ... 41
Cloud Connector panel ... 41
Concepts and terminology ... 42
Distributed primary storage ... 42
Sharing methods and data protection ... 42
Understanding multi-site implementation ... 46
Multi-site implementation characteristics ... 46
Multi-site implementation limitations ... 48
Typical Unity Storage System deployments ... 49
UNITY NV6000 deployment ... 49
UNITY NV10000 deployment ... 51
UNITY NV12000 deployment ... 52

Chapter 2: Getting started ... 55

Setting up the Unity Storage System ... 56
Starting the Unity System Configuration wizard ... 56
Step 1: Configuring Unity System properties ... 56
Step 2: Configuring network settings ... 58
Step 3: Configuring IPMI settings ... 61
Step 4: Allocating storage ... 62
Step 5: Verifying configuration settings ... 64
Step 6: Applying configuration settings ... 64
Starting Unity ... 65
Browser support ... 65
Logging on to Unity ... 66

Chapter 3: Users and access rights ... 69

User authentication modes ... 70
Administrator and user permissions ... 70
Managing Unity user and group access permissions ... 72
User Authentication panel ... 73
Opening the Manage Users and Groups panel ... 75
Adding a user account ... 76
Adding a group ... 78
Managing group membership ... 79
Deleting a user or a group ... 80
Changing a user password ... 80
Changing the nxadmin password ... 81
Configuring and managing CHAP authentication ... 82
Creating CHAP users ... 83
Changing a CHAP user secret ... 85
Setting CHAP authentication for a target ... 86
Deleting a CHAP user ... 87
Managing permissions for CIFS shares ... 88

Chapter 4: Storage pools ... 89

Adding a storage pool ... 90
Before you begin ... 90
Mixing volumes with different RAID levels ... 92

Property settings order of precedence ... 93
Scrubbing a storage pool ... 94
Performing a manual pool scrub ... 95
Modifying the scrub schedule for a storage pool ... 96
Adding volumes to a storage pool ... 98
Adding volumes to a replicated storage pool ... 99
Replacing a volume in a storage pool ... 99
Modifying storage pool snapshot auto-deletion ... 100
Configuring data compression on a storage pool ... 102
Configuring access time on a storage pool ... 103
Viewing space usage information for storage pools ... 105
Setting space usage notification thresholds for a storage pool ... 105
Changing a pool resource group ... 107
Managing FASTier cache devices ... 108
Viewing and clearing storage pool errors ... 110
Deleting a storage pool ... 114

Chapter 5: File Systems ... 115

Data management functions on file systems ... 116
Adding a file system ... 117
Before you begin ... 117
Step 1: Setting the file system name and storage pool ... 118
Step 2: Configuring space settings ... 119
Step 3: Configuring the access protocol ... 122
Step 4: Configuring Data Protection ... 124
Step 5: Configuring Active Archive ... 126
Step 6: Verifying settings ... 128
Step 7: Viewing results ... 129
Viewing file system space usage information ... 130
Modifying file system properties ... 132
Renaming a file system ... 133
Disabling data sharing for a file system ... 134
Modifying file system space configuration settings ... 136
Modifying file system record size ... 138
Setting space usage notification thresholds for file systems ... 140
Enabling or disabling data compression on a file system ... 142
Enabling the Access Time mode on a file system ... 144
Modifying file system sharing methods ... 145
Setting IP restrictions ... 147
Editing or removing IP restrictions ... 150
Share IP permission precedence ... 151
Deleting a file system ... 153
Managing home directories ... 154
Creating file systems for home directories ... 155
Step 1: Setting the name and storage pool ... 155
Step 2: Configuring space settings ... 157
Step 3: Assigning user groups ... 160
Step 4: Assigning administrators ... 161
Step 5: Selecting an access protocol ... 162
Step 6: Enabling data protection ... 164
Step 7: Configuring your archive settings ... 165
Verifying settings ... 167

Viewing results ... 168
Managing group assignments ... 169
Performing file system-level tasks for home directories ... 170
Example file system for home directories ... 172
Managing CIFS shares ... 173
About Managing CIFS shares ... 173
Adding CIFS shares ... 174
Step 1: Setting the CIFS share location and name ... 175
Step 2: Assigning access permissions to a CIFS share ... 176
Step 3: Verifying CIFS share settings ... 178
Step 4: Viewing results ... 179
Accessing CIFS shares ... 180
Accessing a CIFS share from Windows ... 181
Accessing an NFS file system from UNIX/Linux ... 184
Using an NFS version 3 (NFSv3) client to access an NFS share with Microsoft Active Directory ... 185
Using an NFS version 4 (NFSv4) client to access an NFS share ... 186
Renaming a CIFS share ... 189
Moving a CIFS share ... 190
Unsharing a CIFS share ... 192
Viewing file system mount point information ... 192
Managing access permissions to file systems ... 194
Understanding access permissions for file systems ... 194
Read-only and read/write anonymous access ... 194
Windows and UNIX Access Control Lists (ACLs) ... 195
Managing file system- or CIFS share-level access permissions ... 197
Enabling ZFS Encryption for file systems ... 199
Enable ZFS encryption on a file system ... 199
Export encryption key for a file system ... 200
Import encryption key for a file system ... 201
Change encryption key for a file system ... 202
Managing snapshots for file systems ... 204
Viewing file system snapshots ... 204
Sorting the list of snapshots ... 205
Filtering snapshots in the grid ... 205
Searching for a specific snapshot in the grid ... 207
Using the file systems snapshots panel ... 207
Using the file systems snapshot settings panel ... 208
Setting a schedule for automatic file system snapshots ... 208
Taking a manual file system snapshot ... 211
Browsing a file system snapshot ... 212
Stopping file system snapshot browsing ... 214
Rolling back to a snapshot ... 215
Configuring auto-deletion settings for file system snapshots ... 217
Manually deleting file system snapshots ... 218
Immutable snapshots for file systems ... 220
Taking an immutable snapshot for a file system ... 221
Changing an existing file system snapshot to make it immutable ... 222
Extending the retention date of an immutable snapshot ... 224
Scheduling immutable snapshots for File Systems ... 225

Chapter 6: LUNs **231**

Data management functions on LUNs 232
Guidelines for adding and managing LUNs 232
Understanding disk space consumption 233
Space comparison for Thin vs. Thick LUNs 233
Creating a LUN 236
Step 1: Setting the LUN name and block size 237
Step 2: Space configuration settings for the LUN 239
Step 3: Enabling software encryption, data replication and snapshot scheduling 241
Step 4: LUN masking 243
Step 5: Create a new LUN mask 244
Step 6: Verifying settings 245
Step 7: Viewing progress 247
Viewing LUNs 248
Renaming a LUN 250
Configuring data compression on a LUN 251
Disabling Read caching 252
Configuring client-side (host) settings for a LUN 254
Enabling VMware VAAI hardware acceleration for a LUN 254
Enabling client-side space usage notifications for a LUN 254
Changing LUN space configuration 256
Deleting a LUN 257
Using Windows VSS 258
Adding a CHAP user to the Management target 258
Installing the VSS Hardware Provider 258
Enabling the Microsoft VSS client for LUNs 262
Discovering your LUNs with the Windows iSCSI Initiator 263
Configuring the LUNs in Disk Management 267
Creating a VSS snapshot 269
Browsing a VSS snapshot 273
Viewing VSS client information 276
Rolling back data to a VSS snapshot 276
Deleting a VSS snapshot 278
Enabling ZFS Encryption for LUNs 280
Enable ZFS encryption on a LUN 280
Export encryption key for a LUN 281
Import encryption key for a LUN 282
Change encryption key for a LUN 283
Managing snapshots for LUNs 285
Introduction to snapshots 286
Snapshot concepts and terminology 287
Understanding LUN snapshots 289
Snapshots browsing 289
Rollback function 289
Microsoft Volume Shadow Copy Service 289
Browsing replicated datasets and snapshots 290
Using Unity and VSS to manage LUN snapshots 290
Viewing LUN snapshots 291
LUNs Snapshots panel 293
Sorting the list of snapshots 294
Searching for a specific snapshot in the grid 294
Filtering snapshots in the grid 295

Taking a manual LUN snapshot ... 296
Browsing a LUN snapshot ... 297
Rolling back data in a LUN to a snapshot ... 300
Deleting LUN snapshots manually ... 301
Managing LUN Snapshot scheduling ... 302
Setting a schedule for automatic LUN snapshots ... 302
Immutable snapshots for LUNs ... 304
Taking an immutable LUN snapshot ... 305
Making an existing LUN snapshot immutable ... 307
Extending the retention date of an immutable LUN snapshot ... 309
Scheduling immutable snapshots for LUNs ... 311
Managing iSCSI targets ... 315
Adding an iSCSI target ... 315
Step 1: Setting iSCSI target properties ... 316
Step 2: Verifying settings ... 317
Step 3: Viewing results ... 318
Connecting to an iSCSI LUN from Windows ... 318
Adding an iSNS server ... 320
Removing an iSNS server ... 321
Host connectivity: LUN masks and Initiator Groups ... 322
About LUN masks ... 323
Initiator Groups ... 323
Viewing LUN masking information ... 323
Creating a LUN mask ... 324
Editing a LUN mask ... 326
Deleting a LUN mask ... 329
Viewing initiator group information ... 330
Adding an initiator group ... 330
Editing an initiator Group ... 331
Deleting an initiator group ... 333

Chapter 7: Object Stores ... 335

Creating an object store ... 336
Viewing object store system information ... 342
Enabling or disabling TLS on the object store ... 343
Increasing storage capacity for object stores ... 344
Starting the service for an object store ... 346
Stopping the service for an object store ... 347
Deleting an object store ... 347
Resetting object store keys ... 349
Accessing the NexObject Web client ... 349
Creating a data bucket using the Web client ... 353
Adding data to an object store bucket ... 355
Creating an object store S3 Table Bucket ... 357
Creating an object store user ... 360
Managing object store users ... 362
Creating and managing object store groups ... 366
Creating and managing object store service accounts ... 369
Creating and managing object store policies ... 371

Chapter 8: Clustering **375**
Clustering overview 376
Cluster components and terminology 377
Unity Clustering 380
Load balancing with Active-Active Clustering 381
Understanding heartbeats 381
Transient and persistent reservations with disk heartbeats 381
Transient reservation 382
Persistent reservation 382
Unity NV Series Clustering 385
Example of data access in a typical Unity cluster implementation 386
Viewing cluster status 386
Unavailable tasks when a controller is down 387
Moving cluster resources 387
Restarting the cluster or individual controller nodes 389
Shutting down the cluster or individual controller nodes 391
Modifying IP configuration settings 393
Understanding IP address requirements 394
Understanding network interfaces 395
Understanding link layers 396
Setting or modifying IPMI settings 398
Accessing the IPMI Web-based interface 398
Enabling jumbo frames using Unity 399
Enabling jumbo frames using the nxadmin CLI 400
Enabling LACP using the Unity Web interface 400
Requirements and guidelines for implementing LACP 401
Understanding link aggregation 402
Enabling LACP using the nxadmin CLI 402
Configuring TCP flow control 403

Chapter 9: Storage management **405**
Allocating new storage to the Unity System 406
Step 1: Discovering new storage and configuring RAID settings 407
Step 2: Verifying settings 410
Step 3: Viewing results 411
Modifying IP settings for a Nexsan E-Series/BEAST Storage System 412
Renaming a Unity Storage System 413
Adding new drives to a Unity Storage System 414
Resetting the RAID configuration for storage 416
Removing a Unity Storage System 417
Shutting down a Unity Storage System 419
Powering on Unity controllers 421
Shutting down a Nexsan E-Series Storage System 423
Powering on Unity and E-Series Storage Systems 424
Using Self-Encrypting Drives (SEDs) 425
Disabling SED encryption 427

Chapter 10: Using Active Archive **429**
Connecting to an Assureon Server 429
Managing Active Archive settings for file systems 431

Viewing archived file systems ... 434
Performing manual archiving to Assureon ... 435

Chapter 11: Unity System-level tasks ... 437

Changing the Unity Storage System name ... 438
Modifying the time server used ... 438
Setting NDMP configuration options ... 439
Modifying User Interface preferences ... 440
Modifying the auto-refresh interval ... 440
Modifying date and time formats ... 441
Changing the Unity System time zone ... 442
Manually refreshing Unity Storage Systems ... 442
Connecting to a remote Unity System ... 442
Disconnecting a remote Unity Storage System ... 443
Disconnecting Unity Systems in a multi-system implementation ... 444
Updating Unity ... 446
Upgrading to the latest firmware ... 447
Adding new features ... 449
Upgrading the cluster license ... 451
Modifying authentication settings ... 452
About Joining an Active Directory Domain ... 452
Microsoft Active Directory domain requirements ... 452
Creating computer objects on the Active Directory server ... 453
Joining a Microsoft Active Directory domain ... 458
Delegating control to a non-Administrator user account ... 460
Enabling Kerberos for accessing a CIFS file system ... 463
Adding a Reverse Lookup Zone in DNS Manager ... 463
Adding a host for each Resource Controller in DNS Manager ... 467
Configuring the host in Active Directory ... 468
Managing domain controllers ... 469
Discovering new domain controllers ... 470
Selecting alternate primary or secondary domain controllers ... 471
Unjoining Unity from an Active Directory domain ... 472
Connecting to an LDAP Directory Service ... 473
Reverting to Unity Authentication ... 475
Troubleshooting Unity System-level warning and error conditions ... 477
Configuring NFS settings ... 479
Viewing APAL status ... 481
Viewing NVDIMM status ... 481
Enabling FTP support ... 482
Using the CallHome feature ... 484
How CallHome is triggered ... 484
Event-driven CallHome ... 485
Diagnostics-based CallHome ... 488
Enabling CallHome log collection settings ... 491
Enabling SSH remote connectivity for CallHome ... 492
Enabling Internet connectivity ... 493
Connecting to the Internet using a Direct LAN link ... 494
Connecting to the Internet using HTTP ... 495
Connecting to the Internet using a workstation ... 496

Chapter 12: Data replication **499**

Data replication concepts and terminology 500
Asynchronous data replication 501
Usage implementations 501
Before you begin 502
Asynchronous data replication features 504
Setting up asynchronous data replication 506
Adding a remote Unity System and assigning space 506
Configuring a replication schedule 509
Selecting datasets to replicate 510
Allocating FASTier cache devices to replication 513
Verifying settings 514
Viewing results 515
Performing a manual replication 516
Configuring asynchronous replication for a dataset 518
Modifying asynchronous replication properties and configuration settings 520
Modifying a storage pool's replication schedule 520
Disabling a storage pool replication schedule 521
Failing over to a remote Unity Storage System for disaster recovery 523
Failover vs. promote 523
Unity System failover vs. pool failover 524
Performing a failover of the entire Unity Storage System 525
Configuring asynchronous replication settings 528
Configuring network settings for asynchronous replication 528
Configuring compression settings for asynchronous replication 530
Configuring encryption settings for asynchronous replication 530
Removing asynchronous data replication for a storage pool 532
Enabling browsing of a replicated file system snapshot 534
Configuring the network type for data replication 536
Synchronous data replication 538
Synchronous data replication features 538
Usage implementations 539
Cloud Connector 539
Adding cloud storage configurations 539
Editing cloud storage configuration 542
Deleting cloud storage configuration 543
Transferring data manually to cloud storage 544
Scheduling automatic data transfer to cloud storage 546

Chapter 13: System monitoring **549**

Viewing and recording performance metrics 550
Metric selection 550
Site 550
Pool 550
Storage device 550
File system 550
LUN 551
FASTier 551
Starting the performance monitor 551
Filtering live performance metrics 553
Viewing historical performance data 554

Changing the duration to keep sampling data ... 556

Chapter 14: Event logging and notification ... 557

Viewing events ... 558
Configuring event viewer logging options ... 559
Collecting and emailing event logs ... 560
Clearing event logs ... 562
Setting up email notification for events ... 563
Setting up email notification for system events ... 563
Setting up system notifications ... 565
Configuring SMTP server settings for the Unity System ... 566
Setting up SNMP notification ... 567

Chapter 15: Operating in mixed mode environments ... 571

Understanding how changing the mode of a file in NFS affects permission settings in CIFS ... 572
Understanding how using chmod in NFS creates allow and deny entries in CIFS ACLs ... 573
Deny access control entry added for owner and group ... 573
Deny access control entry added for group only ... 573
Examples of CIFS permissions after applying chmod in NFS ... 575
Mapping UNIX accounts on Unity to corresponding Microsoft Active Directory accounts ... 580
nstusermaps ... 581

Appendix A: Unity nxadmin account access ... 583

permissions Terminology ... 589

Index ... 613

About this document

This *Software User Guide* provides information and detailed procedures for configuring and managing your Unity Storage Systems using Nexsan Unity. This guide assumes that you have installed Unity by following the steps provided in the *Nexsan Unity Quick Start Guide* for the corresponding Unity Storage System.

Audience

This guide has been prepared for the following audience:

- IT system administrators
- Engineers
- Technicians
- Any qualified Unity administrator.

Conventions

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

Convention	Description
underline blue	Cross-references, 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).
italics	System messages and non-interactive items in the graphical user interface (GUI) References to Software User Guides
▶ (arrow icon)	A visual cue to indicate an action carried out by the user to accomplish a given task, or to draw attention to key information. Also used to indicate the beginning of, a step within, or what's next after a procedure.

Contacting Nexsan

For questions about Nexsan products, please visit the Nexsan support webpage, which includes service programs and warranty information, support contacts by geography, and documents and downloads by product line

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.

Website:
www.nexsan.com

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.

Related documentation

The following Nexsan product manuals contain related information:

- Nexsan Unity Online Help
- *NexsanUnity Network Configuration Guide*
- *NexsanUnityHardware Maintenance Guide, Unity Next Generation*
- *NexsanUnity Software User Guide*
- *NexsanUnity nxadmin Command-line Interface Reference Guide*
- *NexsanUnity nxcmd Command-line Interface Reference Guide*
- *NexsanUnity NFS Interoperability*
- *NexsanUnity VMware Best Practices Guide*
- *NexsanUnity Networking Best Practices Guide*
- *NexsanUnity Performance Best Practices Guide*
- *NexsanUnity 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 10º to 35º C (50º to 95º 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 Nexsan Unity

Nexsan Unity provides the advantage of adaptability, performance, and reliability to drive ROI while satisfying your industry's unique storage requirements. Unity's comprehensive protocol support and integration capabilities streamline operations and reduce complexity.

Unity v. 7.4 introduces the CloudConnector feature in the GUI to simplify setup between cloud systems and cloud targets, as well as immutable snapshot sheduling in the GUI for efficient creation and management of schedules. NFS capabilities are expanded with added support for protocol versions 4.1 and 4.2, as well as Kerberos authentication. The newlly created Unity NexObject Web client extends object store management and supports multiple instances within the same storage pool. Further additions include special devices for deduplication, consolidated workflow in multi-site management, and delegatd site adminstrator roles. For details, see New features and enhancements on the next page.

This version introduces the UNITY NV12000 to further support the NV-Series of unified storage, as well as the U2F226 Expansionfor an all-flash SSD configuration supported by the NVMe high-speed interface and communication protocol.

This guide provides procedures, illustrations, and guidelines to help you set up and manage Unity Storage Systems, Unity Storage Expansions, and Nexsan E-Series Storage Systems attached to Unity.

New features and enhancements

Here is an overview of the new features and enhancements in the most recent releases:

Features and enhancements	Description
Unity NV12000™ product release	The Unity NV12000™ is a 2U all-flash, 24-bay hot-swap dual-port NVMe drive, PCIe 5.0 modular system. The storage architecture features dual-node redundancy, shared storage access, fault tolerance, and high availability with low latency for peak performance, demanding workloads, and AI applications.
Unity U2F226™ JBOF support	Added support for the U2F226™ expansion, for scalable high-performance NVMe capacity.
Cloud connector in the GUI	Cloud Connector configuration and operation are now available in the Unity graphical user interface, simplifying setup and management of synchronization between Unity file systems and supported cloud targets.
Immutable snapshot scheduling in Unity GUI	Administrators can now create and manage schedules for immutable file-system and LUN snapshots directly from the Unity graphical user interface set by the user.
Kerberos support for NFS	Added Kerberos authentication support for NFS to strengthen client authentication and secure access to exported file systems. Note: The Unity system needs to join with Active Directory to enable this feature.
Special devices for deduplication	Deduplication now supports allocation of metadata to special devices, enabling administrators to optimize deduplication performance and storage placement.
NFS 4.1 and 4.2 support	Added support for NFS protocol versions 4.1 and 4.2, expanding client interoperability and access to newer NFS capabilities.
Multi-site management	Unity systems across multiple sites can now be managed through a consolidated workflow, improving visibility and administration of distributed environments.
Site administrator roles	Local and Active Directory users can now be assigned as site administrators, enabling delegated administration with site-level responsibilities.
Multiple NexObject instances	Unity now supports multiple object store instances within the same storage pool, allowing administrators to separate workloads, namespaces, and access while sharing pool capacity.

Features and enhancements	Description
Resolved issues	• Resolved a potential system crash that could occur when a custom CPU optimization was enabled. • Resolved an issue where the dashboard might not show a pool as full when used space and snapshot consumption together reached 100 percent. • The PCI root device ID could potentially change after a reboot, preventing internal components from recognizing front-bay storage. This has been corrected. • Corrected an issue that could cause the dashboard to report used space inaccurately for a storage system. • Improved the mechanisms used to join Active Directory and update the domain-controller list so that potentially unresponsive domain controllers are ignored.
Replications setting	The number of concurrent async replications permitted on a controller can be set by the user.
Resolved issues	• An absent (or unutilized) SAS card in a PCIe slot no longer produces a SAS layer error in Unity. • Prevention of storage pools from entering a suspended state during SAS HBA IOC resets.
LUN-level UNMAP	Unity can control the UNMAP setting at the LUN level, independently of VAAI.
Object store erasure coding	Unity adds an option to support erasure coding on an object store. By default it is off. When activated, the user can choose the number of datasets for erasure coding parity via the GUI.
Resolved issues	• A file system owner not set to root set up permissions easily. • Logging in to the console as nxadmin works consistently. • Running peer command as nxadmin works consistently. • Maximum LUN size value no longer gets overwritten during an upgrade. • A dataset with software encryption enabled displays the replication button. • Snapshots can be taken on a datasets that have no schedule enabled.
Multiple object store support	Enhanced from single, Unity can now create multiple object store instances, allowing administrators to better separate/segregate data and the access to it.

Features and enhancements	Description
Deduplication	Unity's new deduplication feature can save considerable disk space, especially when many files contain identical or very similar data blocks. Built with flexibility and ease of use, it can be enabled at the storage pool level as well as for individual file systems and LUNs.
Improvements for scrub mechanism	• Configuration enhancements in Unity allow for different scrub types that can run on a pool. The three mechanisms include: • Full - scrubs data and metadata • Metadata - scrubs metadata only • Incremental - scrubs the newly allocated blocks since last full scrub • A scrub operation can be paused / resumed / canceled. • Via CLI ONLY, the user can perform a scrub uniquely on the reported blocks with errors. • The scrub and resilvering settings have been adjusted for better performance.
SMB improvements	The SMB module has been improved, allowing the user to control (via CLI) which authentication protocol to use: Kerberos and/or NTLM. Unity enables both options by default, and disables DES/RC4 options by default for security reasons. The user can change the options via CLI by using the SMB service property.
Customer generated certificates	Added support in Unity to install a customer generated certificate for an object store, as well as for Unity GUI access.
Introduction of the U2G424 Expansion	This new Unity expansion hardware includes the following features: • Support for up to 24 drives (HDD or SSD) • Up to 720TB raw capacity in 4U • Dual-port SAS for high availability • Enterprise grade redundant and hot-swappable PSUs, I/O modules and fans

Features and enhancements	Description
Performance and stability improvements	• Unity will now prioritize block allocations from the newly added volumes into a pool. This allows pools that are being expanded with new volumes to continue servicing the write operations without a performance impact. Newly added volumes within the pool will host, over time, the same amount of data as the existing volumes, thereby keeping all volumes balanced. • In some cases, the import of the pools could take longer than expected; this was caused by a delay in synchronizing the content of a cache file between nodes. This has been resolved. • Previously, the quota could not be changed to a smaller number than initially set; this has been resolved by allowing the quota to be changed to a number that is equal to or greater than the reserved space.

Other important Unity features

This table provides a summary of other important Unity 2.x, and 5.x features.

Feature	Description
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 375.
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. To view an example of *All ports / All LUNs* clustering, see Viewing cluster status on page 386.
Configurable RAID	Unity supports RAID levels 5, 6, and 10, and enables 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 enables you to specify the RAID configuration for each externally-connected storage device (Nexsan E18™, Nexsan E48™, Nexsan E60™, or the Nexsan Unity Storage Expansion).

Feature	Description
Data replication	Unity provides intuitive, wizard-based configuration tools to help you set up asynchronous 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 enables 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 enables you to configure off-site data replications separately for each storage pool on the primary Unity. In addition, the asynchronous data replication feature enables 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. For setting asynchronous data replication bandwidth, please refer to the *Nexsan Unity nxcmd Command-line Interface Reference Guide*. With Synchronous data replication, you can mirror data between two Nexsan E-Series 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 E-Series storage system and a target Nexsan E-Series storage system—both of which are connected to Unity via Fibre Channel or SAS. **Note** Configuration of the synchronous data replication feature is currently supported: ● in the Unity HTML5 user interface. ● using the NestOS `nxcmd SyncReplication` commands. Please refer to the *nxcmd Command Line Interface Reference Guide* on the Nexsan.com/support webpage.
Expandable storage	You can expand storage capacity on the Unity Storage System hardware by: ● connecting a Unity Storage Expansion to a Unity Storage System via a SAS add-on card (available for purchase as an optional component).
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.

Feature	Description
Fibre Channel support	You can expose LUNs over Fibre Channel using a unified Fibre Channel target. The Fibre Channel ports are configured as targets. For Fibre Channel support, please contact your Nexsan reseller or sales representative.
File System creation and management	Unity provides an intuitive wizard-based configuration tool, enabling you to create file systems and shares and expose them to CIFS and NFS clients of Unity; it also enables you to allocate storage, manage space usage quotas, and configure user-level access permissions for each share that you create.
LUN creation and management	Unity provides an easy-to-use wizard-based configuration tool for creating iSCSI or Fibre Channel LUNs in storage pools. The wizard-based configuration tool lets you assign each LUN to an iSCSI or Fibre Channel 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. For Fibre Channel LUNs, you associate the LUN to a common, unique Fibre Channel target.
Multi-site management	Unity enables 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 46.
Snapshots	Unity provides continuous data protection with the Snapshots feature, which enables 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.

Feature	Description
Storage pool creation and management	Unity provides an intuitive wizard-based configuration tool, which enables grouping of underlying volumes into storage pools on Unity. Unity also provides pool management tools, such as pool scrubbing and customizable schedules for automatic pool scrubs. For help with promoting or demoting storage pools, please refer to the *Nexsan Unity nxcmd Command-line Interface Reference Guide* on the Nexsan.com/support webpage.
Support for NDMP backup solutions	Unity includes an NDMP plug-in that enables 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 439.
User management and security	You can configure Unity to join a Microsoft Windows Active Directory domain, to connect to an LDAP (Lightweight Directory Access Protocol) Directory service, and to use CHAP authentication. Nexsan Unity provides an intuitive user management tool, which enables configuration of storage pool-level, and file system-level access permissions on Unity. 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. **Note** In Unity v. 7.4, role-based system and pool administrators are not yet supported in the new graphical user interface. You can however configure role-based administration using the nxcmd CLI. See the "Pool" and "Site" sections of the *Nexsan Unity nxcmd Command-line Interface Reference Guide*, available on the Nexsan.com/support webpage.
Volume management	Unity provides an intuitive wizard-based tool enabling 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.

Finding Unity features

Unity's redesigned Web interface presents Unity Storage Systems in task-oriented and informative panels. You'll find the main features to manage your storage systems from these primary menus:

- **The System menu:** Provides access to system administration operations for all connected Unity Storage Systems. Contains controls for clusters, host connectivity, user management, notifications, the user interface, events, troubleshooting, and available updates. See The System menu on page 29
- **The Storage menu:** Provides configuration options for storage blocks or file structures—storage pools, file systems, volumes, LUNs, and iSCSI targets. See The Storage menu on page 30
- **The Data Protection menu:** Configures active archiving, replication, and snapshots. See The Data Protection menu on page 31
- **The Help menu:** Provides links to the Unity Help, Software User Guide, Unity Classic UI, and About Unity window, which provides version information and access to the Unity release notes and Unity License Agreement.

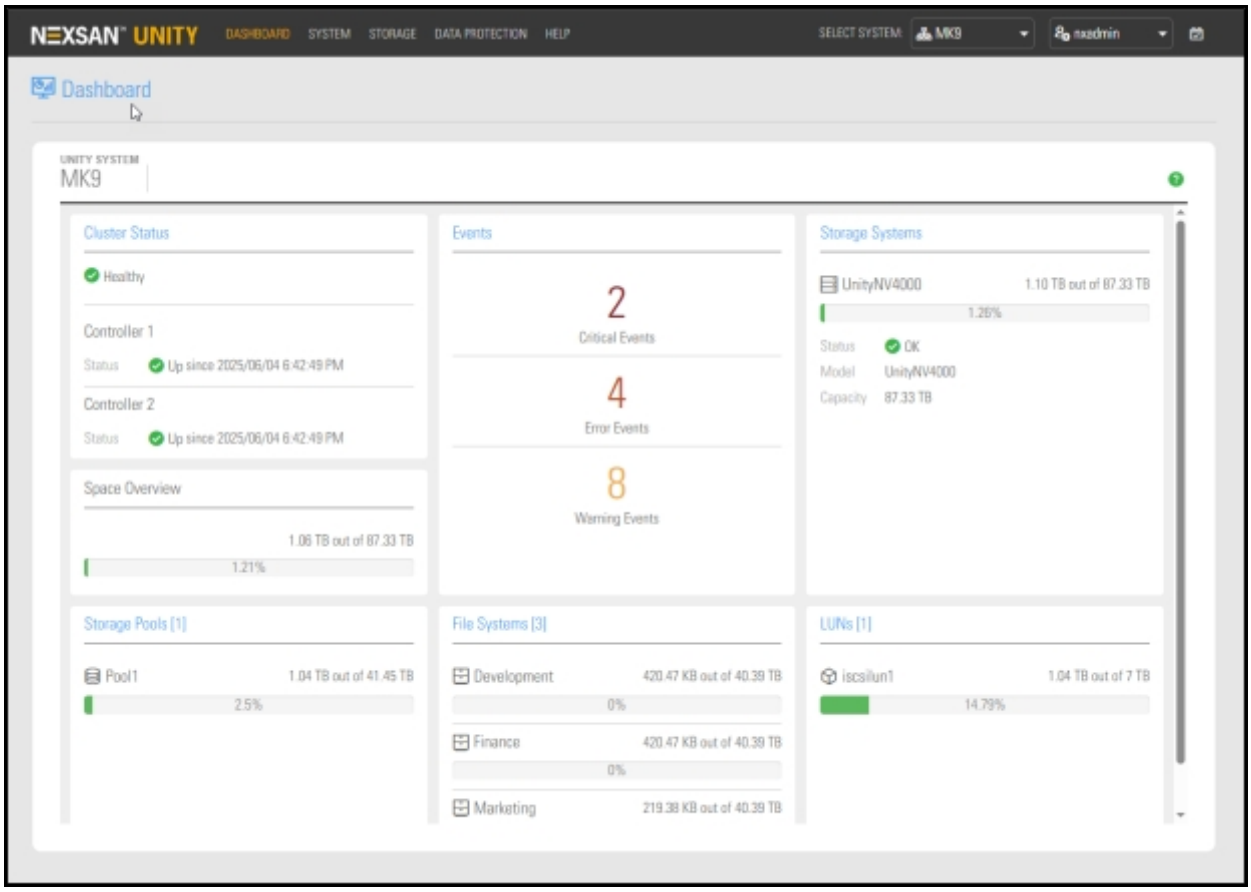
To dig deeper, see

- Unity panels and panel menus on page 32, showing the menu for each Unity panel and links to related documentation.

The Dashboard panel

Unity's dashboard panel displays an overview of the primary and remote Unity Systems. You'll find easy-to-understand information for cluster status, system health, and device and space usage information in graphical and numerical format. Unity's wizards, menus, and property panels provide extensive controls for data configuration.

Figure 1-1: The Dashboard panel



Unity wizards

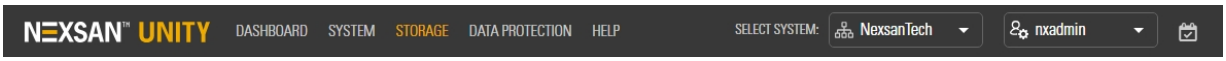
Unity's configuration wizards help to accomplish complex data management tasks, such as creating storage pools, file systems, and setting up data replication. The configuration wizards guide you through these processes, while Unity automatically manages all the disk-level tasks in the background.

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

Using the navigation bar and main menus

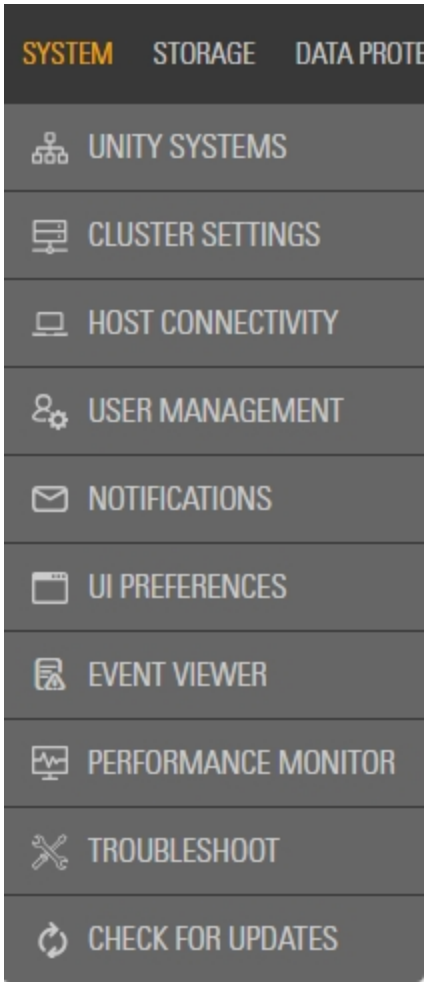
The Unity navigation bar and main menus serve as the access points to Unity functionality.

Use the Unity navigation bar to access the Dashboard, the main menus, and the Unity System selector, login menu, and the task status list.



The main menus

The following table provides basic details about Unity's main menus.



The System menu

Provides access to system administration operations for all connected Unity Storage Systems. The **System menu** provides access to the following panels:

Unity Systems: Provides links to open all connected Unity Storage Systems. Click a link to a **Unity System** to view the **Unity Systems Summary** panel, which displays system information and existing datasets. The Unity Systems panel also includes buttons to connect or disconnect systems and initialize failovers.

Click **Summary** to display the Unity Systems panels.

Cluster Settings: The main panel displays status for the cluster, that is Controller 1 and Controller 2. See Clustering overview on page 376.

Host Connectivity: Provides details about current LUN masks and Initiator Groups. See Host connectivity: LUN masks and Initiator Groups on page 322

User Management: Provides options for setting alternatives to the default Unity user management system: Microsoft Active Directory, LDAP, and CHAP authentication. See Users and access rights on page 69

Notifications: Opens the **Configure Email and SNMP Notification** panel where you configure email and SNMP alerts for the active (local) site, and any remote Unity connected to the site. See Event logging and notification on page 557

UI Preferences: Opens the **UI Preferences > Settings panel**, where you can set the system auto-refresh interval and choose date and time formats. See Modifying User Interface preferences on page 440

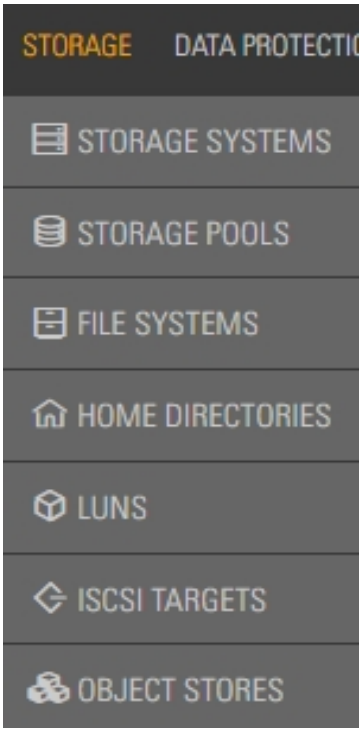
Event Viewer: Provides a sortable and searchable list of Unity System events and event filtering. Viewing events on page 558

Performance Monitor: Displays real-time performance information for Unity. See Starting the performance monitor on page 551

Troubleshoot: Displays current issues identified by Unity and suggested resolution steps.

Check for Updates: Opens the Unity Software Updater, which you can use to update Unity software components. You can also use the Unity Software Updater to update software components on any remote Unity connected to the active (local) Unity system; for more info, see Updating Unity on page 446.

See also Systems panels and menus on page 33



The Storage menu

The **Storage menu** provides access to the following panels:

Storage Systems: The main panel provides links to connected storage systems and storage expansions (storage devices). From the Storage Systems panel, you can also view RAID set (volume) information, rename the storage system, configure and delete RAID sets, and click the menu to open the Volumes panel and view the volumes configured for each storage system. See Storage management on page 405

Storage Pools: Add or remove storage pools, view pool statistics, change resource groups, and scrub or delete pools. From the panel menu, you can access file systems, LUNs, Volumes, Space Usage Alerts, Advanced Settings, Scrub Management, and FASTier caching. See Storage pools on page 89

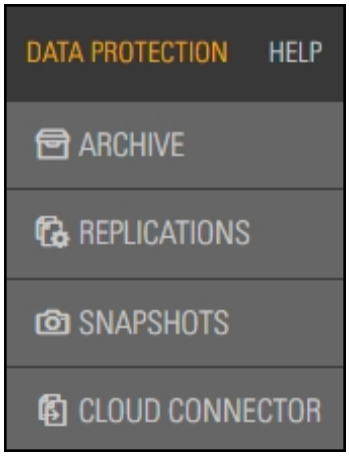
File Systems: The panel menu provides links to file system properties, space configuration, space usage alerts, advanced settings, CIFS shares, Active Archive, snapshots, and snapshot settings. See File Systems on page 115

Home Directories: 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. See Managing home directories on page 154

LUNS: Adds LUNs, shows detailed statistics, and provides options for snapshots and deleting LUNs. The panel menu provides links to properties, client-side (Host) settings, space configuration, VSS, snapshots and snapshot settings. See LUNs on page 231

ISCI Targets: Adds or deletes and shows properties for iSCSI targets.The panel menu provides links to properties and one-way CHAP authentication settings. See Managing iSCSI targets on page 315

Object Stores: Create, increase capacity, show properties, or delete object stores. See Object Stores on page 335



The Data Protection menu

The **Data Protection menu** provides access to the following panels:

Archive: Provides options for configuring an Assureon server and viewing archived file systems. See Using Active Archive on page 429

Replications: Adds asynchronous replications to one or more remote Unity Systems. Once replication is in place, you can view details, calculate space requirements, manually push replication, and remove replication connections. See Data replication on page 499

Snapshots: Use this panel to select a storage pool and then a dataset to view and manage snapshots. You can search snapshots, manage browsing, roll back, and delete snapshots. See Introduction to snapshots on page 286

See also Data Protection panels and menus on page 40

Cloud Connector: Set up and manage synchronization between Unity file systems and supported cloud tartets. See Cloud Connector on page 539



The Help menu

The **Help menu** provides access to the following:

Unity Help: Opens the main Unity Help system, which documents concepts and tasks for using Unity's features.

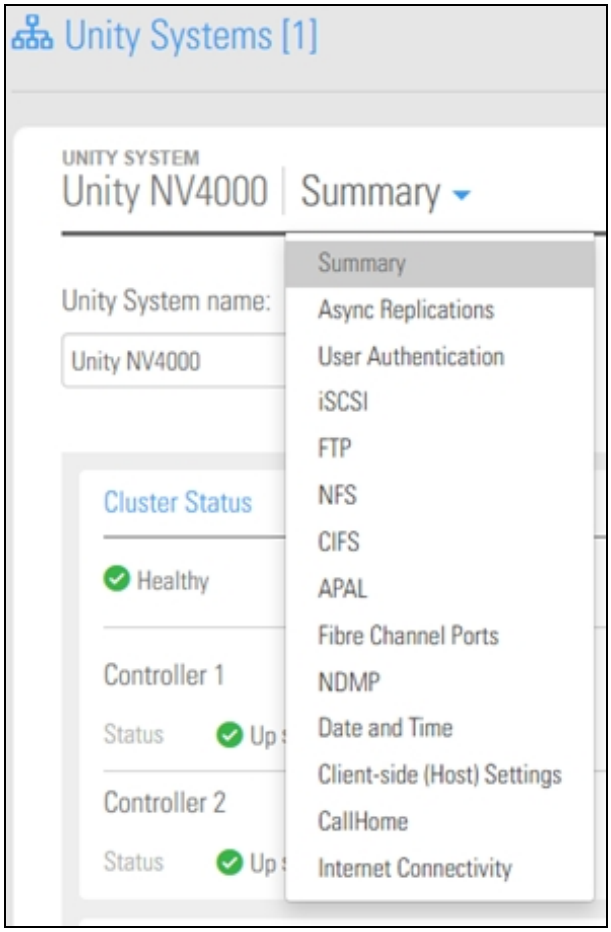
Download Software User Guide: Displays the Unity Software User Guide, for use online or in printed form.

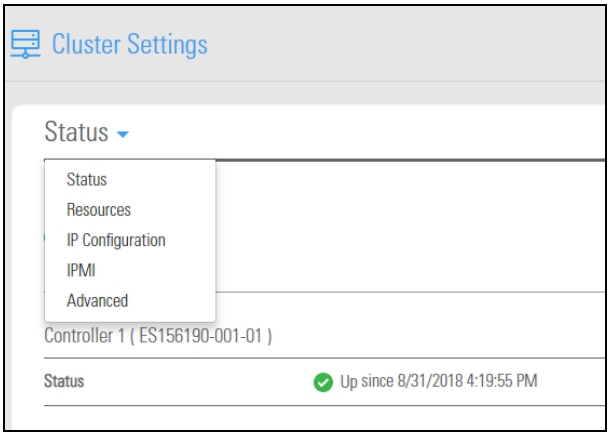
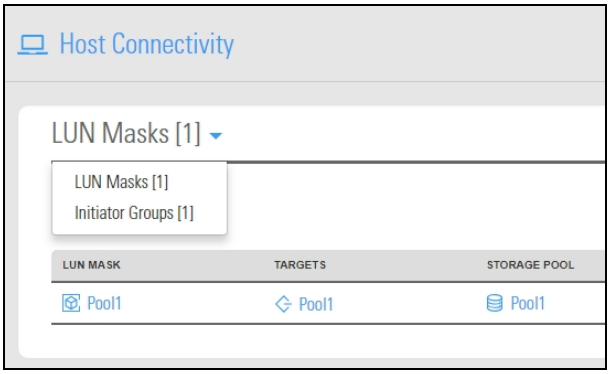
Open Unity Classic UI: Opens the Unity Flash UI, useful if you require a feature that is not yet available in the Unity HTML5 graphical user interface.

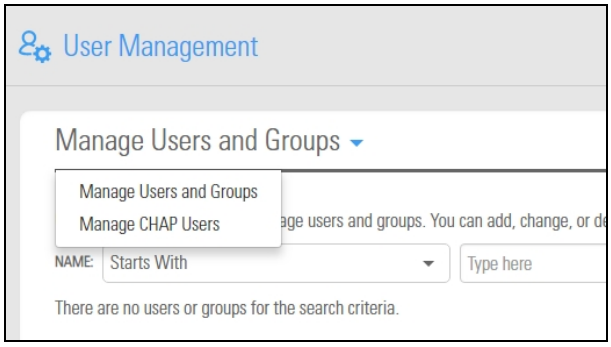
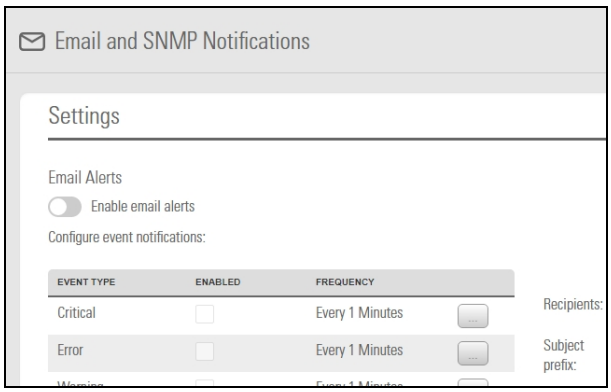
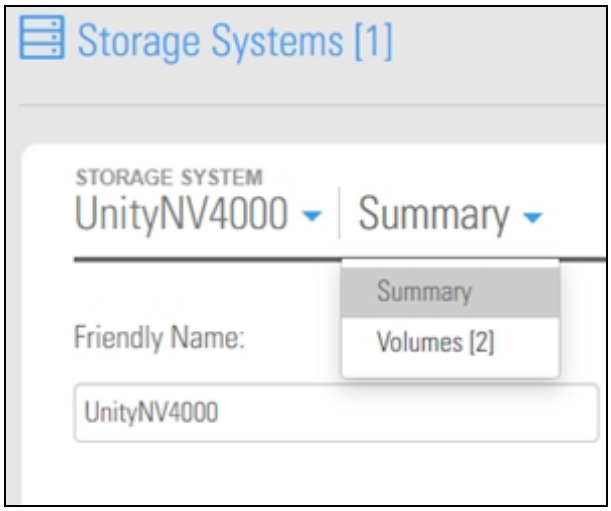
About Unity: Opens the About Unity window, where you can view the Unity System name, serial number, storage capacity, version number, installed features, copyright and patent information, and open the release notes and license agreement.

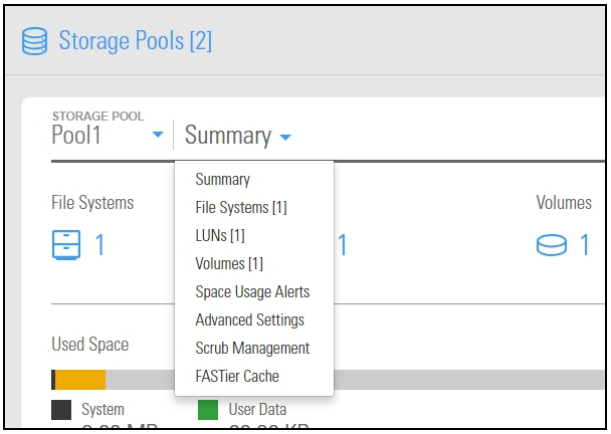
Unity panels and panel menus

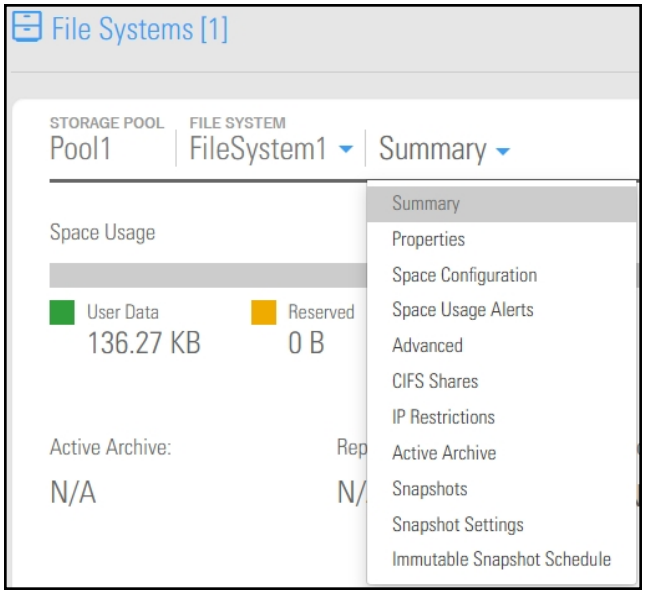
Each of the Unity panels include additional menus providing access to related features. As you get to know Unity, use the following table for help with finding these features and related documentation.

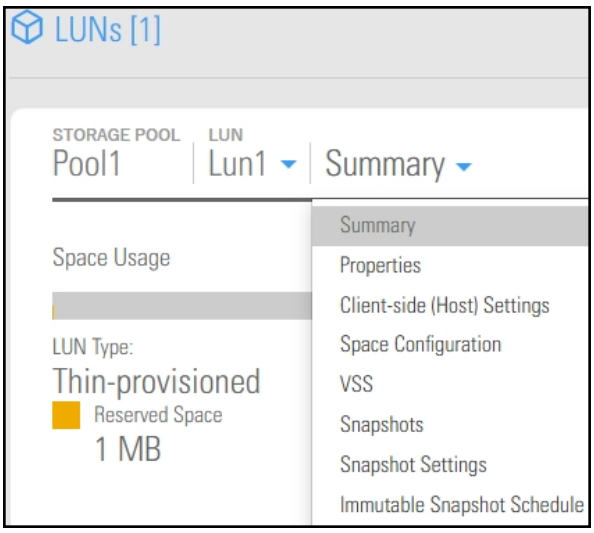
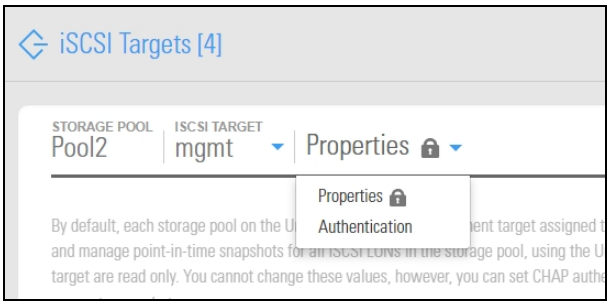
Panels and menus	Where to find them
Systems panels and menus The menus in this section open from the Unity System menu.	
Unity Systems panels 	To display the **Unity Systems panel**, click **System > Unity Systems**, click the link to a Unity System. To open the panel menu, click **Summary**. **Summary**: View or edit System Name, and view IP address, Unity System Status, view Cluster Status, Events, and view graphical statistics and status for Storage Systems, Storage Pools, File Systems, and LUNs. Click the link to any of the main dashlets to go directly to those panels. **Async Replications**: See Asynchronous data replication on page 501 **User Authentication**: See Users and access rights on page 69 **iSCSI**: See Configuring and managing CHAP authentication on page 82 **FTP**: See Enabling FTP support on page 482 **NFS**: See Configuring NFS settings on page 479 **CIFS**: See Managing CIFS shares on page 173 **APAL**: See Viewing APAL status on page 481 **Fibre Channel Ports**: View operational and connection states of fibre channel ports. **NDMP**: See Setting NDMP configuration options on page 439 **Date and Time**: View or change server time zone. **Client-side (Host) Settings**: See Host connectivity: LUN masks and Initiator Groups on page 322 **CallHome**: See Using the CallHome feature on page 484 **Internet Connectivity**: See Enabling Internet connectivity on page 493

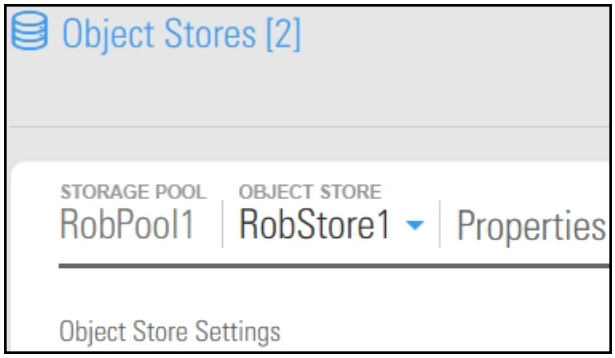
Panels and menus	Where to find them
Cluster Settings panels 	To display the **Cluster Settings** panels and menu, on the **Unity navigation bar**, click **System > Cluster Settings**. To open the panel menu, click **Status**. **Status**: Displays cluster status - overall health, and status for Controller 1 and Controller 2. See Clustering overview on page 376 **Resources**: See Clustering overview on page 376 and Moving cluster resources on page 387 **IP Configuration**: See Modifying IP configuration settings on page 393 **IPMI**: See Setting or modifying IPMI settings on page 398 **Advanced**: See Enabling jumbo frames using Unity on page 399Enabling LACP using the Unity Web interface on page 400, and Configuring TCP flow control on page 403
Host Connectivity panels 	To display the **Host Connectivity** panels, on the **Unity navigation bar** click **System > Host Connectivity**. To open the panel menu, click **LUN Masks**. **LUN masks**: See Host connectivity: LUN masks and Initiator Groups on page 322 and Creating a LUN mask on page 324 **Initiator Groups**: See Adding an initiator group on page 330

Panels and menus	Where to find them
User Management panels 	To display the **User Management** panels, on the **Unity navigation bar** click **System > User Management**. To open the panel menu, click **Manage Users and Groups**. User Management panels: **Manage Users and Groups**: See Managing Unity user and group access permissions on page 72 **Manage CHAP users**: See Configuring and managing CHAP authentication on page 82
Notifications panel 	To display the **Notifications** panel, on the **Unity navigation bar** click **System > Notifications**. **Email Alerts**: See Setting up email notification for system events on page 563 **System Notifications**:Setting up system notifications on page 565 **SMTP**: See Configuring SMTP server settings for the Unity System on page 566 **SNMP**: See Setting up SNMP notification on page 567
Storage panels and menus The menus in this section open from the Storage menu.	
Storage Systems panels 	To display the **Storage Systems** panels, on the **Unity navigation bar** click **Storage > Storage Systems**. Click the link to a **Storage System**. To open the panel menu, click **Summary**. **Summary**: See Storage management on page 405 **Volumes**: See Adding volumes to a storage pool on page 98

Panels and menus	Where to find them
Storage Pools panels 	To display the **Storage Pools** panels, on the **Unity navigation bar** click **Storage > Storage Pools**. Click the link to a **Storage Pool**. To open the panel menu, click **Summary**. **Summary**: See Storage pools on page 89 **File Systems**: See Adding a file system on page 117 **LUNs**: LUNs on page 231 **Volumes**: See Adding volumes to a storage pool on page 98 **Space Usage Alerts**:Setting space usage notification thresholds for a storage pool on page 105 **Advanced Settings**: See Configuring access time on a storage pool on page 103Configuring data compression on a storage pool on page 102, and Enabling the Microsoft VSS client for LUNs on page 262 **Scrub Management**: SeeScrubbing a storage pool on page 94 **FASTier cache**: See Managing FASTier cache devices on page 108

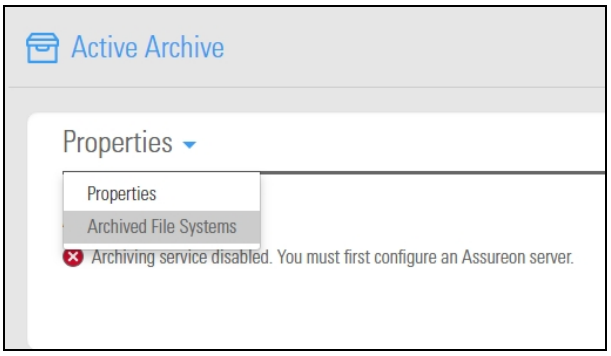
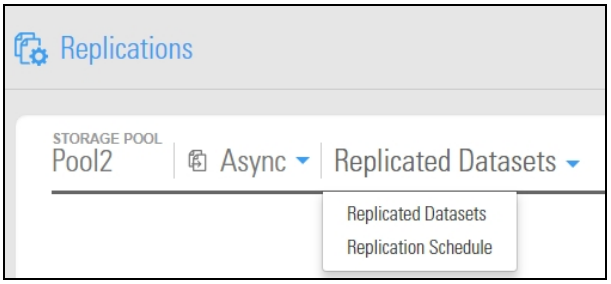
Panels and menus	Where to find them
File Systems panels 	To display the **File Systems** panels, on the **Unity navigation bar** click **Storage > File Systems**. Click the link to a **File System**. To open the panel menu, click **Summary**. **Summary**: See Viewing file system space usage information on page 130 **Properties**: See Modifying file system properties on page 132 **Space Configuration**: See Viewing file system space usage information on page 130 **Space Usage Alerts**: See Setting space usage notification thresholds for file systems on page 140 **Advanced**: See Modifying file system record size on page 138 and Enabling the Access Time mode on a file system on page 144 **CIFS Shares**: See Managing CIFS shares on page 173 **IP Restrictions**: See Setting IP restrictions on page 147 **Active Archive**: See Managing Active Archive settings for file systems on page 431 **Snapshots**: See Managing snapshots for file systems on page 1 **Snapshot Settings**: See Setting a schedule for automatic file system snapshots on page 208 **Immutable Snapshot Schedule**: See Scheduling immutable snapshots for File Systems on page 225

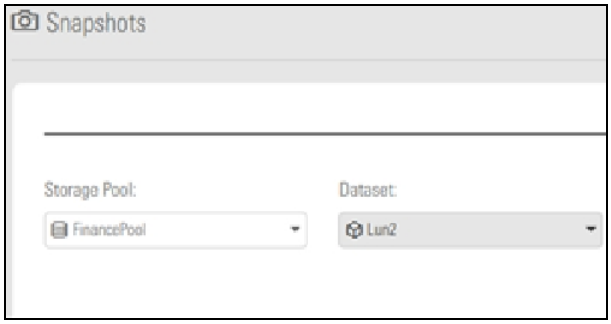
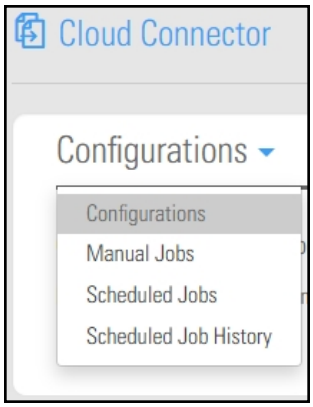
Panels and menus	Where to find them
LUNs panels 	To display the **LUNS** panels, on the **Unity navigation bar** click **Storage > LUNS**. Click the link to a **LUN**. To open the panel menu, click **Summary**. **Summary**: See Viewing LUNs on page 248 **Properties**: See Renaming a LUN on page 250, Disabling Read caching on page 252, and Configuring data compression on a LUN on page 251 **Client Side (Host) Settings**: See Enabling VMware VAAI hardware acceleration for a LUN on page 254 and Enabling client-side space usage notifications for a LUN on page 254 **Space Configuration**: See Changing LUN space configuration on page 256 **VSS**: See Using Windows VSS on page 258 **Snapshots**: See Viewing LUN snapshots on page 291 **Snapshot Settings**: See Managing snapshots for LUNs on page 285 **Immutable Snapshot Schedule**: See Scheduling immutable snapshots for LUNs on page 311
iSCSI Targets panels 	To display the **iSCSI Targets** panels, on the **Unity navigation bar** click **Storage > iSCSI Targets**. Click the link to a **iSCSI Targets**. To open the panel menu, click **Properties**. **Properties**: See Managing iSCSI targets on page 315 **Authentication**: See Configuring and managing CHAP authentication on page 82 See also: Adding an iSCSI target on page 315

Panels and menus	Where to find them
Object Store properties 	To display the **Object Store** properties (there are no specific panel menus), on the **Unity navigation bar** click **Storage > Object Stores**. Click the link of the object store name under **Name**. The **Properties** page appears. **Refresh Status**: See Viewing object store system information on page 342 **Reset Keys**: See Resetting object store keys on page 349 **Stop Object Store**: See Stopping the service for an object store on page 347 **Disable TLS**: See Enabling or disabling TLS on the object store on page 343 **Delete Object Store**: See Deleting an object store on page 347 **Increase Capacity**: See Increasing storage capacity for object stores on page 344 **Browser Access**: SeeAccessing the NexObject Web client on page 349

Data Protection panels and menus

The menus in this section open from the Data Protection menu.

Panels and menus	Where to find them
Active Archive panels 	To display the **Active Archive** panels, on the **Unity navigation bar** click **Data Protection > Archive**. To open the panel menu, click **Properties**. **Properties**: See Connecting to an Assureon Server on page 429 **Archived File Systems**: See Viewing archived file systems on page 434
Replications panels 	To display the **Replications** panels, on the **Unity navigation bar** click **Data Protection > Replications**. To open the panel menu, click **Replicated Datasets**. **Replicated Datasets**: See Data replication on page 499 **Replication Schedule**: See Modifying a storage pool's replication schedule on page 520

Panels and menus	Where to find them
Snapshots panel 	To display the **Snapshots**panel, on the **Unity navigation bar** click **Data Protection > Snapshots**. **File System snapshots**: See Viewing file system snapshots on page 204 **LUN snapshots**: See Viewing LUN snapshots on page 291
Cloud Connector panel 	To display the **Cloud Connector** panel, on the **Unity navigation bar** click **Data Protection > Cloud Connector**. **Configurations**: See Adding cloud storage configurations on page 539 **Manual Jobs**: See Transferring data manually to cloud storage on page 544 **Scheduled Jobs**: See Scheduling automatic data transfer to cloud storage on page 546 **Scheduled Job History**

Concepts and terminology

This section explains basic Unity concepts and terminology.

Distributed primary storage

Unity delivers unified NAS (CIFS/NFS) and block-level (iSCSI and Fibre Channel) storage, with ground-breaking performance for mid-sized organizations requiring true enterprise-class features. Enterprise 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 also features FASTier acceleration technology, which uses both DRAM and flash SSD technology to optimize block and file operations in a fault tolerant architecture.

With Unity, your team can easily manage storage across Microsoft Windows, UNIX, or Linux clients, over a local area network (LAN) or wide-area network (WAN). Unity also features NestOS, an optimized embedded operating system, and an intuitive, Web-based interface for easy deployment, and administration. It adds high-capacity, high-availability storage within the framework of your current network infrastructure.

Sharing methods and data protection

Unity provides CIFS and NFS shared folders as well as iSCSI and Fibre Channel 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 table describes basic Unity concepts and terminology. For more definitions, see Terminology on page 589 and the Help Glossary.

Unity terminology	Description
NestOS	NestOS is an optimized embedded operating system that runs on Unity storage components. 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.
Nexsan Unity or Unity	Unity is the Web-based user interface for managing Nexsan Unity Storage Systems. Unity provides a graphical and statistical views of storage and overall system components. Unity also provides wizard-based configuration tools for creating storage pools, file systems, object stores, replication sites, and for performing other storage management tasks.

Unity terminology	Description
Unity Storage System	A Unity Storage System—also referred to as the local system, active system, or primary system (in a replicated environment)—represents a geographic location that hosts a Unity Storage System. More specifically, a Unity Storage System can contain either: ● a Unity Storage System with no external storage; ● a Unity Storage System with one or multiple Storage Expansions, including Nexsan E-Series Storage Systems, connected to it (via Fibre Channel or SAS). A remote Unity system—also referred to as a secondary system or a replication system (in a replicated environment)—represents either: ● a Unity System that is designated as the data replication system for the local Unity System, or ● a Unity System that is being managed remotely from the local system. A Unity System can be the primary system in a replicated environment and also perform double-duty as the remote data replication site for another Unity System.
Storage Expansion	On Unity, storage expansions (formerly storage enclosures) can include: ● **External storage**: Unity Storage Expansions, such as the U2G424 Expansion, U2G460 Expansion, and the U2G478 Expansion. ● **a Nexsan Unity Storage Expansion connected to Unity via SAS**: Unity storage expansions connect to Unity Storage Systems via a SAS add-on card (optional). **Note** You can allocate a Nexsan E-Series storage expansion to the Unity System, provided that the system was previously configured by a Unity. However, doing so results in the storage system to be reconfigured, and all existing data on the storage system to be removed. Unity displays an appropriate warning and asks you to confirm.

Unity terminology	Description
Storage Pool or pool	A storage pool is a user-defined virtual grouping of volumes available on Unity. Pools allow you to organize your storage into logical groups; expose file systems to Windows-based (CIFS) and/or UNIX/Linux-based (NFS) clients on the network; expose blocks of storage as LUNs to iSCSI or Fibre Channel initiators on the network; and replicate all the data in the pool, or just a subset of it, for disaster recovery. Unity enables you to create as many storage pools as there are available volumes (RAID sets) on the system. If your Unity Storage System has both internal storage and Unity Storage Expansions connected externally via SAS, you can create storage pools by combining volumes from both the main system and the expansions—provided the RAID level configurations are the same on all connected systems and expansions. If Unity has both internal storage and a storage expansion connected externally via SAS, you can create storage pools by combining volumes from both—provided the RAID level configurations are the same on both storage enclosures).
Volume	A volume represents a virtual subset of the aggregated disk space available on Unity, or on a Nexsan E-Series™ attached externally to Unity—for example, a Nexsan E18™, Nexsan E48™, or Nexsan E60™ storage system connected externally to Unity via Fibre Channel or SAS, or a Nexsan Unity Storage Expansion connected to Unity via SAS. In short, Unity presents the disk space available on Unity, and on any Unity Storage System attached externally to Unity, as volumes. The total number of volumes available depends on the RAID level (5, 6, or 10) and RAID sets that you specify during the initial setup of Unity.
File System	Subfolders of storage pools, file systems are Unity organizational structures available as shares exposed on the network via CIFS protocol and/or the NFS protocol.
LUN	A LUN is a term used to describe a block of storage on 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. LUNs can be exposed over iSCSI or Fibre Channel. 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. When exposed to targets over Fibre Channel, a LUN forms a block device identified by a unique HBA port WWN that can be accessed by one or more FC initiators.

Unity terminology	Description
Object Store	An object store holds data in small pieces called objects and is useful for storing large amounts of unstructured data. Object storage is the most recent of the three main forms of data storage. The other forms are file storage and block storage. Unity object storage is based on the S3 protocol.
Controller, controller node, or node	The controller in Unity acts as the interface between Unity and network clients. Unity has two controller nodes, represented by the Clusters node in Unity, for which you can configure both cluster and network settings.

Understanding multi-site implementation

Unity enables you to manage any number of Unity Storage Systems within the Web user interface. Every Unity Storage System has its own set of resources independent from Unity Storage Systems, regardless of their physical location. 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 Unity Storage System that is part of a replicated pair also disconnects the replicated Unity Storage System. If a Unity Storage System disconnects its own replicated site, then only the replicated system is disconnected. However, you must remove the replication beforehand to be able to disconnect from another Unity system.

Note If you connect to a Unity system 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 Unity Storage Systems that have been added to the current site, along with their replicated counterpart.

- the active Unity Storage System (the one you are currently logged into) is displayed with a star;
- the added sites to which the current logged in user has access have regular icons;
- the added sites that are not directly connected to the currently selected site appear grayed out.

1

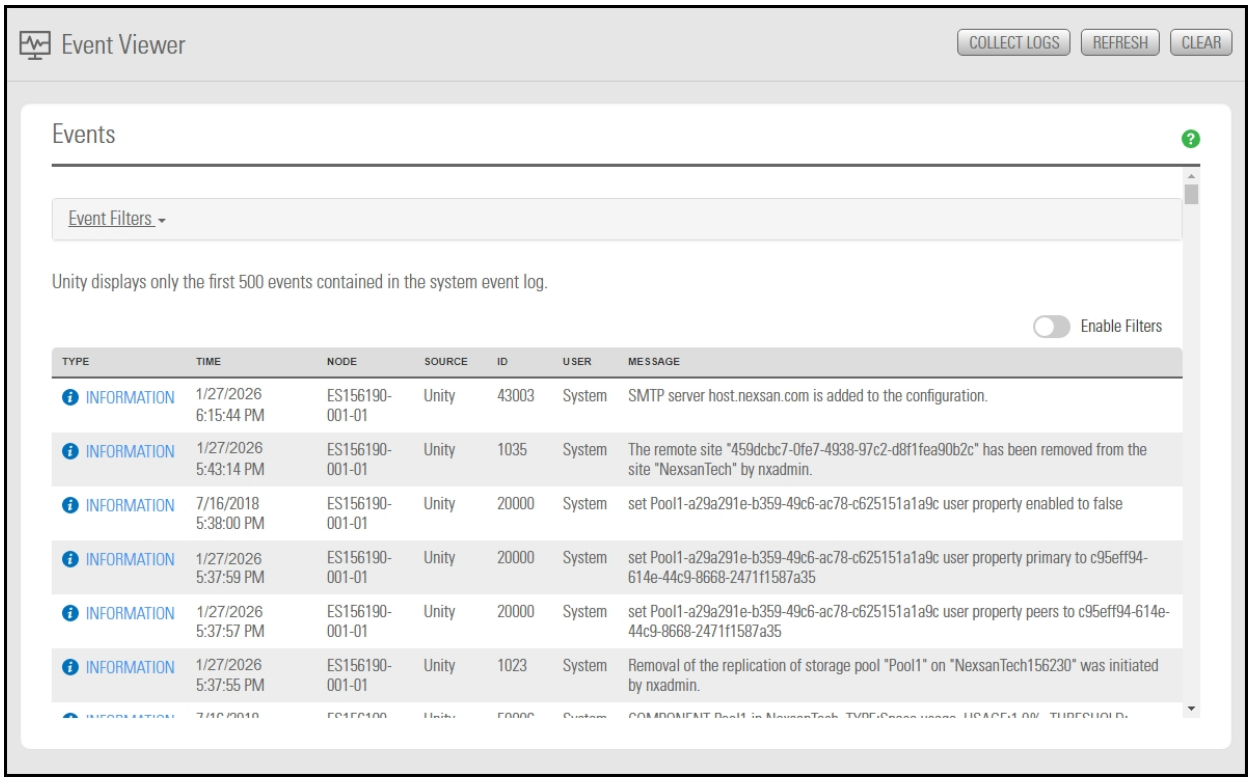
Multi-site implementation characteristics

- If an added Unity Storage System 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 system's node icon in the Unity Systems > Properties panel or Select System menu.

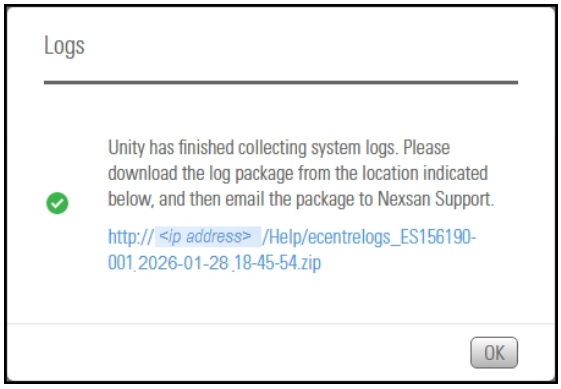
  When you click on the Unity Storage System, you are prompted to enter the credentials of the system.

  When you enter the credentials, Unity can store these credentials for future use. Subsequently, the stored credentials are used to automatically connect to this site.
- If you modify the IP address of a Unity Storage System, Unity automatically reconnects to the new IP address.
- On each Unity Storage System, you can view space usage and volume information for storage pools in other Unity systems.

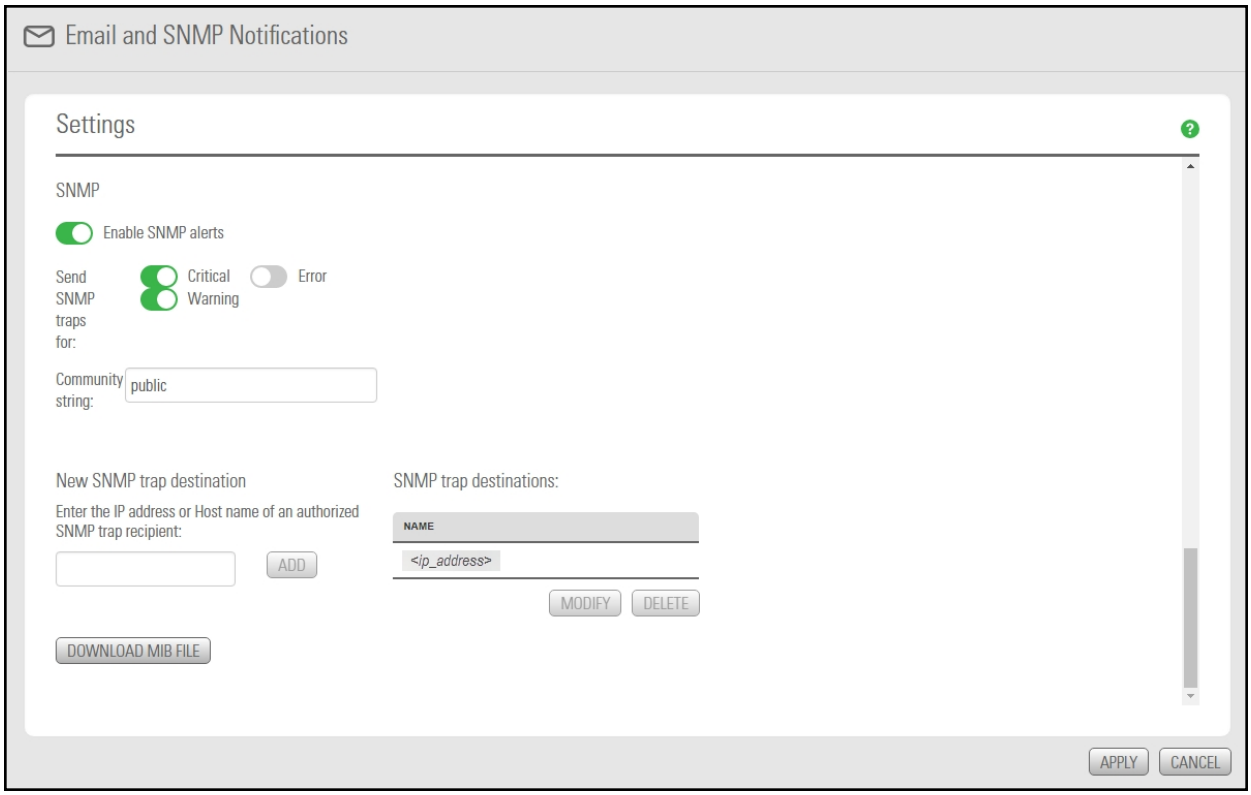
- The Event Viewer enables you to view events for all Unity Storage Systems. You can filter events by Unity System, source, type, and time period.



- You can view logs by clicking **Collect Logs**, which triggers creation of a logs package.



You can configure email, system, SMTP, and SNMP notifications for all Unity Storage System in your implementation from one Unity system by selecting the site from the **Email and SNMP Notifications** panel.



Multi-site implementation limitations

- To upgrade a Unity Storage System to the latest firmware version, you must log in to that site directly, then run the Unity firmware upgrader.
- CHAP users are managed per Unity Storage System. To create CHAP users for a specific site, you must log in to that Unity Storage System directly and open the Manage CHAP users panel from there.
- You cannot completely remove a site connected to multiple Unity Storage Systems at once. You must disconnect all Unity Storage Systems connected to that site. For details, see Disconnecting Unity Systems in a multi-system implementation on page 444.

Typical Unity Storage System deployments

The following sections provide connection details and concepts for deploying Unity v. 7.4 systems.

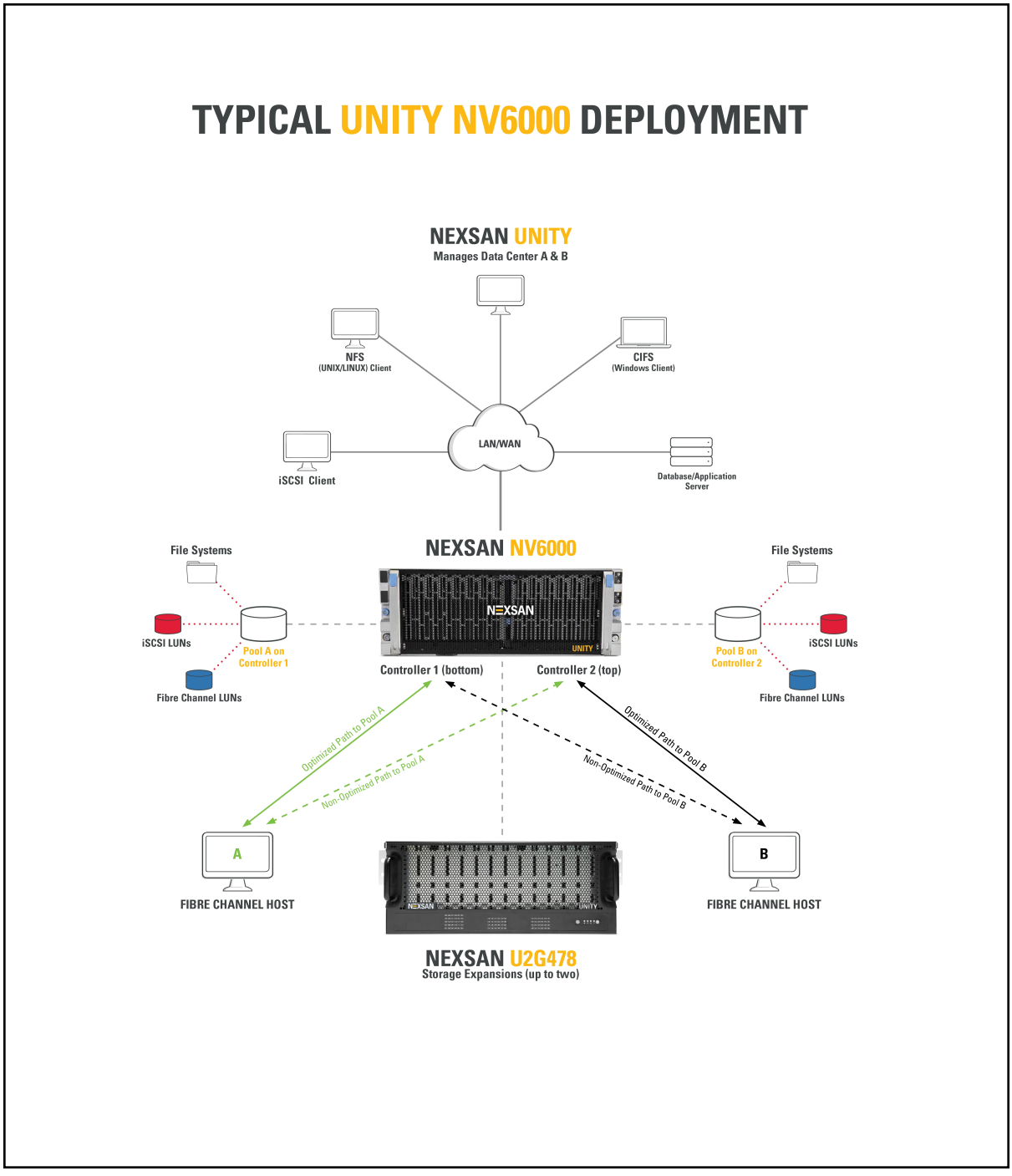
UNITY NV6000 deployment

This diagram provides an example of typical UNITY NV6000 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 UNITY NV6000 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 UNITY NV6000 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 UNITY NV6000 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*.

Figure 1-2: Typical unitUNITY NV6000 deployment



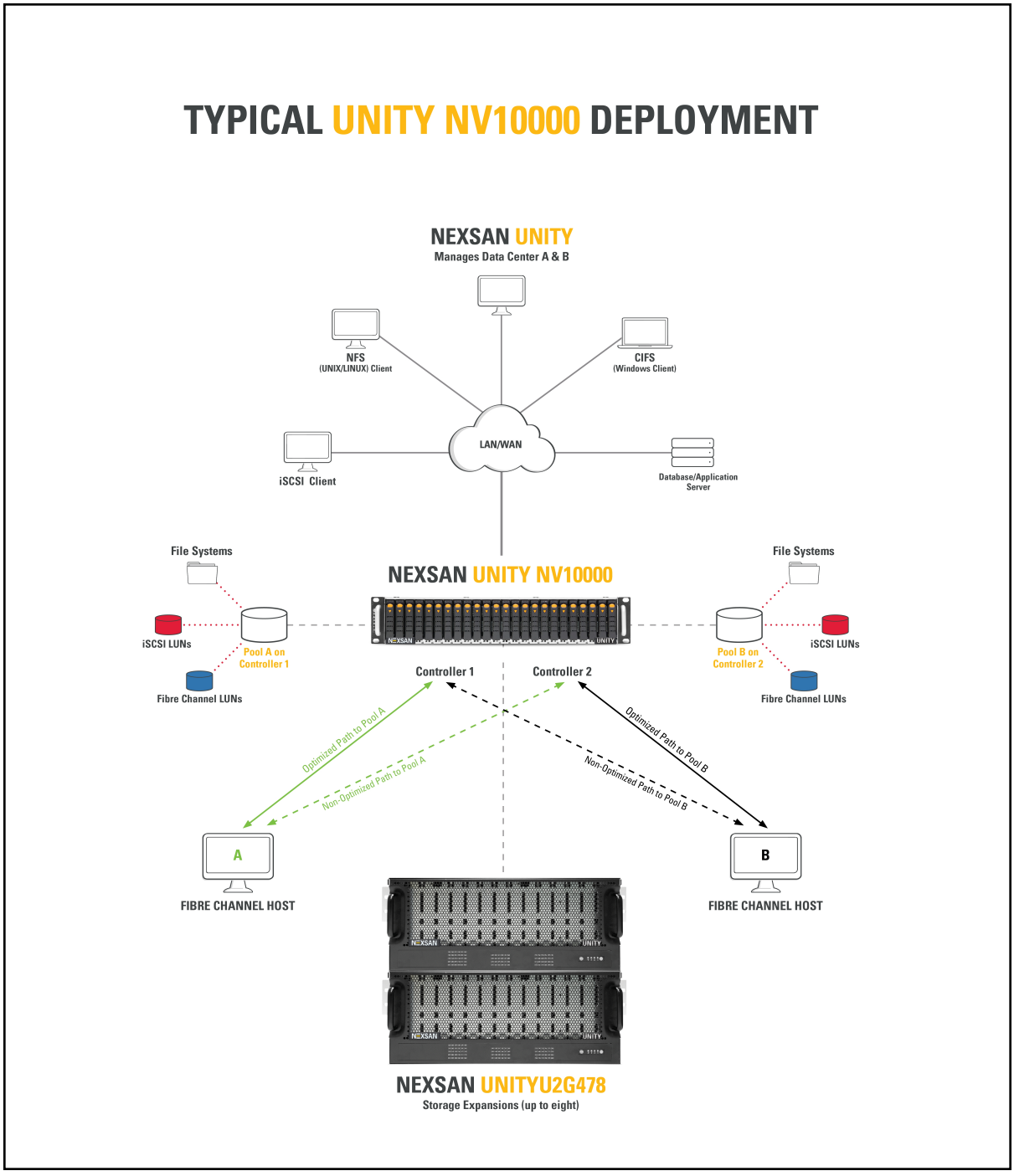
UNITY NV10000 deployment

This diagram provides an example of typical UNITY NV10000 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 UNITY NV10000 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 UNITY NV10000 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 UNITY NV10000 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*.

Figure 1-3: Typical UNITY NV10000 deployment



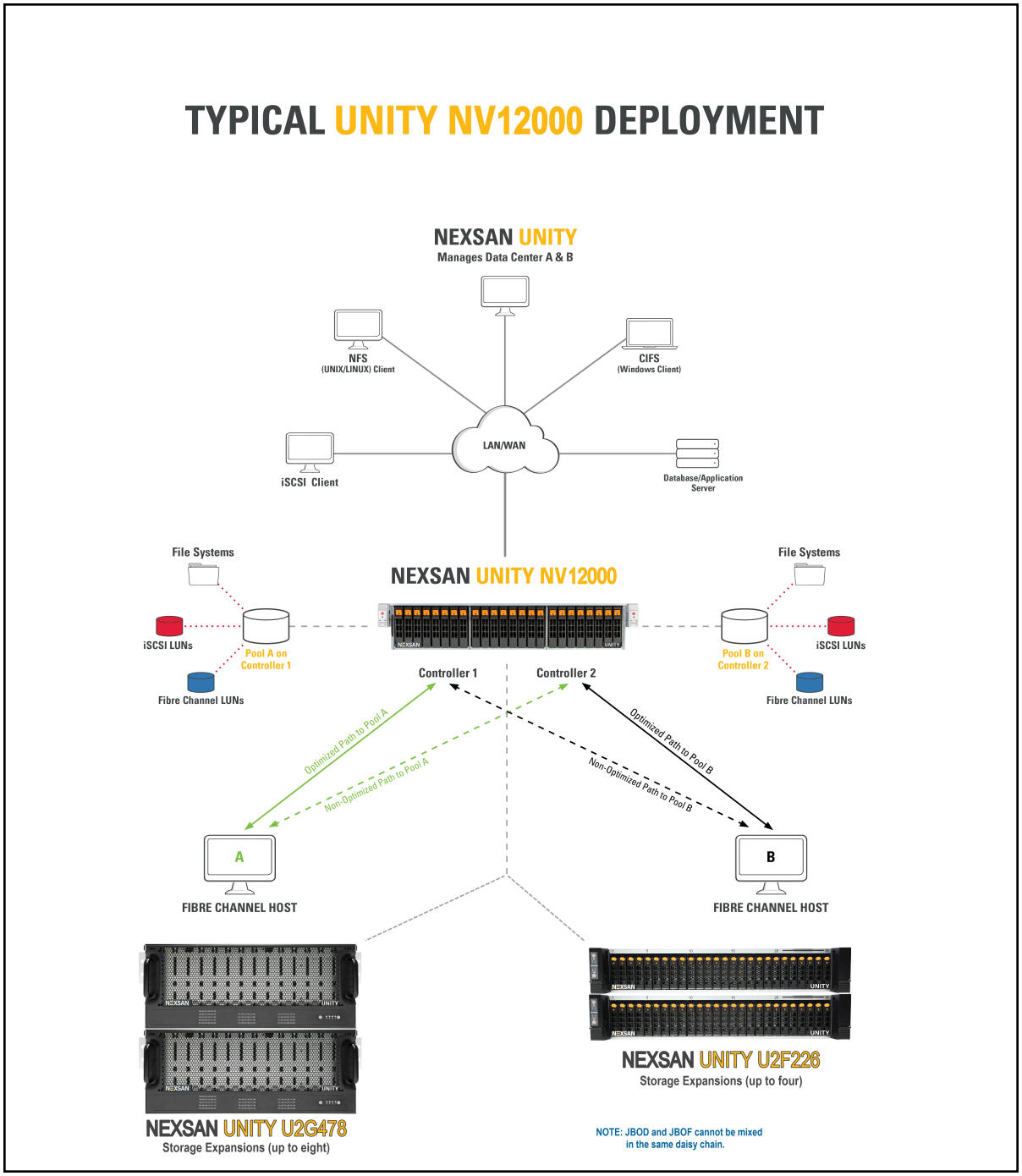
UNITY NV12000 deployment

This diagram provides an example of typical UNITY NV12000 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 UNITY NV12000 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 UNITY NV12000 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 UNITY NV12000 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*.

Figure 1-4: Typical UNITY NV12000 deployment



Chapter 2

Getting started

Once you set up the Unity Storage System, you can use the new Web-based Nexsan Unity user interface to manage your storage infrastructure.

This section includes these topics:

Setting up the Unity Storage System 56
Starting Unity 65
Logging on to Unity 66

Setting up the Unity Storage System

If the Unity System Configuration process was not completed during initial hardware installation and setup (see your Unity Storage System Quick Start Guide), you'll need to complete the **Unity System Configuration** wizard before you start using the Unity Web software interfaces.

Before the wizard starts, you'll be prompted to accept the **license agreement** and then to set a new password. Here are the **Unity System Configuration** wizard steps:

- **Step 1: Configuring Unity System properties below**: First, you'll specify a Unity Storage System name, time zone, and CallHome settings.
- **Step 2: Configuring network settings on page 58**: Here, you'll confirm the IP addresses defined in the initial commissioning of the system using the nx99 and nx0 Management Interfaces or the Discovery wizard.:
- **Step 3: Configuring IPMI settings on page 61**: Next, set up IPMI settings: IP addresses for the controllers, a subnet and IPMI Gateway, and specify the IPMI password.
- **Step 4: Allocating storage on page 62**: Here, you'll configure RAID settings for your **Unity Storage Systems**.
- **Step 5: Verifying configuration settings on page 64**: Last, review your settings and create the system.

Note You must connect the **Primary Data Network Interface (nx0)** before running the **Unity System Configuration** wizard. Typically, this is done during hardware and management software installation on site. See your Unity Quick Start Guide.

Starting the Unity System Configuration wizard

Use these steps to start Unity from the **Unity System Configuration** wizard.

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

1. Open Google Chrome on a system that is installed on the same network and subnet as Unity.
2. In the Chrome address bar, enter the Management Virtual IP address set using the **Management Interface (nx99)**. The **License Agreement** page opens.
3. Click **I accept the terms of the license agreement** and then click **Next**.
4. When prompted, enter the new password for the **nxadmin** account.

The **Unity System Configuration** wizard displays the first step in the setup process.

5. Go to **Step 1: Configuring Unity System properties below**.

Step 1: Configuring Unity System properties

In this step, specify the **Unity System name**, **Server Time Zone**, and **CallHome** log collection properties.

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

1. Open Google Chrome on a system that is installed on the same network and subnet as Unity.
2. In the Chrome address bar, enter the Management Virtual IP address set using the **Management Interface (nx99)**. The **License Agreement** page opens.
3. Click **I accept the terms of the license agreement** and then click **Next**.
4. When prompted, enter the new password for the **nxadmin** account.

The **Unity System Configuration** wizard displays the first step in the setup process.

5. Go to **Step 1: Configuring Unity System properties on the previous page**.

► To configure Unity System properties:

1. Type a name in the **System Name** field.

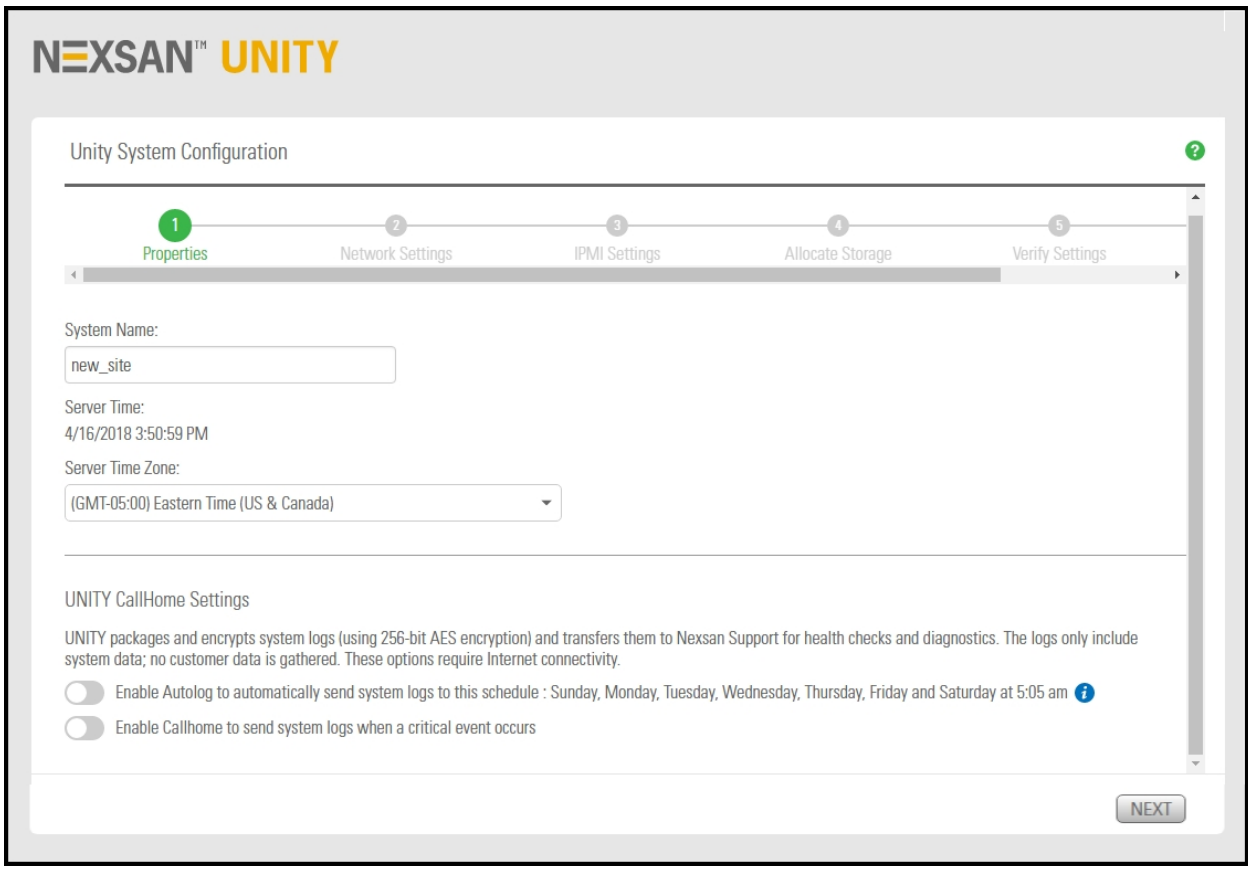
   Restrictions and conventions:

   - Spaces are allowed
   - The Unity System 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 hyphen (-) and period (.), the name can only contain alphanumeric characters, without spaces.

     These characters are NOT allowed:

     ” / \ _ [ ] : ; | = , + * ? < >

Figure 2-1: Configure Unity Properties



2. Optionally, in the **Server Time Zone** drop-down list, select the time zone for the Unity Storage System. The default time zone setting is Eastern Time (US and Canada).

   Note To apply new time zone settings, you'll need to reboot Unity after completing the **Unity System Configuration wizard**.

3. Optionally, enable the Unity CallHome log collection settings to allow Nexsan Technical Support to monitor Unity using system logs. You can enable this feature at a later time, using Unity or the **nxadmin** command-line interface. The options are:
   - **Enable autolog**: The CallHome feature packages and sends all system logs to Nexsan based on daily at 5:05 AM.
   - **Enable CallHome to send system logs when a critical event occurs**: This option sends system logs when major issues are detected, based on events and diagnostics.
4. Click the **Next** button to continue to Step 2: Configuring network settings below.

Step 2: Configuring network settings

In this step, you can change **Network Interface** settings committed during your initial system configuration.

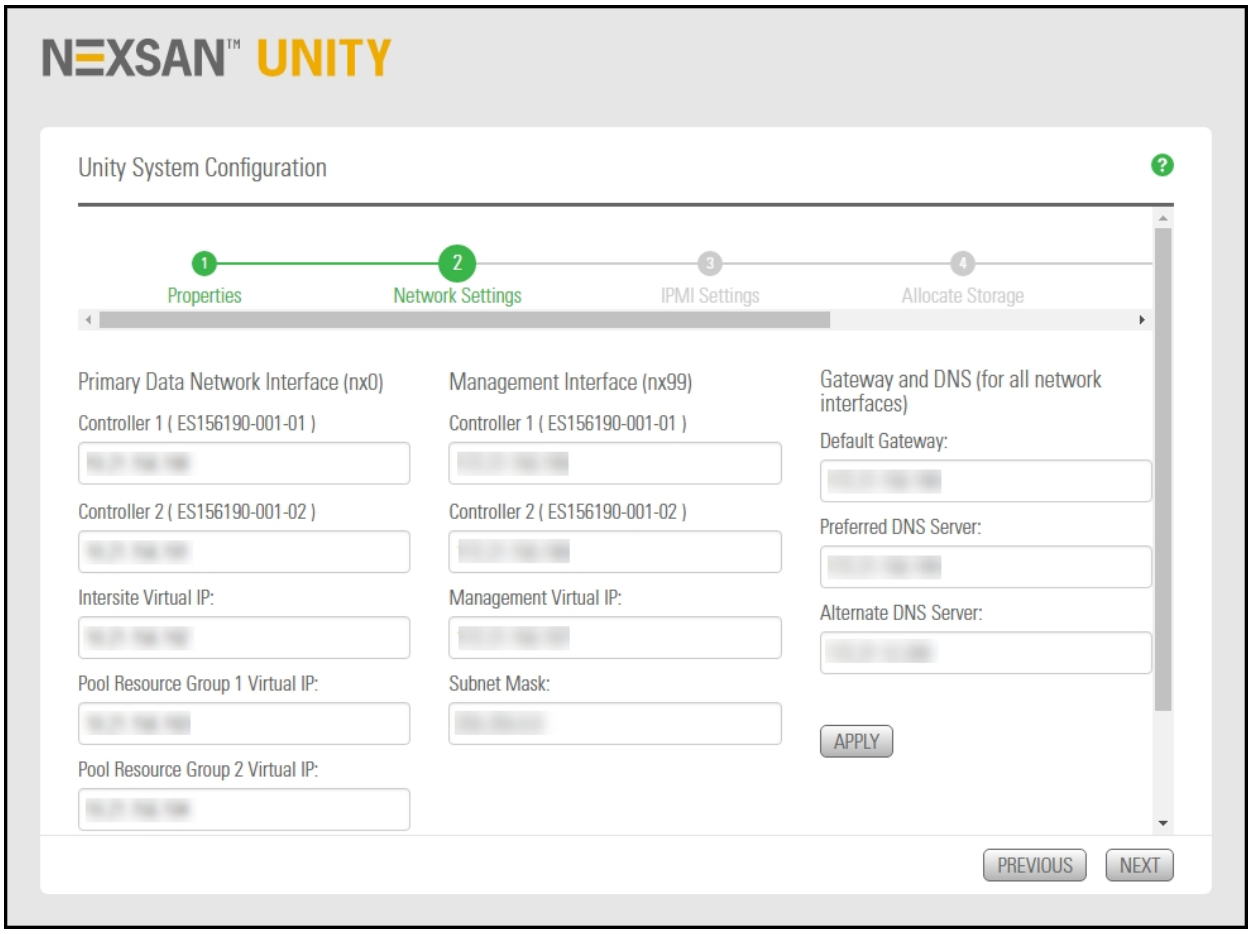
For more information about network interfaces and IP addresses, see Understanding network interfaces on page 395.

To configure network settings:

1. Set up the IP addresses for the **Primary Data Network (nx0)**.

   Note It is strongly recommended to configure the two management interfaces on separate subnets. In a flat network environment, it is acceptable to configure both interfaces on the same subnet.

Figure 2-2: Configure network settings



In the examples shown, with the exception of the subnet mask, the last digit of the network addresses increments from 0 to 10 (or 190 to 200). This practice is a useful standard if you need to manage multiple systems:

Primary Data Network (nx0) interface	Example addresses
Controllers 1 and 2	000.01.002.003 000.01.002.004
Intersite Virtual IP	000.01.002.007
Pool Resources Groups 1 and 2	000.01.002.005 000.01.002.006

2. Set the **Management Interface (nx99)** IP addresses, ideally on a separate subnet.

Management Interface (nx99)	Example addresses
Controllers 1 and 2	001.01.002.003 001.01.002.004
Management Virtual IP	001.01.002.007
Subnet Mask	255.255.0.0

3. Set the **Gateway and DNS** addresses for all network interfaces.

   Note The **Default Gateway** address should be in the same domain as the **Primary Data Network (nx0)**.

Gateway and DNS interface	Example addresses
Default Gateway	010.01.002.003
Preferred DNS Server	010.01.002.004
Alternate DNS Server	010.01.002.005

4. Click the **Apply** button to set the network configuration.
5. Click the **Next** button. The **Unity System Configuration wizard** proceeds to Step 3: Configuring IPMI settings on the facing page.

Step 3: Configuring IPMI settings

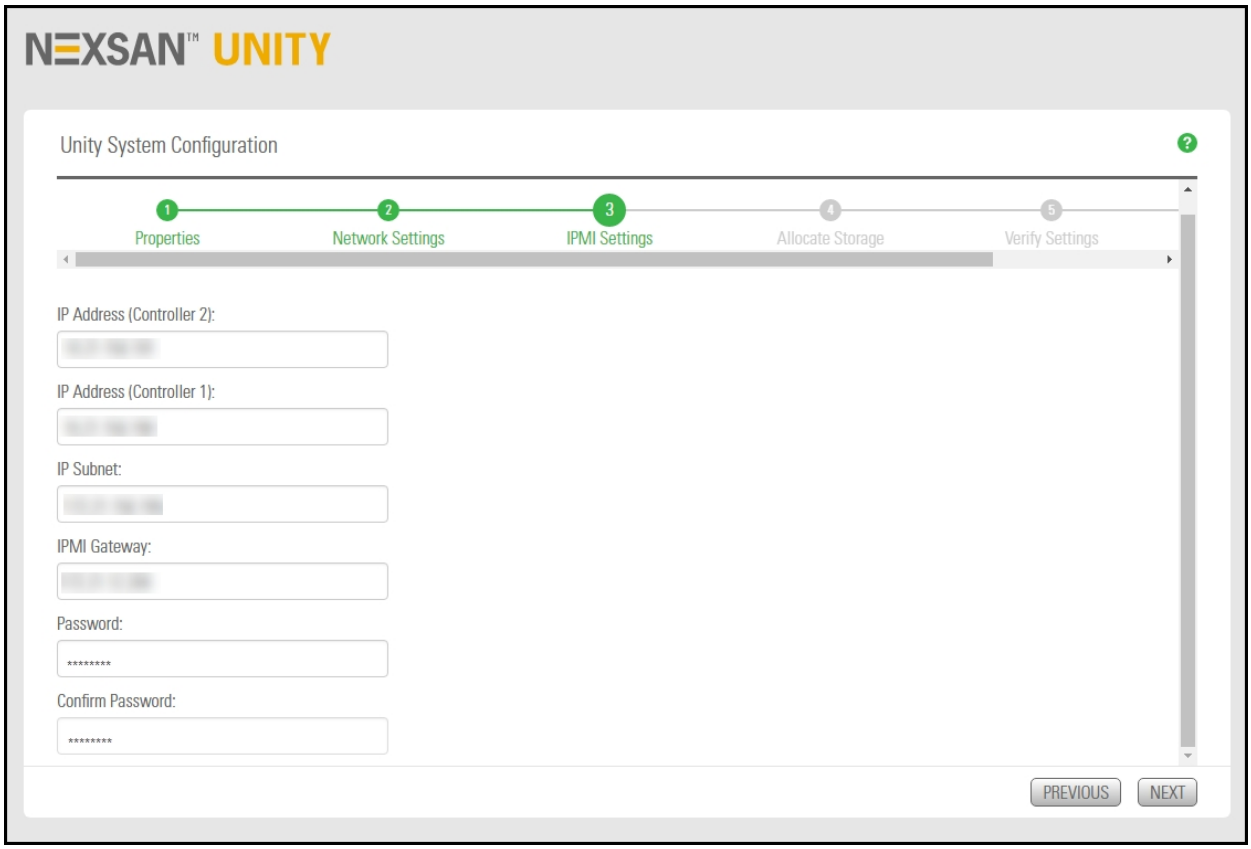
This step enables you to specify Intelligent Management Interface (IPMI) settings. To enable IPMI for Unity, you must connect a network cable to the second on-board 1 Gb LAN port at the back of each controller on the Unity Storage System enclosure; this second LAN port is located at the bottom of each controller, closest to the bottom of the controller box.

For more details, .

To configure IPMI settings:

1. Populate the following fields:
   - IPMI Controller 1 IP Address
   - IPMI Controller 2 IP Address
   - IPMI IP Subnet
   - IPMI Gateway
   - IPMI Password
   - IPMI Confirm Password

Figure 2-3: Configure IPMI settings



2. Click the **Next** button to continue to Step 4: Allocating storage on the next page.

Step 4: Allocating storage

The **Unity System Configuration wizard** automatically discovers all Unity Storage Systems.

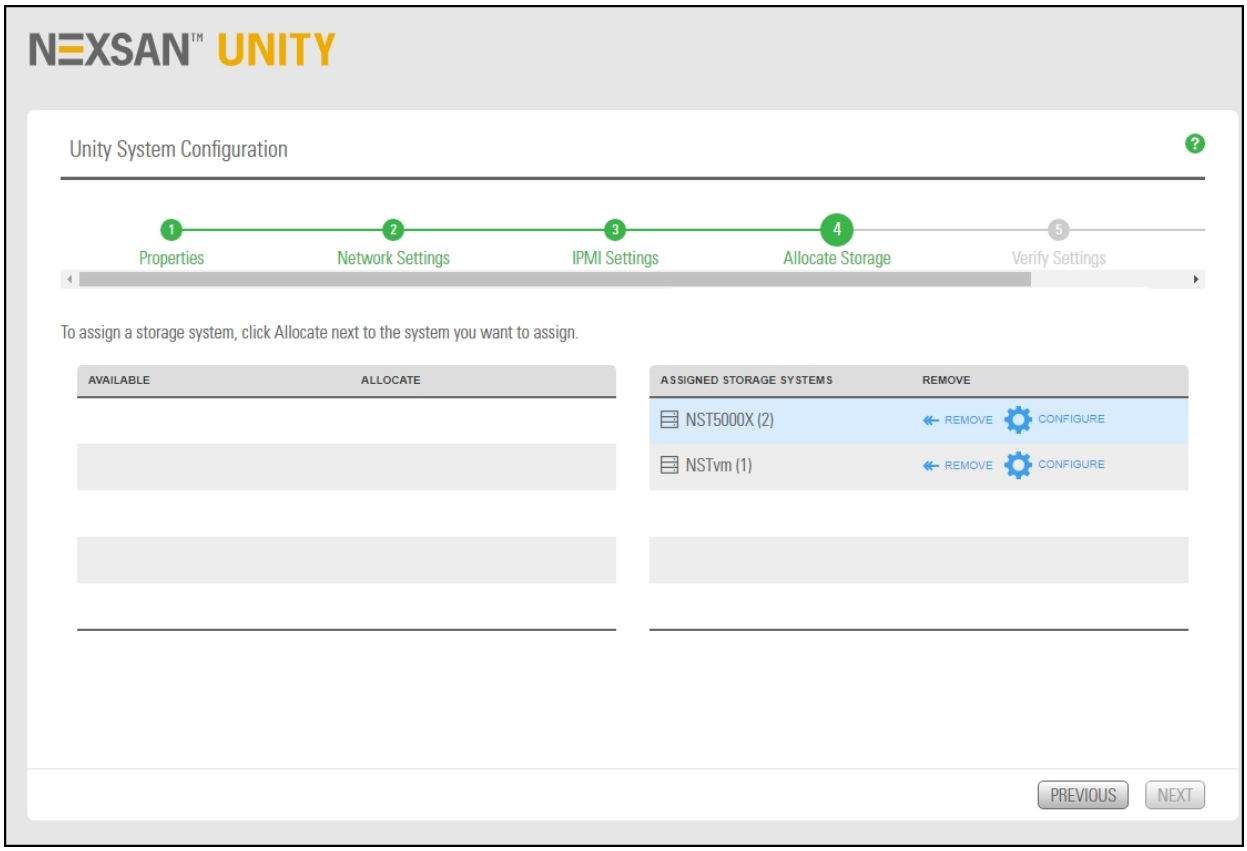
If the wizard fails to discover a Unity Storage System that you want to allocate, make sure those systems are properly connected to Unity and powered on.

For information on RAID levels, see Mixing volumes with different RAID levels on page 92.

► **To configure storage settings:**

1. In the **Available** devices list, click **Allocate** to move storage systems to the **Assigned Storage Systems** list.

Figure 2-4: Allocate Storage



2. Click **Configure**. The **Configure RAID** window opens. If Unity has only one storage device installed or connected, the **Configure RAID** window opens automatically when this step displays.
3. For **RAID level**, select the RAID level (5, 6, or 10) that you want Nexsan Unity to configure. Unity recommends the optimal RAID level.
4. Select the number of RAID sets. Unity creates a volume for each RAID set that you specify. See Mixing volumes with different RAID levels on page 92.

5. From the **Hot spares** list, select the number of hot spare disks that you want to assign to the system.

   More on Hot spares

   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.

6. (Optionally) Enter a new name for the storage system.
7. Click the **Apply** button to save your selections.
8. Repeat these steps for each connected storage device that you want to configure.
9. Click the **Next** button to continue.

For Nexsan E-Series storage expansions

If your Unity Storage System is connected to a Nexsan E-Series storage expansion with DHCP enabled, the **Unity System Configuration wizard** prompts you to specify a static IP address for the storage expansion controllers.

You MUST set a static IP address for the storage expansion.

▶ **To set a static IP address 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 addresses 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.

   Once the System Configuration wizard sets static the IP addresses on the Nexsan E-Series™ storage system, the Storage Configurator window opens, where you configure RAID settings for the system.

When you finish configuring and allocating storage, the System Configuration wizard automatically moves forward to Step 5: Verifying configuration settings on the next page.

Step 5: Verifying configuration settings

This step of the **Unity System Configuration wizard** summarizes your configuration settings and applies them to the system. Review the summary carefully before applying configuration settings.

To finalize the Unity System setup:

- If you are satisfied with the configuration settings, click the **Create** button. The System Configuration wizard begins applying your settings, displaying the progress as the wizard configures Unity.

To change a configuration setting:

- Click the step identifier at the top of the System Configuration wizard panel to go back to a specific step. For example, if you want to change the Unity System name, click **Step 2**.

OR

- Click the **Previous** button to navigate back to the corresponding configuration step.

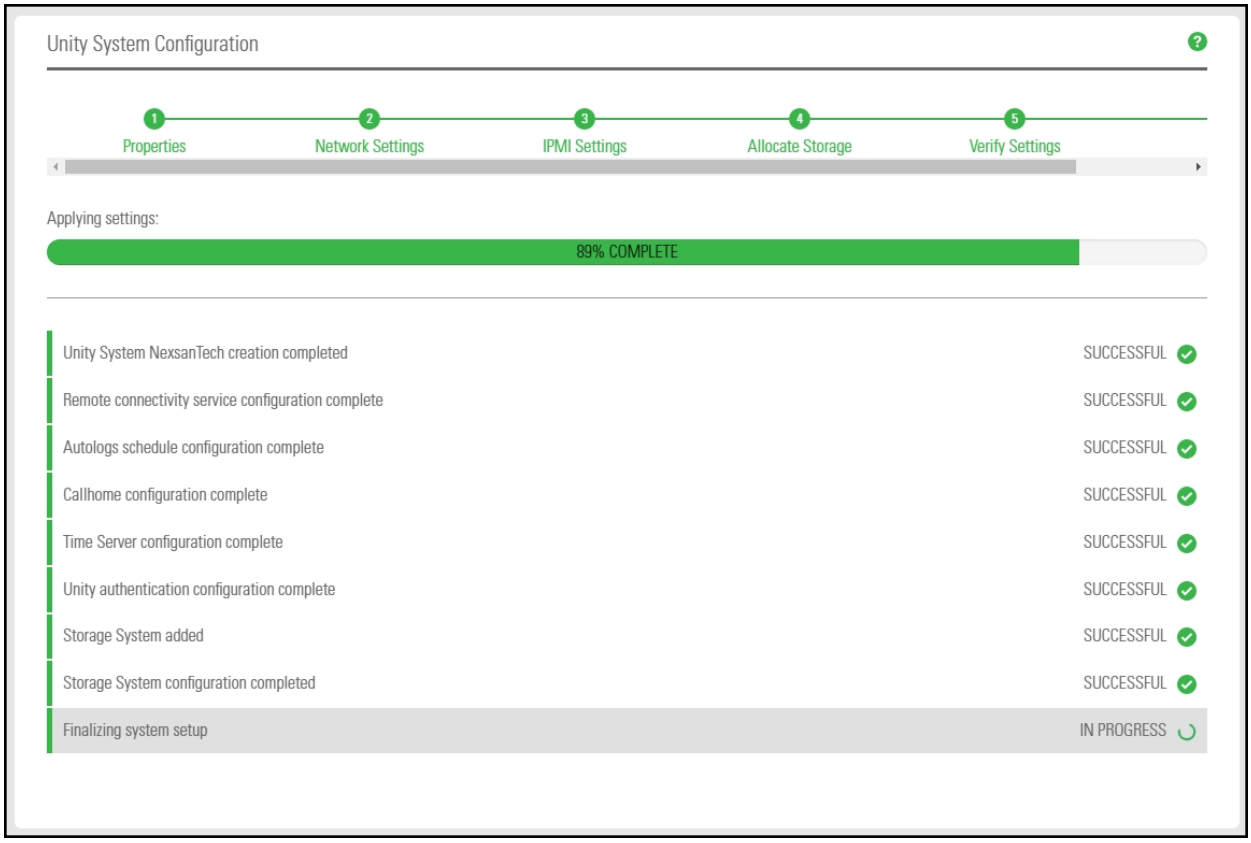
Step 6: Applying configuration settings

This step of the **Unity System Configuration wizard** summarizes your configuration settings and applies them to the system. Review the summary carefully before applying configuration settings.

To apply system settings:

- After you click the **Create** button in the previous step, the System Configuration wizard begins applying your settings, displaying the progress as the wizard configures Unity.

Figure 2-5: Unity System Configuration: Applying the configuration



If a step is unsuccessful, click the error for details.

Starting Unity

Typically, you'll launch Unity from a Web browser.

To launch Unity from a Web browser:

1. On the same network (and subnet) as Unity Storage Systems that you want to manage, enter the Unity management virtual IP address in a Web browser. Use the format `https://<management virtual IP address>/`
2. Enter the login and password set up during discovery. Unity's Web-based interface launches and displays the log on dialog.

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

Browser support

Unity features support for the latest version of these major Web browsers:

Windows	Mac
Chrome	Chrome
Firefox	Apple Safari
Microsoft Edge	

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

Logging on to Unity

You can log on to Nexsan Unity with a user account that has system-level access, or with the Nexsan Unity Administrator account (nxadmin); for more information, see Users and access rights on page 69.

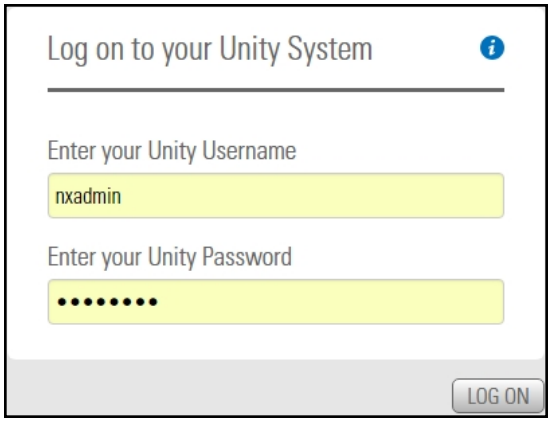
Unity's Web-based user interface uses a self-signed SSL certificate to ensure a secure communication link between the Unity Storage System and the system where Unity is running. When you initially launch Unity, you are required to accept the certificate, and it may be necessary to add the Unity url to 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 with the system default `nxadmin` administrator account. After the initial log on, you can add more users, and use any of these administrator accounts for subsequent log-ins. For more information about adding user accounts, see Users and access rights on page 69.

► To log on with Unity authentication:

1. In the **User name** field, type your user name.

Figure 2-6: Unity login panel



2. In the **Password** field, type your password.
3. Click the **Log on** button. Unity starts loading Unity System and configuration information and displays the main user interface.

► To log on with Active Directory or LDAP authentication:

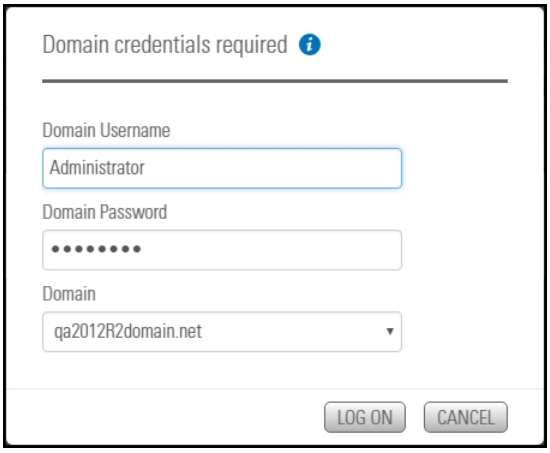
In Active Directory and LDAP implementations, you log in to Unity as nxadmin. Once per session, Unity requests the credentials for those systems for administrative operations on Unity Systems, file systems, and CIFS shares.

Example

1. On the **Unity navigation bar**, select **Storage > File Systems**.
2. Click the **Manage Access Permissions** icon.
3. Enter the AD credentials in the window.

4. Click **Log On**.

Figure 2-7: Example Active Directory login popup



2

Chapter 3

Users and access rights

The Unity user authentication interface protects your Unity Storage Systems—including all your storage pools and underlying file systems—from unauthorized access.

Note In Unity v. 7.4, role-based system and pool administrators are not yet supported in the new graphical user interface. You can however configure role-based administration using the nxcmd CLI. See the "Pool" and "Site" sections of the *Nexsan Unity nxcmd Command-line Interface Reference Guide*, available on the Nexsan.com/support webpage.

This section includes these topics:

User authentication modes 70
Administrator and user permissions 70
Managing Unity user and group access permissions 72
Configuring and managing CHAP authentication 82
Managing permissions for CIFS shares 88

User authentication modes

During the initial setup of your site, you select the that you want to use with your Unity deployment.

Unity supports these user authentication modes:

- **Unity authentication (default):** Unity verifies that, when a user enters a user name and password to log on to Unity, they match the corresponding user name and password stored locally.
- **Microsoft Windows Active Directory domain:** When a user enters a user name and password in the same Unity login window, Unity checks the Microsoft Windows Active Directory server for a matching user record. See Joining a Microsoft Active Directory domain on page 458
- **CHAP authentication:** Challenge-Handshake Authentication users can be set up to restrict iSCSI access to LUNs on Unity Storage Systems. See Configuring and managing CHAP authentication on page 82

CLI only

- **LDAP Directory service (in UNIX/Linux environments):** When a user enters a user name and password in the same Unity login window, Unity checks the LDAP Directory server for a matching user record. See "Connecting to an LDAP directory service" in the *nxadmin Command Line Interface Reference Guide* on the Nexsan.com/support webpage

▶ **To set up local Unity users and groups:**

- Use the Manage Users and Groups panel and Reverting to Unity Authentication on page 475

▶ **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.

Administrator and user permissions

Before assigning access rights and file system-level and CIFS share-level access permissions to users and groups in Unity, it is important to understand the key concepts of Unity user and group accounts, and the access rights of the Unity administrator.

The administrator role has write permissions for all actions available in Unity, while Unity users can only manage resources that they are expressly given access to, either on file systems or CIFs shares.

The Unity Administrator **nxadmin** account is a built-in account that is preconfigured on every Unity Storage System. 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 Administrator account, you can be reset if you are still logged in; otherwise, please call Nexsan Support to reset the password. See Changing the nxadmin password on page 81.

- 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.

Managing Unity user and group access permissions

This section describes how to view and manage Unity user and group access rights in the **Manage Users and Groups** panel.

See also Configuring and managing CHAP authentication on page 82

User Authentication panel 73
Opening the Manage Users and Groups panel 75
Adding a user account 76
Adding a group 78
Managing group membership 79
Deleting a user or a group 80
Changing a user password 80
Changing the nxadmin password 81

3

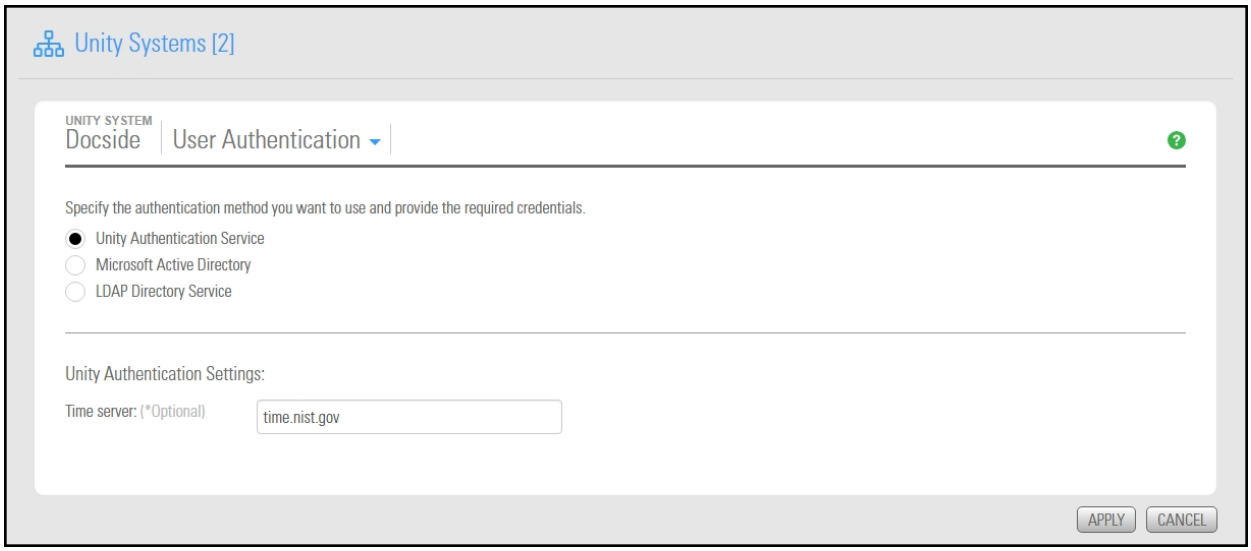
User Authentication panel

Use the **Manage Users and Groups** panel to create and manage users and groups. This panel displays users and groups based on the **User Authentication** options specified for the current Unity Storage System. Authentication is defined in **System > Unity Systems > User Authentication**.

You can define local Unity Authentication, Microsoft Active Directory Authentication, or LDAP User Authentication.

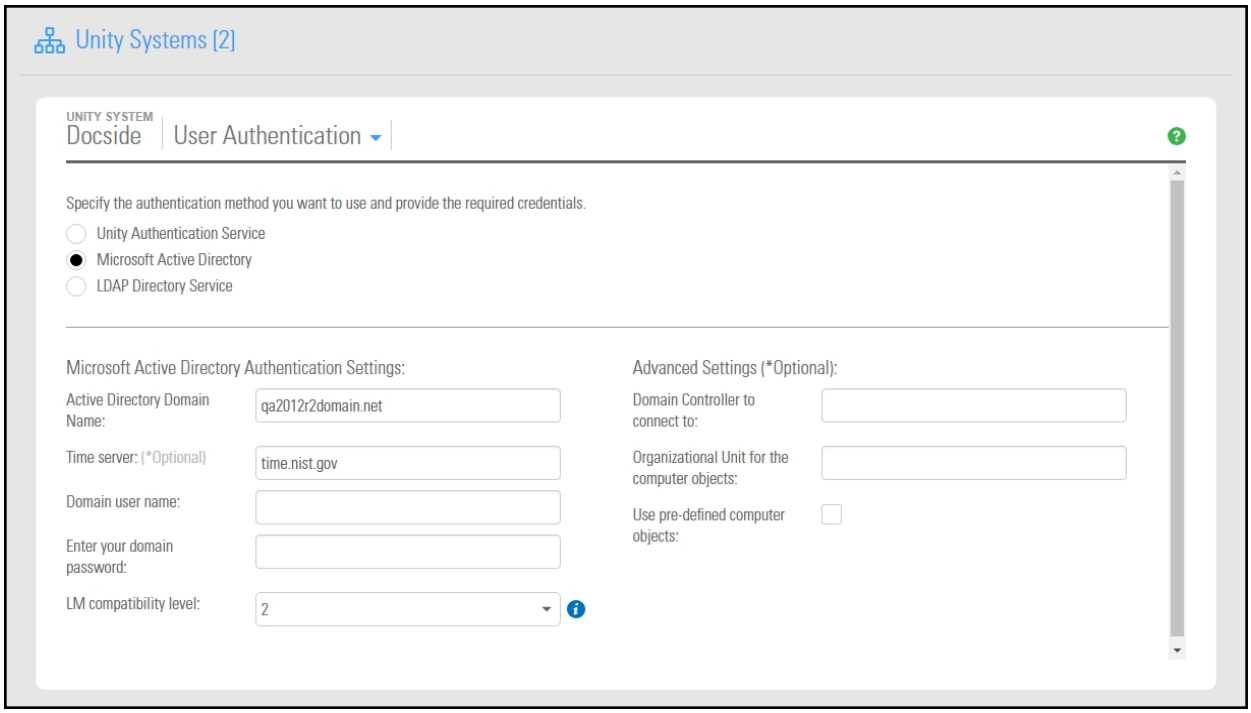
Unity Authentication Service

Figure 3-1: Unity User Authentication



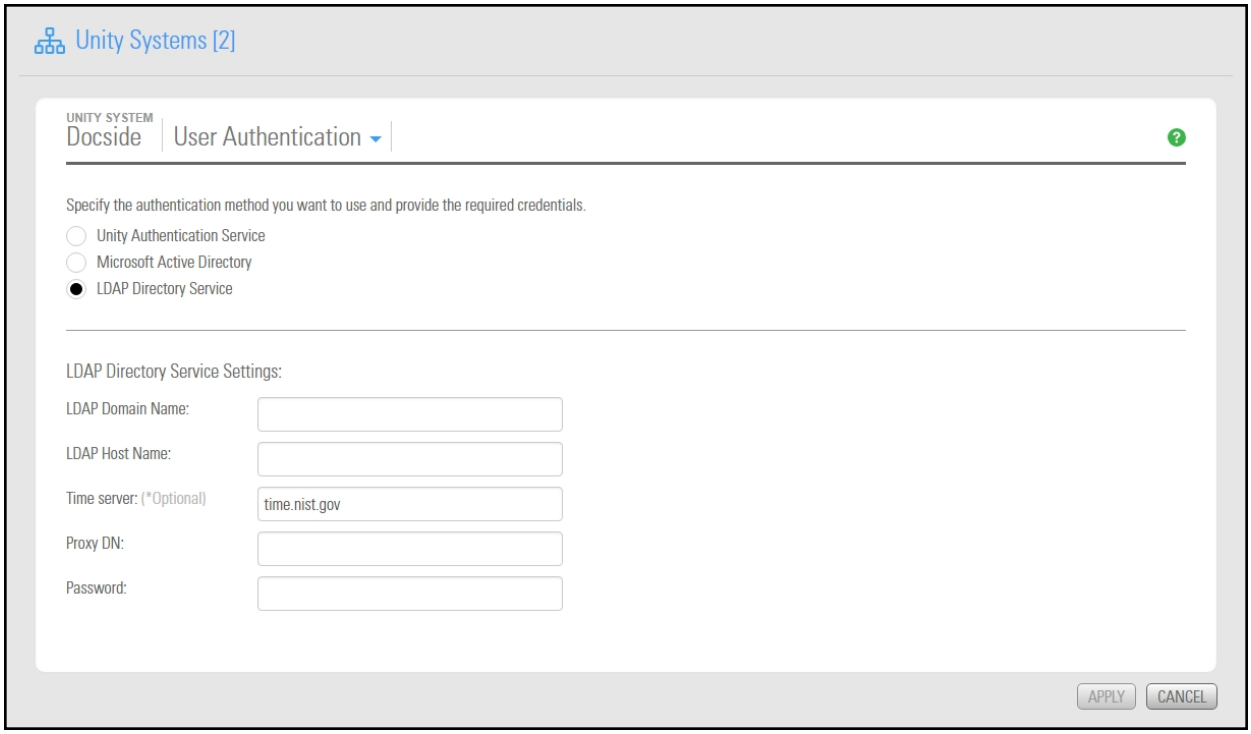
Microsoft Active Directory

Figure 3-2: Active Directory User Authentication



LDAP Directory Service

Figure 3-3: LDAP User Authentication



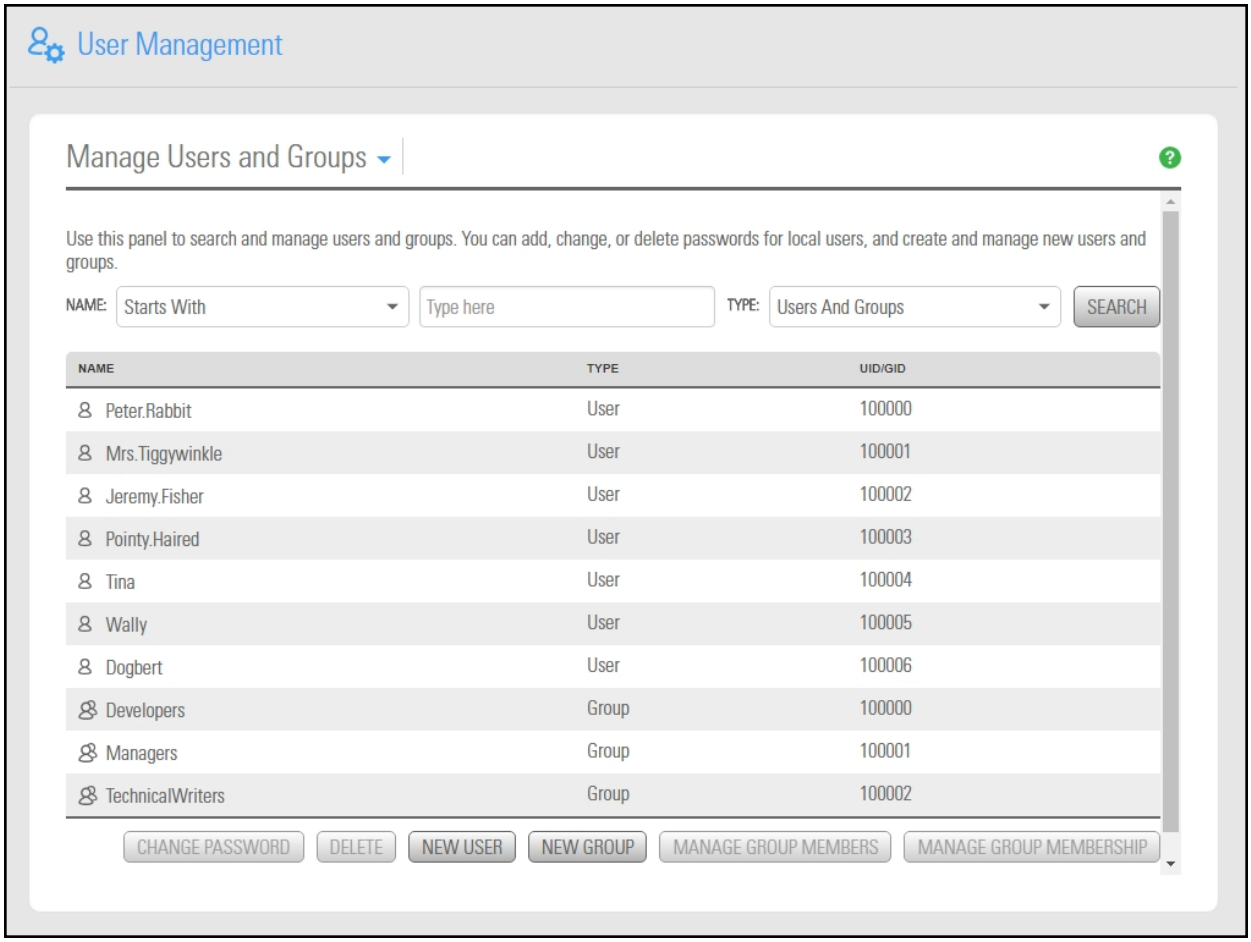
Opening the Manage Users and Groups panel

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

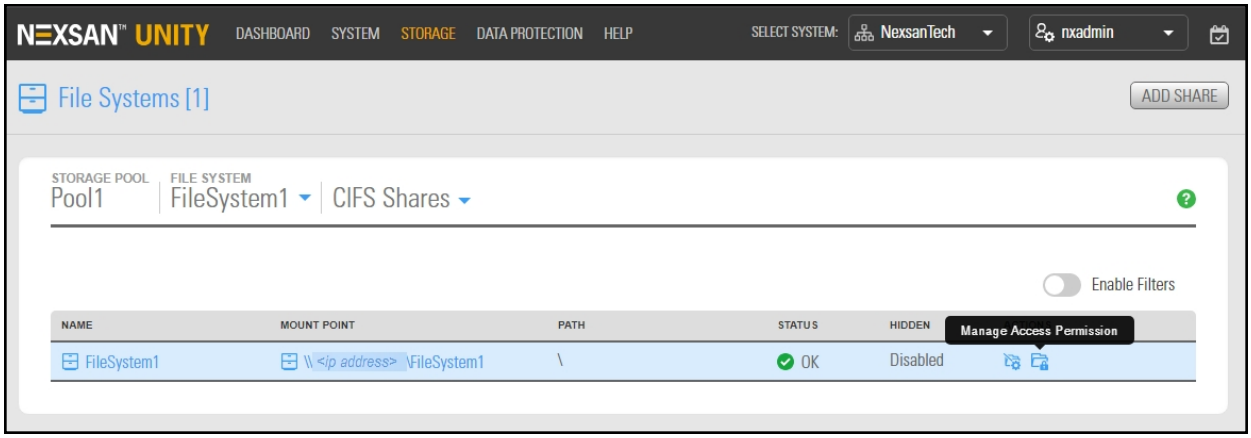
▶ **To access the Manage Users and Groups panel:**

- On the **Unity navigation bar**, select **System > User Management**.

Figure 3-4: Manage Users and Groups panel



Use the **File Systems > CIFS Shares** panel to set user and group access rights and share permissions.



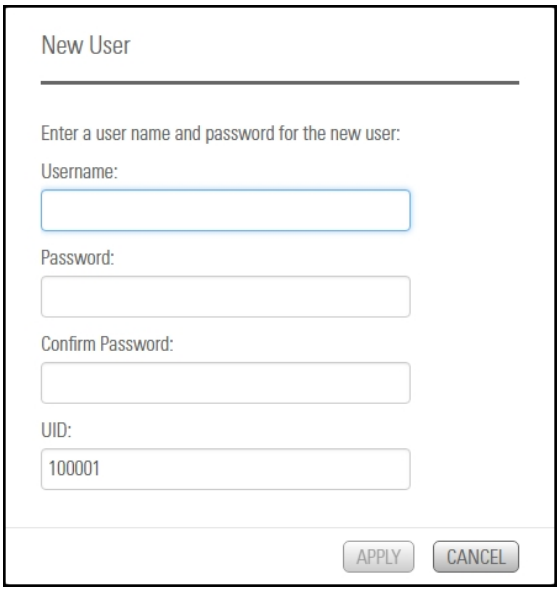
Adding a user account

This section describes how to add a user account to the system using Unity authentication.

► **To add a user account:**

1. On the **Unity navigation bar**, select **System > User Management**.
2. In the **Manage Users and Groups** panel, click **New User**. This displays the **New User** popup window.

Figure 3-5: New User popup window



3. 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, excluding these 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, users are required to enter the user name using the same combination of lower- and upper-case letters that you entered when creating the account.

4. 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 password on page 80.

5. Repeat the password in the **Confirm password** field.

6. 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.

7. Click the **Apply** button. The new user appears in the list of users and groups.

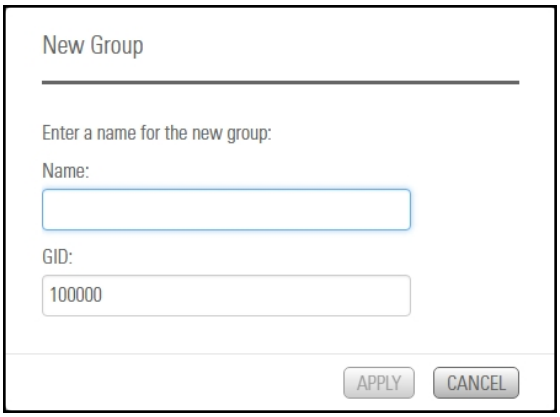
Adding a group

This section describes how to add a group to the system when using Unity authentication.

To add a group:

1. On the **Unity navigation bar**, select **System > User Management**.
2. In the **Manage Users and Groups** view, click **New Group**. This displays the **New Group** popup window.

Figure 3-6: New Group popup window



3. 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, excluding 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.

4. 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.

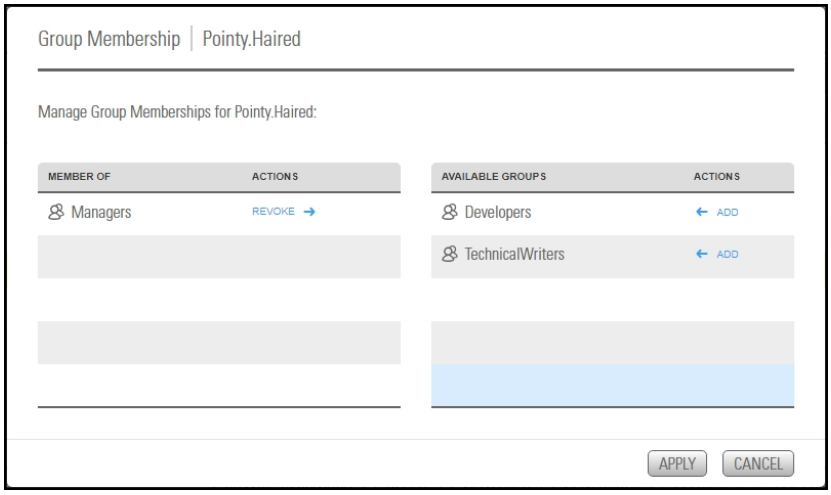
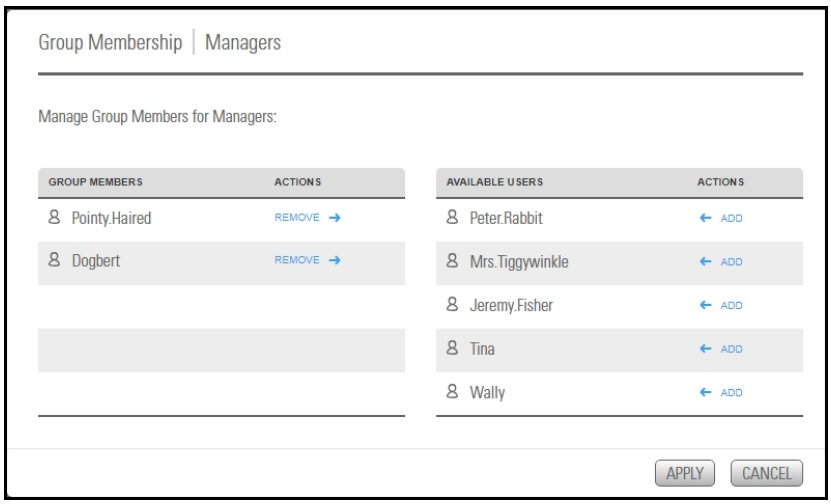
5. Click the **Apply** button. The new group appears in the list of users and groups.

Managing group membership

This section describes how to manage group membership, starting from the group or the user.

▶ **To add a user to a group:**

1. On the **Unity navigation bar**, select **System > User Management**.
2. In the **Manage Users and Groups** view, perform one of the following actions:

To...	Do this
Manage group membership for a user	a. Select a user. b. Click **Manage Group Membership**. c. Add or revoke group membership for the user. 
Manage group members	a. Select a group. b. Click **Manage Group Members**. 

3. Click the **Apply** button.

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:

1. On the **Unity navigation bar**, select **System > User Management**.
2. In the **Manage Users and Groups** view, select a user or group.
3. Click **Delete**.
4. Type **delete** in the confirmation window.

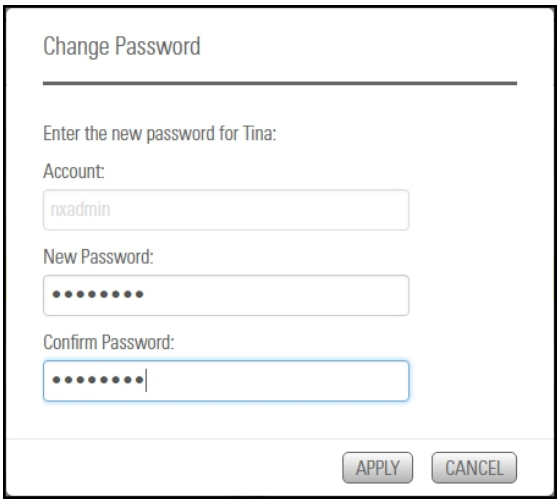
Changing a user password

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

To change a user password:

1. On the **Unity navigation bar**, select **System > User Management**.
2. In the **Manage Users and Groups** view, select the user you want to change the password for.
3. Click **Change Password**. The **Change Password** view opens.

Figure 3-7: Changing a user password



4. 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 password above.

5. Repeat the password in the **Confirm password** field.
6. Click the **Apply** button to set the new password.

Changing the nxadmin password

This section describes how to change the password for the nxadmin, the built-in Unity administrator account.

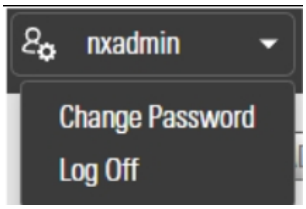
Prerequisites

To perform this procedure, you must already be logged in to Unity. If you are locked out and you do not remember your password, please call Nexsan Support for assistance.

To change the nxadmin password:

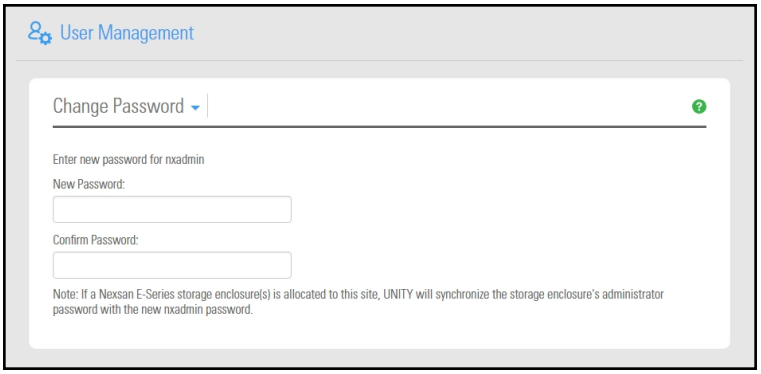
1. On the **Unity navigation bar**, select **nxadmin > Change Password**. The **Change Password** panel opens.

Figure 3-8: Navigation bar Change Password



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

Figure 3-9: Change Password panel



3. 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 Unity 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 the **Apply** button to set the new password.

Configuring and managing CHAP authentication

iSCSI initiators and targets prove their identity to each other using CHAP.

Note This section does not apply to Fibre Channel initiators.

Unity's iSCSI implementation provides three levels of CHAP authentication:

- Unity System-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. Unity System-level CHAP authentication works independently of both one-way CHAP authentication and mutual CHAP authentication.

This section includes these topics:

Creating CHAP users on the facing page
Deleting a CHAP user on page 87
Changing a CHAP user secret on page 85
Setting CHAP authentication for a target on page 86

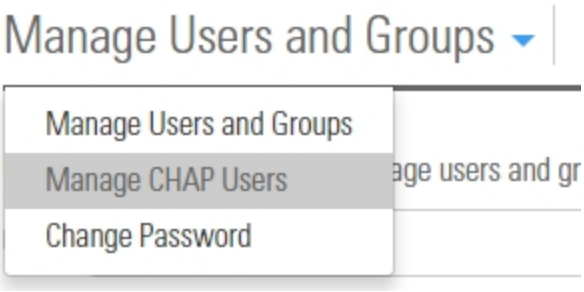
Creating CHAP users

This section describes how to create CHAP users. Use CHAP (Challenge-Handshake Authentication Protocol) users to restrict iSCSI access to LUNs on Unity. Create CHAP users by specifying a user name and secret (password) for each user.

To add a user account:

1. On the **Unity navigation bar**, select **System > User Management**.
2. If you are using the **Unity Authentication Service**, select **Manage Users and Groups > Manage Chap Users**.

Figure 3-10: Manage Users drop down



If you are using **Microsoft Active Directory** authentication, continue to step 3.

The Mange CHAP Users panel opens.

3. Enter the new user name in the **CHAP User name** box.

   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.

4. Enter the CHAP secret.

   The CHAP secret must be between 12 and 16 characters long, and you must use a combination of lower case and upper case letters and numbers, and include at least one space or special characters.

   As an example, this is a valid password:

   ITUnow$ITUnow$

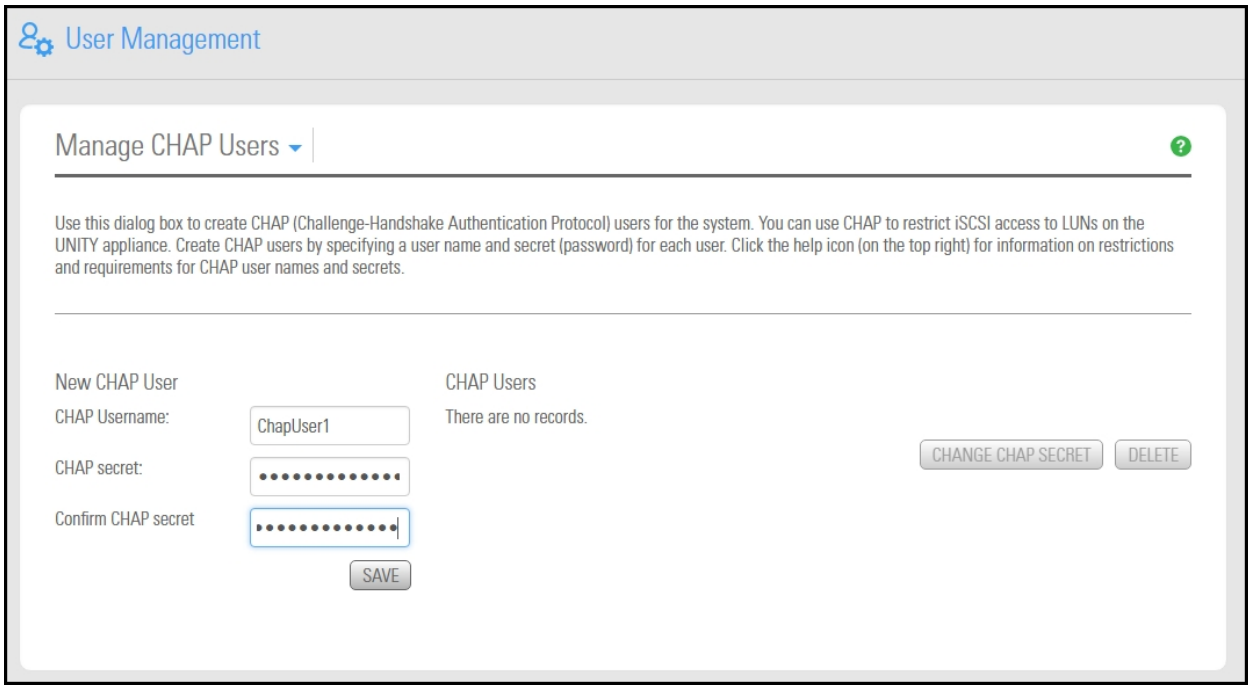
   But this is **not** a valid password:

   ITUnowITUnow

   Notes:

   - 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 the user forgets the password, it cannot be recovered. However, the password can be reset; see .

Figure 3-11: Manage CHAP Users panel



5. Repeat the password in the **Confirm CHAP secret** field.
6. Click the **Save** button. The new CHAP user appears in the list of users and groups.

Changing a CHAP user secret

This section explains how to change a CHAP user secret.

CAUTION: It is not recommended to change 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 change a CHAP user secret:**

1. On the **Unity navigation bar**, select **System > User Management**.
2. Select **Manage Users and Groups > Manage Chap Users**.
3. From the CHAP users list, select the CHAP user that you want to change the secret for.
4. Click the **Change Chap secret** button. The Change Chap Secret window opens.

Figure 3-12: Change CHAP Secret window



5. Enter the CHAP secret.

   The CHAP secret must be between 12 and 16 characters long, and you must use a combination of lower case and upper case letters and numbers, and include at least one space or special characters.

   As an example, this is a valid password:

   ITUnow$ITUnow$

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

   ITUnowITUnow

   Note If the user forgets the password, it cannot be recovered. However, the password can be reset; see .

6. Repeat the password in the **Confirm CHAP secret** field.
7. Click the **Apply** button to complete your changes.

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:**

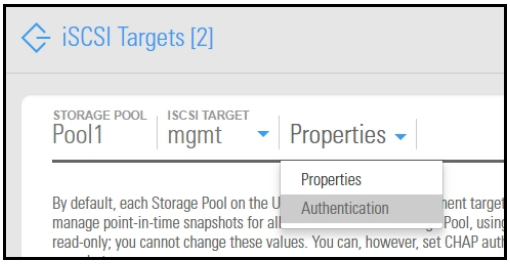
1. On the **Unity navigation bar**, select **Storage > iSCSI Targets**.

Figure 3-13: iSCSI Targets panel

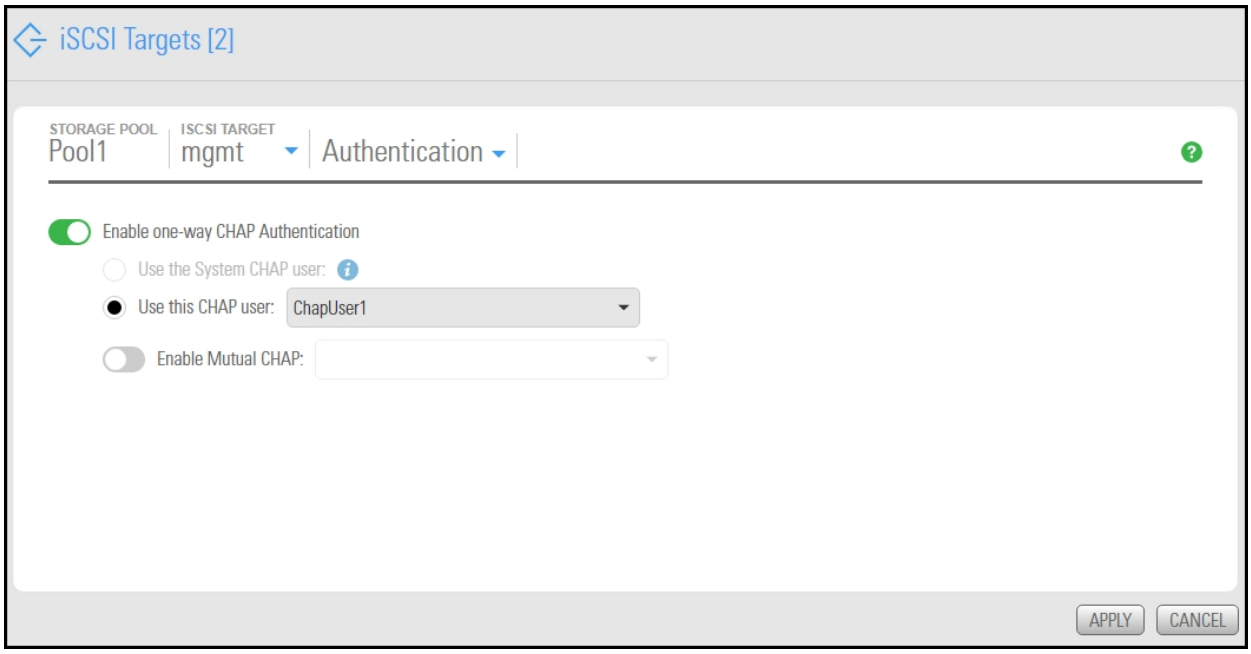


2. Click the **Public Alias** link to open the target's **Authentication** panel.
3. Select **Properties > Authentication**.

Figure 3-14: iSCSI targets panel—Authentication



4. Select **Enable one-way CHAP authentication** for the target.



5. To enable one-way CHAP authentication, **Use this CHAP user** and select a user.
6. To enable mutual CHAP authentication, select the **Enable 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.

Deleting a CHAP user

This section explains how to delete a CHAP user.

CAUTION: It is not recommended to delete *active* CHAP users from the system—specifically, CHAP users that are assigned to the Unity System, or to targets on Unity for CHAP authentication. Initiators that have these CHAP users set for authentication to lose their connection to any corresponding LUNs on Unity.

To delete a CHAP user:

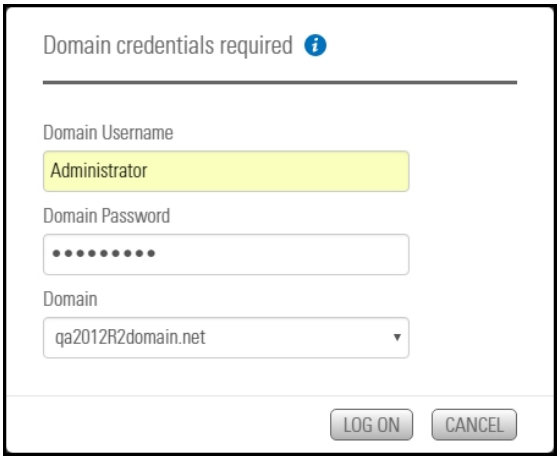
1. On the **Unity navigation bar**, select **System > User Management**.
2. Select **Manage Users and Groups > Manage Chap Users**.
3. From the CHAP users list, select the CHAP user that you want to delete from the system.
4. Click the **Delete** button.
5. Type **Delete** in the box and click the **Delete** button to confirm. Unity removes the CHAP user from the list of users on the system.

Managing permissions for CIFS shares

This section shows how to view and manage CIFS share permissions if using Microsoft Active Directory.

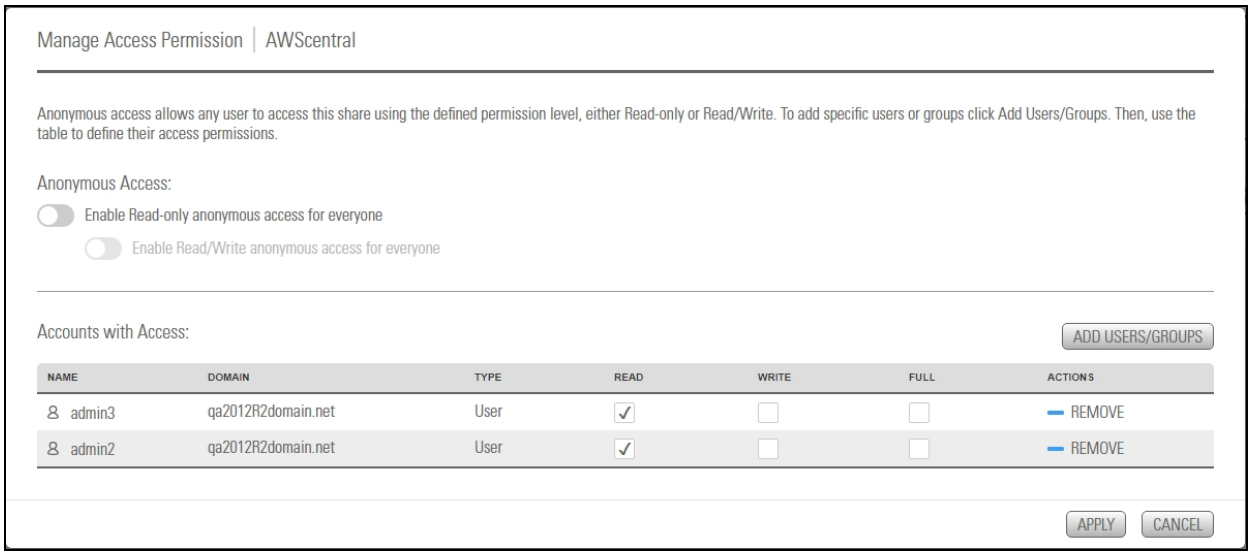
To view and manage user or group access rights:

1. From the **Unity navigation bar**, select **Storage > File Systems**.
2. Click **Summary > CIFs Shares**.
3. Click the **Manage Access Permissions** icon.



4. Enter the AD administrator user name and password when prompted and click the **Log On** button.
5. Click **Add Users/Groups**. Unity displays available **Active Directory** users and groups.
6. Select the user or group that you want to add and click the **Apply** button.
7. Select **Read**, **Write** or **Full access** for each user and group as required.

Figure 3-15: Manage Access Permission panel



8. Repeat step 5, as necessary. When done, click the **Apply** button.

Chapter 4

Storage pools

A storage pool (also referred to as a "pool") groups disks into volumes, to which you can add file systems, LUNS, and object stores.

With storage pools, you can:

- 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 includes wizard-based configuration tools to help you create a storage pool, and then add file systems, LUNs, and object stores within that pool.

This section includes these topics:

Adding a storage pool 90
Scrubbing a storage pool 94
Adding volumes to a storage pool 98
Adding volumes to a replicated storage pool 99
Replacing a volume in a storage pool 99
Modifying storage pool snapshot auto-deletion 100
Configuring data compression on a storage pool 102
Configuring access time on a storage pool 103
Viewing space usage information for storage pools 105
Setting space usage notification thresholds for a storage pool 105
Changing a pool resource group 107
Managing FASTier cache devices 108
Viewing and clearing storage pool errors 110
Deleting a storage pool 114

Adding a storage pool

Unity provides the **Create a Storage Pool** wizard to guide you through the process of creating a storage pool.

Before you begin

You may want to add user accounts for file system-level access; you can then configure the relevant access permissions when you create file systems.

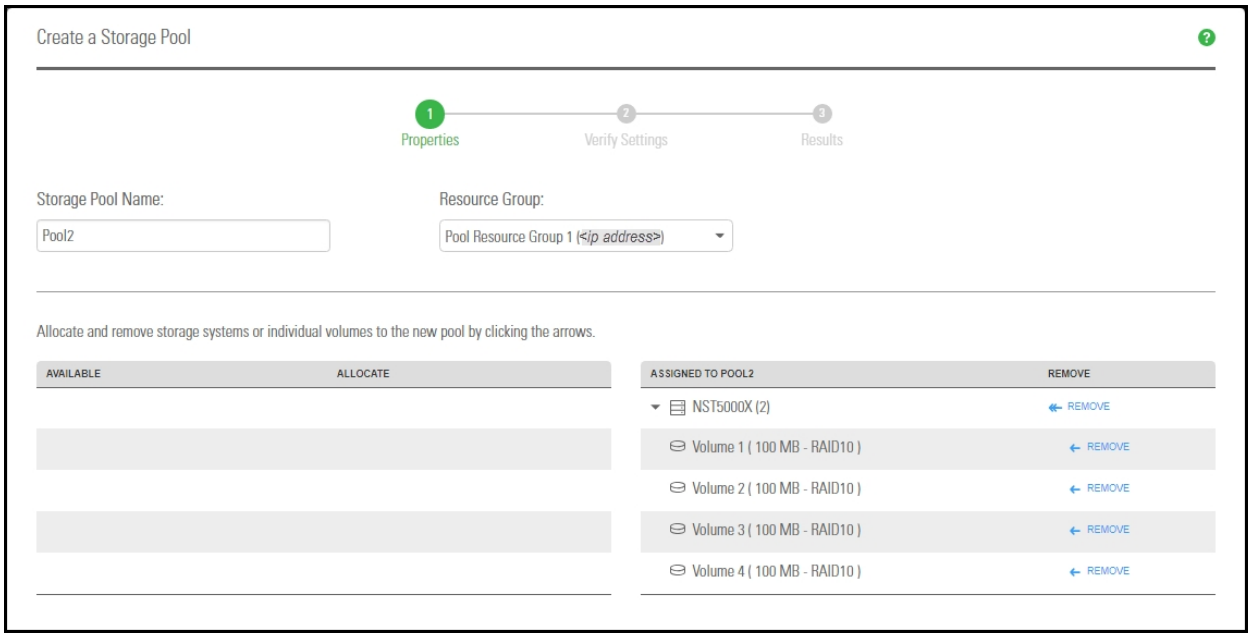
How to allocate storage with Unity

- 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 (to Windows-based systems), (to UNIX/Linux-based systems), or using both 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 the 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.

To create a storage pool:

1. On the **Unity navigation bar**, click **Storage > Storage Pools**.
2. In the **Storage Pools** panel, click **Add Storage Pool**. The **Create a Storage Pool** wizard opens.
3. In the **Available** listing, select a storage system or volume and click **Allocate** to add storage systems or volumes to the pool.

Figure 4-1: Create a Storage Pool: Properties



4. Optionally, change either of the following:
   a. the **Storage Pool** name.
   b. the **Resource Group** that you want to assign the storage pool to.

   Click the **Next** button.
5. If the new pool has FASTier drives, specify whether they should be used for **READ** or **WRITE** (see "Assigning FASTier devices," below). Click the **Next** button.
6. Verify your settings and click the **Create** button.

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.

For more information about FASTier cache devices, please contact your Nexsan reseller or Nexsan Support Representative.

Next steps

After the pool is created, these are typical follow-on tasks:

- Creating another storage pool
- Adding a file system on page 117
- Creating a LUN on page 236
- Creating an object store on page 336

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 4-1: Storage systems and volume combinations

Storage systems	Volume mixing supported
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
UNITY NV4000, UNITY NV6000, UNITY NV10000 (all three with internal storage) and Unity Storage Expansions (U2G424 Expansion, U2G460 Expansion, U2G478 Expansion)	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)	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 4-2: 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)

[1] Inherited from storage pool update

[2] Inherited from storage pool creation

Table 4-3: 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[1]	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)

Scrubbing a storage pool

Unity provides a mechanism that checks for and repairs read and write errors to the meta data that comprise Unity storage pools and volumes. This is called "pool scrubbing". Performing routine scrubbing on a storage pool prevents parity errors and data corruption.

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.

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

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

This section includes these topics:

- Performing a manual pool scrub on the facing page
- Modifying the scrub schedule for a storage pool on page 96

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

Performing a manual pool scrub

Tip You can also initiate a manual pool scrub on a storage pool's replica on remote Unity Storage Systems see the *Nexsan Unity Snapshots and Replication Guide*.

WARNING: A Storage Pool scrub operation can consume significant system resources, depending on the amount of data to be processed, and can only proceed as fast as the corresponding storage system disks allow. It is strongly recommended to schedule pool scrub operations during off-peak business hours to prevent performance degradation on the system.

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

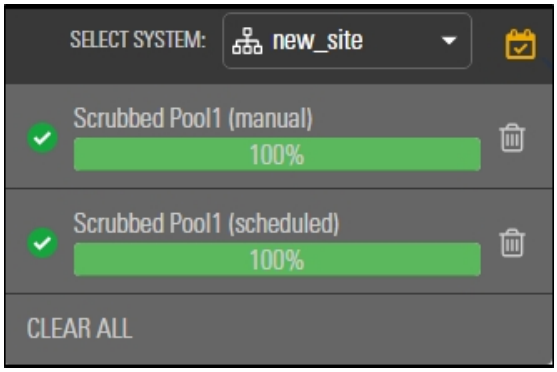
1. On the **Unity navigation bar**, select **Storage > Storage Pools**.
2. In the main **Storage Pools** panel, open the **Storage Pool** that you want to scrub.
3. In the **Storage Pools** properties panel, click the **Scrub Pool** button. The **Manual Pool Scrub Initiated popup window** opens, displaying a warning about

Figure 4-2: Manual Pool Scrub Initiated popup window



4. When you are ready to proceed, click the **Scrub Pool Now** button to start the scrubbing operation.

Unity starts the pool scrub operation. The progress of the scrub operation is displayed in the **Tasks in progress** panel on the **Unity navigation bar**. Click the tasks icon to display progress.



If needed, you can stop the pool scrub operation by selecting the relevant task in the **Tasks in progress** panel, and clicking the **Stop** 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 Unity System, Unity enables scheduled pool scrubbing.

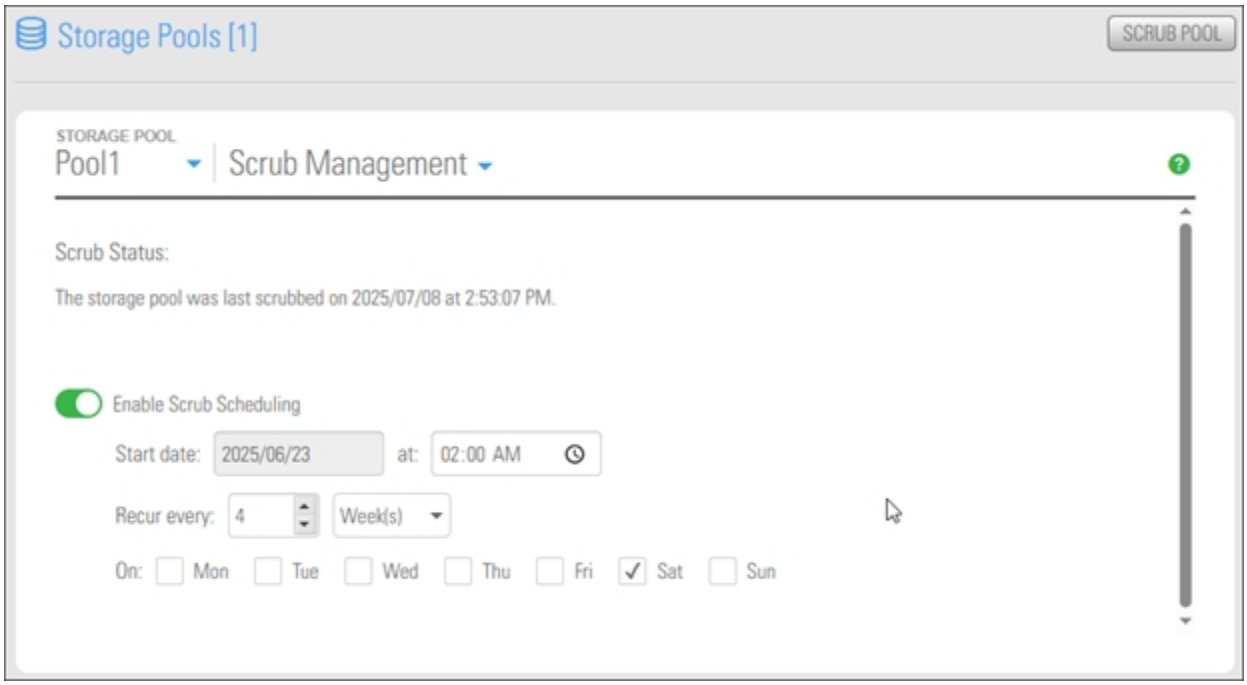
Pool scrubbing is scheduled once every 4 weeks, on Saturday, at 02:00 AM. The default schedule assumes that 02:00 AM on Saturdays is an off-peak business hour—an ideal time to perform pool scrub operations. If you change the default schedule, we recommend that you schedule scrub operations during off-peak 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. On the **Unity navigation bar**, select **Storage > Storage Pools**.
2. In the main **Storage Pools** panel, open the **Storage Pool** that you want to set the scrub schedule for.
3. Select **Summary > Scrub Management**. The **Scrub Management** panel opens, showing the last time the pool was scrubbed and the current schedule.

Figure 4-3: Storage Pools Scrub Management panel



4. To modify the scrub schedule for the storage pool:
   a. Enter a new recurrence value in the **Recur Every** field.
   b. Modify the weekday or time Unity to perform pool scrub operations on the storage pool.

   Alternatively, you can click the **Enable Scrub Scheduling** button to disable scheduled pool scrubbing.
5. When you finish modifying the scrub schedule for the storage pool, click the **Apply** button 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** 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

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 the facing page.

Prerequisites

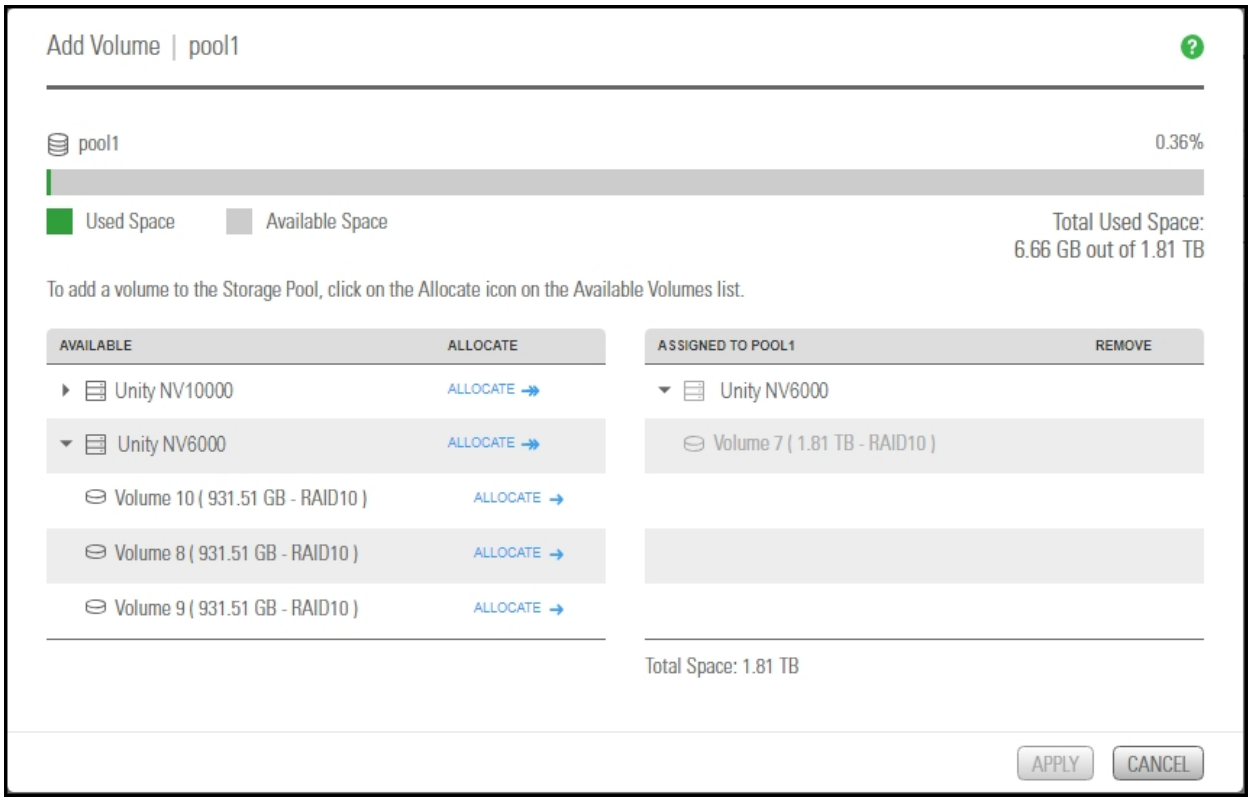
- Before you begin this procedure, ensure that you have an available unmapped volume on the primary or remote Unity Storage System.

To add volumes to a storage pool:

1. On the **Unity navigation bar**, select **Storage > Storage Pools**.
2. In the main **Storage Pools** panel, open the **Storage Pool** that you want to add volumes to.
3. Select **Summary > Volumes**. The **Volumes** panel opens, showing the existing volumes in the storage pool and connected Unity Storage Systems.
4. Click the **Add Volumes** button to open the **Add Volume** popup.

   Note For performance considerations, we highly recommend that you only add volumes with the same RAID level as the existing volumes in the storage pool. See Mixing volumes with different RAID levels on page 92.

Figure 4-4: Add Volume popup



5. In the **Available** list, expand a storage system to display its available volumes, as shown.
6. Select the volume that you want to add to the storage pool, and click **Allocate** to assign it to the pool.
7. Click the **Apply** button when you finish allocating volumes. Unity adds the volumes to the storage pool.

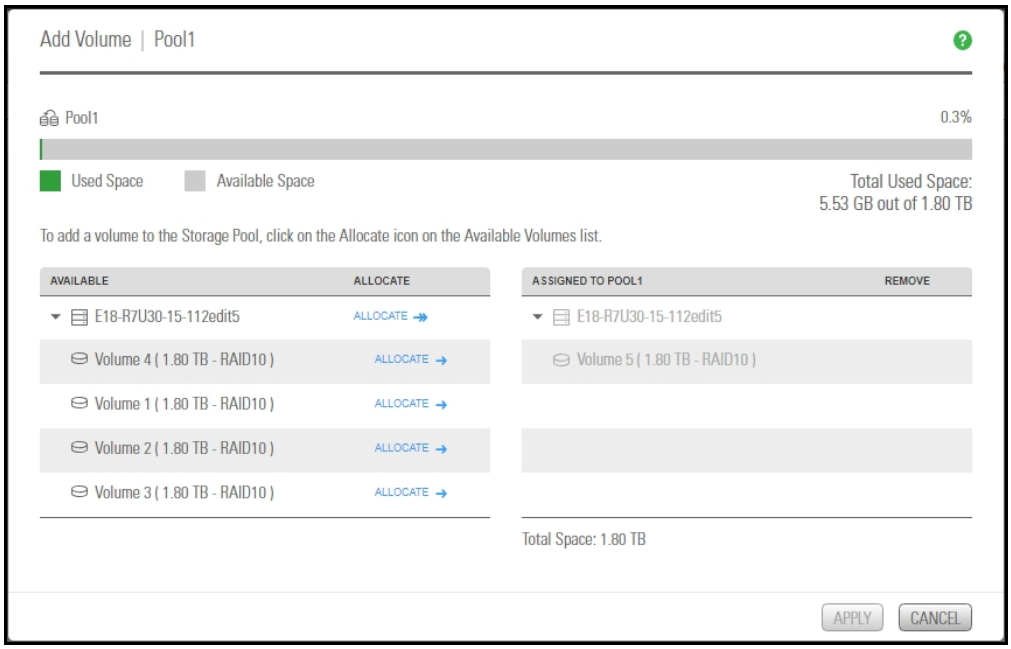
Adding volumes to a replicated storage pool

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. Select the Unity System where you want to add volumes to a storage pool.
2. On the **Unity navigation bar**, select **Storage > Storage Pools**.
3. Under **Actions**, click the **Add Volume** icon The Add Volumes popup opens.



4. Click the down arrow on the left side of the table to expand the available storage.
5. Click **Allocate** next to the volumes you want to add to move it to the right, indicating that it will become an assigned pool.
6. Click the **Apply** button to complete the process.

Replacing a volume in a storage pool

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

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

To replace a volume:

1. On the **Unity navigation bar**, select **Storage > Storage Pools**.
2. In the **Storage Pools** panel, click the link to the pool you want to change.
3. Click **Summary > Volumes**.
4. Select the volume to be replaced from the list.
5. 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/BEAST 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 systems connected to Unity. For performance considerations, we highly recommend that the replacement volumes you select has the same RAID level as the volumes you are replacing; see Mixing volumes with different RAID levels on page 92.
6. In the **Available Volumes:** list on the **Replace Volume** panel, expand a storage system to display its available volumes.
7. 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.
8. Click the **Apply** button.
9. 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 110.

Modifying storage pool snapshot auto-deletion

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.

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

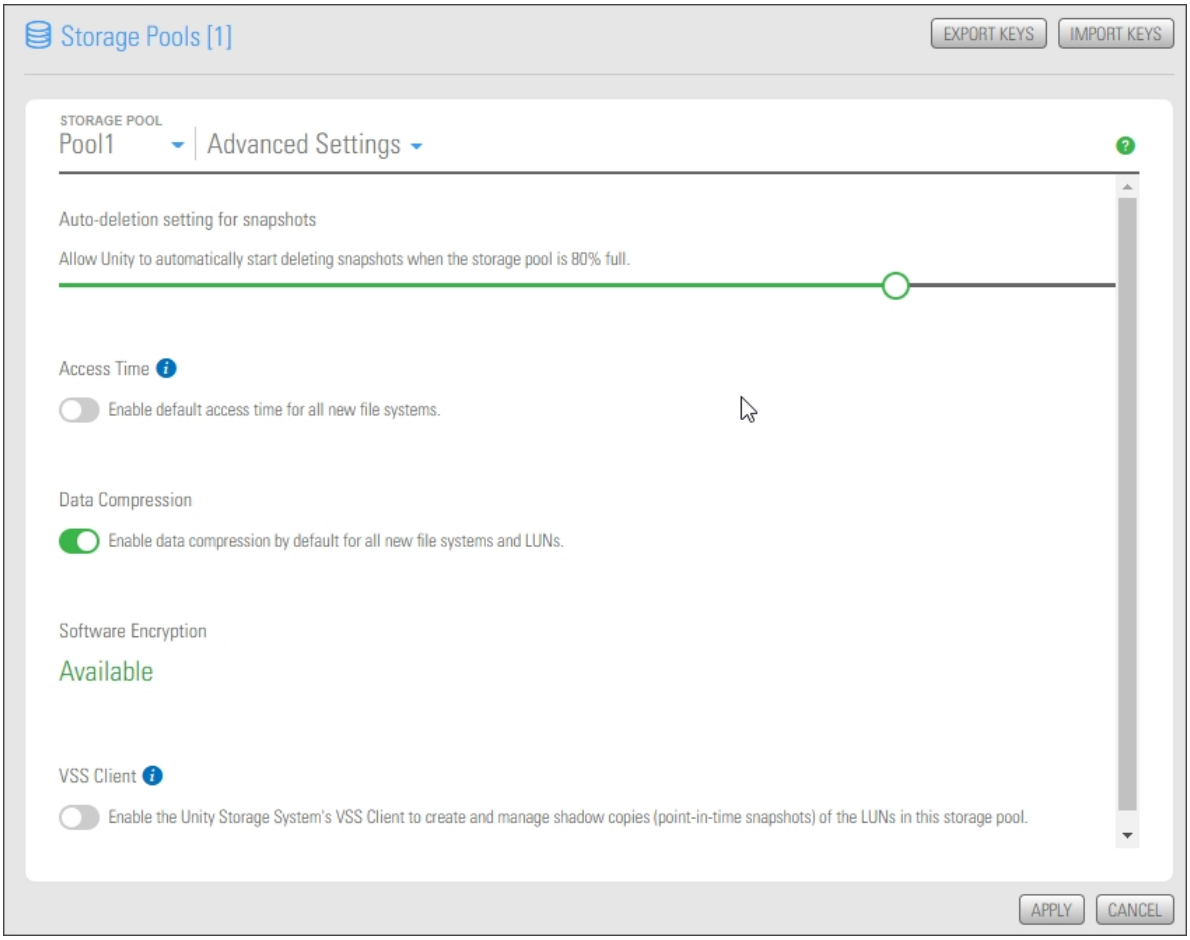
Unity ONLY deletes snapshots for datasets (file systems and iSCSI LUNs) that have the snapshot auto-deletion function enabled.

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. On the **Unity navigation bar**, select **Storage > Storage Pools**.
2. Click the link to the pool that you want to update.
3. In the **Storage Pools** panel, click **Summary > Advanced Settings**.

Figure 4-5: Advanced Settings



4. Drag the slider to the left to decrease the percentage of the storage pool capacity at which snapshots will be auto-deleted or to the right to increase the percentage.
5. When you finish modifying the snapshot auto-deletion setting for a storage pool, click the **Apply** button.

Configuring data compression on a storage pool

You can enable compression at the pool level on Unity. Any new dataset (file systems or LUNs) created in that pool will inherit the pool settings, and thus will also have compression enabled. Existing datasets are not affected. To enable or disable compression on a specific file system or LUN, see Configuring data compression on a LUN on page 251 or Enabling or disabling data compression on a file system on page 142.

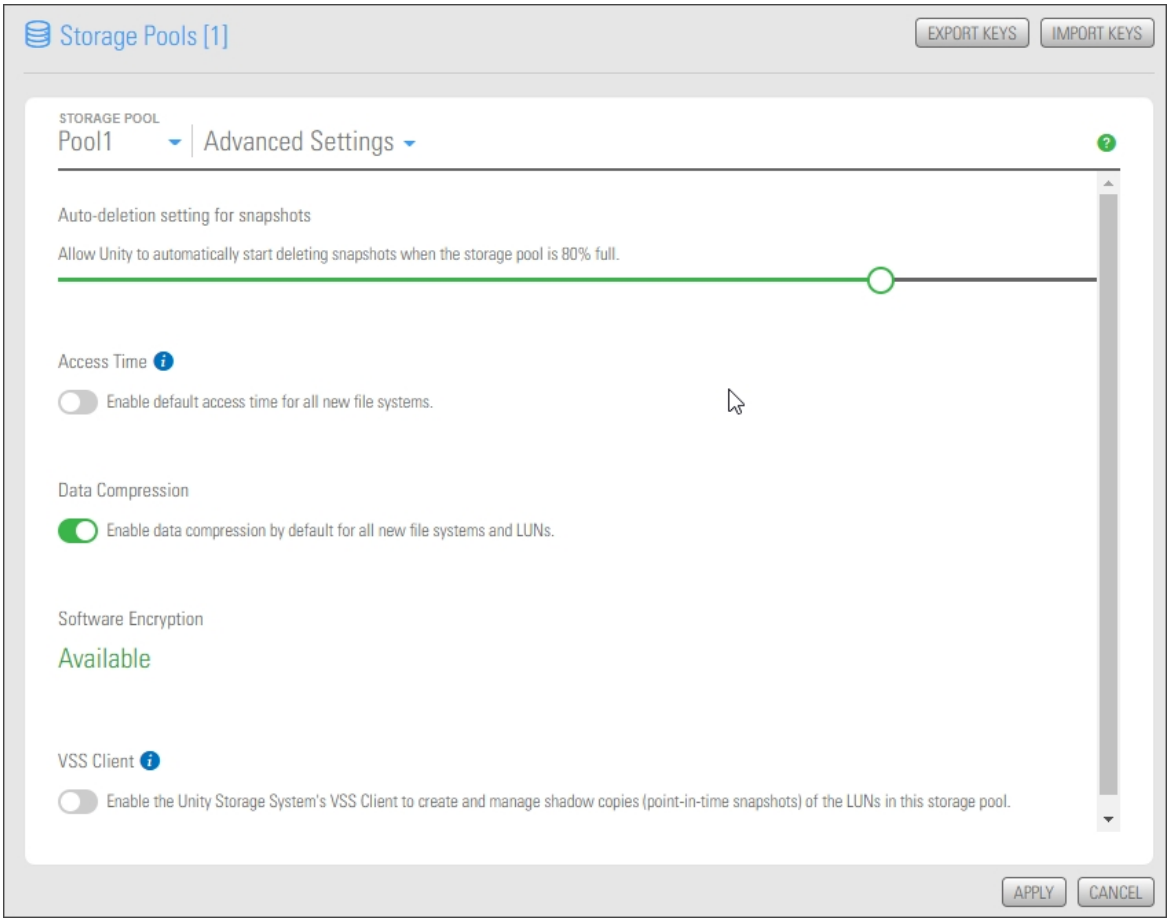
Compression allows for better performance of the storage pool since the files to read/write are much smaller. However, it will also increase CPU usage. Compression can be enabled or disabled at any time. Disabling data compression affects all new data written to the storage pool; existing data remain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

To configure compression for a storage pool:

1. On the **Unity navigation bar**, select **Storage > Storage Pools**.
2. Click the link to the pool that you want to update.
3. In the **Storage Pools** panel, click **Summary > Advanced Settings**.

Figure 4-6: Advanced Settings



4. Click the **Data Compression** button to enable or disable default data compression.
5. Click the **Apply** button to save your changes.

Configuring access time on a storage pool

The Access Time setting specifies whether the access time for files is updated when during read operations. By default, Access Time mode is disabled, which avoids producing write traffic when reading files, and results in significant performance gain.

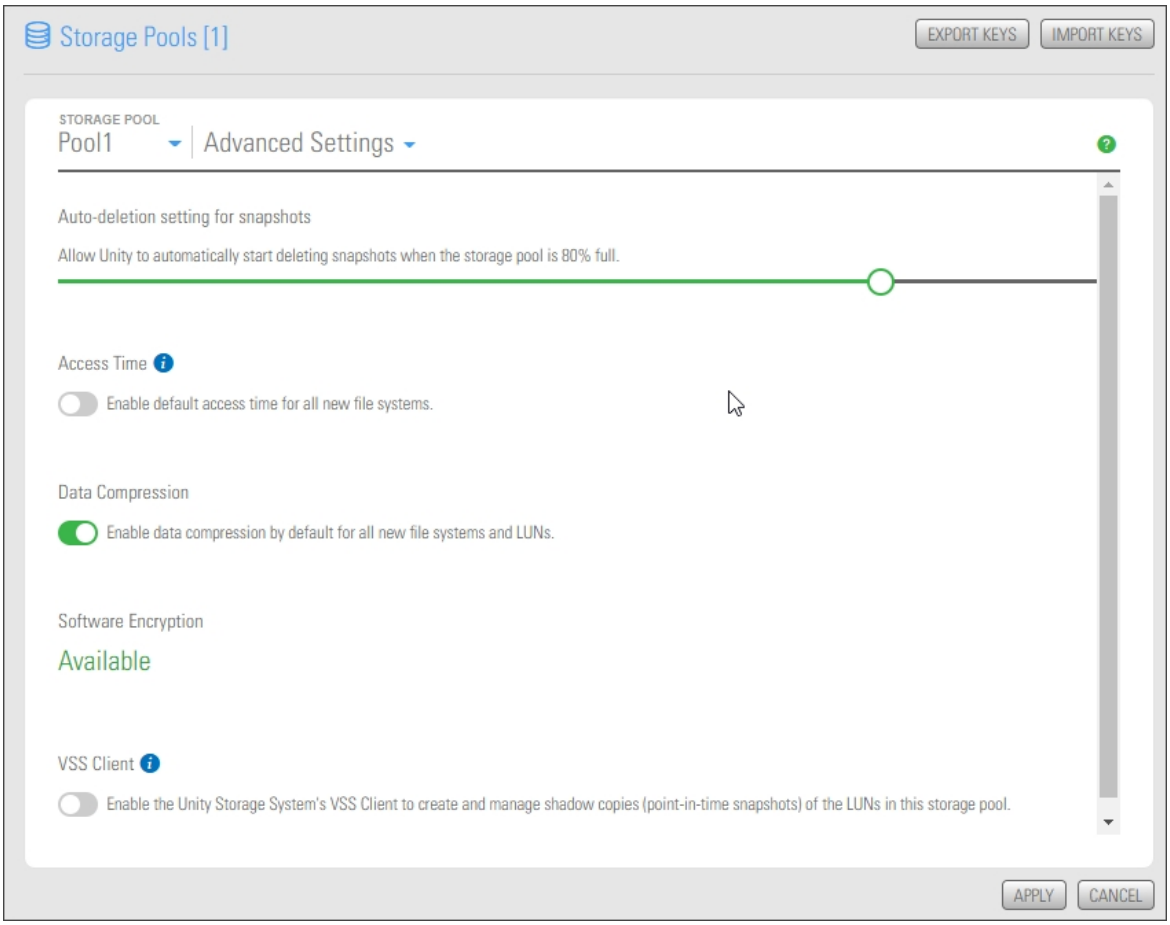
Access Time can be set at the file system level or pool level, and modified at any time. To enable Access Time for a specific file system, see Enabling the Access Time mode on a file system on page 144.

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 pools will inherit the pool settings; however, replicated file systems always keep the Access Time mode disabled.

To enable the Access Time mode for a pool:

1. On the **Unity navigation bar**, select **Storage > Storage Pools**.
2. Click the link to the pool that you want to update.
3. In the **Storage Pools** panel, click **Summary > Advanced Settings**.

Figure 4-7: Advanced Settings



4. Click the **Enable Access Time** button  to enable the setting.
5. Click the **Apply** button to save your changes.

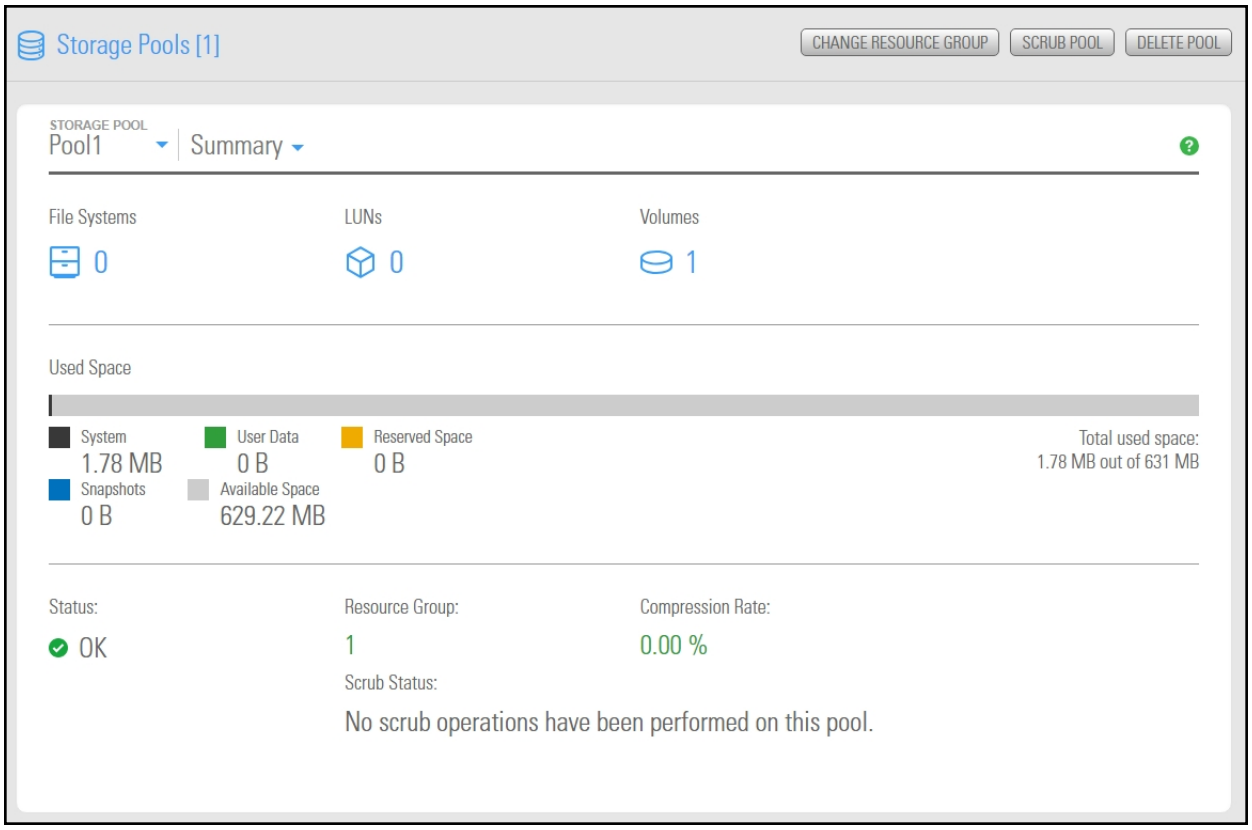
Viewing space usage information for storage pools

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. On the **Unity navigation bar**, select **Storage > Storage Pools**.
2. Select the link to the storage pool that you want to view. The **Storage Pools Summary** panel opens.

Figure 4-8: Storage Pools, Summary panel



Related topics:

Setting space usage notification thresholds for a storage pool below

Adding volumes to a storage pool on page 98

Increasing storage capacity for object stores on page 344

Setting space usage notification thresholds for a storage pool

Unity enables 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.

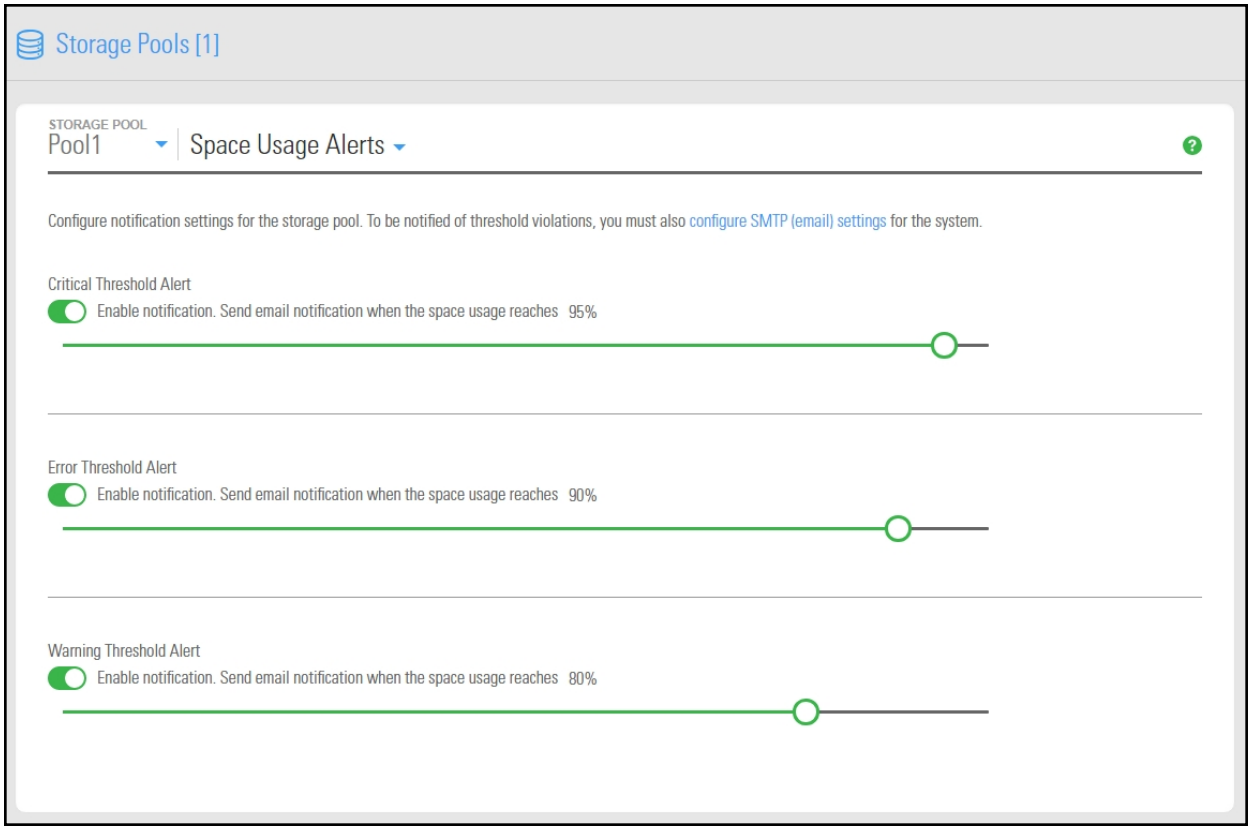
- Error: An email notification is triggered when the space consumption in the storage pool reaches the value that you set for this threshold. An email notification is triggered again when space consumption exceeds this threshold. The default error threshold is set to 90% of the total available disk space 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 Unity Storage System; for more information, see Event logging and notification on page 557.

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

1. On the **Unity navigation bar**, select **Storage > Storage Pools**.
2. Select the link to the storage pool that you want to configure.
3. In the **Storage Pools** panel, click **Summary > Space Usage Alerts**.

Figure 4-9: Space Usage Alerts



4. Adjust the **Critical Threshold Alert** percentage by moving the slider to the left, which will issue the email alert to you at a lower percentage, or the right, to set the email alert to be sent at a higher percentage of total space usage. The default is 95 per cent.

5. Adjust the **Error Threshold Alert** percentage by moving the slider to the left, which will issue the email alert to you at a lower percentage, or the right, to set the email alert to be sent at a higher percentage of total space usage. The default is 90 per cent.
6. Adjust the **Warning Threshold Alert** percentage by moving the slider to the left, which will issue the email alert to you at a lower percentage, or the right, to set the email alert to be sent at a higher percentage of total space usage. The default is 80 per cent.

Changing a pool resource group

You can move a storage pool from its current Pool Resource Group on one controller to the Pool Resource Group on the peer controller.



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 (file systems, LUNs, object stores) 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 file system, LUN, and object storel 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 386.

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

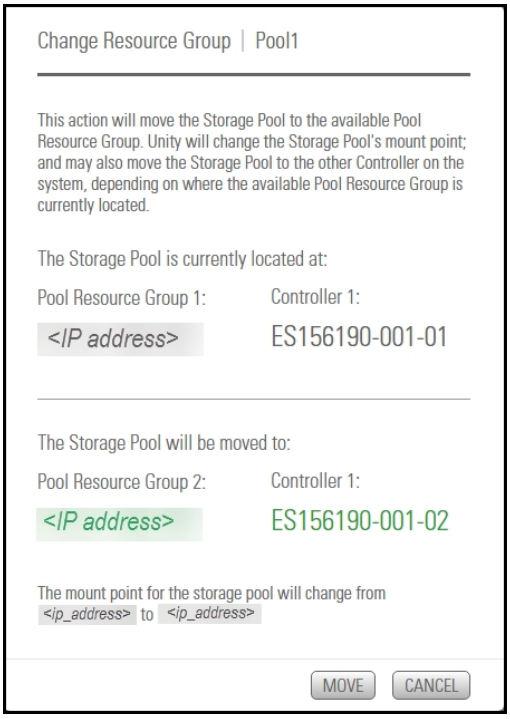
You can move a storage pool from the pool's properties panel.

To move a storage pool using the Storage Pool Summary panel:

1. On the **Unity navigation bar**, select **Storage > Storage Pools**.
2. In the **Storage Pools** panel, click the link to the pool you want to change.
3. Click the **Change Resource Group** button.

4. The **Change Resource Group** popup opens. Unity selects the other Pool Resource Group node automatically. When you are ready, click the **Move** button.

Figure 4-10: Change Resource Group popup

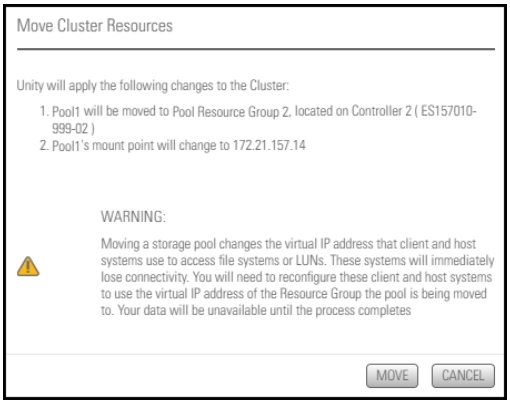


4

► **To change the Pool Resource Group using the Cluster Settings > Resources panel:**

1. On the **Unity navigation bar**, select **System > Cluster Settings**.
2. Click **Status > Resources**.
3. Select the storage pool that you want to move and click **Move**.
4. Click the **Apply** button. The **Move Cluster Resources** popup opens.

Figure 4-11: Move Cluster Resources popup



5. Click the **Move** button. Unity moves the resource group.

Managing FASTier cache devices

When you install FASTier cache devices on Unity, they are automatically detected by the system.

FASTier devices display from the **Storage Pools** panel. Click **Summary > FASTier Cache**. The panel includes the following options:

- View the device size of the device
- Specify read or write options
- Discover FASTier devices

To access the FASTier Cache panel:

1. On the **Unity navigation bar**, select **Storage > Storage Pools**.
2. Click the link to the pool that you want to access.
3. Select **Summary > FASTier cache**.
4. Do any of the following:
   - View the FASTIER disk size
   - Specify read or write options.
   - Click the **Discover FASTier Devices** button if you have more FASTiers to add.

Viewing and clearing storage pool errors

Unity displays the health status of storage pools and their underlying volumes using error or warning indicators in the Event Viewer. You can click an error in the table to display the information in a popup window.

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

Table 4-4: Storage pool error conditions

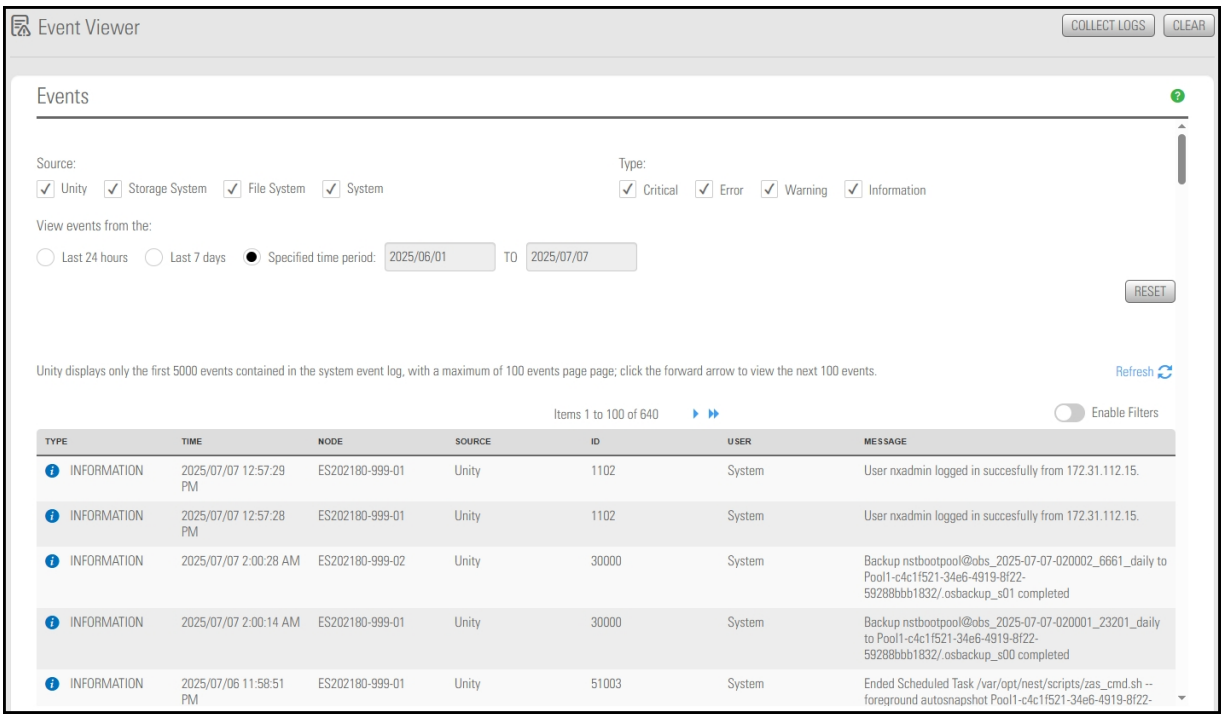
Error condition indicator	Error condition
	**ERROR**: this error condition indicates that one or more disks associated with the corresponding storage pool's volume(s) has failed. The storage pool continues functioning, but in a degraded state.
	UNAVAILABLE: this error condition indicates that one or 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.
	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.
	**CRITICAL**: this error condition indicates that a resilvering operation is currently underway on the storage pool. Unity triggers a resilvering operation when: • 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. During the resilvering operation, Unity copies the data from one disk to another, or from one volume to another. The storage pool continues functioning, but in a degraded state. This error condition is cleared once the resilvering operation completes. 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.

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:

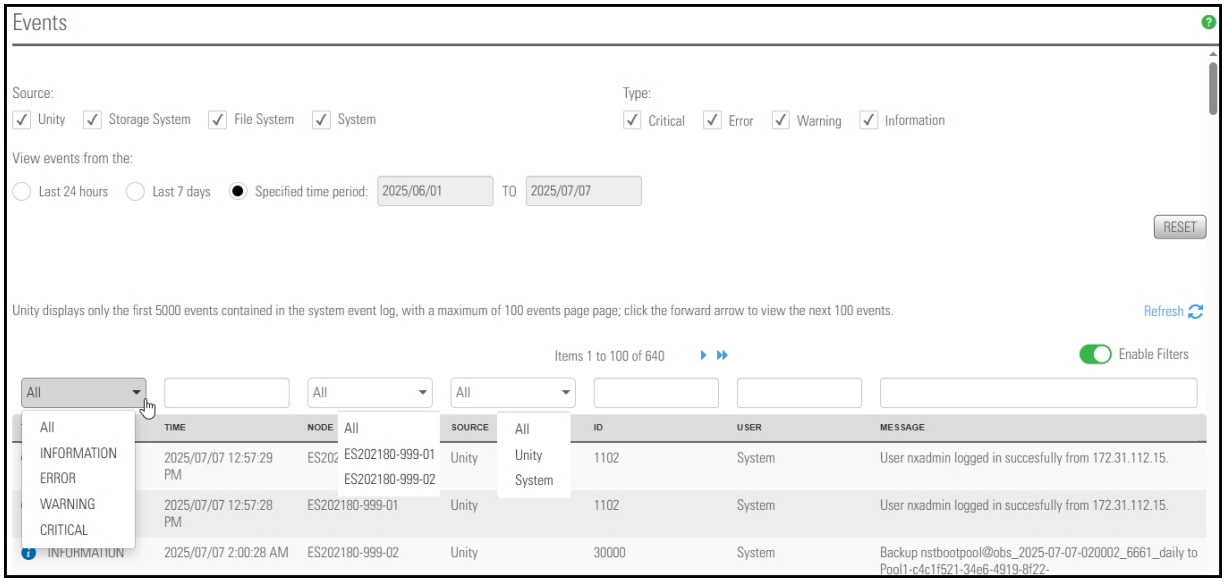
1. On the **Unity navigation bar**, select **System > Event Viewer**.

Figure 4-12: Event Viewer panel



2. Apply the appropriate **Event Filters**, as shown and described here:

Figure 4-13: Event Filters



Setting	Description
Source	Choose the sources from which Unity derives events notifications: • Unity • Storage System • File System • System
Type	Critical Error Warning Information
Time period	Last 24 hours Last 7 days Specified time period

3. Click the **Apply** button if you made changes to view events.
4. Scroll down until you see any existing event notifications. If applicable, the notification provides suggestions or instructions for resolving the error condition. For example, if a disk associated with the corresponding storage pool's volume has failed, the message 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 enclosure.

5. Once you take the necessary corrective measure to resolve the error condition—for example, you replace the failed disk drive on Unity—click the **Clear** button at the top of the Event Viewer panel to clear the error condition.
6. Optionally, you can also filter the list by clicking the Enable Filters button . The following data types are available:
   a. Event type
   b. Date and time
   c. Node
   d. Source
   e. ID
   f. User
   g. Message

See also Event logging and notification on page 557

Deleting a storage pool

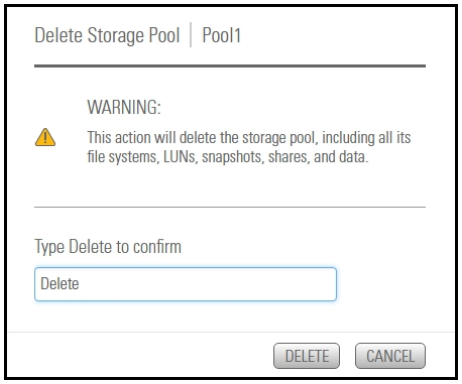
This section explains how to delete a storage pool on Unity.

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. On the **Unity navigation bar**, select **Storage > Storage Pools**.
2. In the **Storage Pool** panel, click the link to the pool you want to delete.
3. Click the **Delete Pool** button. The **Delete Storage Pool** confirmation popup opens.

Figure 4-14: Delete Pool popup



4. Type **Delete** in the text box.
5. Click **Delete** to delete the storage pool.

Chapter 5

File Systems

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

- **CIFS sharing** enables you to expose a share to Windows-based systems using the Common Internet File System (CIFS) protocol.
- **NFS sharing** enables you to expose a share to UNIX/Linux-based systems using the Network File System (NFS) protocol.
- **FTP sharing** enables you to expose a share to Windows-based 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 on the Unity Storage System beforehand; see Enabling FTP support on page 482.

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:

Data management functions on file systems 116
Adding a file system 117
Viewing file system space usage information 130
Modifying file system properties 132
Setting IP restrictions 147
Editing or removing IP restrictions 150
Share IP permission precedence 151
Deleting a file system 153
Managing home directories 154
Managing CIFS shares 173
Managing access permissions to file systems 194
Enabling ZFS Encryption for file systems 199
Managing snapshots for file systems 204
Immutable snapshots for file systems 220

Data management functions on file systems

Unity includes several data management functions that protect the data in your file systems 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 file systems on page 194.
- Space usage configuration and capacity planning: Unity enables 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 184.
- Disaster recovery with Data Replication: Unity enables 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 enables 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 enables you to take point-in-time snapshots of the data contained in each file system, including scheduled automatic snapshots. This enables 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 enables you to configure Unity as a Network Data Management Protocol (NDMP) host to participate in remotely-coordinated automatic backups.

Adding a file system

Unity provides the **Create a File System** wizard to guide you through the process of file system setup.

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. See .

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:

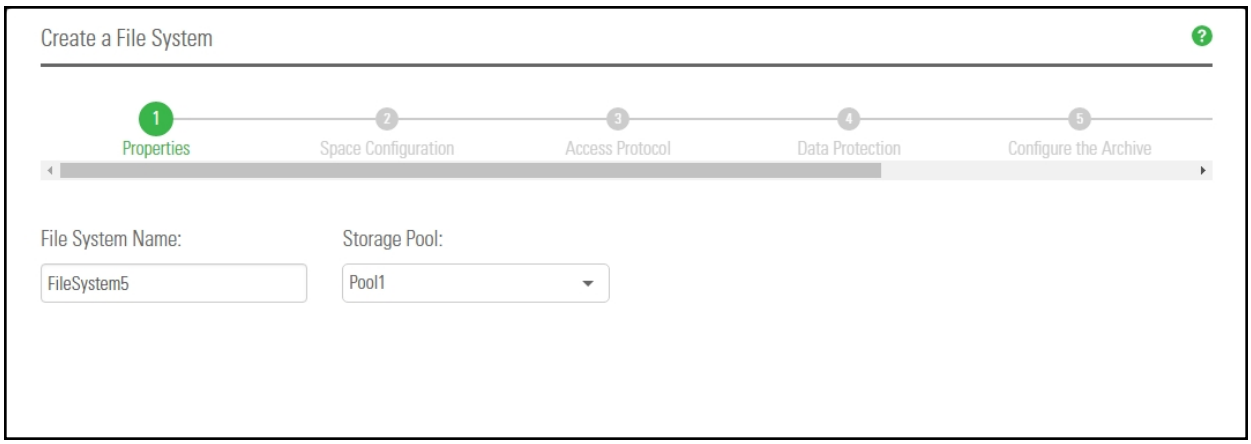
- Take into account the number of file systems that you need per storage pool, and divide the disk space in the storage pool accordingly. When allocating disk space, keep in mind that file system metadata and snapshots also consume storage.
- Consider future capacity requirements, particularly when allocating 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.

Step 1: Setting the file system name and storage pool

To assign a file system name and storage pool:

1. On the **Unity navigation bar**, select **Storage > File Systems**.
2. Click **Add File System**. The **Create a File System** wizard opens.

Figure 5-1: Step 1: Naming the File System and choosing the pool



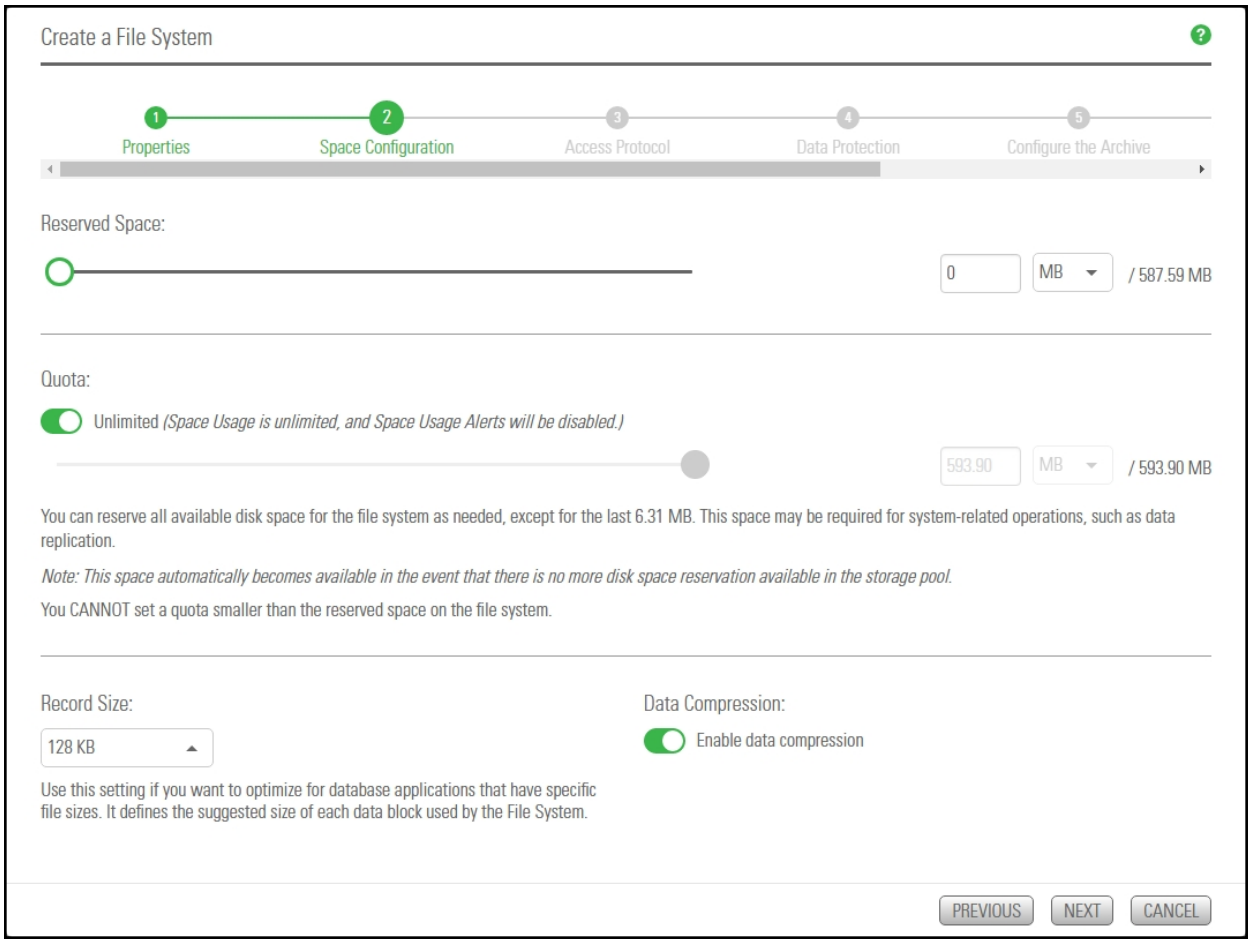
3. You can accept or change the:
   a. **File System Name**
   b. **Storage Pool** assignment, if more than one storage pool exists. Select which pool you want to assign to the file system to.

   Click the **Next** button.

Step 2: Configuring space settings

In this step, configure reserved space, quota, and record size.

Figure 5-2: Step 2: Space settings



To configure space settings:

1. In the wizard step 2 **Space Configuration** panel, you can specify:

Setting	Description
Reserved Space	***You can reserve a set amount of disk space in the storage pool for the exclusive use of the file system. (Read more ...)*** 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. ▶ **To reserve space for the file system in the storage pool:** ● Move the slider left or right to set the desired amount of reserved space, Or ● Enter a value in the box to the right of the slider. **Note** 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. (Read more ...)*** You can reserve all available disk space for the file system, if needed, except for the last 6.31 MB, which space 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.) ▶ **To specify the file system quota:** 1. Click the **Quota** button. 2. Do one of the following: ● Move the **Quota** slider left or right to decrease or increase the quota limit. ● Enter a value in the box to the right of the slider.

Setting	Description
Record Size	***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 ...)*** 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 the database record size is precisely known. File systems have a default record size of 128 KB, which is the maximum size.
Data Compression	**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. You can enable/disable compression at the file system level. 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. 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. 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.

2. Click the **Next** button.

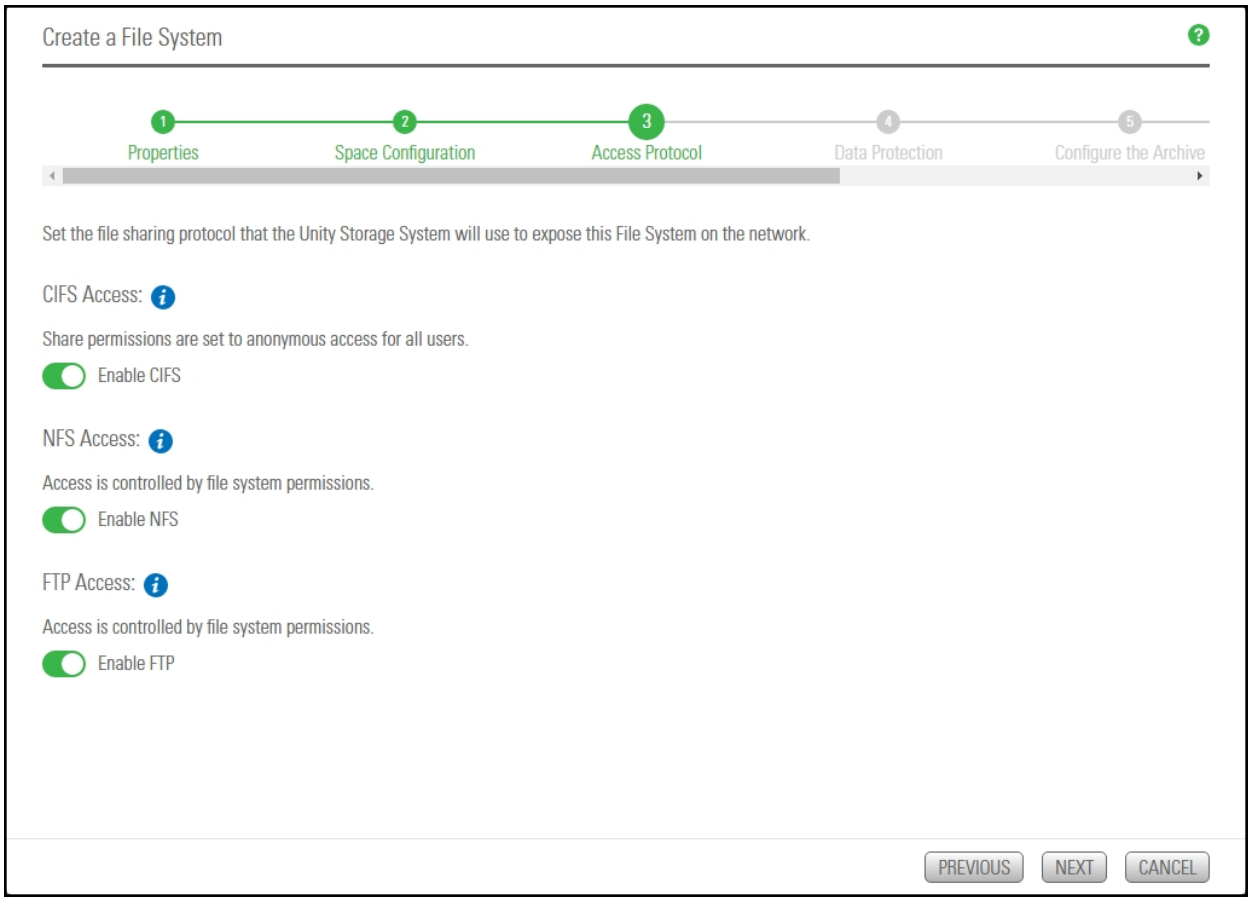
Note Step 3: Configuring the access protocol below is only displayed if your Unity deployment includes Unity's Data Protection feature. For more information about Snapshots and Data Replication, please contact your Nexsan reseller or Nexsan Support Representative.

Step 3: Configuring the access protocol

Now select the **Access Protocol** for the 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; 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.
- If the file system will be accessed over IIS, do not enable case-sensitivity for the share.

Figure 5-3: Step 3:Configuring the access method



To configure the access protocol:

- Choose any of the following:

Now select the **Access Protocol** for the 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; 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.
- If the file system will be accessed over IIS, do not enable case-sensitivity for the share.

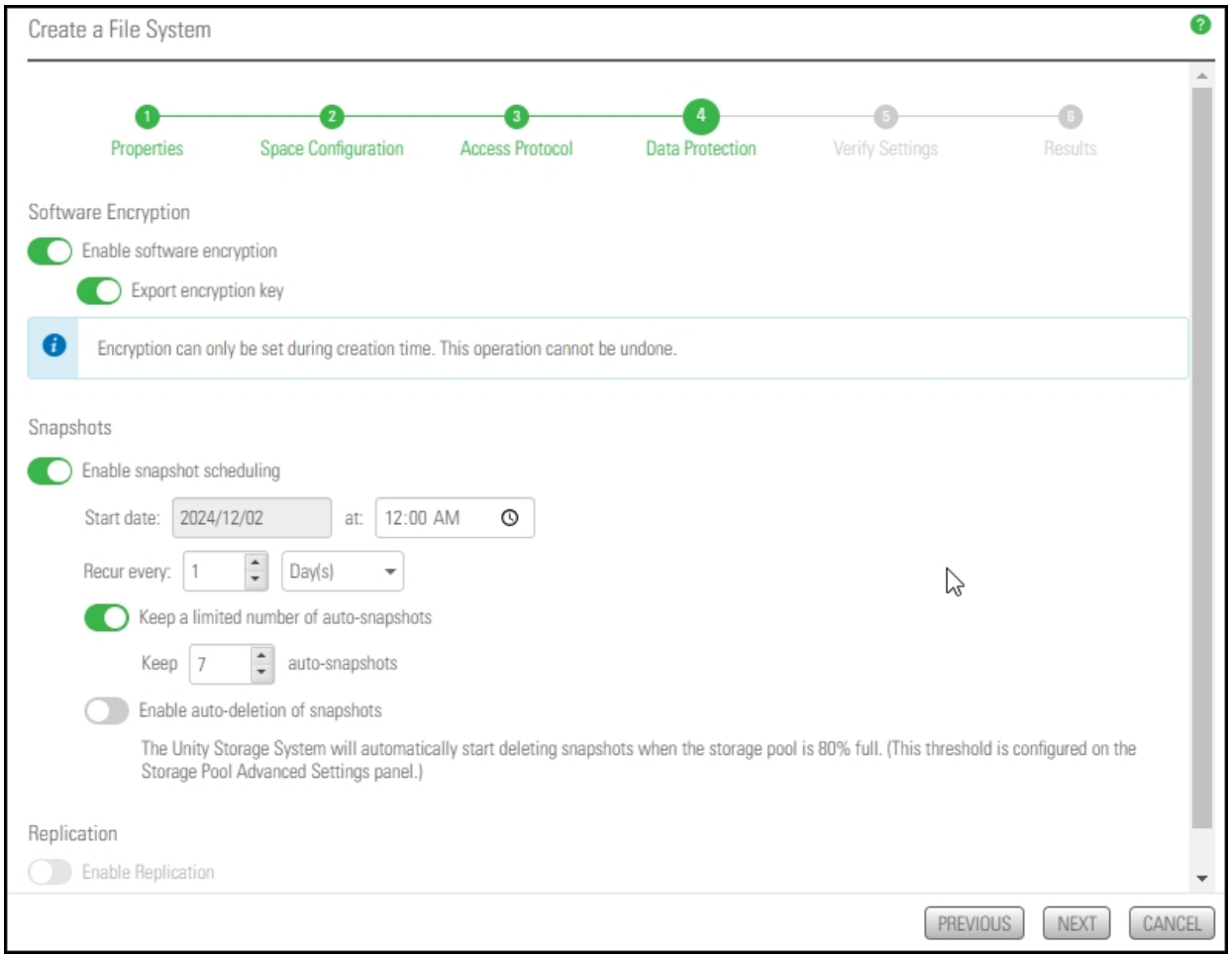
Step 4: Configuring Data Protection

Now you need to enable:

- Software encryption
- Snapshots scheduling
- Replication

To enable replication for a file system, you need a second Unity Storage System that you can connect the current system to.

Figure 5-4: Step 4: Setting Encryption, Replication, and Snapshots scheduling



To configure data protection for the file system:

1. To enable software encryption, select **Enable software encryption**. By default, **Export encryption key** is pre selected. **NOTE**: Encryption can only be set during creation time. The operation cannot be undone.
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. If your Unity System is connected to a remote Unity System and has replication set up, select **Enable Replication**.
7. Click the **Next** button.

Step 5: Configuring Active Archive

If you have **Unity Active Archive** configured, this step of the **Add File System** wizard prompts you to select the **Archive Settings** for the file system.

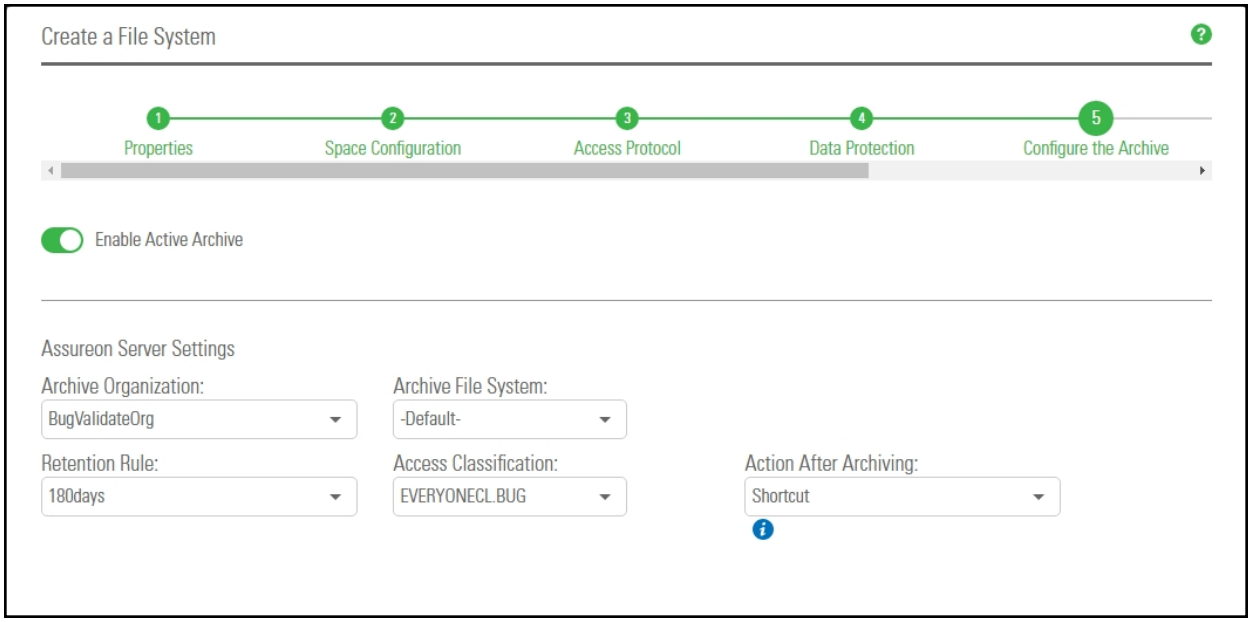
This step only appears if you have Unity Active Archive on this Unity Storage System. Unity Active Archive enables you to set data retention policies to automatically offload stale data and release primary storage. This in turn enables increase the performance of your primary storage without increasing its size.

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

To configure Active Archive settings:

1. Select the **Enable Active Archive** button

Figure 5-5: Step 5: Enable Active Archive



2. 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 5-1: 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. For example, create a shortcut to the files, leave them as they are, or remove them from the file system. **Note** Files will not be converted to shortcuts, or removed if asynchronous replication is enabled.
Real Time Archiving	Performs a persistent and ongoing archive of files, as changes are detected. Files are checked and archived if necessary every minute. Enabled or disabled on the Assureon Server under **Advanced Settings**, or using the nxcmd command line interface. See "Setting the realtime delay" in the *nxcmd Command Line Interface Reference Guide*, or visit Nexsan.com/support.
Scheduled Archiving	Performs a complete archive of the file system, either manually or on a schedule. This feature does not affect Real Time Archiving. Enabled or disabled on the Assureon Server on the **Advanced Settings > General tab**. Select the **Sync** checkbox.

3. Click the **Next** button.

Step 6: Verifying settings

Now you review the summary of your settings carefully before applying the configuration settings.

To review your settings:

1. Review the summary of the settings shown on screen.
2. To revise any of your settings, you can click **Previous** to go back.

   OR

3. Click any of the step numbers at the top of the panel to jump to that section of the wizard. For example, if you want to change **Properties**, click:

4. When you are ready to proceed, click **Create**.

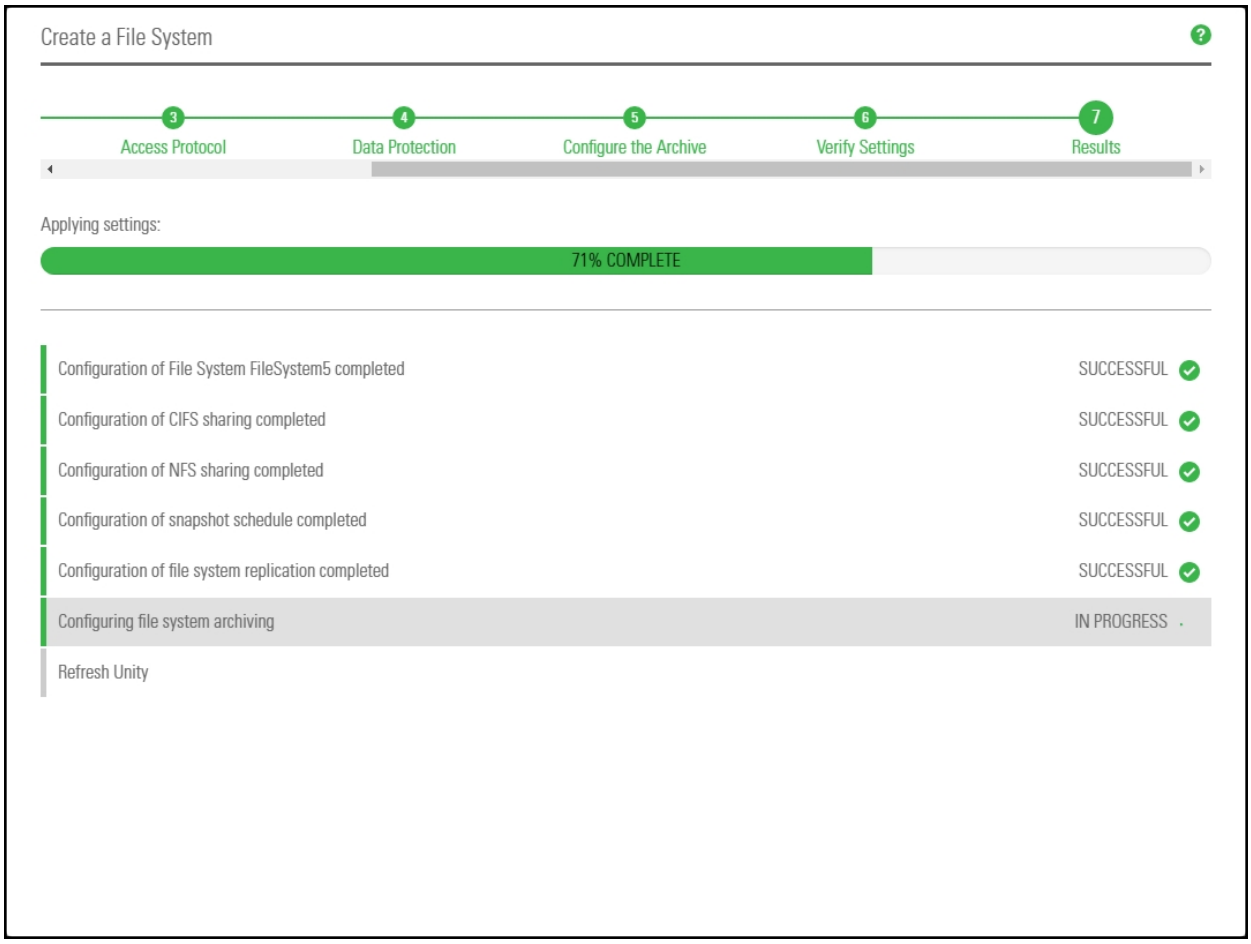
The wizard displays file system creation progress as it applies your settings.

Now you can **Add another file system** or click **No, I'm finished**.

Step 7: Viewing results

In this step, the wizard displays results as Unity creates the new File System.

Figure 5-6: File System wizard: 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 **View Error** link 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.

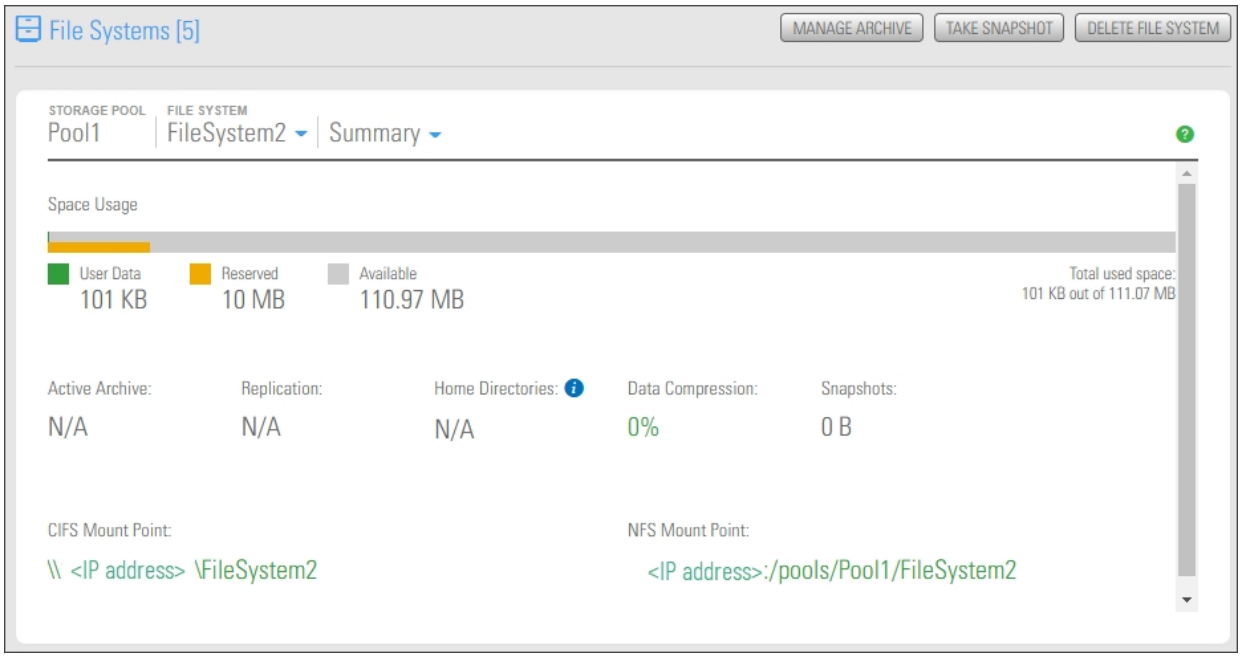
Viewing file system space usage information

Unity gives you a detailed overview of each file system's used and available disk space. To modify space usage settings, see Modifying file system space configuration settings on page 136.

To access the File System Summary panel:

1. On the **Unity navigation bar**, click **Storage > File Systems**.
2. Click the storage pool containing the file systems for which you want to view space usage information.

Figure 5-7: File Systems Summary panel



Property	Description
User Data	The amount of space currently consumed by user data, excluding snapshots.
Reserved	The current setting for reserved space. If there is none, nothing is displayed in the column.
Available	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.
Total Used Space	The total amount of space for user data, plus reserved space.
Active Archive	Indicates whether Active Archive is enabled or disabled.
Replication	Indicates whether Replication is enabled or disabled.
Home Directories	To enable this feature, you must connect the Unity appliance to a Microsoft Active Directory Domain.

Property	Description
Data Compression	The percentage of compressed data and its equivalent in units (megabytes or terabytes).
Snapshots	The amount of space currently consumed by snapshots.
Mount Point	CIFS or NFS Mount Points. Can be set to allow non-root users permissions to access shares or directories.

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. See also Managing home directories on page 154

This section includes these topics:

Renaming a file system 133
Disabling data sharing for a file system 134
Modifying file system sharing methods 145
Modifying file system space configuration settings 136
Modifying file system record size 138
Setting space usage notification thresholds for file systems 140
Enabling or disabling data compression on a file system 142
Enabling the Access Time mode on a file system 144
Setting IP restrictions 147
Managing home directories 154

Renaming a file system

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

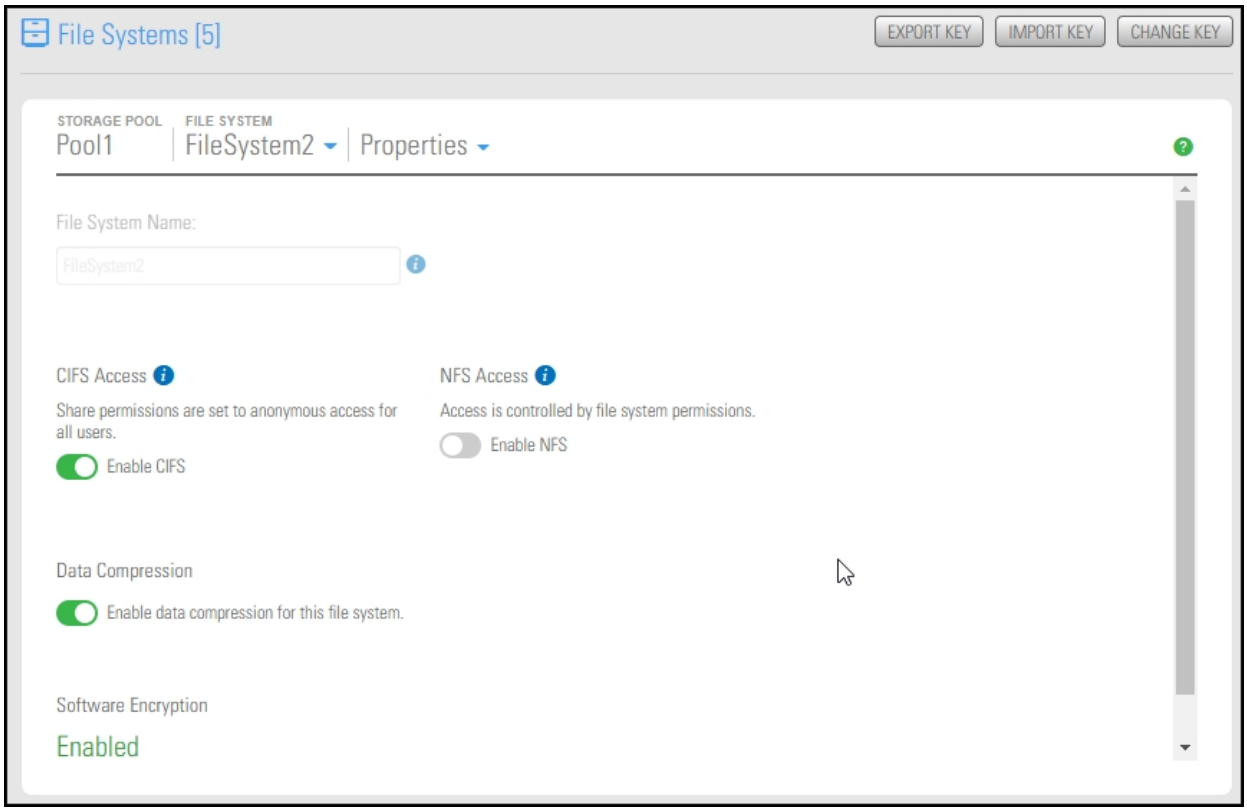
CAUTION: An encrypted dataset cannot be renamed. If you rename a file system, client systems on the network will be disconnected from the file system; this could result in data loss. Before renaming a file system, make sure that client systems with an active connection to the file system disconnect any 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.

To rename a file system:

1. On the **Unity navigation bar**, select **Storage > File Systems**.
2. Click the file system name to open the **File Systems > Summary** panel.
3. Click **Summary > Properties**.

Figure 5-8: File Systems Properties panel



4. Edit the name 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 hyphen (-) and period (.), the name can only contain alphanumeric characters, without spaces.

   These characters are NOT allowed:

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

5. Click the **Apply** button to change the file system's name.

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.

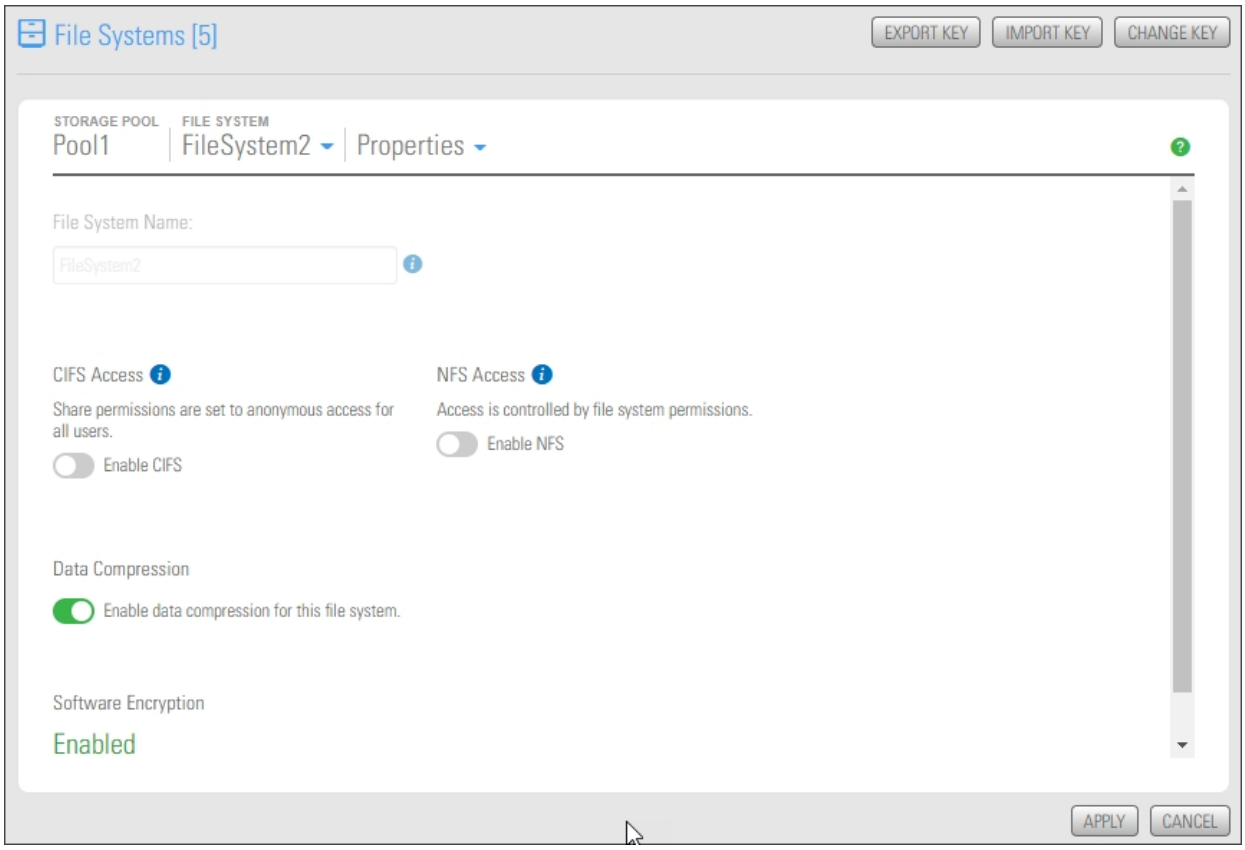
Note Disabling data sharing for a file system does not affect shares that reside within the file system; any share that exists in a file system on which you disable data sharing remains accessible over the network until you manually unshare it; for more information, see .

5

► **To disable data sharing for a file system:**

1. On the **Unity navigation bar**, select **Storage > File Systems**.
2. Click the file system name to open the **File Systems > Summary** panel.
3. Click **Summary > Properties**.

Figure 5-9: File Systems Properties panel



4. Clear all selected sharing options.
5. Click the **Apply** button. The file system will no longer be accessible over the network.

Modifying file system space configuration settings

Use this topic for information about space configuration settings and how to modify them.

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.

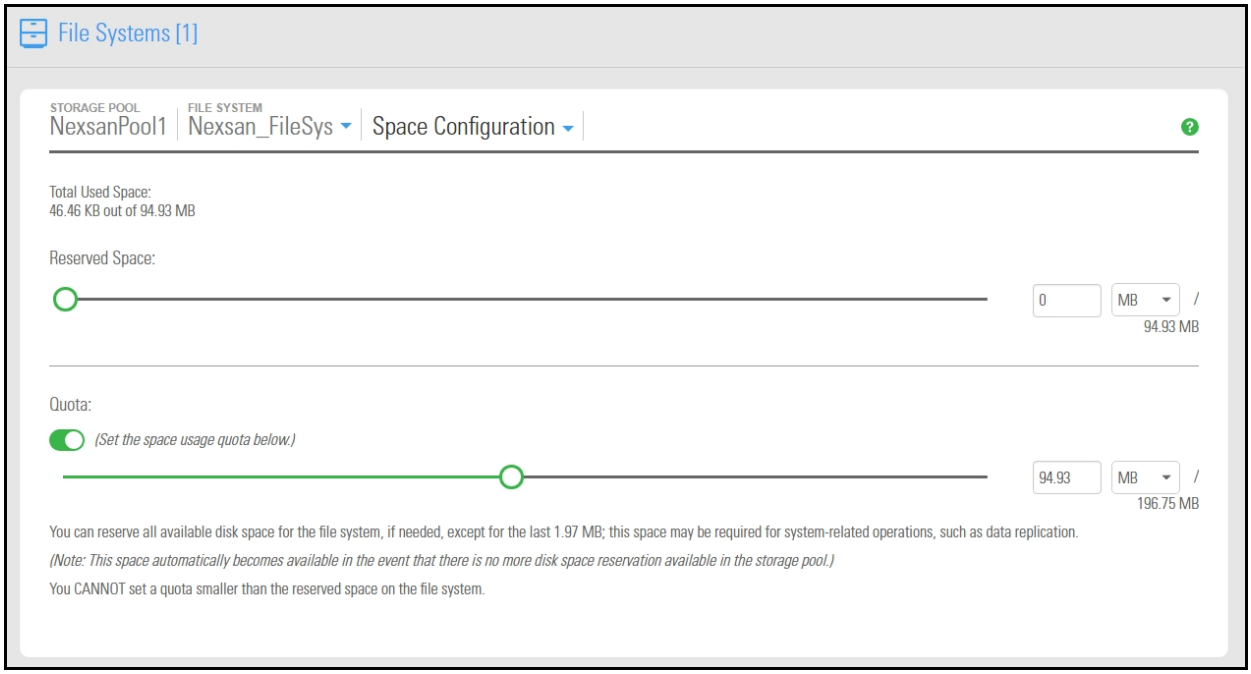
Table 5-2: Distribution of disk space to file systems when setting reservations and quotas for file systems

Space usage settings	Total available space in storage pool: 10 TB		
	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 *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.*	3 TB *Total available space cannot exceed set quota limit.*	3 TB *7 TB reserved for File System 1 and File System 2*

To modify file system space usage settings:

1. On the **Unity navigation bar**, select **Storage > File Systems**.
2. Click the file system name to open the **File Systems > Summary** panel.
3. Click **Summary > Space Configuration**.

Figure 5-10: File System Space Configuration panel



4. Modify space usage settings for the file system by selecting or changing one of the available options.
5. Click the **Apply** button to save your changes.

Modifying file system record size

File system 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.

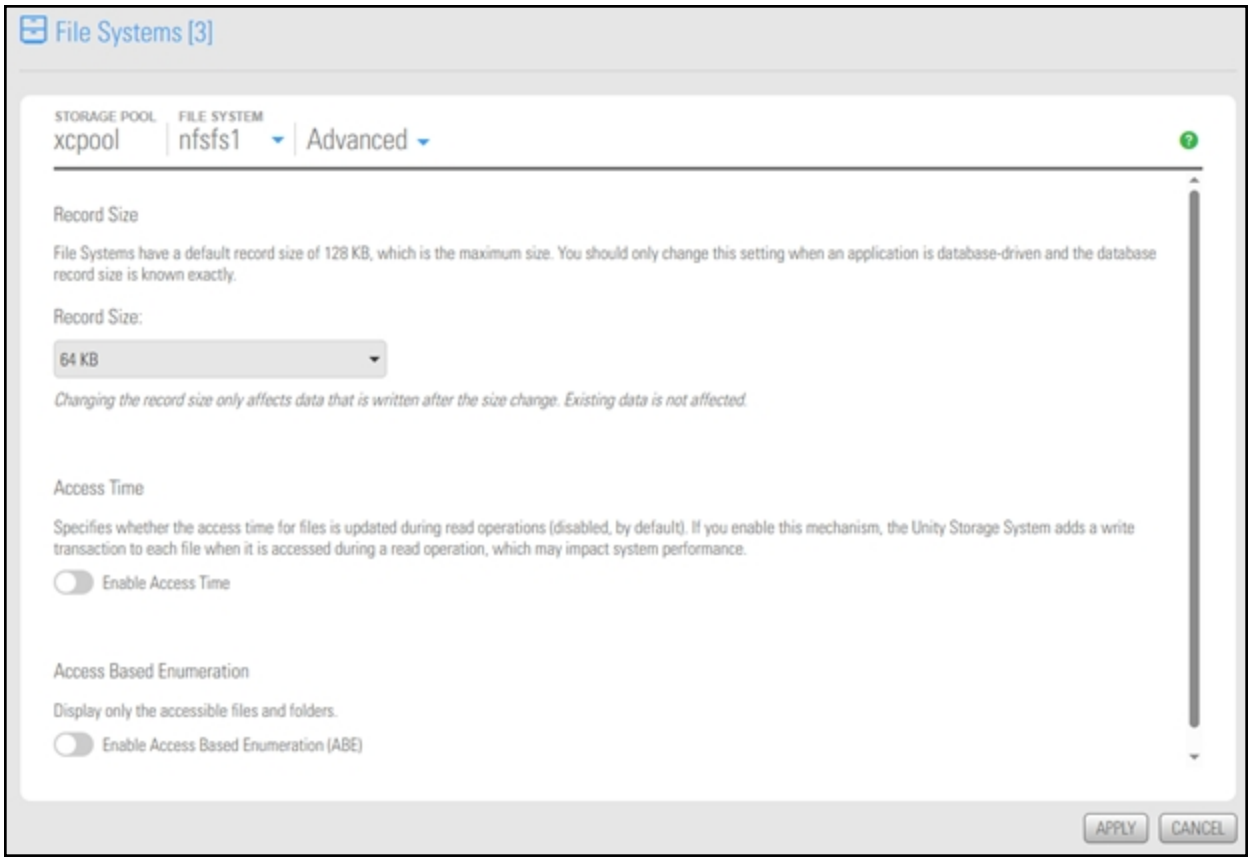
For the recommended record size according to the application used, see Step 3: Configuring the access protocol on page 122.

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. On the **Unity navigation bar**, select **Storage > File Systems**.
2. Select the file system you would like to modify.
3. Select **Summary > Advanced**.

Figure 5-11: File System Advanced panel



4. Modify the record size by choosing one of the available record sizes:
   - 512 B, 1 KB, 4 KB, 8 KB, 16 KB, 32 KB, 64 KB, 128 KB (default)
   - 1 KB
   - 4 KB
   - 8 KB
   - 16 KB
   - 32 KB
   - 64 KB
   - 128 KB (default)
5. Click the **Apply** button.

Setting space usage notification thresholds for file systems

Unity enables you to set space usage thresholds for file systems to trigger email notifications if space consumption in the file system reaches or exceeds a set threshold. You can only set space usage thresholds for a file system when you enable a space usage quota; for more information, see Modifying file system space configuration settings on page 136.

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 557.

Unity lets you set these space usage thresholds for a file system:

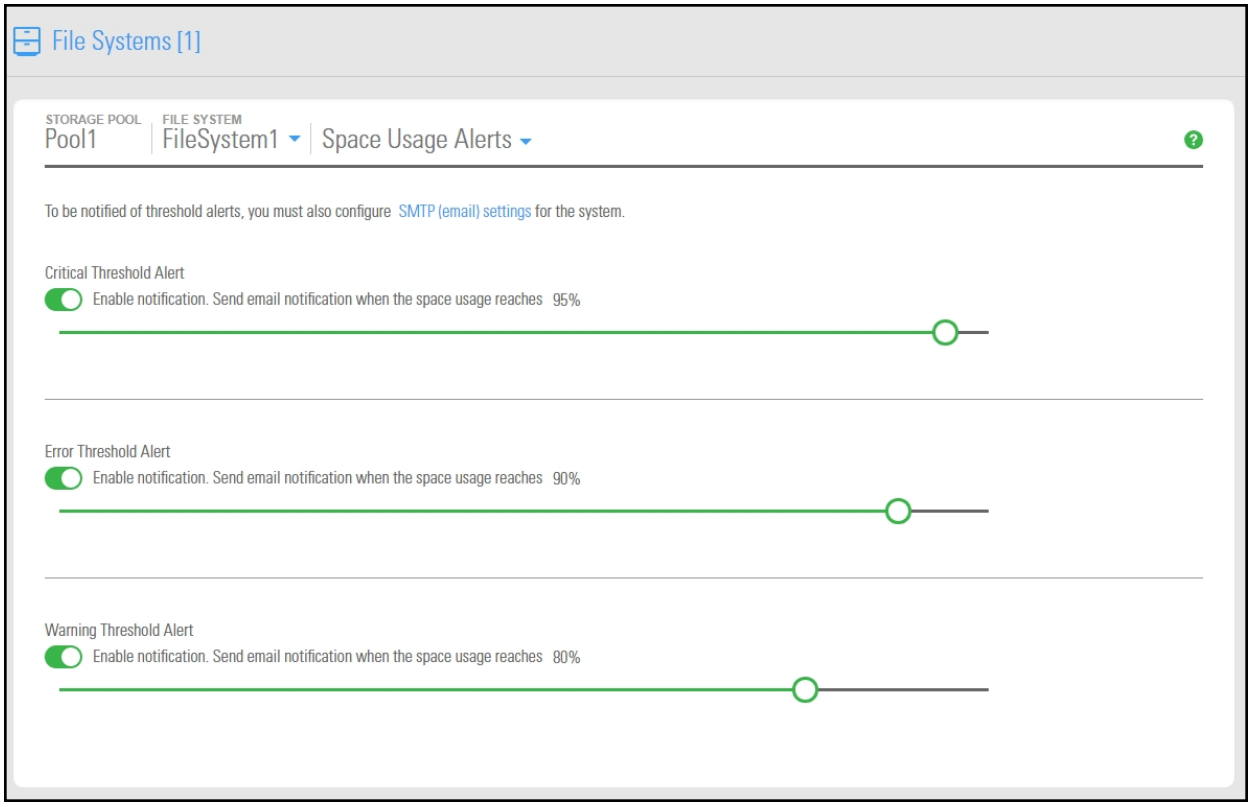
- Critical: The default critical threshold for a file system is set to the same value that you configured for the storage pool where the file system resides: if the storage pool's critical threshold is set to 95%, the default critical threshold for any new file system that you add to the storage pool 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. On the **Unity navigation bar**, select **Storage > File Systems**.
2. Select the file system you would like to modify.

3. Select **Summary > Space Usage Alerts**.

Figure 5-12: File System Space Usage Alerts panel



4. Move the slider to select the threshold setting when you want to receive email notifications. The options are:
   a. **Critical Threshold Alert**.
   b. **Error Threshold Alert**
   c. **Warning Threshold Alert**

   By default, threshold settings are enabled. To disable a threshold setting, click its button
5. Click the **Apply** button to set the new threshold settings for the file system.

Enabling or 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 Configuring data compression on a storage pool on page 102. 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 Unity System 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:

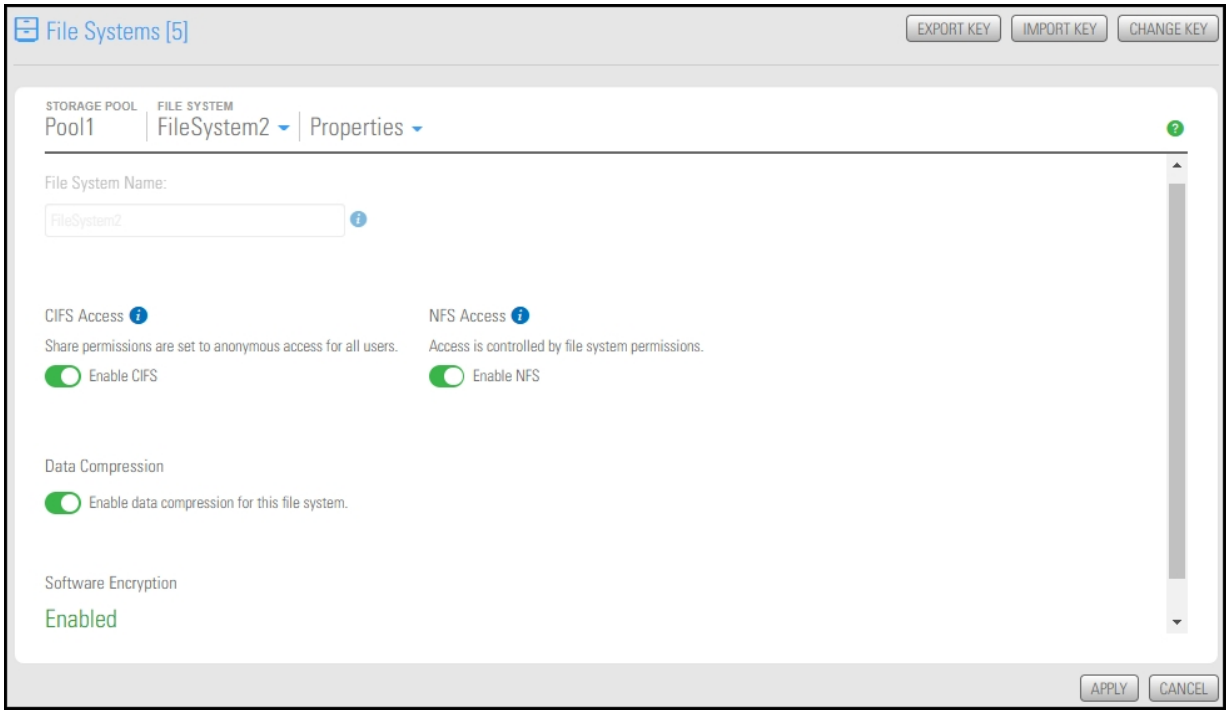
- Increase the quota to match the actual space used by data on the file system.
- Set the quota to *Unlimited*.
- Enable data compression on both sites.

To enable data compression on a file system:

1. On the **Unity navigation bar**, select **Storage > File Systems**.
2. Select the file system you would like to modify.

3. Select **Summary > Properties**.

Figure 5-13: File System Properties panel



4. Click the **Data Compression** button  to toggle compression on or off.
5. Click the **Apply** button.

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.

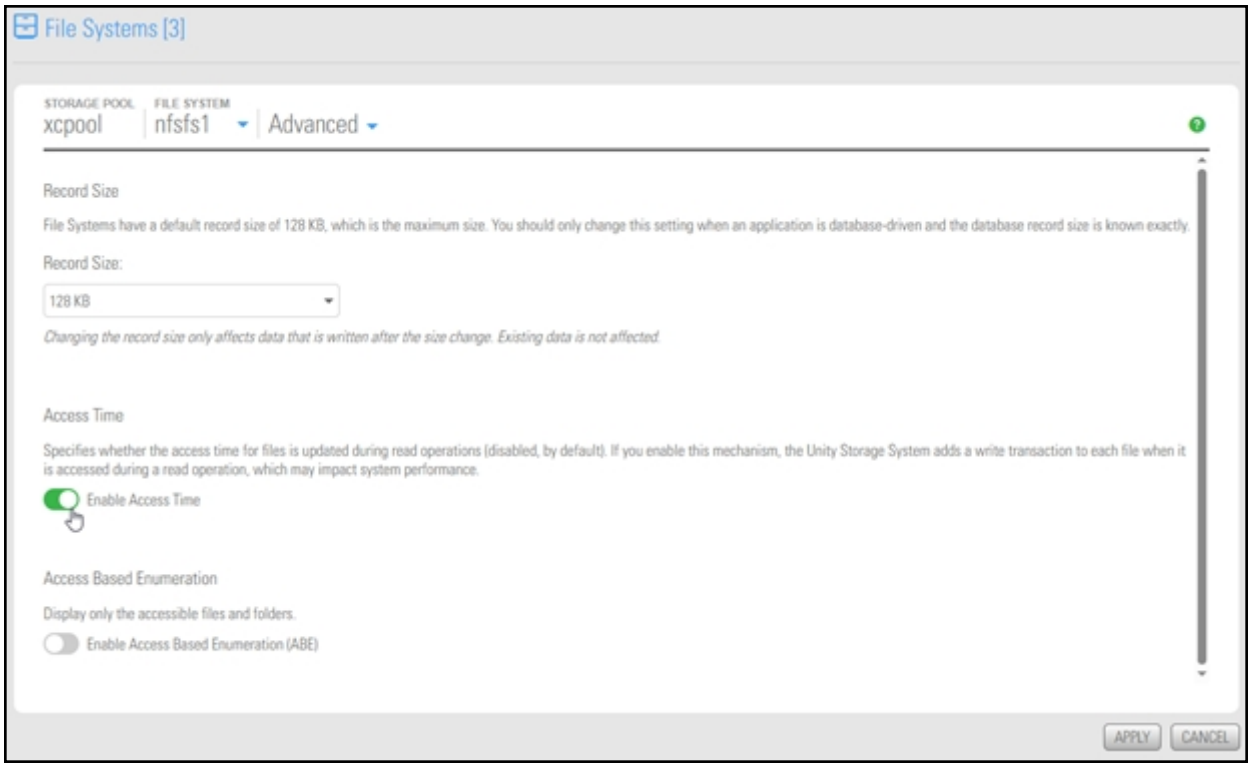
The Access Time mode can be set at the file system level or pool level. This value can be modified at any time. To enable it for the pool, see Configuring access time on a storage pool on page 103.

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. On the **Unity navigation bar**, select **Storage > File Systems**.
2. Click the file system name to open the **File Systems > Summary** panel.
3. Click **Summary > Advanced**.

Figure 5-14: File System Advanced panel



4. Select the **Enable Access Time** option.
5. Click the **Apply** button to save your changes.

Modifying file system sharing methods

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 482.

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 drives mapped 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 enables 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 enables 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>$`

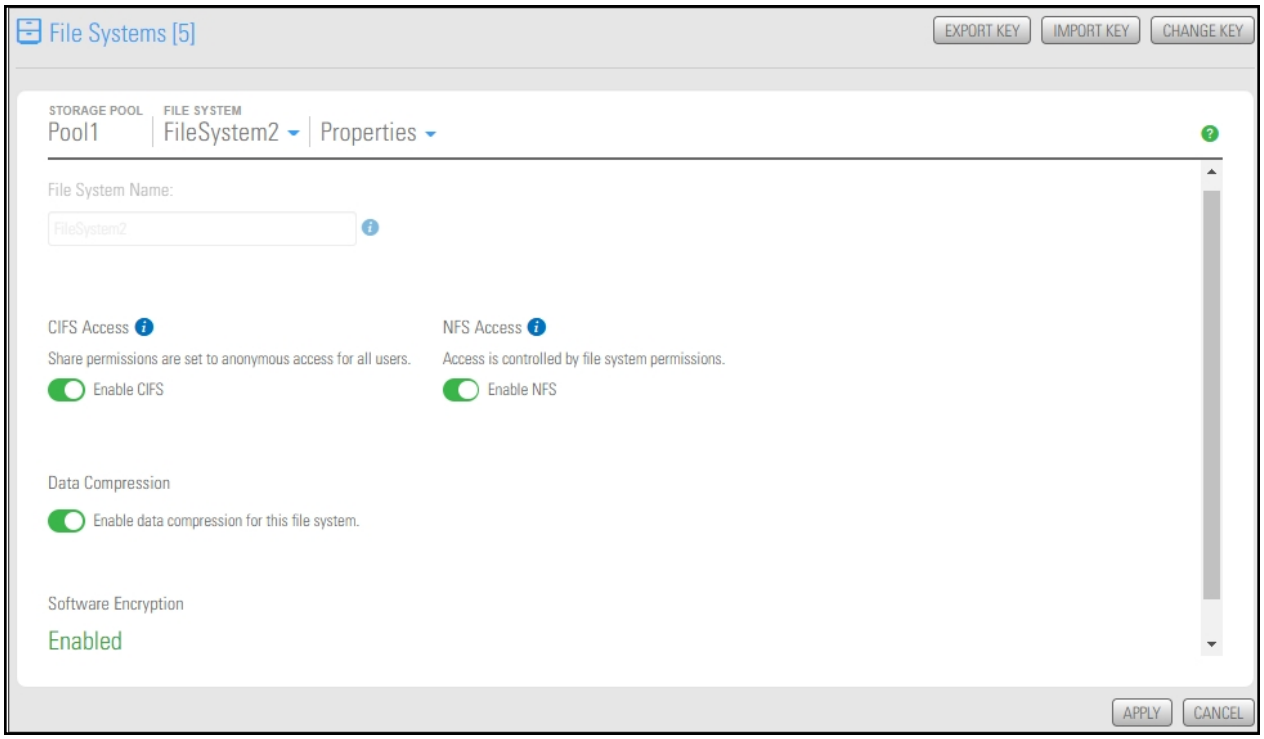
Where `<File SystemName>` is the name of the hidden (CIFS) share on Unity.

▶ To modify the file system sharing method:

1. On the **Unity navigation bar**, select **Storage > File Systems**.
2. Click the link to file system that you want to open.
3. Click **Summary > Properties**.

4. Modify the sharing method for the file system by clearing or selecting the relevant options.

Figure 5-15: File Systems Properties panel



5. Click the **Apply** button.

Setting IP restrictions

Unity enables you to restrict access to CIFS and NFS shares based on a client system's IP address. This process is referred to as setting IP restrictions.

See also

You can also set up IP restrictions using the nxcmd CLI. See

- "Setting IP-based access restrictions" in the *nxcmd Command Line Interface Reference Guide*.
- "Setting IP-based access restrictions on a file system" in the *nxcmd Command Line Interface Reference Guide*, "IP-based restrictions" in the *Network Configuration Guide,*or visit https://www.nexsan.com/support/.
- For more information about CIFS, NFS, and mixed mode sharing, see Sharing methods on page 605 of the Terminology section.

Using IP restrictions, 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 is 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 151.

You can also set the *no_root_squash* property to allow NFS clients with `root` privileges to access files on an NFS share on Unity.

► 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.

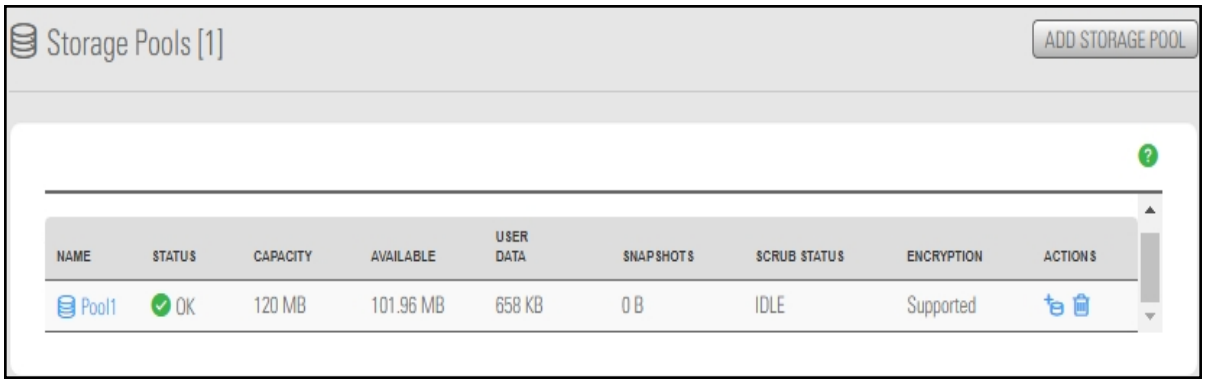
Notes:

- **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 151.

To set IP restrictions for shares:

1. On the **Unity navigation bar**, click **Storage > Storage Pools**.

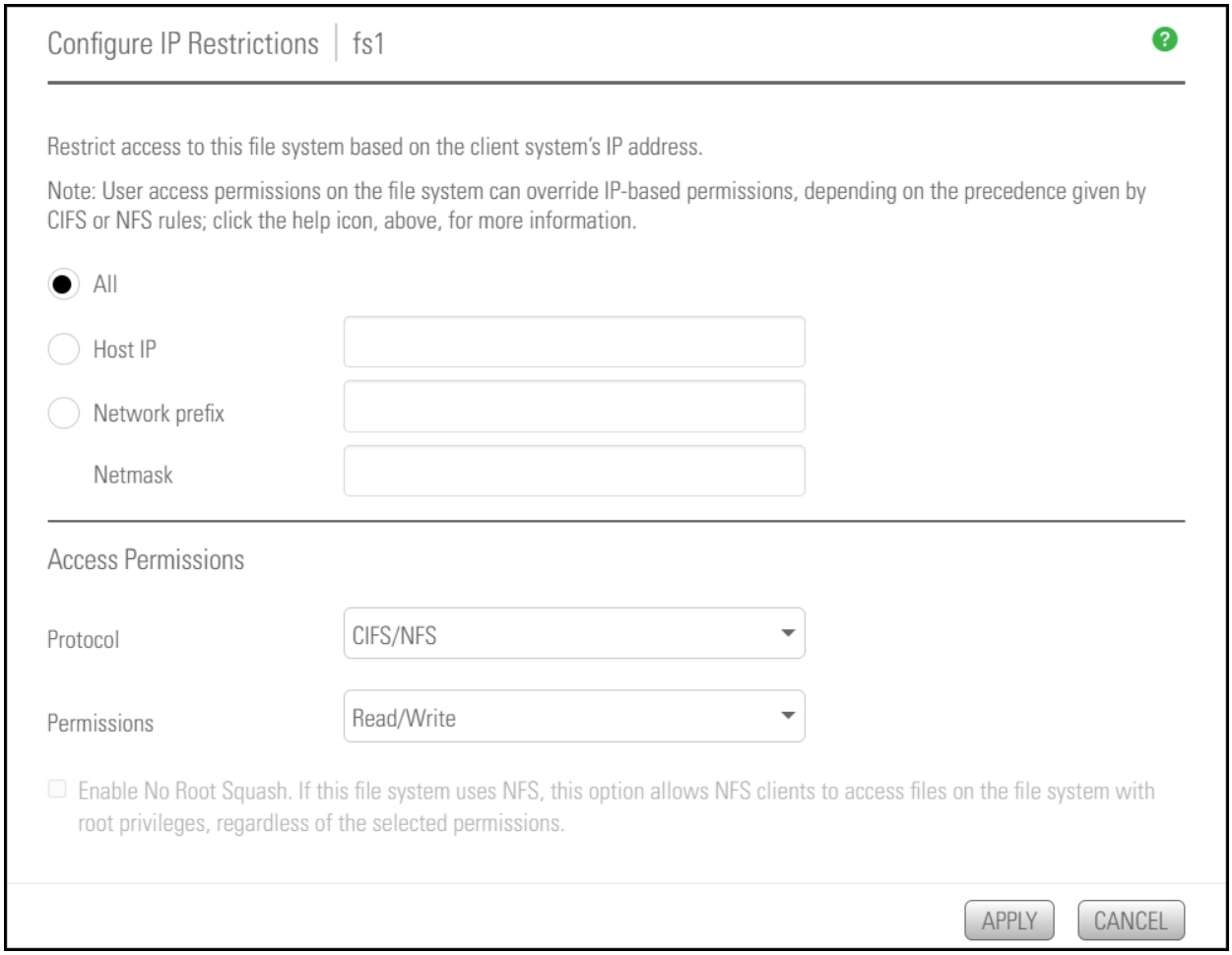
Figure 5-16: Storage Pools panel



2. Click the link to the pool where the share is hosted.
3. Click **Summary > File Systems** to open the **File Systems** panel.
4. Select the share.
5. Select **IP Restrictions** from the drop-down menu to the right of **Summary**.

6. Click the **Add IP Restriction** button on the upper right. The **Configure IP Restrictions** dialog appears.

Figure 5-17: Configure IP Restrictions dialog



7. Select the client systems you want to configure the IP restriction for:
   - **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.
8. 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.
9. From the **Permissions** drop-down list, select one of the access levels (**Read/Write**, **Read only**, or **No access**).
10. (Optionally) You can select the **Enable No Root Squash** option if this share uses NFS clients with `root` privileges; it will allow NFS clients to access files on this share.
11. Click the **Apply** button.
12. Repeat these steps for other client systems, as required.

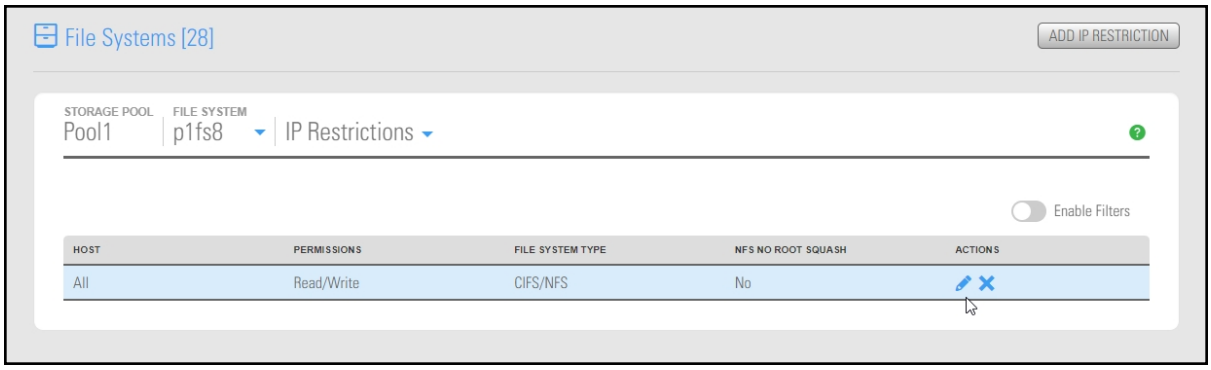
Editing or removing IP restrictions

Unity enables you to edit or to remove IP restrictions after they have been set.

▶ To edit IP restrictions for shares:

1. From the **IP Restrictions** panel for the target share, click the **Edit IP Restrictions** icon in the **Actions** column.

Figure 5-18: File Systems, IP Restrictions panel



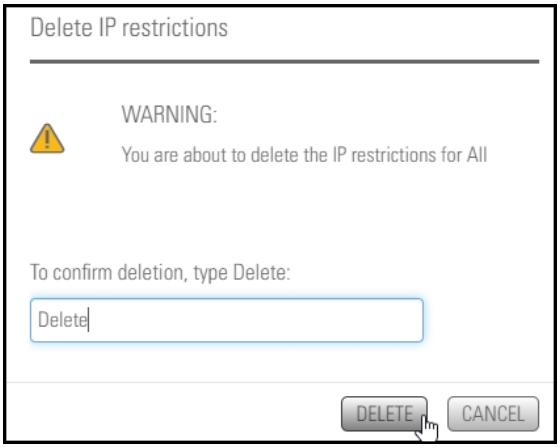
The **Configure IP Restrictions** dialog appears.

2. Edit the settings as needed, then click the **Apply** button.

▶ To remove IP restrictions for shares:

1. From the **IP Restrictions** panel for the target share, click the **Remove IP Restrictions** icon in the **Actions** column. The **Delete IP Restrictions** dialog appears.
2. Type `Delete`, then click the **Delete** button.

Figure 5-19: Delete IP Restrictions dialog



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 5-3: 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	
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 5-4: 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=@172.21.1`
	`Read-Only=@172.21.14.30 local`

Read/Write access to an IP address and Read-only access to a subnet.	Read/Write for the IP address
	`Read/Write=@172.21.14.30`
	`Read-Only=@172.21.14 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=@172.21.14.30`
	`Read/Write=* local`

Deleting a file system

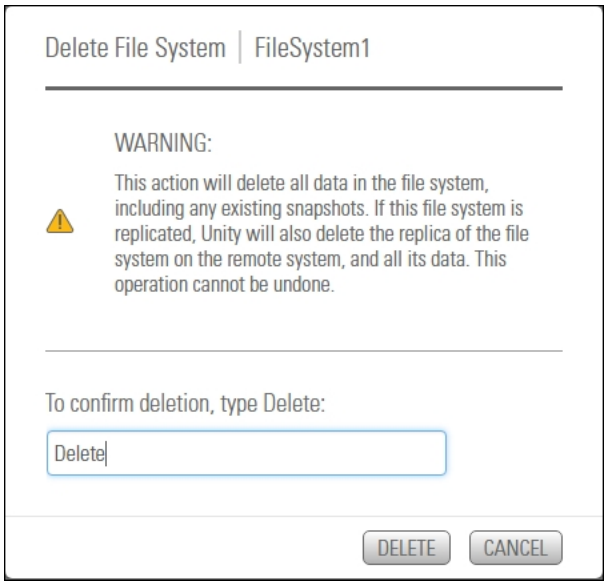
This section describes how to delete a file system from a storage pool.

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 Unity Storage System, the replicated file system, including all data in the replicated file system is permanently removed as well.

To delete a file system:

1. On the **Unity navigation bar**, select **Storage > File Systems**.
2. Click the **Delete File System** icon. The **Delete File System** popup opens.

Figure 5-20: Delete File System popup



3. Type **Delete** in the text box.
4. Click the **Delete** button.

Managing home directories

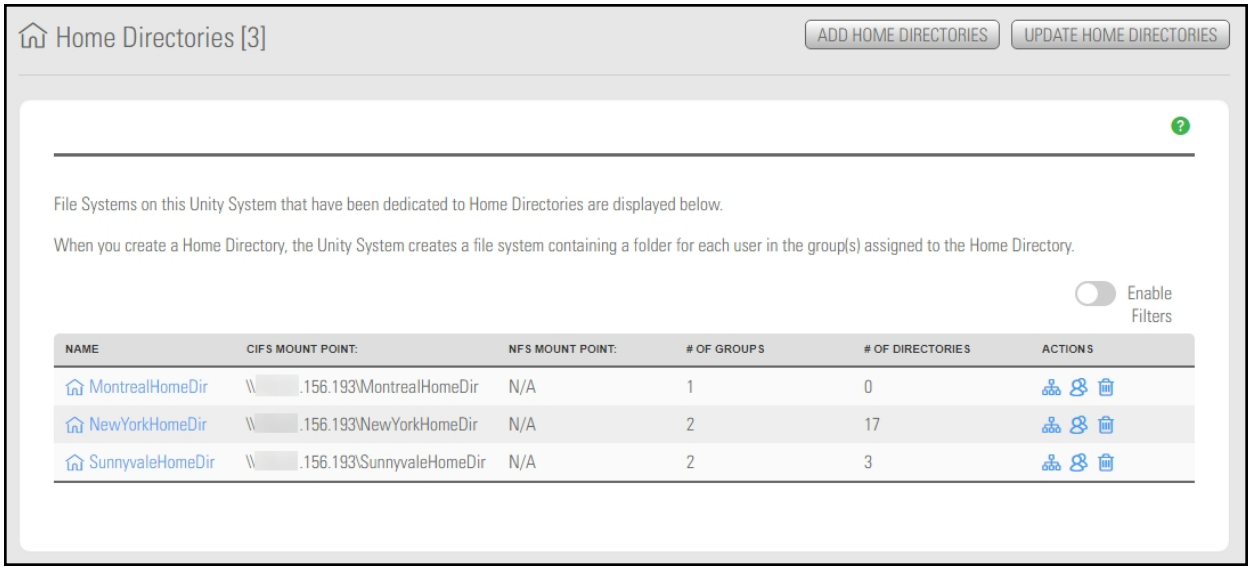
The new Home Directories feature enables you to quickly create a file system with Active Directory administrators and user groups, and automatically creates a home folder for each user in the associated group.

First you'll need to run the **Home Directories** wizard to create the file system dedicated to home directories, which includes assigning user groups and administrators. See Creating file systems for home directories on the facing page

To open the Home Directories panel:

- On the Unity navigation bar, click **Storage > Home Directories**.

Figure 5-21: The Storage > Home Directories panel



To...	Click...
Create home directories	The **Add Home Directories** button to open the File Systems for Home directories wizard, to create a new set of home directories.
Show updates to home directories	The **Update Home Directories** button to update the **Home Directories** properties panel with recent changes. Unity performs a background update every 5 minutes, but you can force an update at any time using the Update Home Directories button.
Open the File Systems > Summary panel	The icon or the name for the file system for home directories in the **Name** column. In the example above, SunnyvaleHomeDir
List directories	The **List Directories** icon to display a popup showing details about the directories created under the current file system for home directories.

To...	Click...
Modify the groups in file systems for home directories	The **Manage Groups** icon to open a popup where you can assign groups that will have home directories. See Managing group assignments on page 169
Delete home directories	The **Delete home directories** 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.

In this panel, you can also view:

- the names of all file systems set up for home directories
- the CIFS or NFS mount points for file systems for home directories
- the number of groups and directories for each file system for home directories

Creating file systems for home directories

Use the **Create a File System for Home Directories** wizard to guide you through the process of setting up a file system and home directories for groups of users.

5

Prerequisites

The home directories feature requires that Unity be configured to use Microsoft Active Directory for user authentication. To join Unity to AD, click **System > User Management**.

For general guidelines about file system management, see Before you begin on page 117

Step 1: Setting the name and storage pool below
Step 2: Configuring space settings on page 157
Step 3: Assigning user groups on page 160
Step 4: Assigning administrators on page 161
Step 5: Selecting an access protocol on page 162
Step 6: Enabling data protection on page 164
Step 7: Configuring your archive settings on page 165

Step 1: Setting the name and storage pool

In this step, set the name and storage pool assignment.

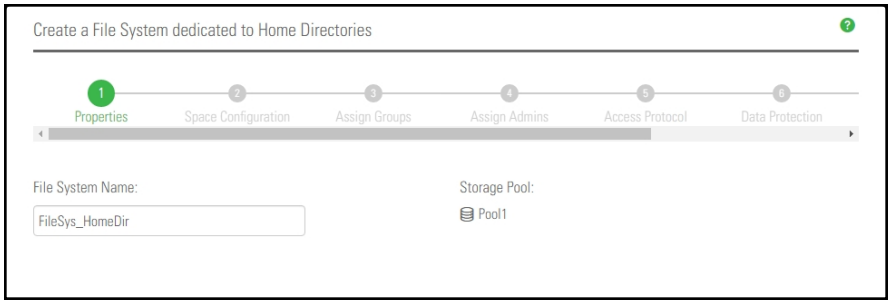
Prerequisites

- 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 5: Selecting an access protocol on page 162. In the **Unity Systems panel**, select **Summary > User Authentication**.

To set the Home Directory name:

1. On the **Unity navigation bar**, select **Storage > Home Directories**.
2. If necessary, log in with the required Active Directory credentials.
3. Click **Add Home Directories**. The wizard opens.

Figure 5-22: Setting the name and storage pool



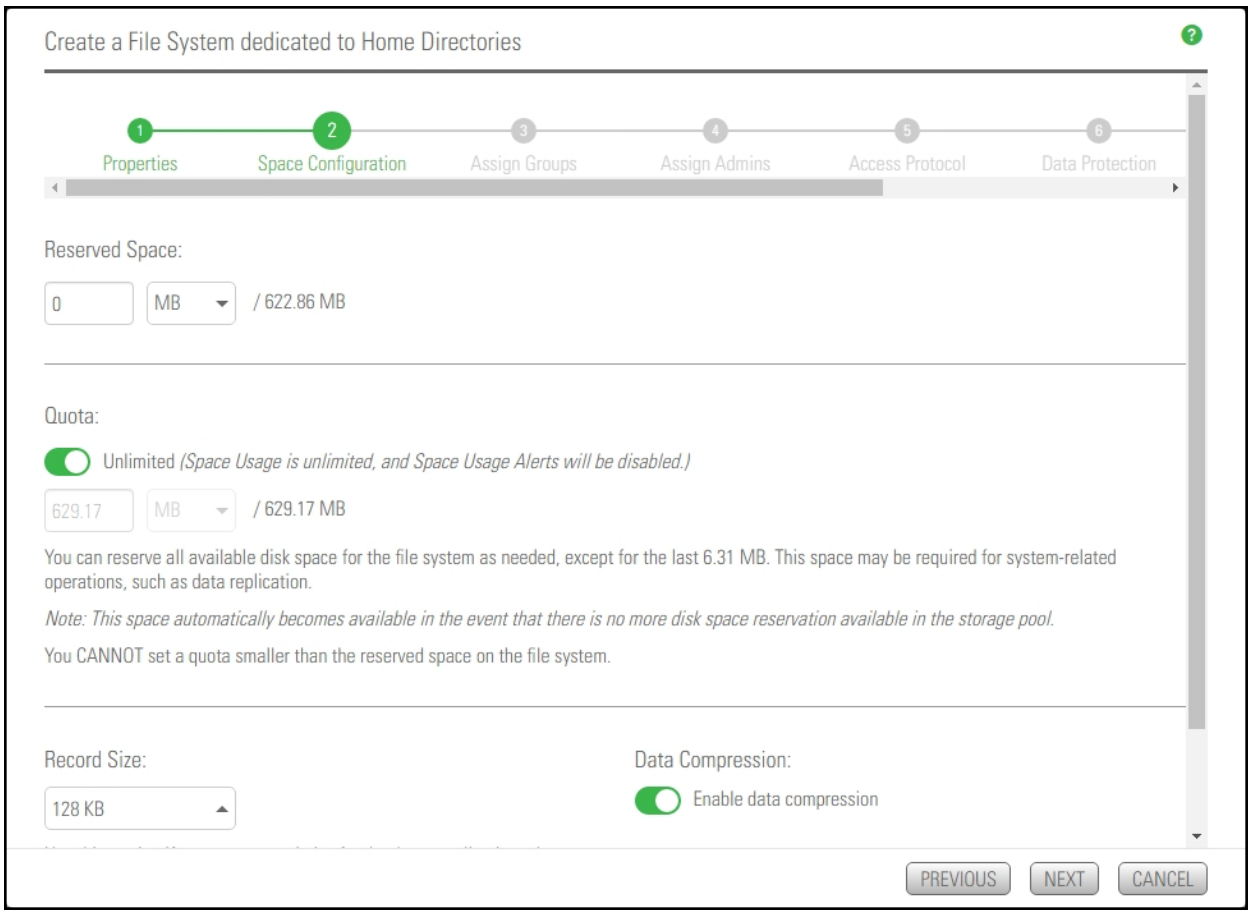
4. You can accept or change the:
   a. **File System Name**
   b. **Storage Pool** assignment, if more than one storage pool exists. Select which pool you want to assign the home directory to.

   Click the **Next** button to proceed.

Step 2: Configuring space settings

In this step, configure reserved space, quota, and record size.

Figure 5-23: Space settings



To configure space settings:

1. In the wizard step 2 **Space Configuration** panel, you can specify:

Setting	Description
Reserved Space	***You can reserve a set amount of disk space in the storage pool for the exclusive use of the file system. (Read more ...)*** 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. **To reserve space for the file system in the storage pool:** ● Move the slider left or right to set the desired amount of reserved space, Or ● Enter a value in the box to the right of the slider. **Note** 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. (Read more ...)*** You can reserve all available disk space for the file system, if needed, except for the last 6.31 MB, which space 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.) **To set an unlimited quota:** ● Enable the **Unlimited** quota checkbox. **To specify a quota:** 1. Uncheck the **Unlimited** quota checkbox. 2. Enter a value in the text box.

Setting	Description
Record Size	***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 ...)*** 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 the database record size is precisely known. File systems have a default record size of 128 KB, which is the maximum size.
Data Compression	**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. You can enable/disable compression at the file system level. 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. 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. 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.

2. Click the **Next** button.

Note Step 5: Selecting an access protocol on page 162 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.

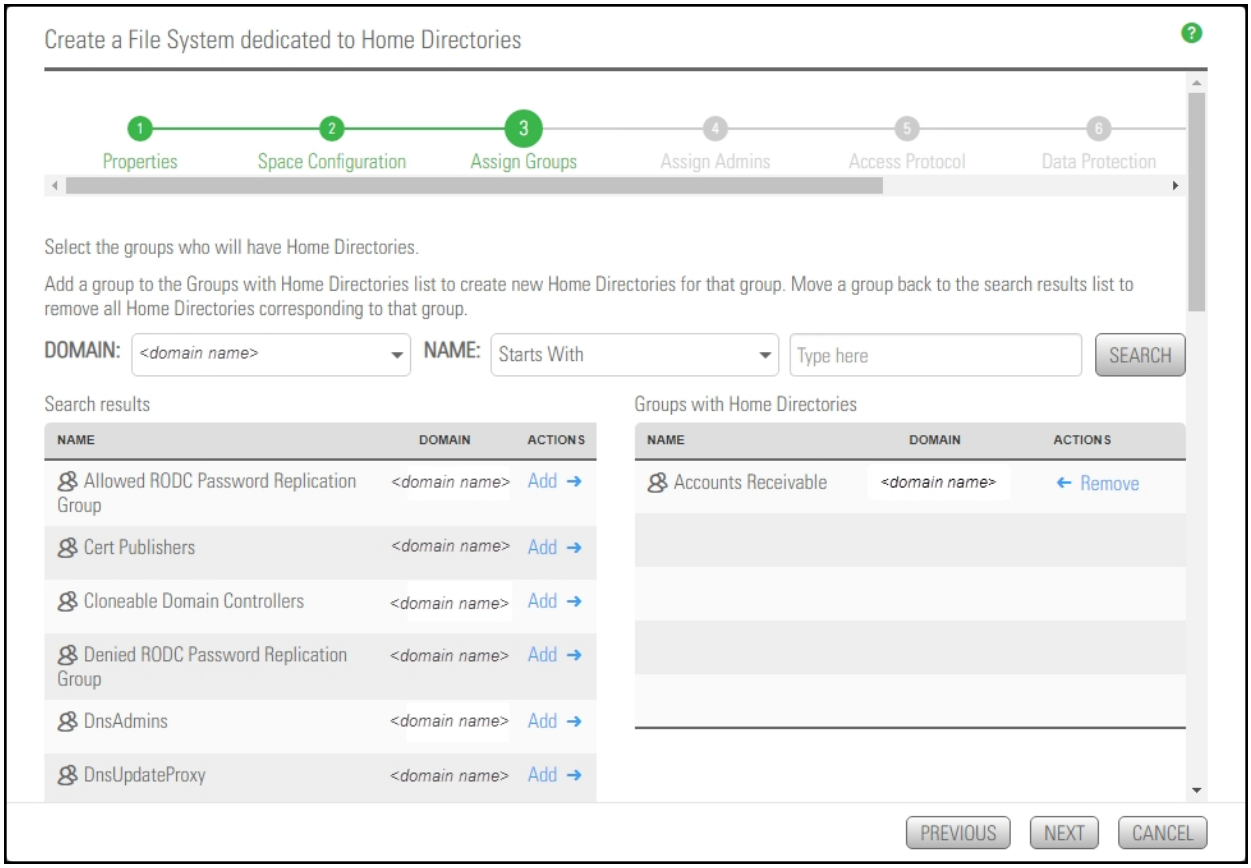
Step 3: Assigning user groups

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 5-24: 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 **Add** in the **Search results** list for the group or groups you want to create home directories for.

   You can click **Remove** in the **Groups with Home Directories** list to remove the assignment. See also Managing group assignments on page 169
3. Click the **Next** arrow to proceed.

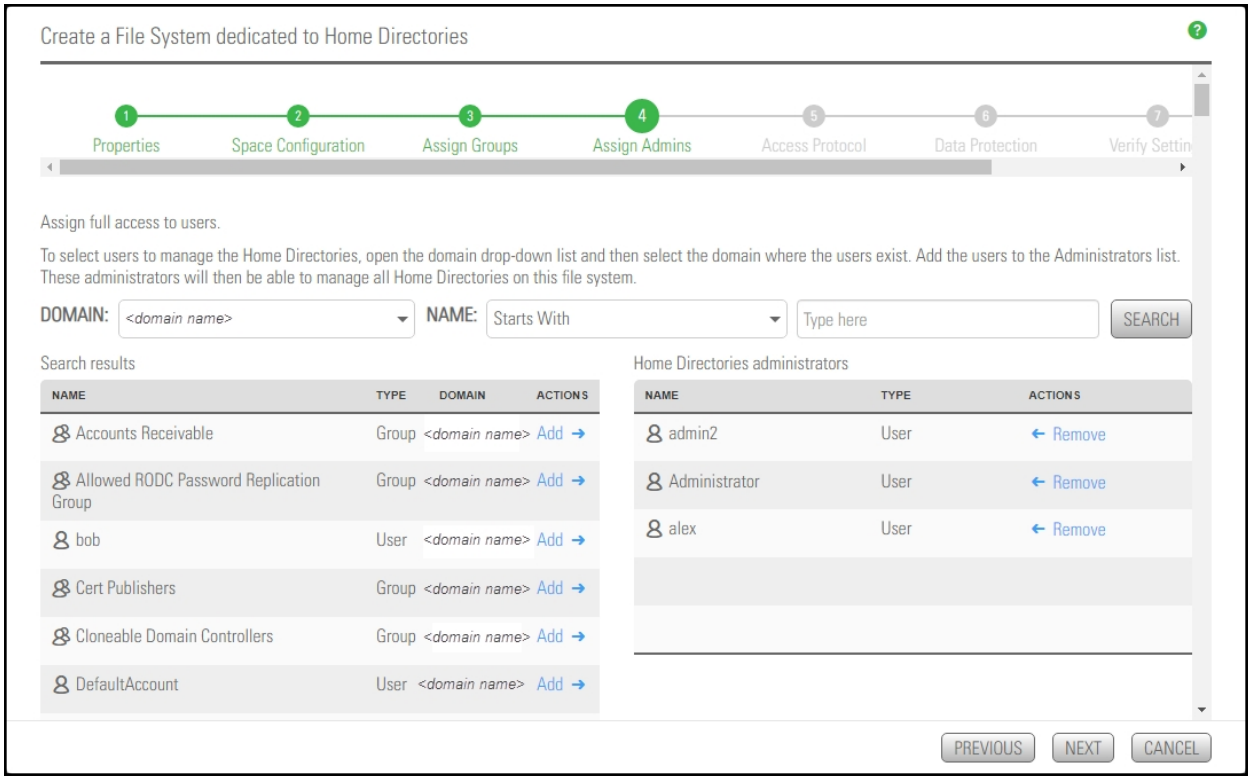
Step 4: Assigning administrators

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 5-25: Assigning administrators



▶ **To assign administrators to manage home directories:**

1. Click to select users or group from the **Search results**.
2. Click **Add** in the **Search results** list for the users or groups you want to assign as administrators to manage the new home directories.

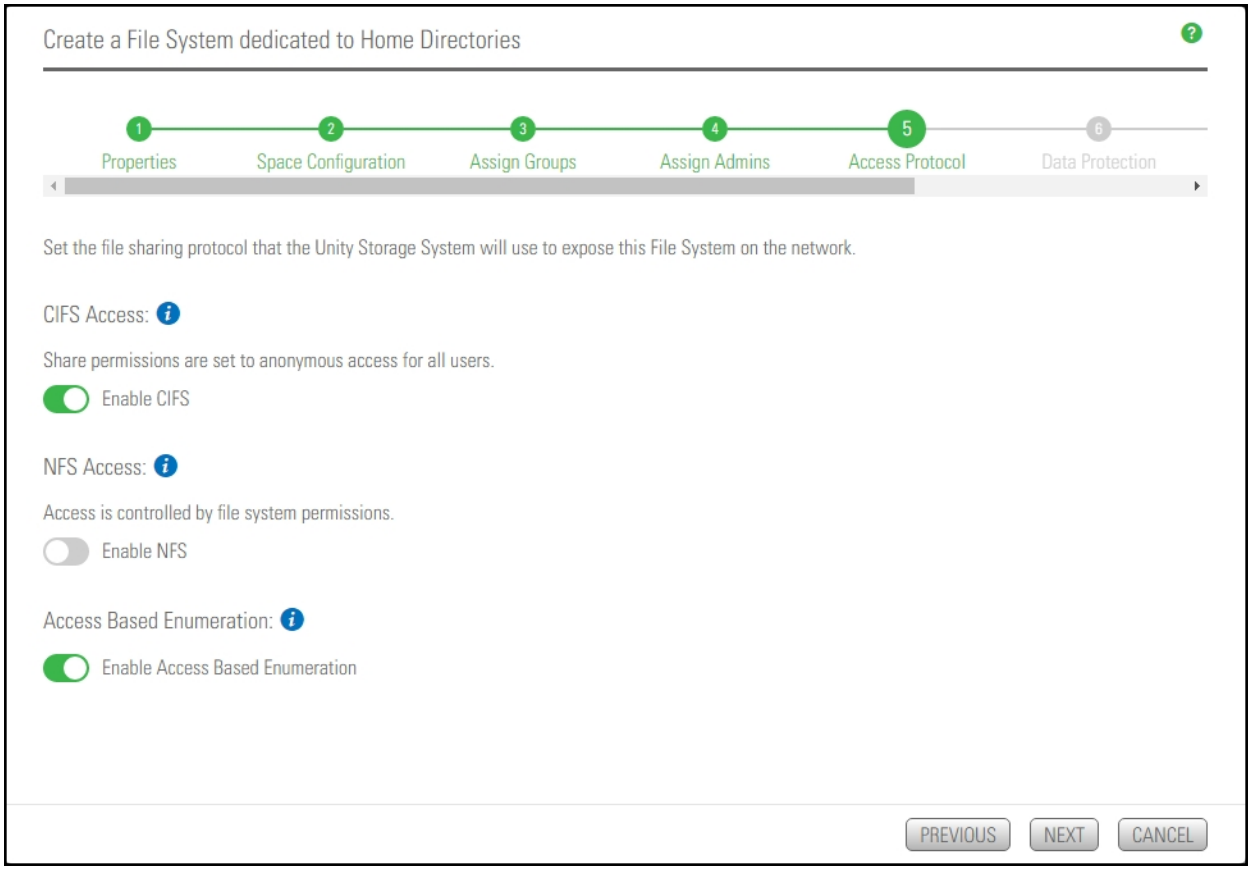
   You can click **Remove** in the **Groups with Home Directories** list to remove the assignment.
3. Click the **Next** arrow to proceed.

Step 5: 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 5-26: 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.

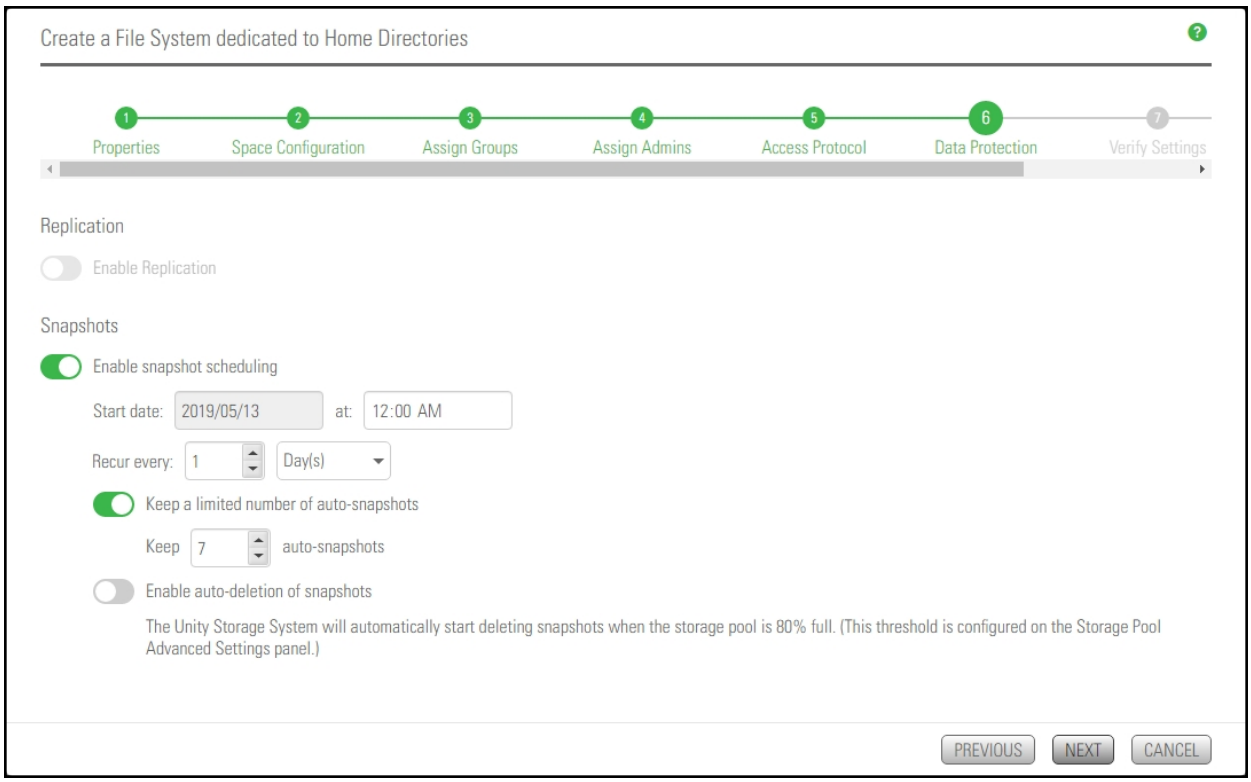
Step 6: Enabling data protection

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.

Figure 5-27: Enabling data protection



To enable data protection for the file system for home directories:

1. To enable software encryption, select **Enable software encryption**. By default, **Export encryption key** is pre selected. **NOTE**: Encryption can only be set during creation time. The operation cannot be undone.
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.

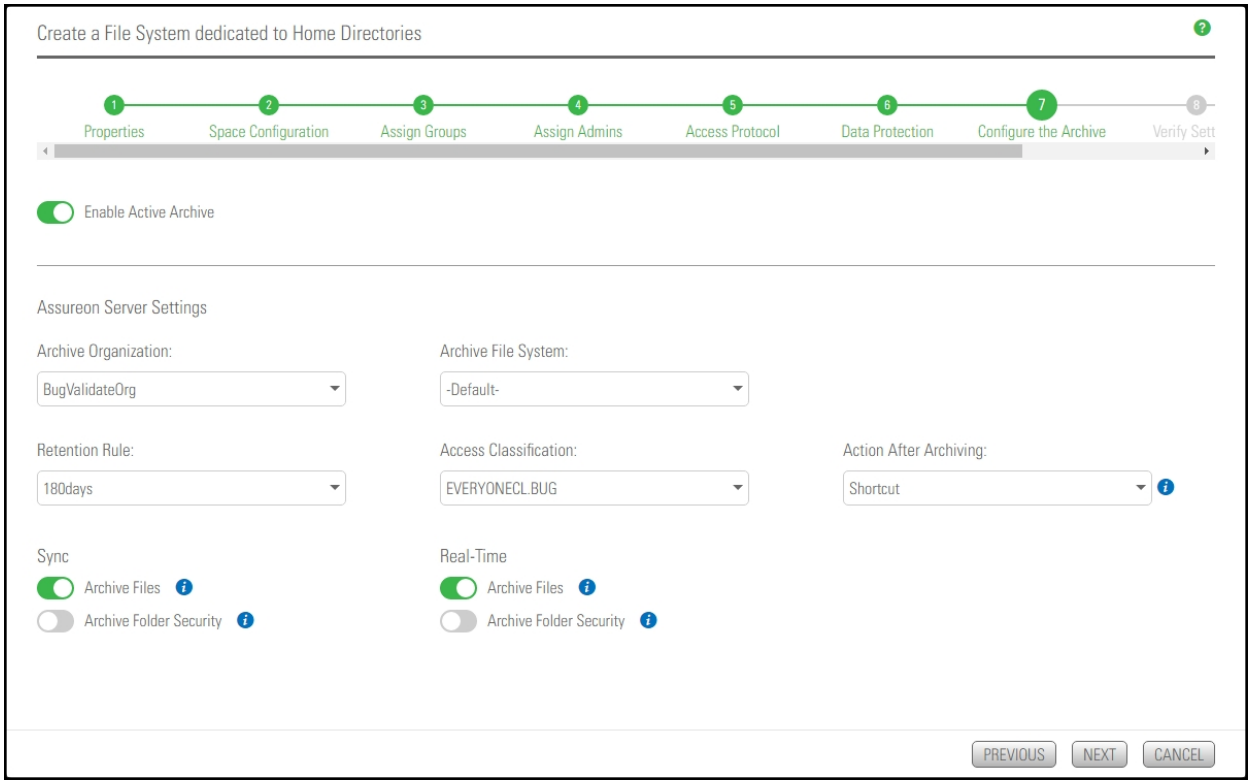
6. If your Unity System is connected to a remote Unity System and has replication set up, select **Enable Replication**.
7. Click the **Next** button.

Step 7: 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 Unity Active Archive on this Unity. 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.



To configure Active Archive settings:

1. Select **Enable Active Archive**.
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.

   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.

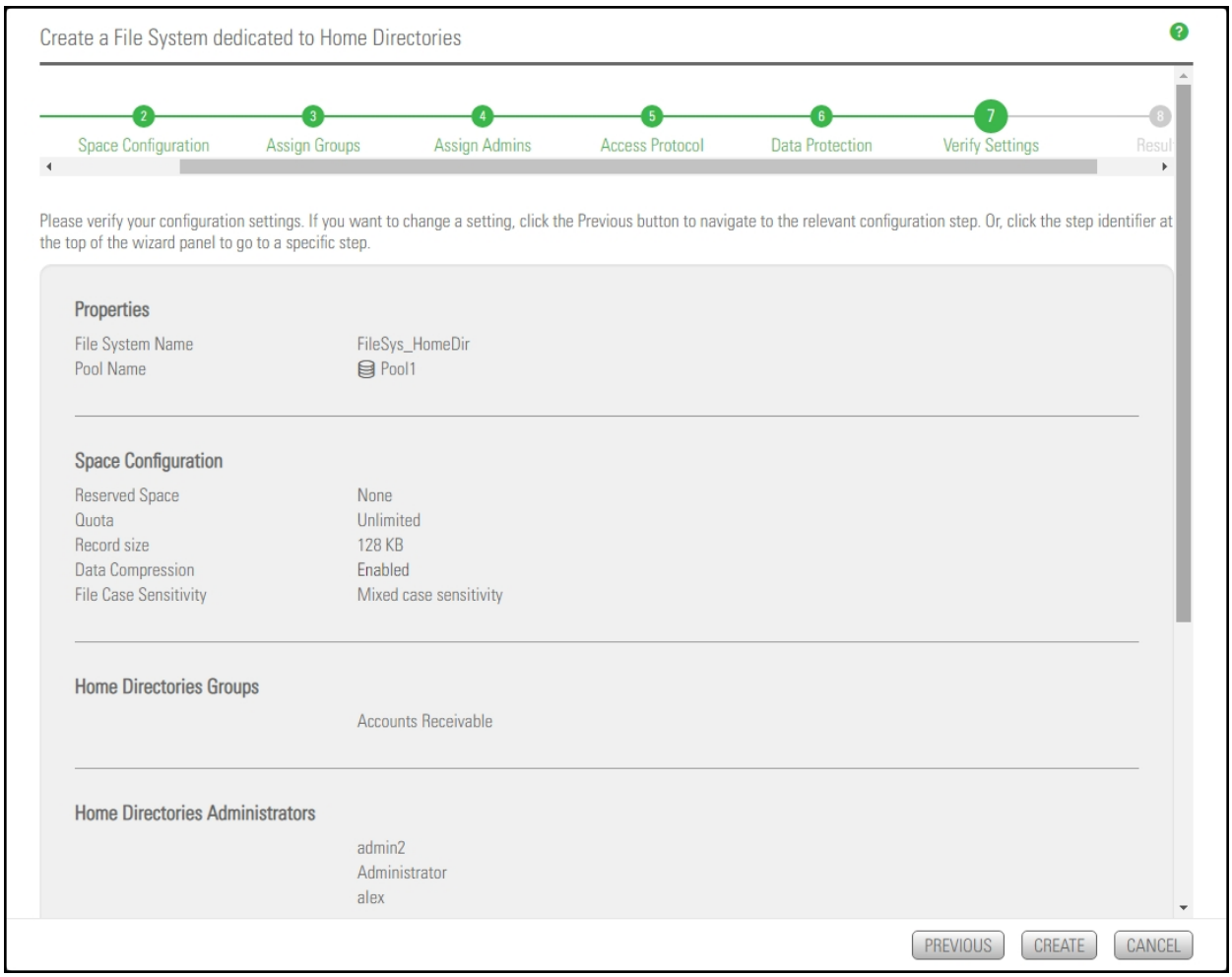
   Table 5-5: Assureon Server Settings

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. For example, create a shortcut to the files, leave them as they are, or remove them from the file system. **Note** Files will not be converted to shortcuts, or removed if asynchronous replication is enabled.
Real Time Archiving	Performs a persistent and ongoing archive of files, as changes are detected. Files are checked and archived if necessary every minute. Enabled or disabled on the Assureon Server under **Advanced Settings**, or using the nxcmd command line interface. See "Setting the realtime delay" in the *nxcmd Command Line Interface Reference Guide*, or visit Nexsan.com/support.
Scheduled Archiving	Performs a complete archive of the file system, either manually or on a schedule. This feature does not affect Real Time Archiving. Enabled or disabled on the Assureon Server on the **Advanced Settings > General tab**. Select the **Sync** checkbox.

Verifying settings

In this step, the wizard displays the file system for home directories settings for review.

Figure 5-28: Verifying settings

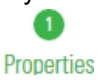


To review your settings:

1. Review the summary of the settings shown on screen.
2. To revise any of your settings, you can click **Previous** to go back.

   OR

3. Click any of the step numbers at the top of the panel to jump to that section of the wizard. For example, if you want to change **Properties**, click:

4. When you are ready to proceed, click **Create**.

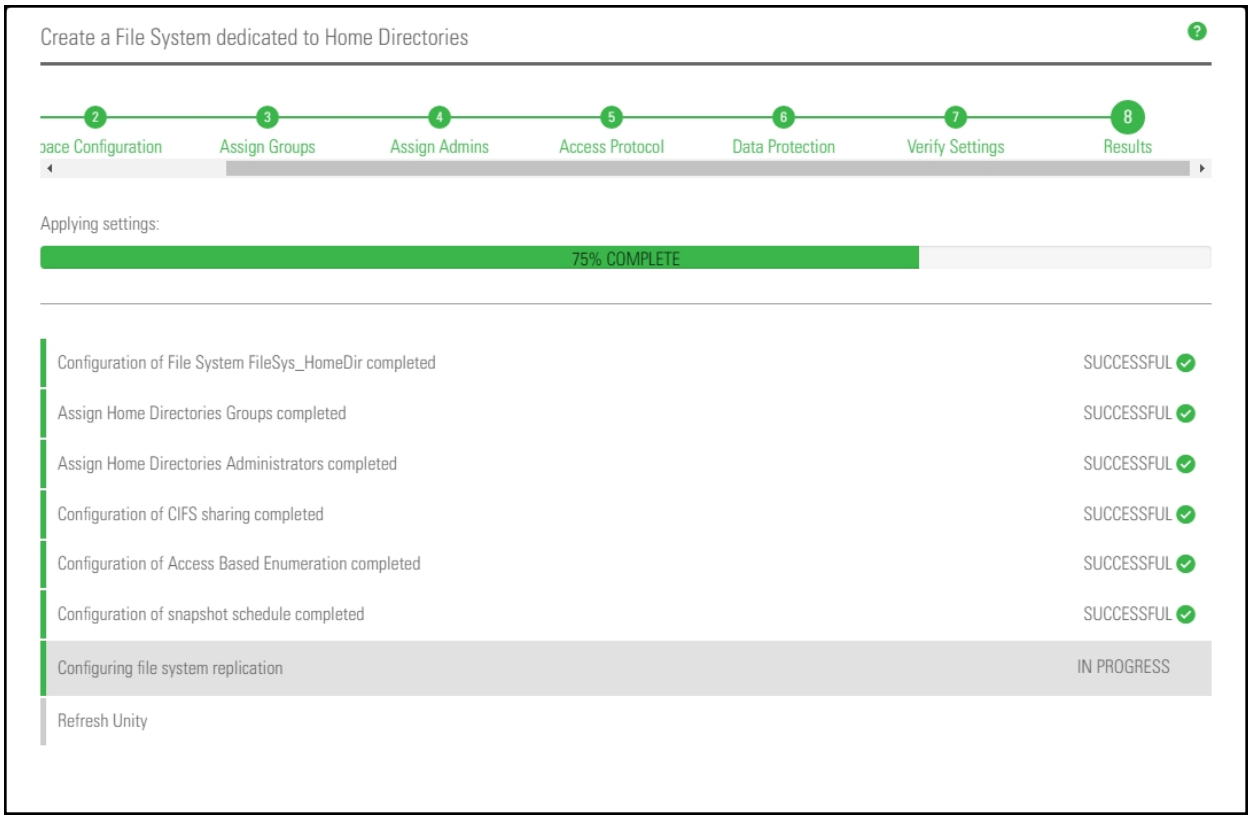
The wizard displays file system creation progress as it applies your settings.

Now you can **Add another file system** or click **No, I'm finished**.

Viewing results

In this step, the wizard displays progress and results as Unity creates the new file system for home directories.

Figure 5-29: 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 **View Error** link corresponding to the error event.

Unity informs you when it successfully creates the file system and home directories.

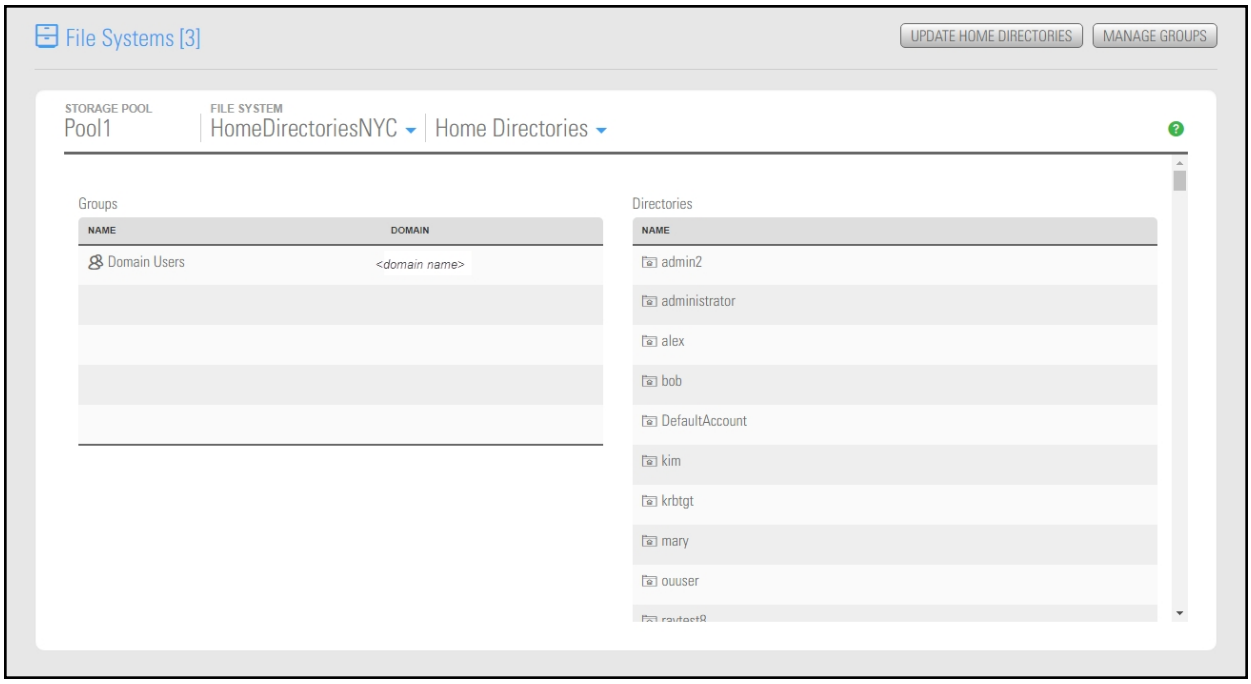
Managing group assignments

Use this procedure for help with 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 5-30: File Systems > Home Directories panel



To modify the groups in a file system for home directories:

1. Click **Storage > File Systems** and click the link to open the file system for the home directory.
2. Click **Summary > Home Directories**. The **Home Directories** panel opens.
3. Click the **Manage Groups** button to open a popup window, where you can assign groups that will have home directories.
4. Click the **Add** or **Remove** buttons beside any given group. The domain you use when you set up the file system for home directories determines the available groups.
5. Click the **Apply** button.
6. 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.

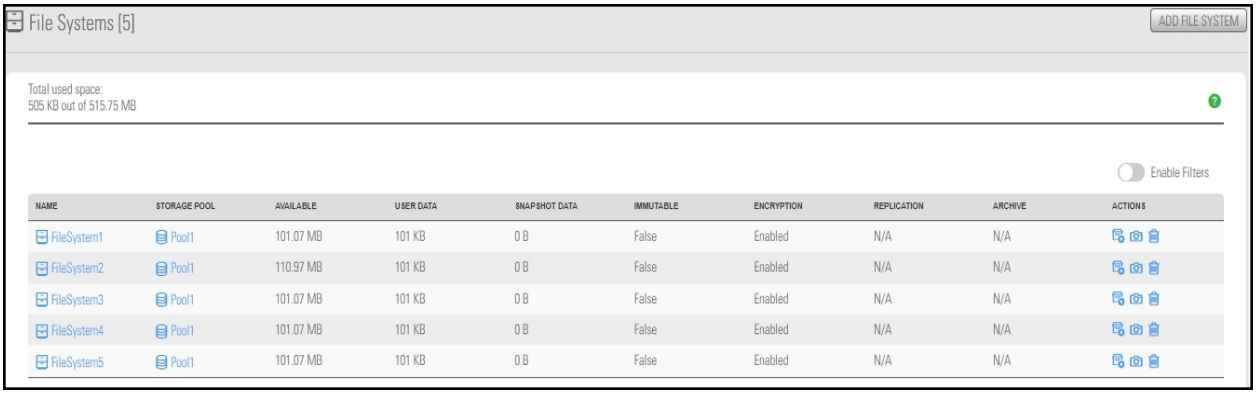
Performing file system-level tasks for home directories

Use this topic for information about file system-level features available for home directories.

▶ **To open the File Systems panel:**

- Click **Storage > File Systems**.

Figure 5-31: File Systems panel

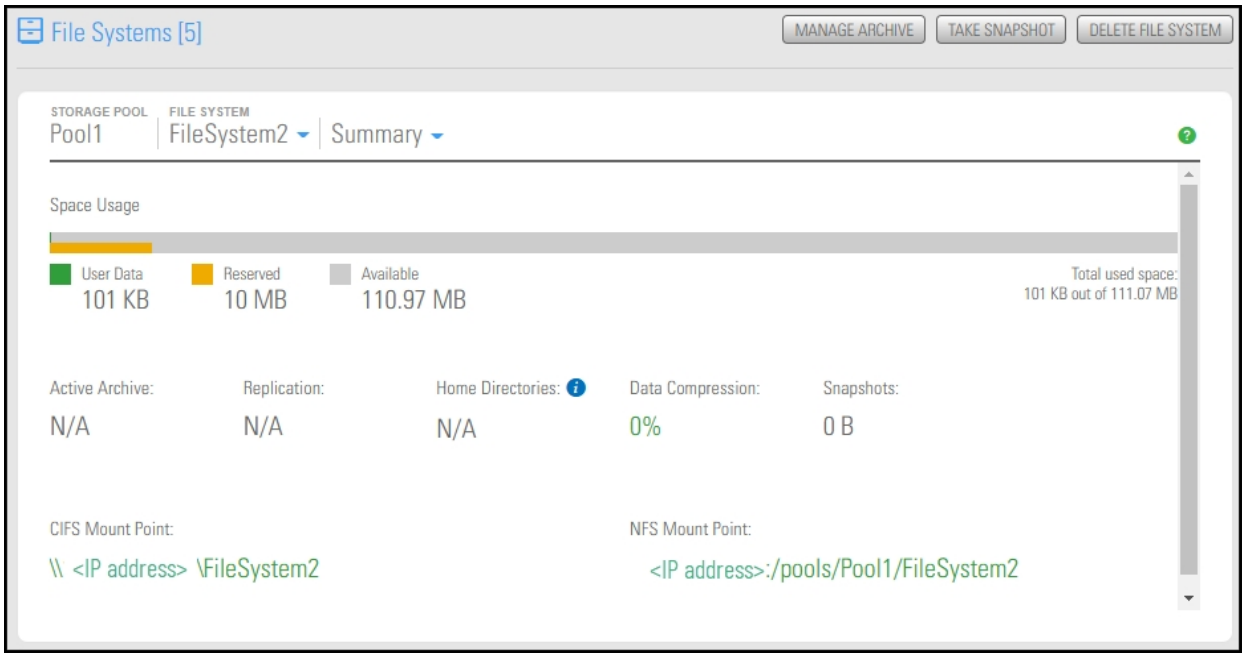


To...	Click...
Open the File Systems > Summary panel for the home directory	The icon or the name for the file system for home directories in the Name column. In the example above, FSHomeDirs
Delete a file system for home directories	The **Delete Home Directory** icon to open a popup where you can delete 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.

▶ **To open the File Systems > Summary panel for a file system for home directories:**

1. Click **Storage > File Systems**.
2. Click the icon or the name for the file system for home directories. In the example above, FSHomeDirs

Figure 5-32: File Systems > Summary panel



To...	Click...
View or update Active Archive settings	The **Manage Archive** button in the **File Systems** panel. See Managing Active Archive settings for file systems on page 431
Take a snapshot of the data	The **Take Snapshot** button. See also Viewing file system snapshots on page 204
Delete a file system for home directories	The **Delete Home Directory** button 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.

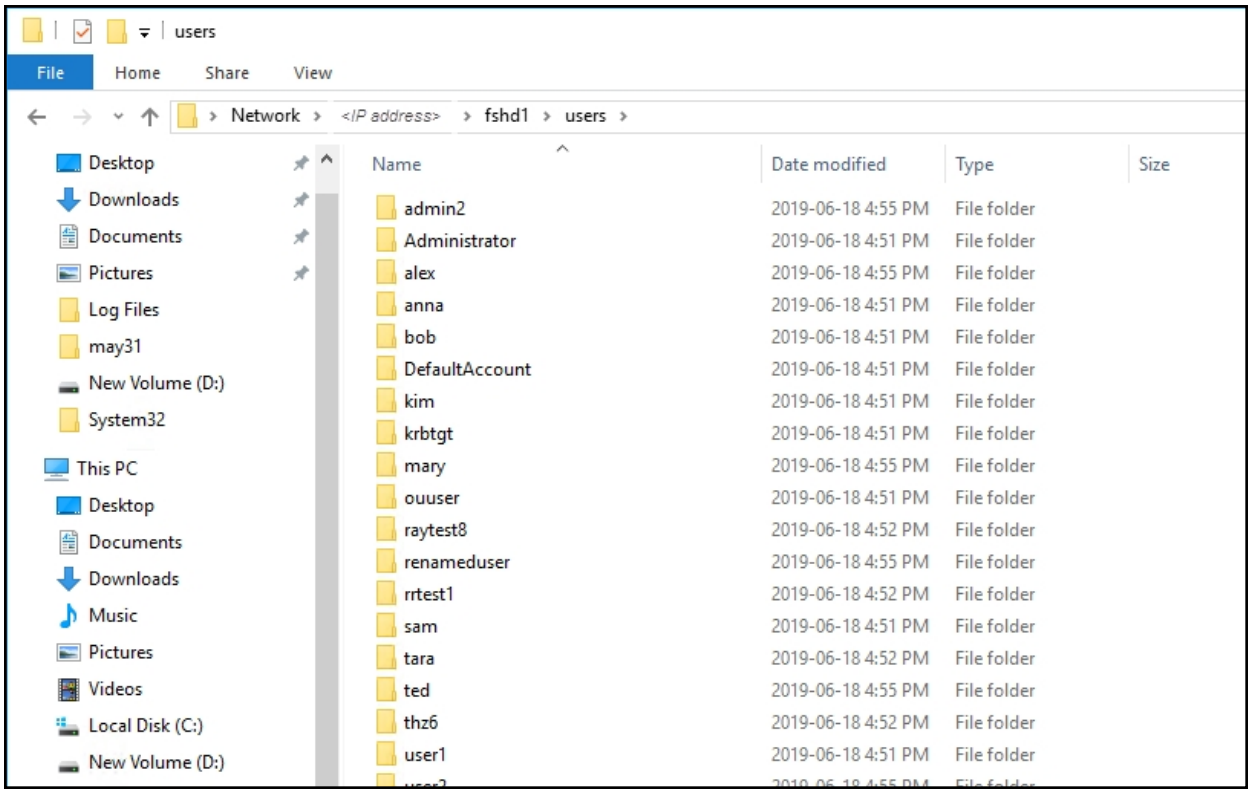
In this panel, you can also view:

- Statistics for the pool and file system containing the home directories
- Active Archive status and details
- The CIFS Mount Point

Example file system for home directories

Here is an example of a file system set up for home directories in Windows:

Figure 5-33: Viewing a file system for home directories in Windows



For instructions about how to connect to a Unity file system, see Accessing CIFS shares on page 180.

Managing CIFS shares

Unity enables you to add CIFS shares to file system on Unity. A CIFS share is a shared network folder that resides inside a parent file system. Unity exposes a CIFS 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.

About Managing CIFS shares

You can add CIFS shares to Unity file systems. A CIFS share is a shared network folder that resides inside a parent file system. Unity exposes a CIFS 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.

Note Unity currently does not support exposing a file system over the NFS protocol. When you add a file system to an NFS share, Unity automatically exposes the file system over the CIFS protocol.

- **Access permissions:**

A share inherits access permissions from its parent file system, so a user or group that has access to the parent file system will automatically have access to all shares within the parent file system. However, you can set user access to it independently from its parent file system. That is, you can give a different set of users and/or groups access permissions to the share.

This mechanism enables you to set up a secure and dedicated network repository for each user and/or group on the network, while preventing unauthorized access to potentially sensitive data in the parent file system, or in other shares that reside within the parent file system.

In a more specific context, you may only want to give an administrator *Full* access to a share, and allow individual users and/or groups on the network restricted access to specific data in the share in order to limit exposure to sensitive information; the traditional way of doing this is to set access restrictions for individual users and/or groups at the folder and/or file level within the share, by configuring Windows and/or UNIX/Linux ACLs.

For example, you can add a Finance share for the Finance group to Unity—assigning only an administrator *Full* access permissions to the share; then, you can add a share for each member of the Finance group to the Finance share—assigning each member access permissions to their respective share. In this scenario, the administrator will have *Full* access to all the data in Finance share, including all the data in the shares; while individual user accounts in the Finance group will only have access to their respective share in Finance share—either *Read*, *Read/Write*, or *Full* access. Depending on the share-level access permissions set, a user in the Finance group accessing the Finance share from a client computer on the network will see either both the parent file system and the share, or only the share.

- **Space usage settings, snapshots, and Data Replication for shares:**

A CIFS 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 Storage System—provided that you enable and configure Snapshots and Data Replication on the parent file system.

Adding CIFS shares

Unity provides the Create CIFS Share wizard to guide you through the process of adding a CIFS share.

To start the Create CIFS Share wizard:

1. On the **Unity navigation bar**, select **Storage > File Systems**.
2. Select the file system you need to add the CIFS share to.
3. Select **Summary > CIFS Shares**.

Figure 5-34: CIFS Shares panel



4. Click the **Add Share** button. The Create CIFS Share wizard opens to guide you through the process of adding a share.

5

This section includes these steps:

Step 1: Setting the CIFS share location and name 175
Step 2: Assigning access permissions to a CIFS share 176
Step 3: Verifying CIFS share settings 178

Step 1: Setting the CIFS share location and name

Step 1 of the Create CIFS Share 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 CIFS share as hidden, the share is not visible to Windows-based clients on the network; Windows-based clients interpret a hidden CIFS share as an administrative share on the network, and prevent its display when you browse shares on Unity. This mechanism enables you to further restrict access to a CIFS share, as 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:

- When you add a CIFS share to an NFS share, Unity automatically exposes the share over the CIFS protocol. Unity currently does not support exposing a CIFS share over the NFS protocol. This restriction also applies when you add a CIFS share to a file system 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 file system to NFS sharing.

Figure 5-35: Setting the CIFS share location and name



To create a CIFS share:

1. Enter a path and name for the CIFS share in the open text field.

   You can click plus ✚ to add a new folder.

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

   These characters are NOT allowed:

   ” / \ [ ] : ; | = , + * ? < >

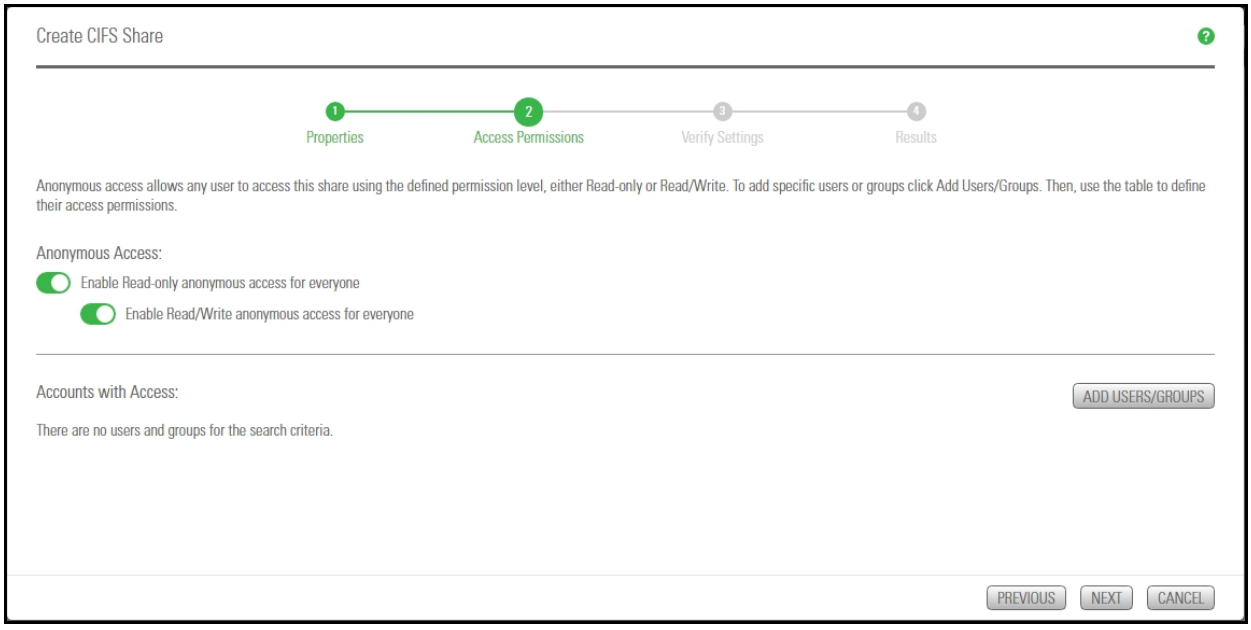
   Note You can also manually enter a new location for the share, using the Path Bar. Or, you can use the Share Explorer to navigate to the new location for the share. Click plus ✚ to create additional locations within the file path.

2. (Optionally) Select the **Make this a hidden CIFS share** option.
3. Click the **Next** button to continue to Step 2: Assigning access permissions to a CIFS share below.

Step 2: Assigning access permissions to a CIFS share

Step 2 of the Create CIFS Share wizard prompts you to select the users and/or groups that will access the CIFS 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, you can search for users and/or groups that you defined on the system.

Note 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 CIFS share:

1. Disable the default Anonymous Access permissions.

   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 CIFS share, if needed.

2. Click the **Add Users/Groups** button. The list of existing users and groups displays.
3. 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).
4. 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.

   Click the **Apply** button to display access permission options for each user and/or group added.
5. In 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 CIFS share, click the **Next** button to continue to Step 3: Verifying CIFS share settings on the next page.

Note You can modify the CIFS Shares later as required in the **File Systems > CIFS Shares panel**.

CIFS Share actions table

The following icons and actions display in the CIFS Shares panel after you create a share. For tool tips, hover the mouse pointer over the icons in Unity.

Icon	Action
	Rename CIFS Share
	Manage Hidden CIFS Share
	Manage Access Permissions for CIFS Share
	Move CIFS Share
	Unshare CIFS share

Step 3: Verifying CIFS share settings

Step 3 of the Create CIFS Share wizard summarizes the settings you selected for your share and creates the share when you click **Create**. 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 Create CIFS Share wizard panel. For example, if you want to rename the CIFS share, click **Step 1**.

If you are satisfied with the configuration settings, click the **Create** button at the bottom of the panel. The Create CIFS Share Setup wizard applies your settings. You can then click **Yes** to run the wizard again or click **No** to close it.

Step 4: Viewing results

Step 4 of the Create CIFS Share wizard displays progress as Nexsan Unity creates the new CIFS share.

Figure 5-36: Create CIFS Share wizard: Viewing results



The Create CIFS Share wizard displays error events that the system encounters during the CIFS 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 **View Error** link next to the error in the **Results** panel.

Unity informs you when it successfully creates the CIFS 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 CIFS 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 page 181.

Accessing CIFS shares

This section explains how to access a CIFS share on a Unity Storage System from Windows and UNIX/Linux-based systems.

Table 5-6: Supported accessibility methods

CIFS sharing	NFS sharing	FTP sharing	CIFS and/or NFS and/or FTP sharing
The CIFS share can be accessed from:			
• Windows-based systems using CIFS	• Windows-based systems using an NFS version 3[1] client	• Windows-based systems using FTP	• Windows-based systems using CIFS and/or FTP
• UNIX/Linux-based systems using a CIFS client	• UNIX/Linux-based systems using NFS version 3 and/or NFS version 4	• UNIX/Linux-based systems using FTP	• UNIX/Linux-based systems using a CIFS client and/or FTP
		Note FTP sharing is only supported for local authentication.	• Windows-based systems using an NFS version 3 client and/or FTP
			• 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 181
Accessing an NFS file system from UNIX/Linux 184
Using an NFS version 3 (NFSv3) client to access an NFS share with Microsoft Active Directory 185
Using an NFS version 4 (NFSv4) client to access an NFS share 186

[1] If 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.

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.

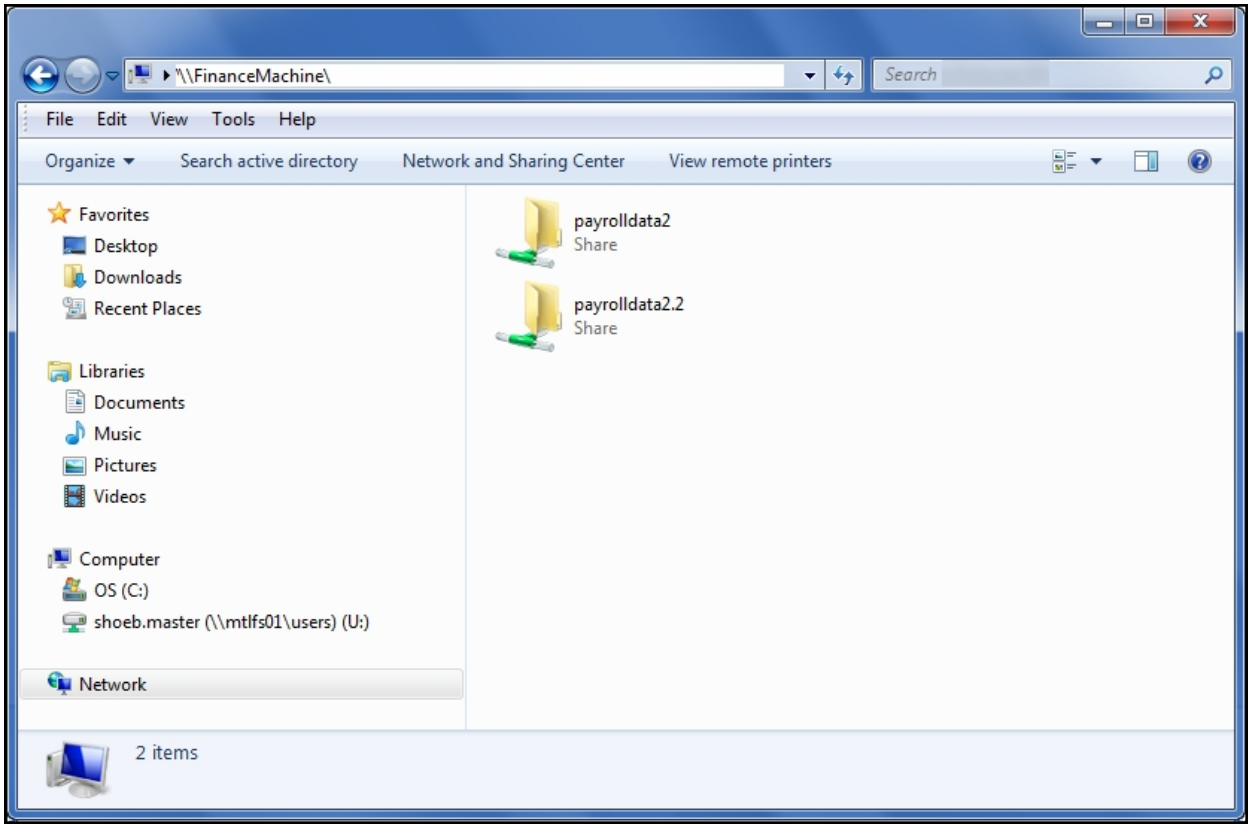
Note To access a share, your user account must be granted access permissions to the share in Unity (or it must be a member of a group that is granted access); see Viewing file system mount point information on page 192.

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 a virtual IP address, Enter:

   `\\<virtual IP address>\`

   Tip You can also access a share directly on Unity by adding the share's name in the address path; for example: `\\<virtual IP address>\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 70.

     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 file systems on page 194.



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 Managing file system- or CIFS share-level access permissions on page 197.

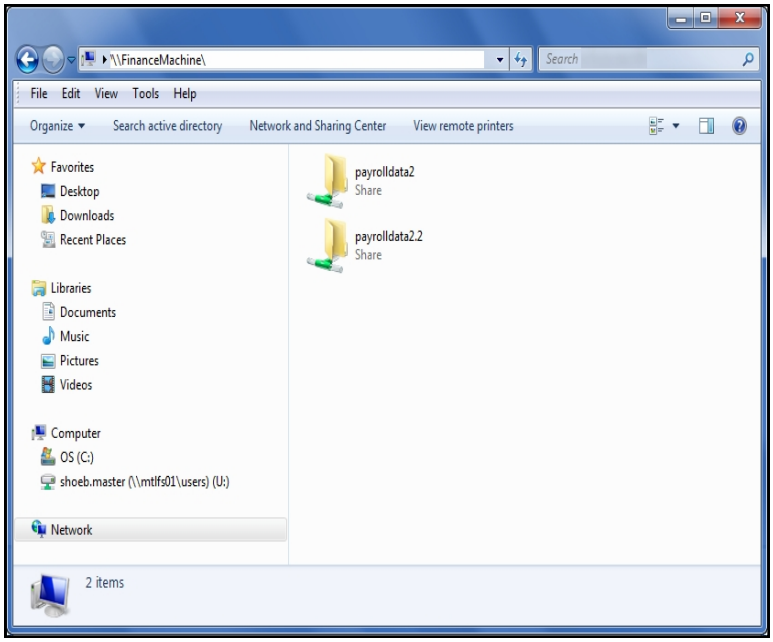
To map a CIFS share to a drive letter on a Windows-based system:

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 a virtual IP address, type:

   `\\<virtual IP address>\`

   Tip You can also access a share directly on Unity by adding the share's name in the address path; for example: `\\<virtual IP address>\payrolldata2`.
3. Press the Enter key. This displays all the CIFS shares on Unity.

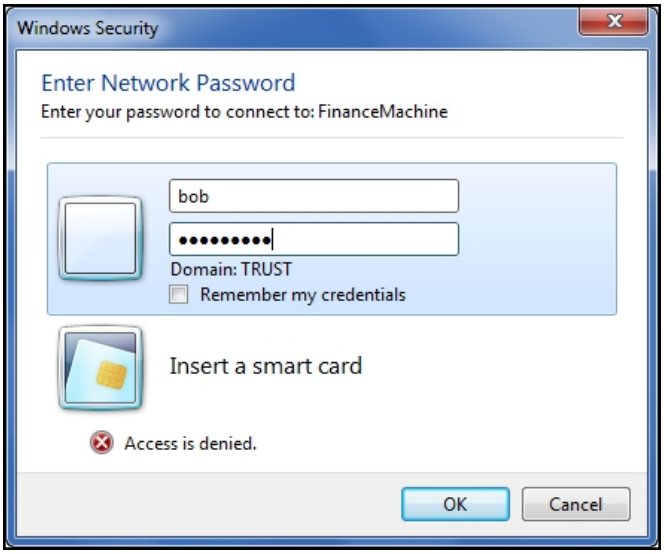
Figure 5-37: Mapping a CIFS share to a drive letter on a Windows-based system



4. Right-click the share that you want to access and select the **Map network drive** option.

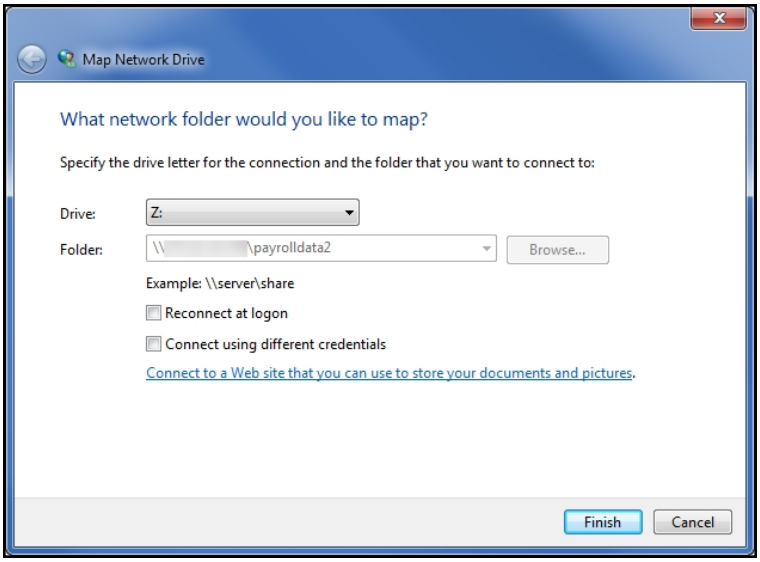
5. You may be prompted for a user name and password to access the share. Enter a valid user name and password and click **OK**.

Figure 5-38: Specify a user name and password to map the CIFS share



6. 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 5-39: Map network drive



7. 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 <virtual IP address>:/pools/FinancePool/PayRollData2
   /mnt/payrolldata/
   ```

   Substitute `<virtual IP address>` 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 file system mount point information on page 192.

   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 NSFv4 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. Use the nxadmin CLI to specify a domain name to enable user/group mapping between Unity and your NFSv4 clients.
   For example, `nfs domain set nst.domain`
2. 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 (for example, Linux/CentOS), you must:

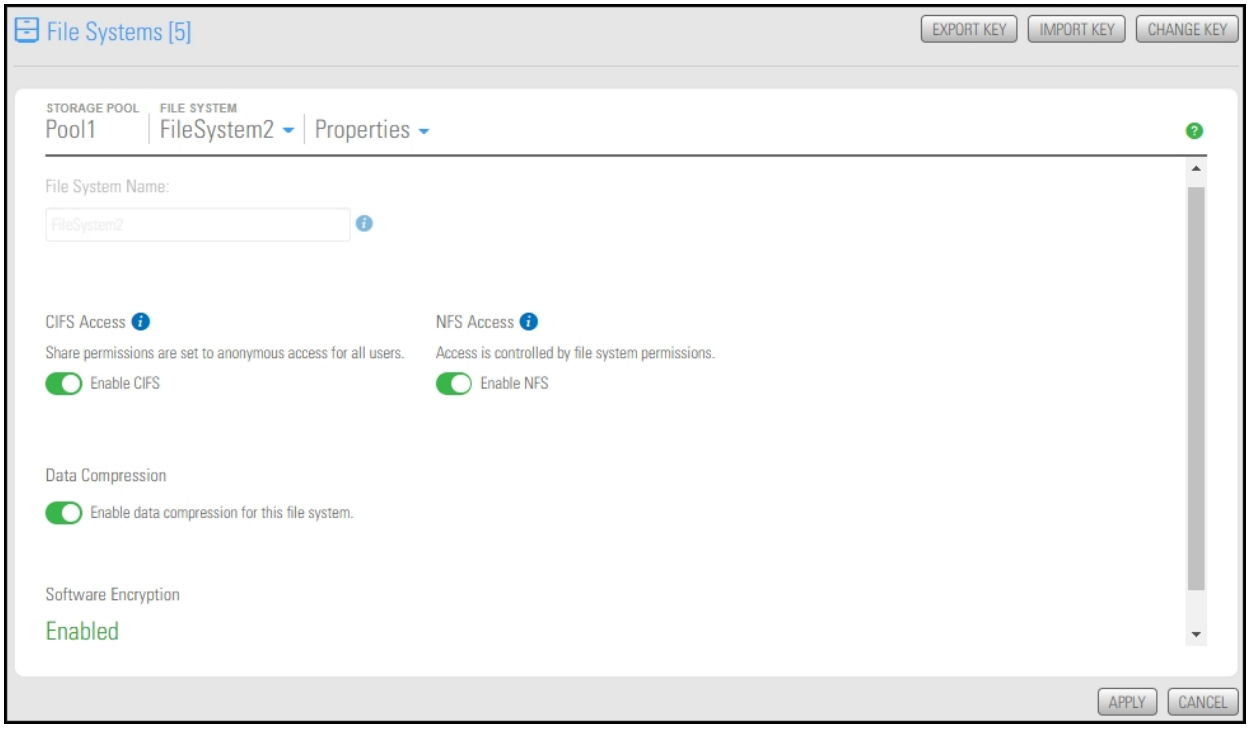
1. Add the NFSv4 domain name you specified on Unity to the `/etc/idmapd.conf` file.
2. Stop and then restart the `idmap` (Identity Mapping) service.
3. Make sure this service starts on system boot up: `chkconfig rpcidmapd on`
4. Mount the NFS share.

To configure NFSv4 support:

1. On the **Unity navigation bar**, select **Storage > File Systems**.
2. Click the link to the file system you need to access.
3. Select **Summary > Properties**.

4. Click the **Enable NFS** button 

Figure 5-40: File System Properties panel



5. Click the **Apply** button to save your settings.

6. Use the nxadmin 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. Enter `menu`.
   d. In the NestOS Admin Menu, enter **4** (**Run a Command**).
   e. At the `command:` prompt, enter 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 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.
   f. At the `command:` prompt, enter 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
      - 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.
7. Mount the NFS share.

Renaming a CIFS share

If you rename a CIFS share, client systems on the network that have a network drive mapped to the share will lose connection to the share; this could result in data loss. Before renaming a CIFS share, make sure that client systems with an active connection to the share disconnect any mapped drives to the share; also make sure to quiesce any applications with an active connection to the share.

CAUTION: Renaming a CIFS share will disconnect any users or applications currently accessing the CIFS share. If the share is mapped to any Windows-based client computers, you will need to recreate the mappings using the share's new name.

To rename a CIFS share:

1. On the **Unity navigation bar**, select **Storage > File Systems**.
2. Click the link to the file system you need to access.
3. Click **Summary > CIFS shares**.
4. In the **Actions** column, click the **Rename Share** icon for the CIFS Share that you want to rename.

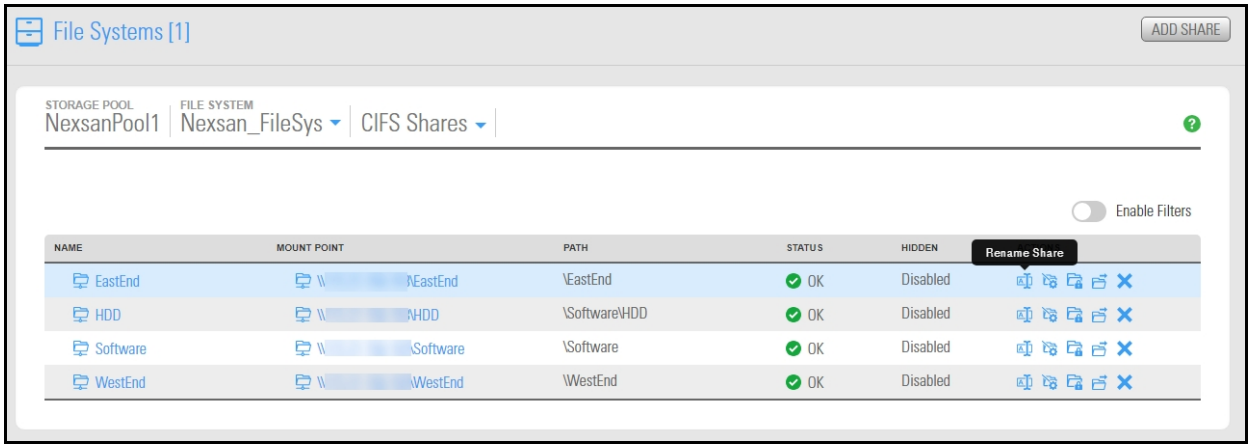
   You can search f a specific CIFS share in the grid filter the list, by enabling filters entering characters in the text boxes located above the columns or or by choosing from the options in the **Status** and **Hidden** columns.
5. Enter a new name for the share.

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

   These characters are NOT allowed:

   ” / \ _ [ ] : ; | = , + * ? < >

Figure 5-41: Renaming a CIFS Share



6. Type **Rename** in the bottom text box to confirm your choice.
7. Click **Rename**.
8. 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.

Moving a CIFS share

This section describes how to move a CIFS share.

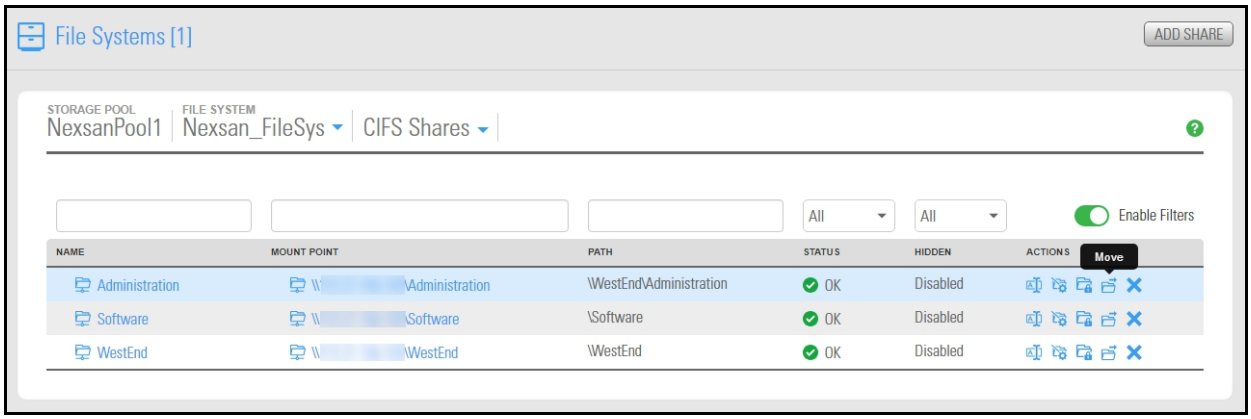
CAUTION: Moving a CIFS share will disconnect any users or applications currently accessing the share. If the CIFS share is mapped to any Windows-based client computers, you will need to recreate the mappings using the share's new name.

To move a CIFS share:

1. On the **Unity navigation bar**, select **Storage > File Systems**.
2. Click the link to the file system you need to access.
3. Click **Summary > CIFS shares**.
4. In the **Actions** column, click the **Move** icon for the CIFS Share that you want to move.

   You can search f a specific CIFS share in the grid filter the list, by enabling filters entering characters in the text boxes located above the columns or or by choosing from the options in the **Status** and **Hidden** columns.

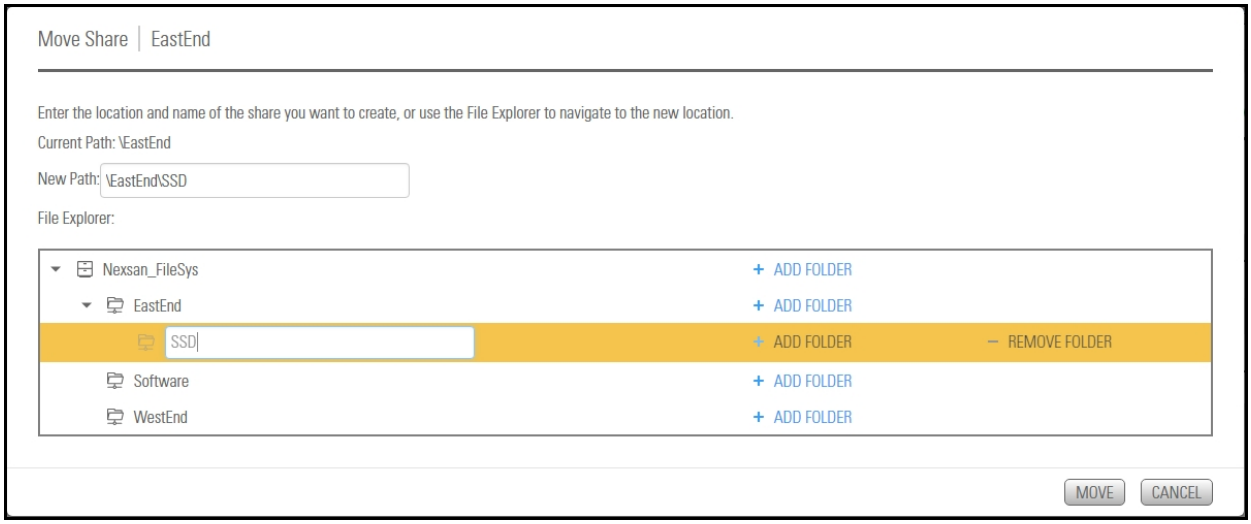
Figure 5-42: File Systems CIFS Shares panel



5. Review the **Move Share** warning information, and type **Confirm** when you are ready to move the share.

6. Click the **Confirm** button. The **Move Share** window opens.

Figure 5-43: Move Share window



7. Do any of the following:
   - Enter a new name for the share in the New Path box.
   - Select a new location from existing CIFS Share locations.
   - Click the plus sign icon to add a new folder.
8. Click the **Move** button. Unity moves the CIFS share.

Unsharing a CIFS share

When you unshare a CIFS share, you remove the sharing connection, without affecting the data contained in the shared space.

CAUTION: Unsharing a CIFS share makes it inaccessible on the network, although data in the share remains intact, but if the share is being replicated, the replica on the remote system will also no longer be accessible on the network. The share will no longer be displayed in Unity.

To unshare a CIFS share:

1. On the **Unity navigation bar**, select **Storage > File Systems**.
2. Click the link to the file system you need to access.
3. Click **Summary > CIFS shares**.
4. In the **Actions** column, click the **Unshare** icon for the CIFS Share where you want to remove sharing.

   You can search f a specific CIFS share in the grid or filter the list, by enabling filters entering characters in the text boxes located above the columns or or by choosing from the options in the **Status** and **Hidden** columns.
5. Review the message in the **Unshare** window, and type Unshare in the text box.
6. Click the **Unshare** button to complete the action.

5

Viewing file system mount point information

Once you add a file system to Unity and enable CIFS Access or NFS Access, the mount points for the file system appear in the **File Systems > Summary** panel. 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—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 `<IP address>`, the mount point for the file system is represented as:

  `\\<IP address>\PayRollData2`
- If you add an NFS file system, `PayRollNFS1`, to the FinancePool1 on Pool Resource Group 1, with the virtual IP address `<IP address>`, the mount point for the file system is represented as:

  `<IP address>:/pools/FinancePool/PayRollNFS1`
- If you expose a file system over FTP, `FinanceFileSystem`, with the virtual IP address `<IP address>`, the FTP URL is represented as:

  `ftp://<IP address>/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.

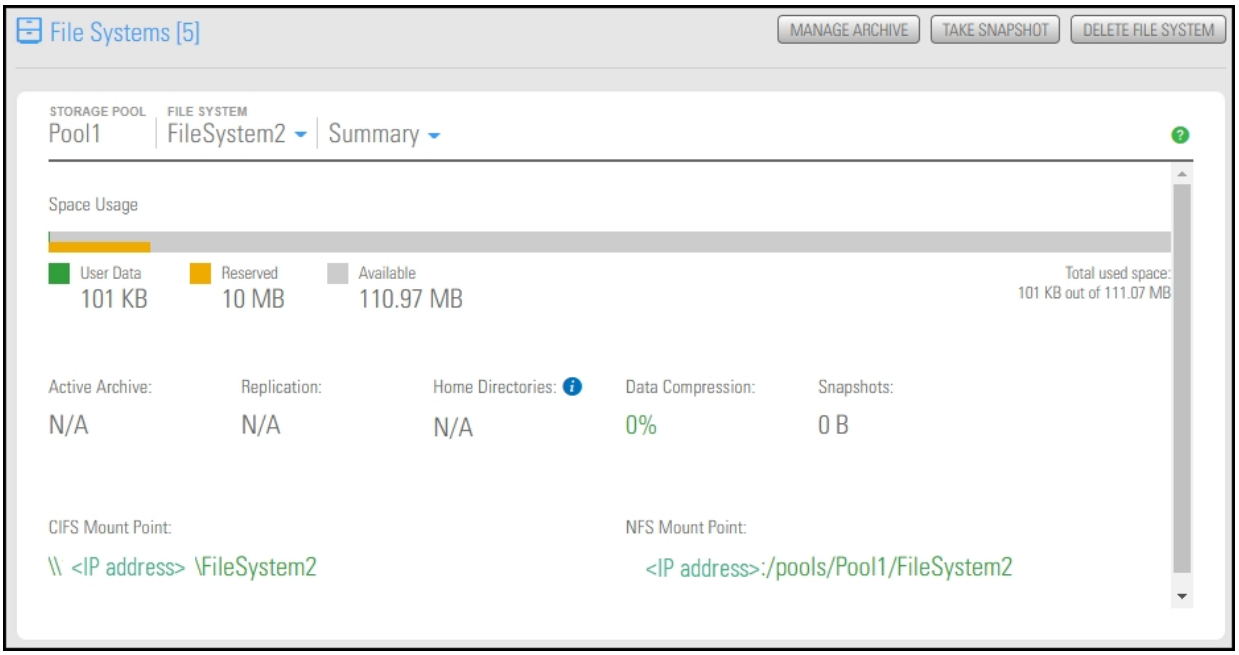
Prerequisites

To view a CIFS or NFS mount point, access must be enabled in the **File Systems Properties** panel.

To view file system mount points:

1. On the **Unity navigation bar**, select **Storage > File Systems**.
2. Click the link to the file system you need to access.
3. View the mount points In the **File Systems Summary** panel.

Figure 5-44: File Systems Summary panel



Managing access permissions to file systems

When you add a file system, you can set access permissions for individual users and/or groups in the Microsoft Active Directory domain or LDAP Directory service that Unity is connected to. If the Unity system is configured to use Unity authentication, you set access permissions for individual users and groups that you define on the Unity system.

Access permissions protect your data from unauthorized access by enabling you to define the type of access granted to a user or group for a file system 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 file system named PayrollData, only members of the Finance group can perform Read and Write operations on the contents of the PayrollData file system from their Windows systems.

This section includes these topics:

Understanding access permissions for file systems 194
Managing file system- or CIFS share-level access permissions 197

Understanding access permissions for file systems

When you set permissions, you specify the level of access that a user or a group has to a specific file system that you create in Unity. For example, you can let one user or group view the contents of a file system (read access), let another user or group make changes to files in the file system (read/write or full access), and prevent all other users and/or groups from accessing the file system. 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 file system (read-only anonymous access or, let all users and groups *anonymously* perform read/write operations on the contents of a file system (read/write anonymous access); for more information about anonymous access, see Read-only and read/write anonymous access below.

Unity applies file system-level permissions cumulatively. For example, if you give Jack Read-only access to the PayRollData file system, and then you give the Finance group—of which Jack is a member—write access to the PayRollData file system, Jack will automatically have read/write access to the PayRollData file system.

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 file system in Unity, *bob* is automatically granted full access to all files and folders in the file system; similarly, if you revoke *bob's* access to a file system, *bob's* access to all files and folders in the file system is revoked as well.

Unity supports these permission settings on file system:

- Read
- Write
- Full

Read-only and read/write anonymous access

Unity supports both read-only and read/write anonymous access to file systems. For example, if you have a file system that contains generic policies and forms, like blank expense reports, you may want all users on your network to access the file system—in which case, you can set the file system'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 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 Windows-based (CIFS) system, the *Everyone* account on the system has either read-only or read/write access to the file system, depending on the anonymous setting you specify for the file system in Unity. And on a UNIX/Linux-based (NFS) system, the *guest* account has either read-only or read/write access to the file system.

Windows and UNIX Access Control Lists (ACLs)

Unity supports both UNIX/Linux and Windows NTFS-style ACL (Access Control List) access privileges on file systems; for example:

- If you enable NFS sharing for a file system: Unity supports traditional UNIX-style ACL attributes (such as, rwx) for owner, group owner, and other.
- If you enable CIFS sharing for a file system: Unity supports the semantics of Windows NTFS ACLs, including configuration, enforcement, and inheritance models.



CAUTION: If you run the `chmod` command on an NFS file system, all Windows ACLs are cleared.

This table shows how Unity maps permissions that you set for file system to ACL access privileges in Windows (CIFS sharing) and UNIX/Linux (NFS sharing) environments.

Table 5-7: 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 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) Write ACL (C) Change Owner (o)	Read Data (r) Write Data (w) Execute (x)

Managing file system- or CIFS share-level access permissions

This section describes how to manage user and/or group access permissions on a Unity file system or CIFS share.

Prerequisites

- a storage pool
- a file system defined on the system
- at least one user or group

To give file system-level access permissions to a user or group:

CAUTION: If you give a user access permissions to a file system or CIFS share, the new permission settings are applied on all files and folders in the file system. For example, if you give the user *bob* read, read/write, or full access to a file system, *bob* is automatically granted read, read/write, or full access to all files and folders in the file system.

1. On the **Unity navigation bar**, select **Storage > File Systems**.
2. Click the link to the file system that you want to modify user or group access for.
3. Select **Summary > CIFS Shares**.
4. Click the **Manage Access Permissions** icon for the file system or CIFS share that you want to manage access for.
5. Make sure **Anonymous Access** permissions are disabled.
6. Click the **Add Users/Groups** button.
7. If Unity is integrated with a Microsoft Windows Active Directory domain or an LDAP Directory service, from the **Domain** drop-down list, select the domain servers where the user or group that you want to give file system-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.
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, and then, click the **Search** 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*:

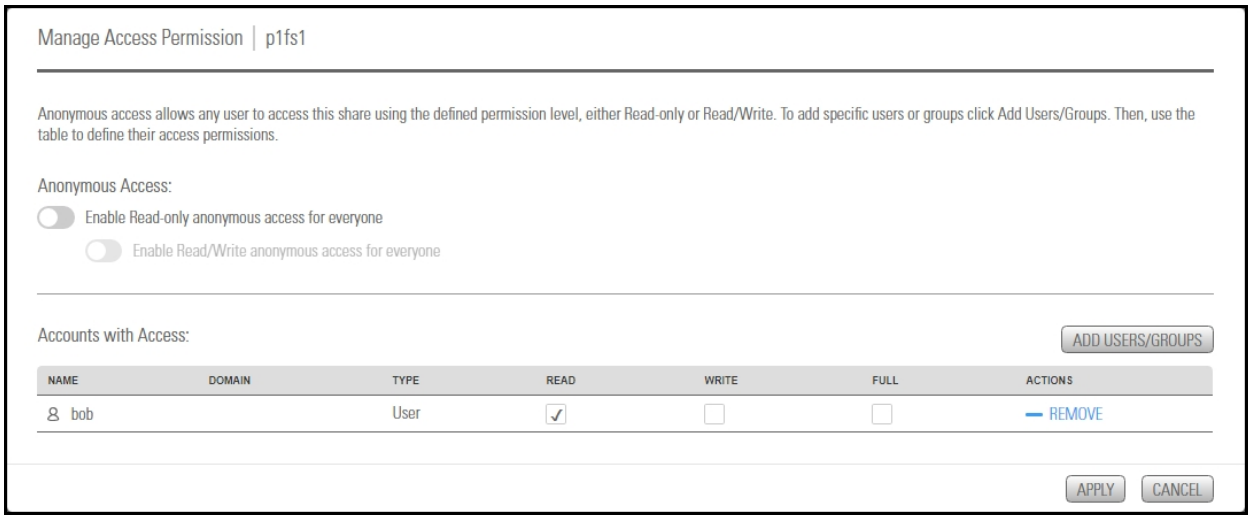
   a. Select the **Starts with** option from the pick list next to the Name text box.

   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).
9. After you have selected one or more users or groups, click the **Apply** button to add them to the system.

10. In the **Manage Access Permission** window, select the relevant check boxes in the **Read**, **Read/Write**, or **Full** column corresponding to the needed access levels.
    - If you select the **Read** check box, the user or group is granted only read-level access permissions to the file system.
    - 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 file system, and both the **Read** and **Read/Write** check boxes are also automatically selected.

Figure 5-45: Manage Access Permissions window



11. Click the **Apply** button to save your settings.

Repeat these steps to give the user or group access permissions to more file systems on the system.

Enabling ZFS Encryption for file systems

Enabling the encryption feature allows for the creation of encrypted file systems and volumes. This will encrypt file and volume data as well as the metadata.

This section includes these topics:

Enable ZFS encryption on a file system 199
Export encryption key for a file system 200
Import encryption key for a file system 201
Change encryption key for a file system 202

Enable ZFS encryption on a file system

Use this topic to enable ZFS encryption on a file system.

Prerequisites

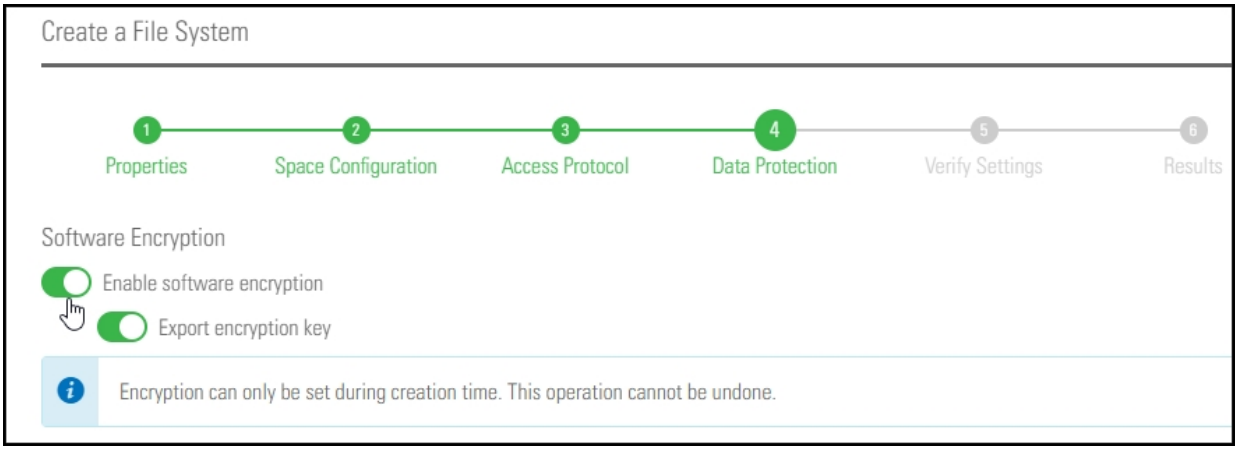
To complete this procedure, you'll need to have completed the first three of six steps using the Unity Create a File System wizard.

To enable ZFS encryption:

1. On the **Unity navigation bar**, select **Storage > File Systems**.
2. On the upper right of the page, click the **Add File System** button. The Create a File System wizard pop-up appears.
3. Complete **Steps 1 to 3** (Properties, Space Configuration, and Access Protocol).
4. At Step 4, Data Protection, click the **Enable software encryption** as well as **Export encryption key** slider buttons in the top section of the window. Complete the remaining settings in this step and then click the **NEXT** button at the bottom right.

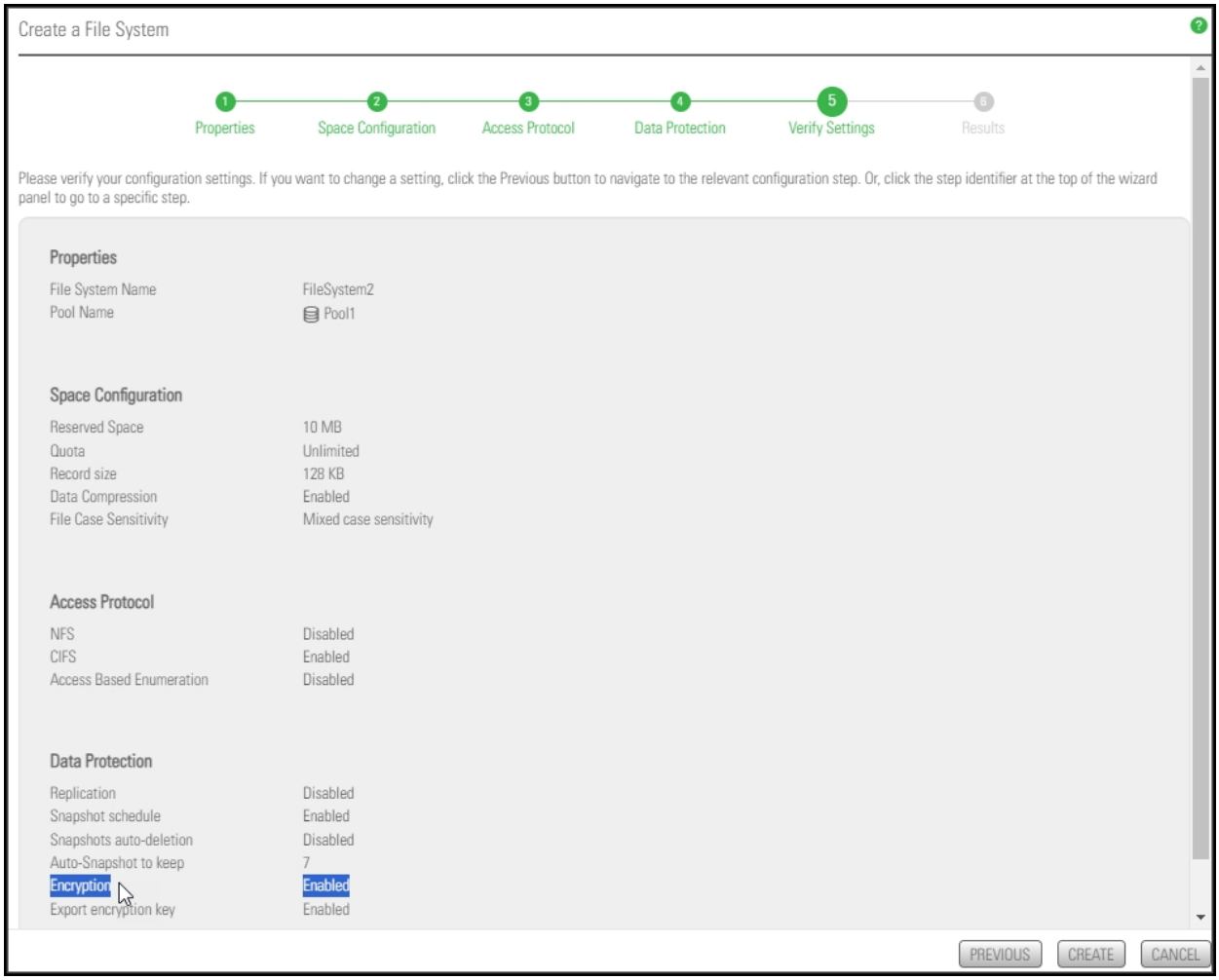
CAUTION: Encryption can only be set during creation time. This operation cannot be undone.

Figure 5-46: Enable Software Encryption settings



5. In **Step 5**, Verify Settings, in the Data Protection section, ensure that Encryption indicates Enabled. After all settings have been verified, click the CREATE button on the bottom right.

Figure 5-47: Verify configuration settings for Encryption Enabled



6. **Step 6**, Results, indicates the successful creation of a File System including encryption.

Export encryption key for a file system

Use this topic to export an encryption key for a file system.

Prerequisites

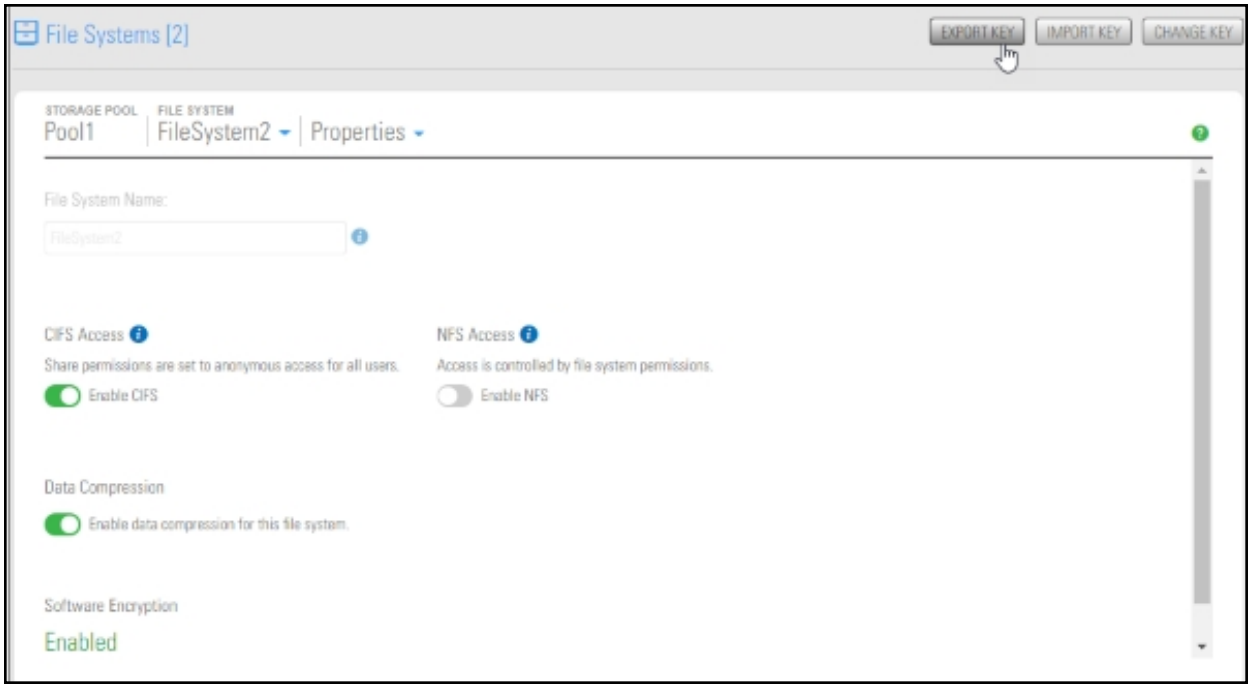
To complete this procedure, you'll need an existing file system.

► **To export an encryption key:**

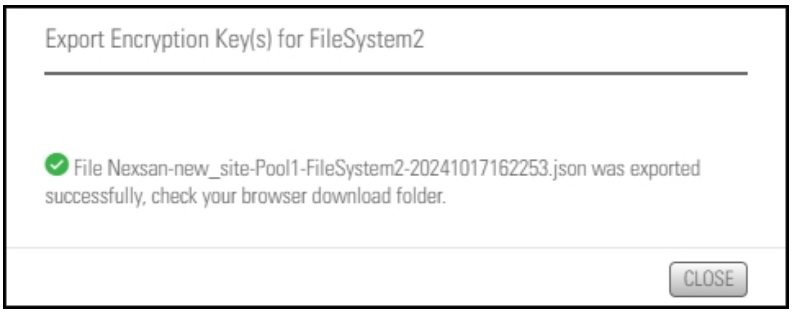
1. On the **Unity navigation bar**, select **Storage > File Systems**.
2. Click the link to the file system you would like to export the encryption key for. The **File Systems Summary** page appears.

3. Select **Summary > Properties**.The **File Systems Properties** panel appears.

Figure 5-48: selected file system Properties panel



4. Click the **Export Key** button on the upper right. A pop-up window appears indicating that the key export was successful.



Import encryption key for a file system

Use this topic to import an encryption key for a file system.

Prerequisites

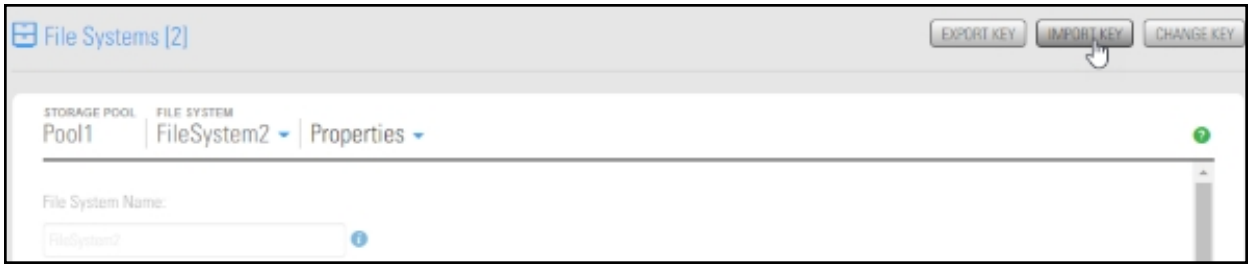
To complete this procedure, you'll need an existing file system.

► **To import an encryption key:**

1. On the **Unity navigation bar**, select **Storage > File Systems**.
2. Click the link to the file system you would like to import a key for. The **File Systems Summary** page appears.

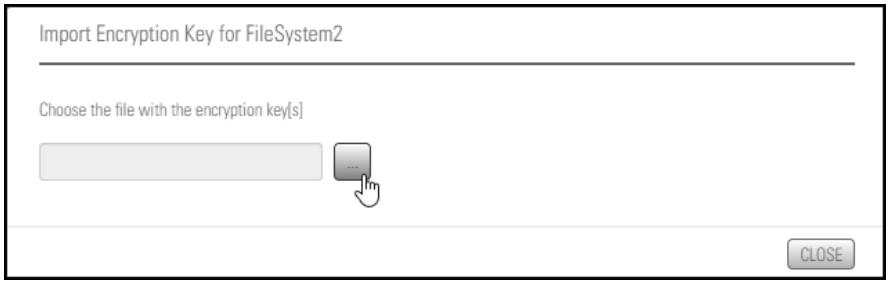
3. Select **Summary > Properties**.The **File Systems Properties** panel appears.

Figure 5-49: selected file system Properties panel



4. Click the **Import Key** button on the upper right. An Import Encryption Key pop-up window appears for the selected file system. Select the key file using the blank field, or the browse button just beside it.

Figure 5-50: Import Encryption Key pop-up window - select file



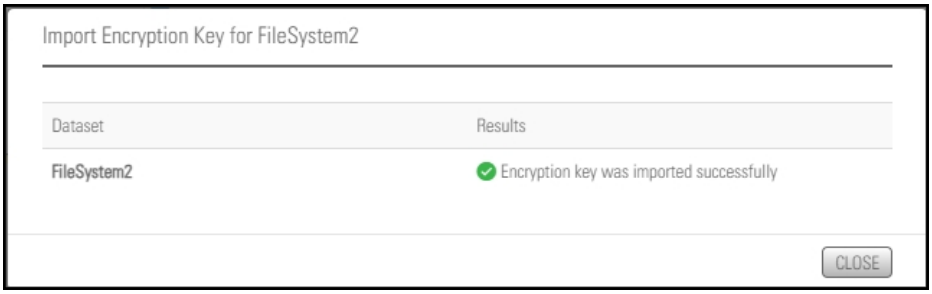
5. An Import Encryption Key pop-up window appears, confirming the date and time which the encryption key file was exported. Click the **Import** button on the bottom right.

Figure 5-51: Import Encryption Key pop-up window - import file



6. An Import Encryption Key pop-up window appears, indicating that the import was successful.

Figure 5-52: Import Encryption Key pop-up window - import successful



Change encryption key for a file system

Use this topic to change an encryption key for a file system.

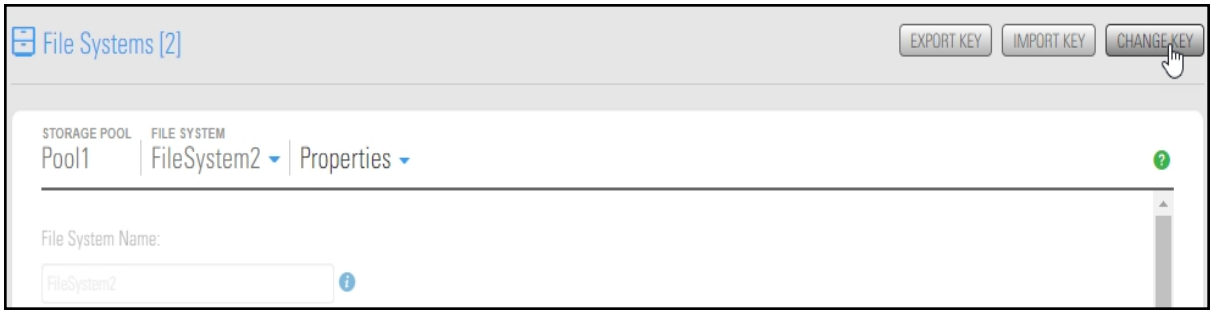
Prerequisites

To complete this procedure, you'll need an existing file system.

To change an encryption key:

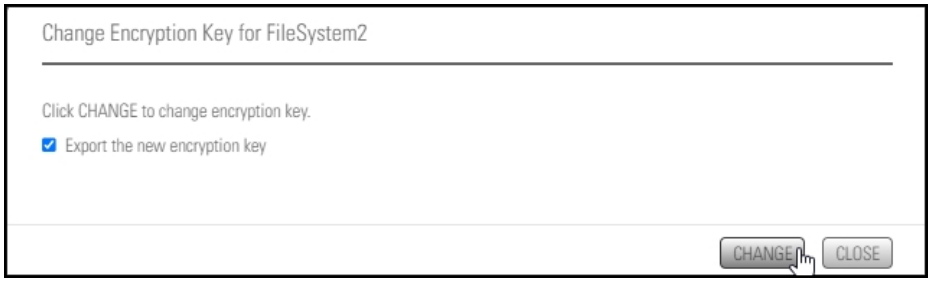
1. On the **Unity navigation bar**, select **Storage > File Systems**.
2. Click the link to the file system you would like to change a key for. The **File Systems Summary** page appears.
3. Select **Summary > Properties**.The **File Systems Properties** panel appears.

Figure 5-53: selected File System Properties panel



4. Click the **Change Key** button on the upper right. A Change Encryption Key pop-up window appears for the selected file system. Ensure the **Export the new encryption key** check box is selected. Then click the **Change** button on the lower right to complete the operation.

Figure 5-54: Change Encryption Key pop-up window



5. A Change Encryption Key pop-up window appears, indicating the change and the export was successful.

Figure 5-55: Change Encryption Key pop-up window - change and export successful



Managing snapshots for file systems

Unity provides continuous data protection with the Snapshots feature, which enables you to capture, store, and access point-in-time copies of the data in Unity file systems.

This section includes these topics:

Viewing file system snapshots 204
Using the file systems snapshots panel 207
Using the file systems snapshot settings panel 208

Viewing file system snapshots

The File Systems Snapshots panel lists all the snapshots for the corresponding file system, and provides options and settings for the following actions:

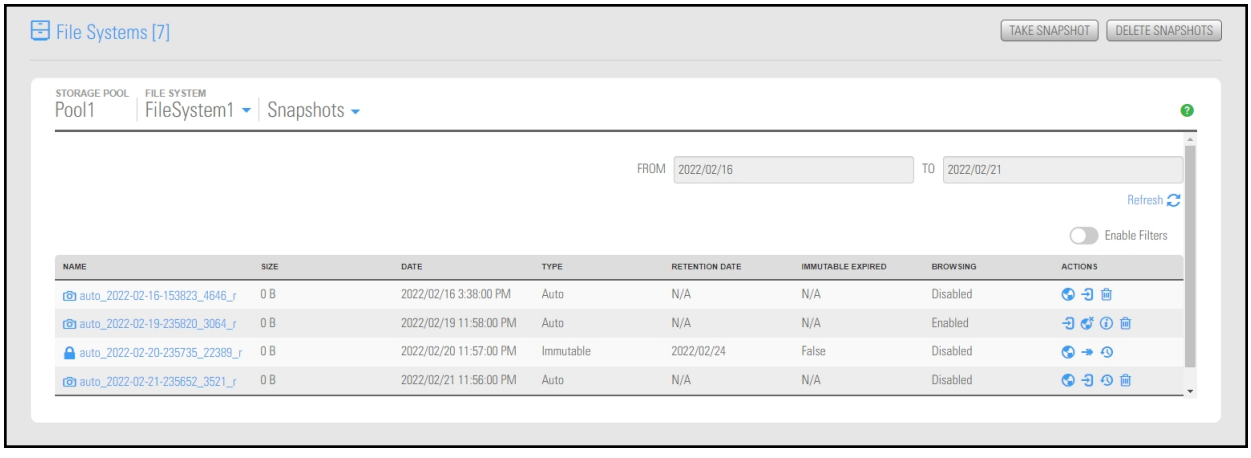
- taking manual snapshots
- enabling and disabling snapshot browsing
- making snapshots immutable
- deleting snapshots
- rolling back snapshots

5

To access file system snapshots from the File Systems panel:

1. On the **Unity navigation bar**, select **Storage > File Systems**.
2. Click the link to the File System you would like to view snapshots for.
3. Select **Summary > Snapshots**.

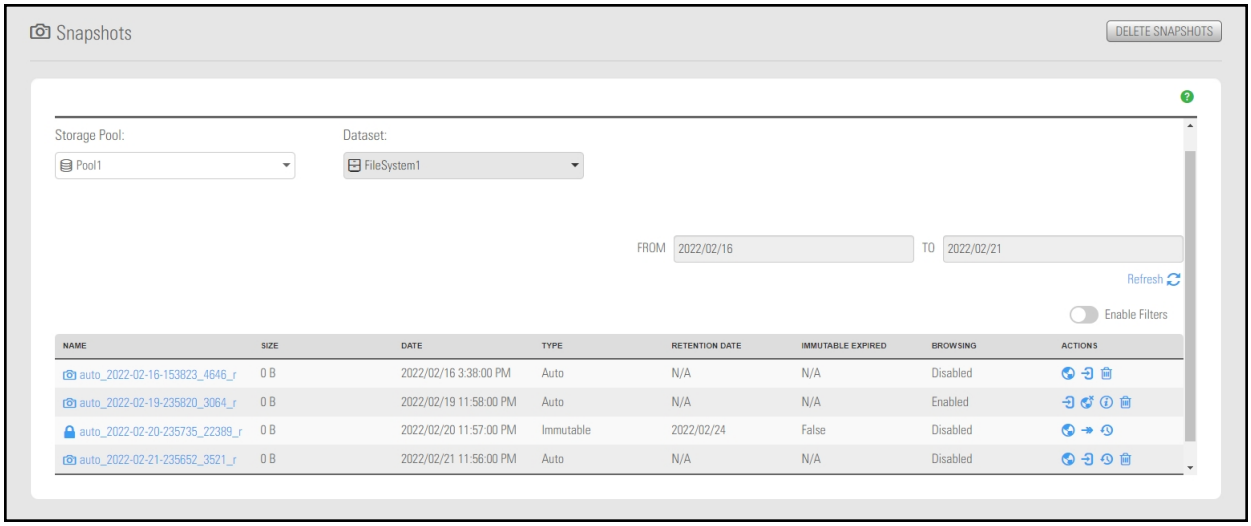
Figure 5-56: The File Systems Snapshots panel



To view File System snapshots from the main Snapshots panel:

1. On the **Unity navigation bar**, select **Data Protection> Snapshots**.
2. Select a **Storage Pool** and then select **Dataset > File System**, as shown.

Figure 5-57: Snapshots panel with File Systems selected

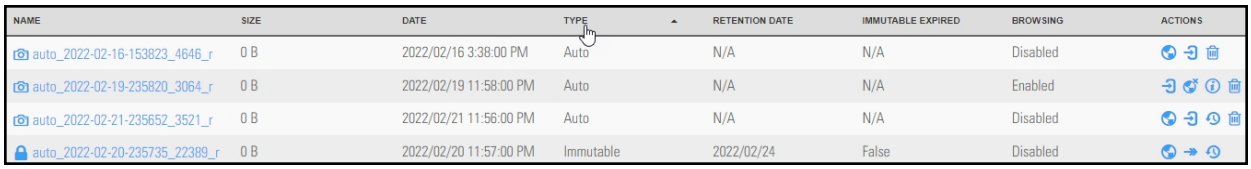


From the panel, you can view LUN snapshots, or click the icons to **Manage Browsing**, **Change to Immutable**, **Roll back**, **or Delete** snapshots.

Sorting the list of snapshots

You can sort the list of snapshots displayed in the grid by clicking column headers.

Figure 5-58: File Systems Snapshots panel - sorting by column header



▶ **To sort the list:**

- Click a column header.

You can sort snapshots by individual columns **Name**, **Size**, **Date**, **Type**, **Retention Date**, **Immutable Expired**, and **Browsing** status.

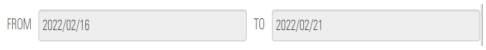
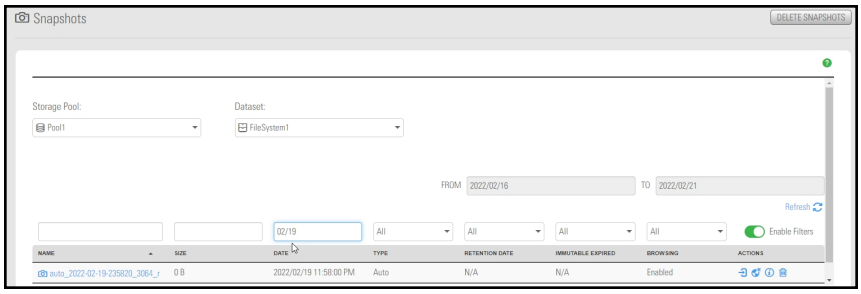
Filtering snapshots in the grid

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 filter the list of snapshots:**

1. On the **Unity navigation bar**, select **Data Protection > Snapshots**.
2. Select Enable Filters
3. Do any of the following, as required:

Table 5-8: Filter snapshots

To...	Do this
only display snapshots recorded within a specific time period	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.  2. Click the **To** date field, and select an end date for the time period.
filter by alphanumeric string	Type text for any of the data types applicable in the column header boxes. For example: 
only display snapshots with a specific Browsing status	1. Open the drop-down list above the **Browsing** column heading in the grid. 2. Select the browsing status (**All**, **Disabled**, or **Enabled**) that you want to display snapshots for in the grid. The default filter setting is **All**.
only display snapshots of a specific type	1. Open the drop-down list above the **Type** column heading in the grid. 2. Select the type (**All**, **Auto**, **Immutable**, or **Manual**) that you want to display snapshots for in the grid. The default filter setting is **All**.
only display immutable snapshots of a specific type	1. Open the drop-down list above the **Immutable Expired** column heading in the grid. 2. Select the type (**All**, **N/A**, or **False**) 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 **Auto**, and which were recorded between February 16, 2022 and February 21, 2022, set these filter settings in the grid: 1. Click the **From** date field above the snapshots grid, and select February 16 in the calendar. 2. Click the **To** date field, and select February 21 in the calendar. Unity filters the grid to only display snapshots recorded within the time period. 3. Open the drop-down list above the **Browsing** column heading in the grid and select **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 **Auto**. Unity filters the grid again to only display scheduled (automatic) snapshots.

Searching for a specific snapshot in the grid

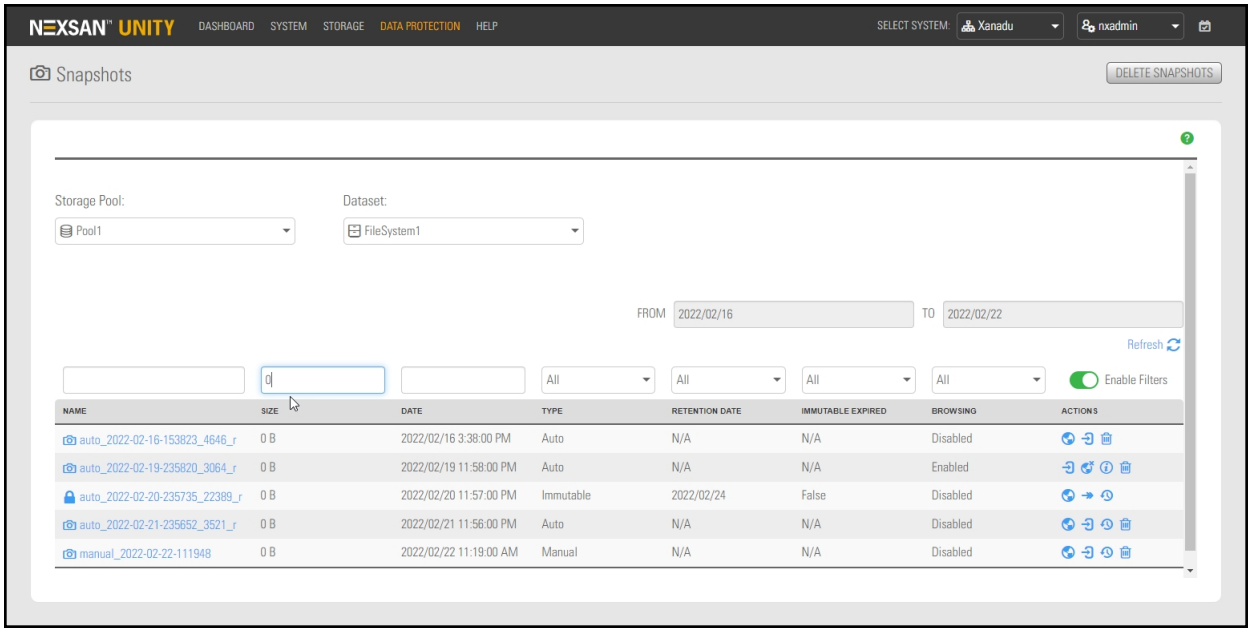
You can search for a specific snapshot in the grid by entering a search string in the text boxes above the corresponding column headings.

To search for a specific snapshot in the grid:

- Enter a search string in the text boxes above the 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 5-59: File Systems Snapshots panel



Unity displays all snapshots matching your search criteria.

Using the file systems snapshots panel

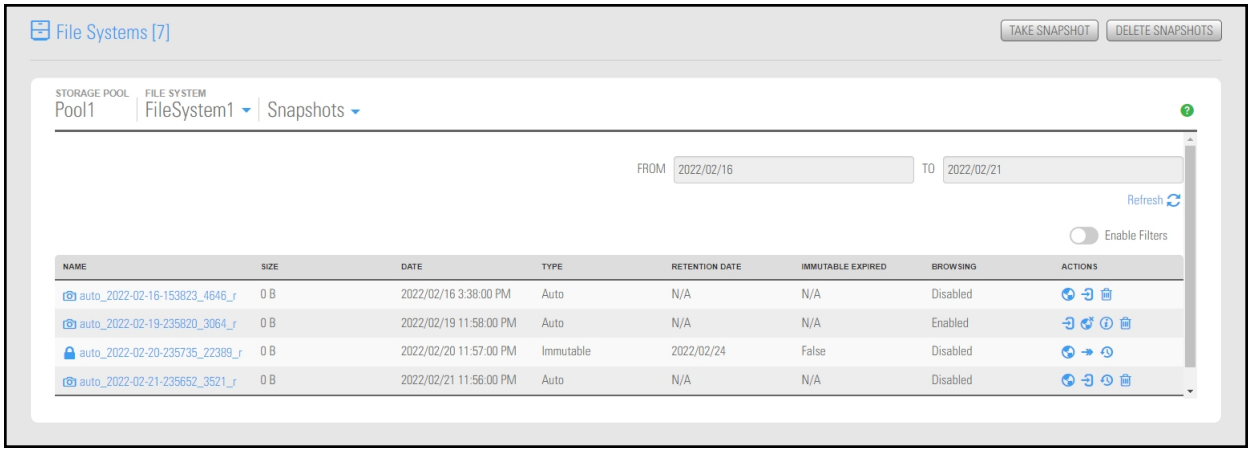
The File Systems Snapshots panel lists all the snapshots for the corresponding file system, and provides options and settings for the following actions:

- taking manual snapshots
- enabling and disabling snapshot browsing
- making snapshots immutable
- extending snapshot retention date
- deleting snapshots
- rolling back snapshots

To access file system snapshots:

1. On the **Unity navigation bar**, select **Storage > File Systems**.
2. Select **Summary > Snapshots**.

Figure 5-60: The File System Snapshots panel



Using the file systems snapshot settings panel

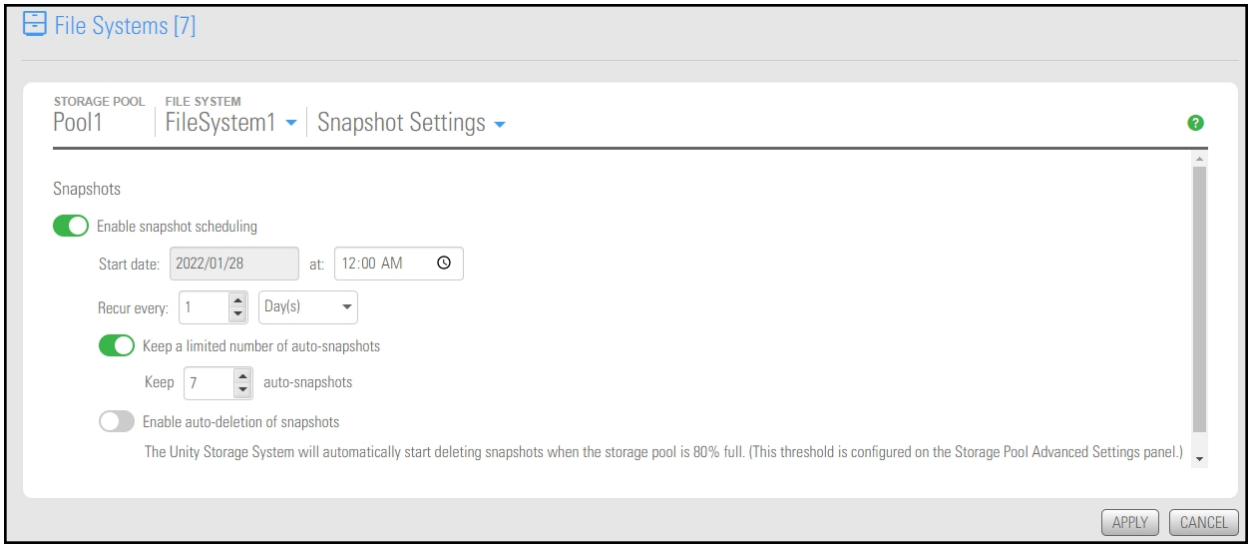
The **File Systems Snapshot Settings** panel provides options for configuring a snapshots schedule and for specifying auto-deletion settings for snapshots.

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 retain 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 217.

Figure 5-61: File System Snapshot Settings panel



Setting a schedule for automatic file system snapshots

This section describes how to take automatic snapshots for file systems. For instructions about how to take manual snapshots, see Taking a manual file system snapshot on page 211.

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 Snapshot Settings panel.

Note There can only be one snapshot schedule per file system.

To set or modify a schedule for automatic snapshots:

1. On the **Unity navigation bar**, select **Storage > File Systems**.
2. Select the link to the file system you need to update.
3. Select **Summary > Snapshot Settings**.

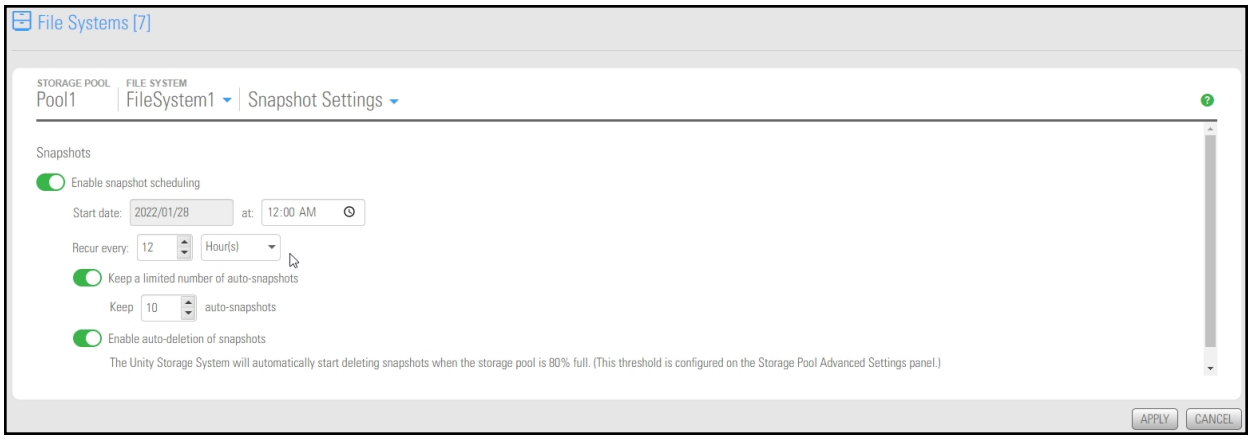
Figure 5-62: File Systems panel menu



4. In the **Snapshot Settings** panel, configure the snapshots schedule:
   a. **Enable snapshot scheduling** 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 when you initially created it, the default setting is once a day at 12 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. Accept or change the value for the number of auto-snapshots to be kept. The default is 7.
   d. Click the **Enable auto-deletion of snapshots** button if you want Unity to start deleting snapshots when the storage pool is 80% full.
   e. 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 immediately after you set the schedule. Thereafter, Unity takes an automatic snapshot according to the schedule you specify.

Figure 5-63: Snapshot Settings panel - configure a schedule



Note By default, Unity Storage System information refreshes every 5 minutes; as a result, a scheduled snapshot that Unity records may not be immediately visible in the snapshots grid. To force a refresh, click Refresh in the grid.

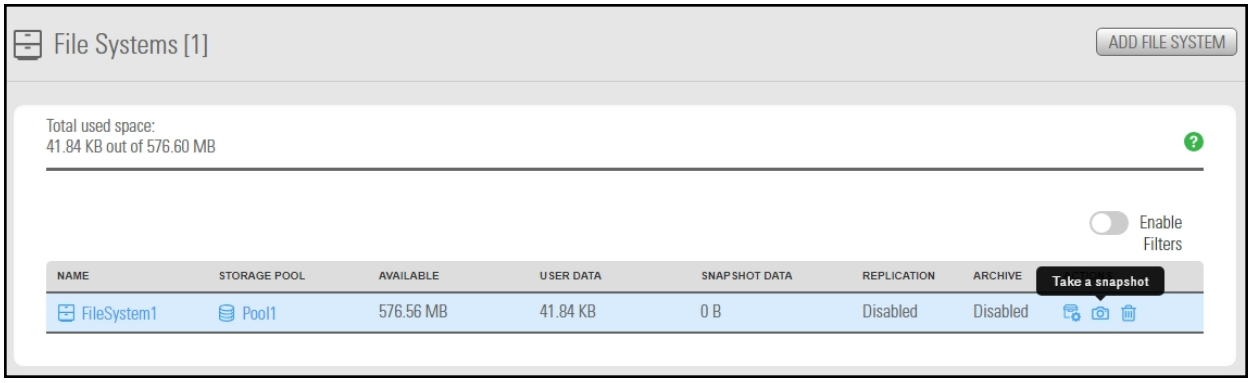
Taking a manual file system snapshot

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.

To take a manual snapshot:

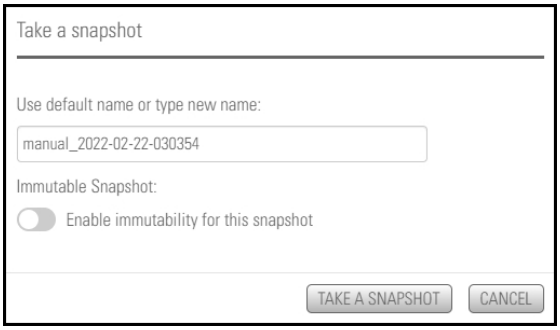
1. On the **Unity navigation bar**, select **Storage > File Systems**.
2. Under **Actions**, click the **Take Snapshot** button

Figure 5-64: File Systems panel



3. The **Take a Snapshot** window opens.

Figure 5-65: Take a snapshot pop-up window



Do one of the following:

Table 5-9: Taking a manual snapshot - actions

To...	Do this
specify a name for the manual snapshot	a. Clear the **Automatically assign a name** option (selected by default). b. 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. c. Click the **Take a Snapshot** button to set the name and close the window. Unity immediately takes a snapshot and adds it to the snapshots grid.
allow Unity to automatically assign a name to the manual snapshot	a. Use the default name. b. Click the **Take Snapshot** button to close the window. 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 `manual_` and includes the date and time the manual snapshot is recorded; for example: if you take a manual snapshot on February 22, 2022 at 3:03PM and 54 seconds, Unity assigns this name to the snapshot: `manual_2022-02-22-030354`
make the snapshot immutable	a. Click the **Enable immutability for this snapshot** button. b. Click the **Take Snapshot** button to close the window.

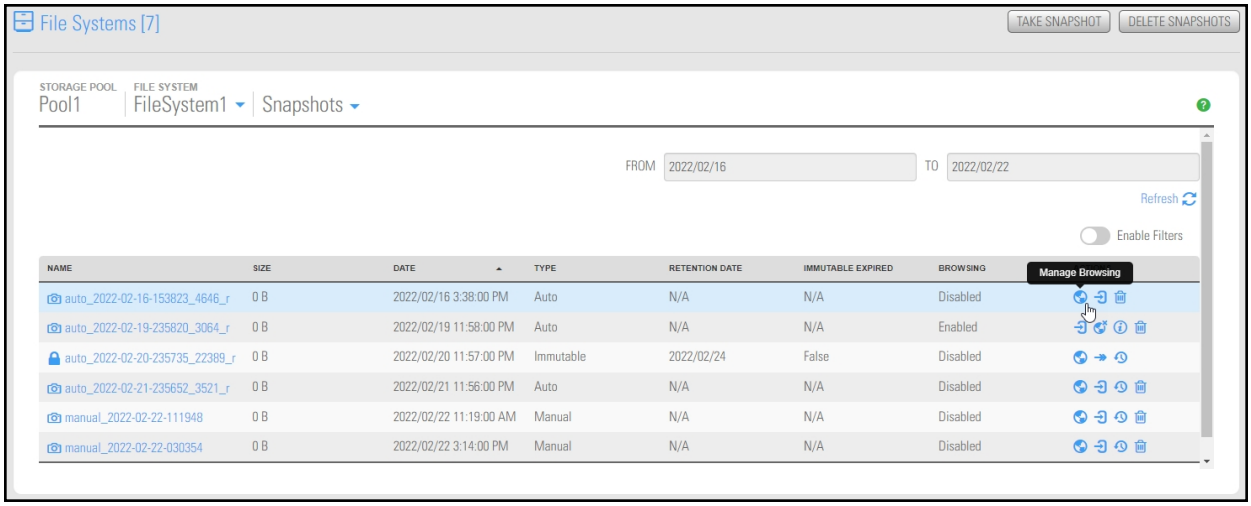
Browsing a file system snapshot

Setting browsing for a snapshot enables 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:

1. On the **Unity navigation bar**, select **Storage > File Systems**.
2. Select the file system where you want to browse snapshots.
3. Select **Summary > Snapshots**.
4. Click the **Manage Browsing** icon

Figure 5-66: File Systems Snapshots panel



5. Specify a browsing name for the snapshot and set the way Unity exposes it:
   a. In the **Manage Browsing** window, type a file system name for the snapshot.

      The name must start with an (upper-case or lower-case) alphabetic or numeric character; and, with the exception of 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:

      Table 5-10: Set browsing for a snapshot - select sharing methods

To...	Do this
expose the snapshot to Windows-based systems over the CIFS protocol	Select **Enable CIFS** option.
make the snapshot a hidden CIFS file system	Select **Make this a hidden CFS file system**
expose the snapshot to UNIX/Linux-based systems over the NFS protocol	Select the **Enable 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 the **Browse** button to save your settings and close the **Manage Browsing** window.

Once Unity completes this process, the **Browsing** 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**.

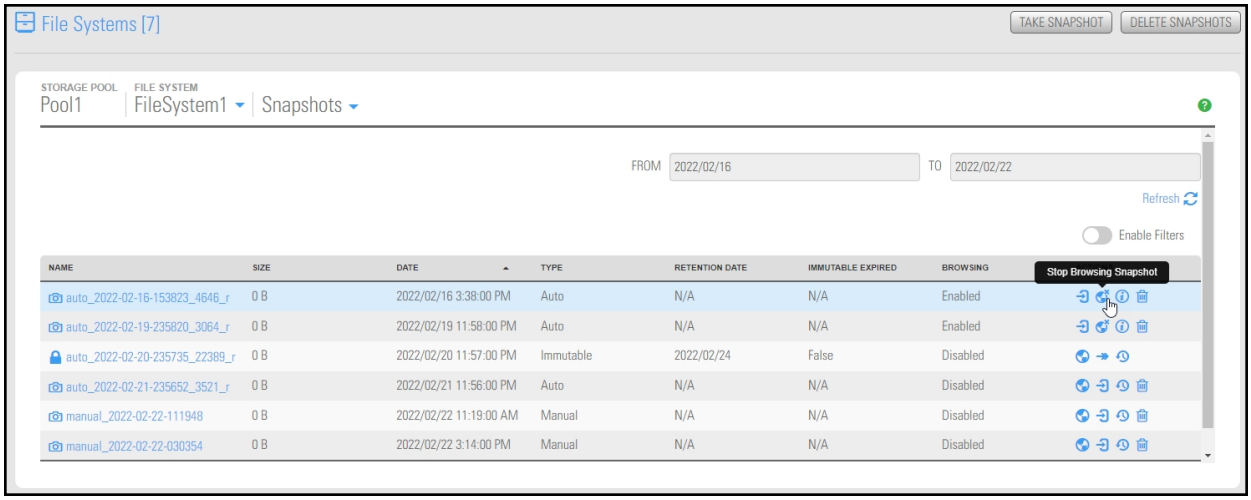
Stopping file system snapshot browsing

► **To disable browsing for a snapshot:**

1. On the **Unity navigation bar**, select **Storage > File Systems**.
2. Select the file system where you want to stop browsing the snapshot.
3. Select **Summary > Snapshots**.

4. Click the **Stop Browsing Snapshot** icon

Figure 5-67: File Systems Snapshots panel



5. Type **Stop** in the **Stop Browsing Snapshot** window to confirm.
6. Click the **Stop** button to complete the operation.

Note The **Stop browsing** button is only displayed if you select a snapshot in the grid that has browsing enabled.

5

Rolling back to a snapshot

The rollback function reverts the contents of a file system or LUN 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 or LUN 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. On the **Unity navigation bar**, select **Storage > File Systems**.
2. Select the file system where you want to browse snapshots.
3. Select **Summary > Snapshots**.
4. Click the **Roll back Snapshot** icon .
5. Type **Rollback** in the Stop Browsing Snapshot window to confirm.
6. Click the **Rollback** button to complete the operation.

Using the Windows Volume Shadow Copy service to roll back

If Unity is joined to a Microsoft Active Directory domain and Microsoft Windows client computers that use Microsoft Volume Shadow Copy (VSS), Unity automatically exposes all of its file system snapshots to Microsoft Windows (CIFS) clients that access them.

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, or roll back a file system to a specific point-in-time snapshot.

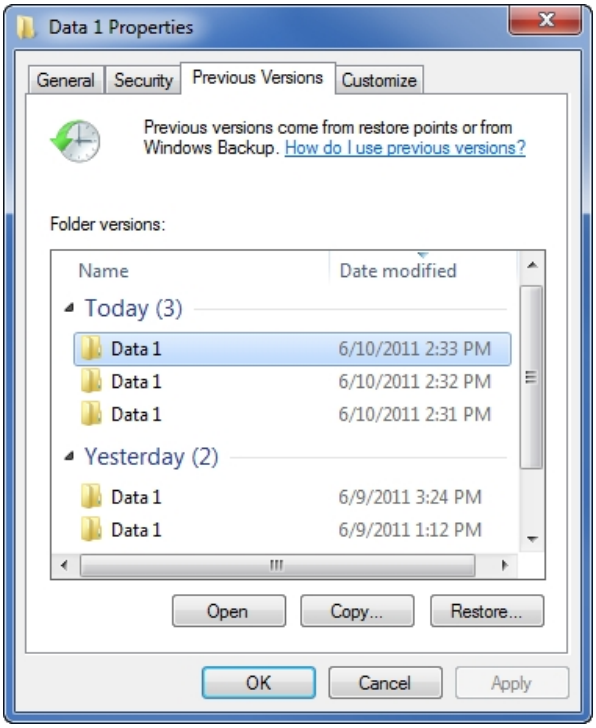
CAUTION: The restore operation cannot be undone.

To use Microsoft VSS on a Windows client computer to roll back the data in a file system:

1. In Unity:
   a. Make sure the file system has CIFS sharing enabled.
   b. Make sure the file system has manual or automatic (scheduled) snapshots recorded; see Setting a schedule for automatic file system snapshots on page 208.
2. Access the file system 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 CIFS share to a snapshot, right-click the CIFS share and then click **Restore previous versions**.)

   Microsoft Windows displays a list of available previous versions or snapshots of the file, folder, or file system.

Figure 5-68: Microsoft VSS, Restore previous version of file, folder, or file system



4. Before restoring a previous version of a file, folder, or file system, 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 it in the list, and click the **Restore** button.

Similar to the roll back function in Unity, Microsoft VSS rolls back all the data in the file system to the contents of the snapshot you select—this includes all file- and folder-level permission settings and file system-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 file system 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 file system 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 seven snapshots for the file system, set the auto-deletion setting to seven; 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 storage pool snapshot auto-deletion on page 100.

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.

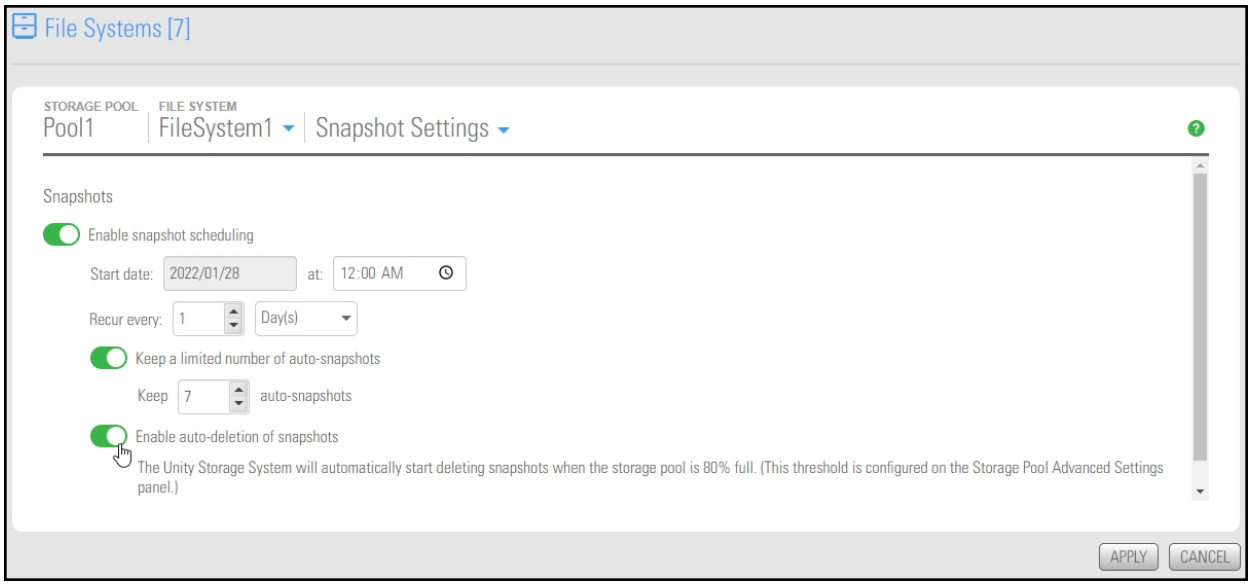
To set auto-deletion settings for snapshots:

1. On the **Unity navigation bar**, select **Storage > File Systems**.
2. Select the file system you need to update.
3. Select **Summary > Snapshot Settings**.

Figure 5-69: File Systems panel menu



4. Do either of the following:
   - Revise the default number of snapshots retained. The default is seven.
   - In the **Snapshot Settings** panel, click the Enable auto-deletion of snapshots button 



5. Click the **Apply** button to save the changes.

Manually deleting file system snapshots

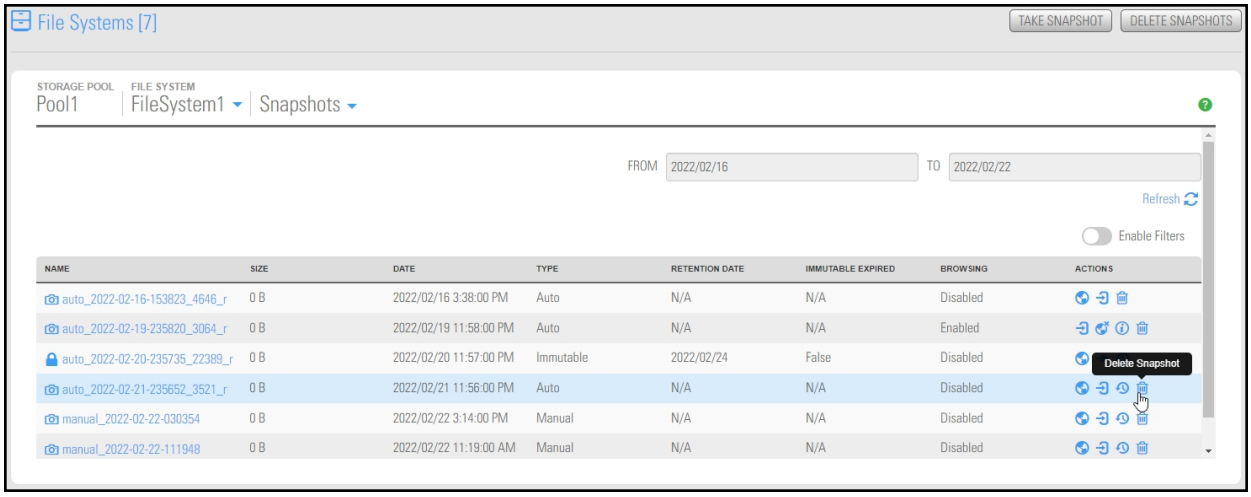
This section describes how to delete snapshots for a file system. You can delete both manual snapshots and automatic (scheduled) snapshots.

To manually delete snapshots for a file system:

1. On the **Unity navigation bar**, select **Storage > File Systems**.
2. Select the file system where you want to delete the snapshot.
3. Select **Summary > Snapshots**.

4. Click the **Delete Snapshot** icon .

Figure 5-70: File Systems Snapshots panel



5. Type **Delete** in the **Delete Snapshot** window to confirm.
6. Click the **Delete** button to complete the operation.

Immutable snapshots for file systems

Use the topics in this section to create immutable snapshots for a file system, to make existing file system snapshots immutable, to change the retention date of a file system snapshot, or to create an immutable snapshots schedule.

A snapshot is immutable when it is locked for a specified period of time, and protected from modification or deletion. Having immutable snapshots ensures

- availability of snapshot data for disaster recovery, and,
- faster recovery compared to traditional recovery using backups

The File Systems Snapshots panel lists all the snapshots for the corresponding file system, and provides options and settings for immutable snapshots actions.

This section includes these topics:

Taking an immutable snapshot for a file system 221
Changing an existing file system snapshot to make it immutable 222
Extending the retention date of an immutable snapshot 224
Scheduling immutable snapshots for File Systems 225

Taking an immutable snapshot for a file system

Use this topic to take an immutable snapshot for a file system.

Prerequisites

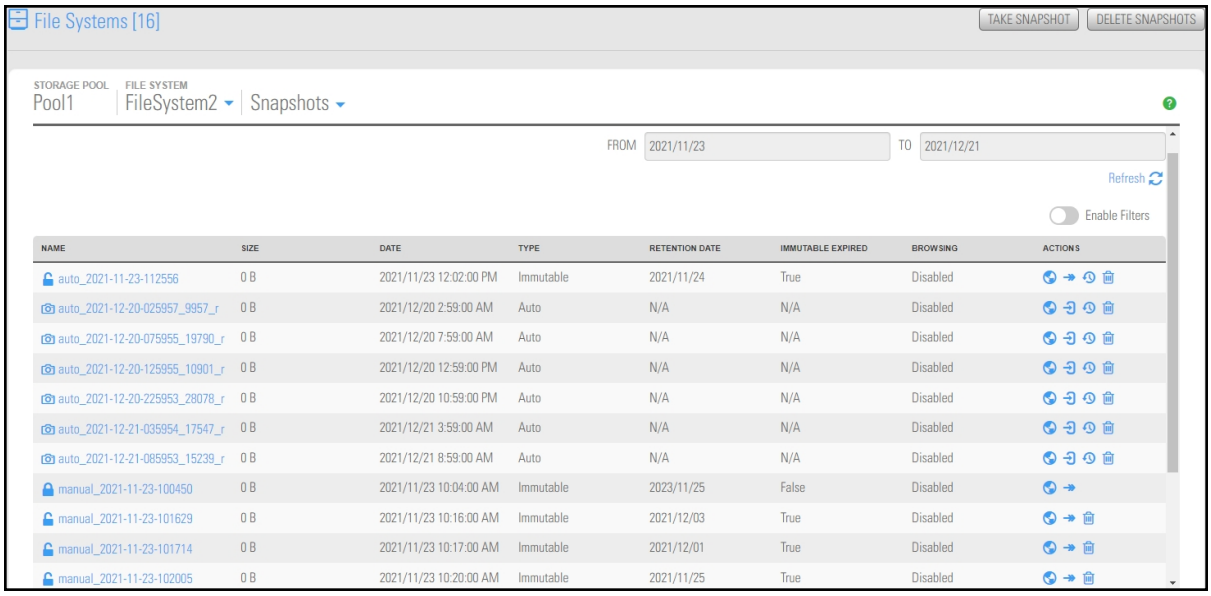
To complete this procedure, you'll need a Unity Storage System set up with storage pools, file systems, LUNs, and snapshots.

To take an immutable snapshot:

1. On the **Unity navigation bar**, select **Storage > File Systems**.
2. Click the link to the File System you would like to view snapshots for. **The File Systems Summary** page appears.

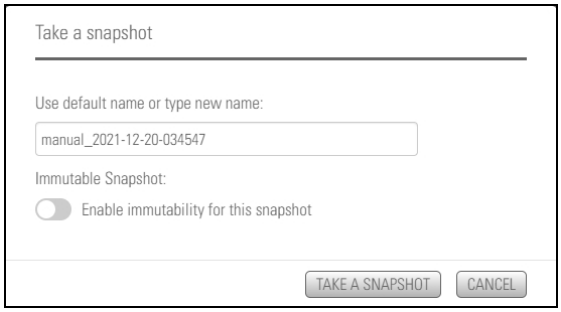
   Select **Summary > Snapshots**.The **File Systems Snapshots** panel appears.

Figure 5-71: The File Systems Snapshots panel



3. Click the **Take Snapshot** button on the upper right. The **Take a Snapshot** pop-up appears.

Figure 5-72: Take a snapshot pop-up window

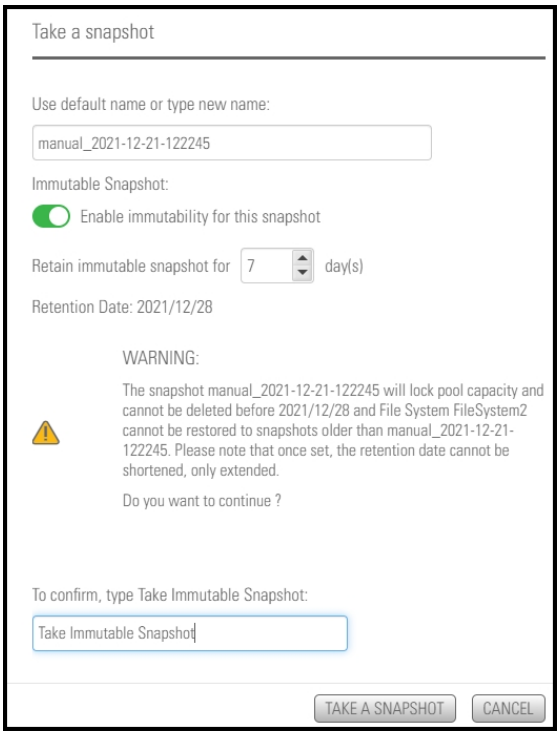


4. Click the **Enable immutability for this snapshot** slider button . The subsequent **Take a snapshot** pop-up appears.

5. Use the default name or type a new name. The **Enable immutability for this snapshot** slider button appears green . Select the number of days to retain the immutable snapshot. The minimum number of days is one and the maximum number of days is 365. To confirm, type 'take immutable snapshot' (not case sensitive) and click the **Take a Snapshot** button.

CAUTION: Immutable snapshots lock pool capacity, cannot be deleted before the retention date, and the associated file system cannot be restored to a time before the immutable snapshot is created.

Figure 5-73: Take Immutable Snapshot confirmation pop-up window



Changing an existing file system snapshot to make it immutable

Use this topic to change an existing snapshot to make it immutable.

Prerequisites

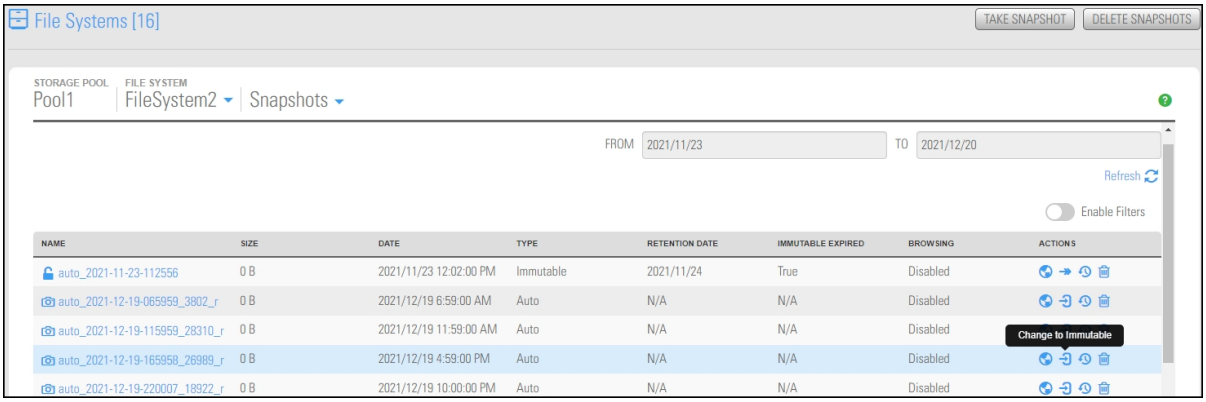
To complete this procedure, you'll need a Unity Storage System set up with storage pools, file systems, LUNs, and snapshots.

► **To change a snapshot to immutable:**

1. On the **Unity navigation bar**, select **Storage > File Systems**.
2. Click the link to the File System you would like to view snapshots for. **The File Systems Summary** page appears.
3. Select **Summary > Snapshots**. The **File Systems Snapshots** panel appears.

4. For the target snapshot, click the **Change to Immutable** icon . The **Change to Immutable Snapshot** pop-up appears.

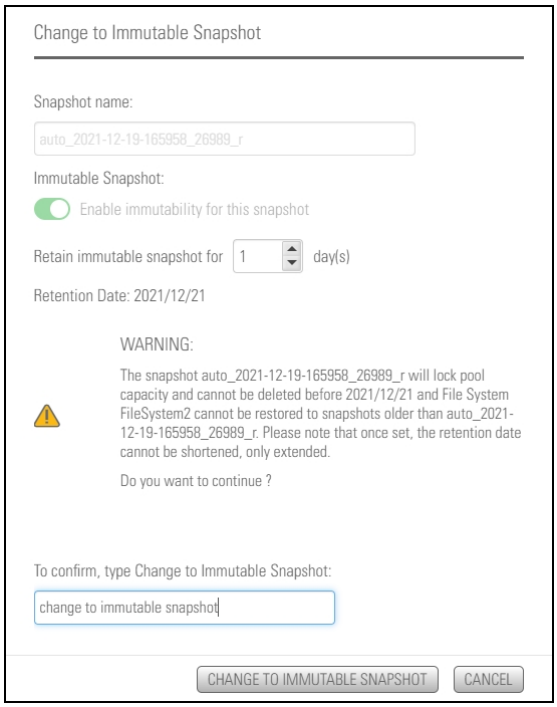
Figure 5-74: Change to immutable action icon in Snapshots panel



5. Select the number of days to retain the immutable snapshot. The minimum number of days is one and the maximum number of days is 365. To confirm, type 'change to immutable snapshot' (not case sensitive) in the confirmation field, then click the **Change to Immutable Snapshot** button.

CAUTION: Immutable snapshots lock pool capacity, cannot be deleted before the retention date, and the associated file system cannot be restored to a time before the immutable snapshot is created.

Figure 5-75: Change to Immutable Snapshot pop-up window



Extending the retention date of an immutable snapshot

Use this topic to extend the retention date of an immutable snapshot.

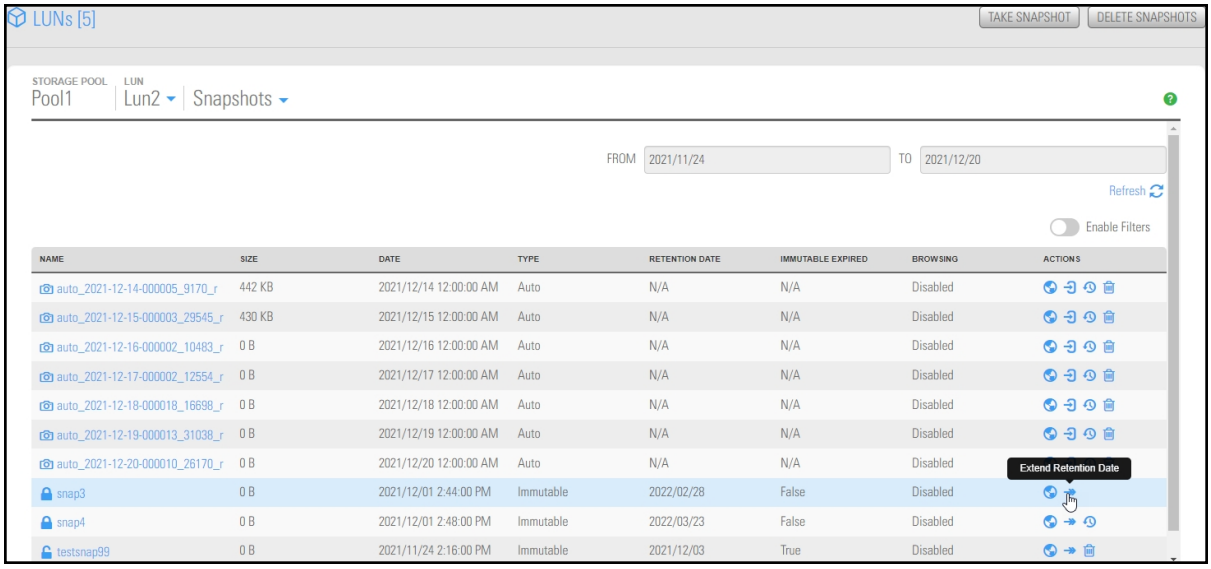
Prerequisites

To complete this procedure, you'll need a Unity Storage System set up with storage pools, file systems, LUNs, and snapshots.

To extend the retention date of an immutable snapshot:

1. On the **Unity navigation bar**, select **Storage > File Systems**.
2. Click the link to the File System you would like to view snapshots for **The File Systems Summary** page appears.
3. Select **Summary > Snapshots**.The **File Systems Snapshots** panel appears.
4. For the target snapshot, click the **Extend Retention Date** icon . The **Extend Retention Date** pop-up appears.

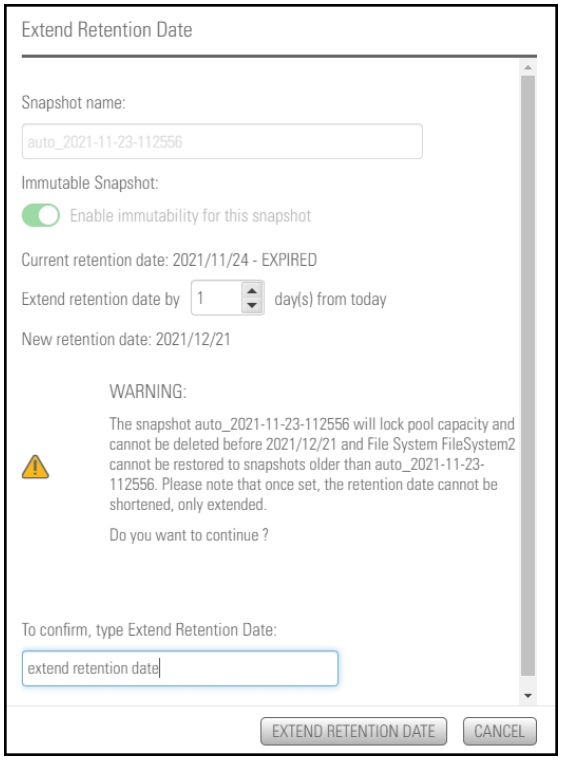
Figure 5-76: Extend Retention Date action icon in Snapshots panel



5. Select the number of days to extend the retention date. The minimum number of days is one and the maximum number of days is 365. Type 'extend retention date' (not case sensitive) in the confirmation field, then click the **Extend Retention Date** button.

CAUTION: Immutable snapshots lock pool capacity, cannot be deleted before the retention date, and the associated file system cannot be restored to a time before the immutable snapshot is created.

Figure 5-77: Extend Retention Date pop-up window



Scheduling immutable snapshots for File Systems

Use this topic to add, edit, or delete an immutable snapshot schedule for a file system.

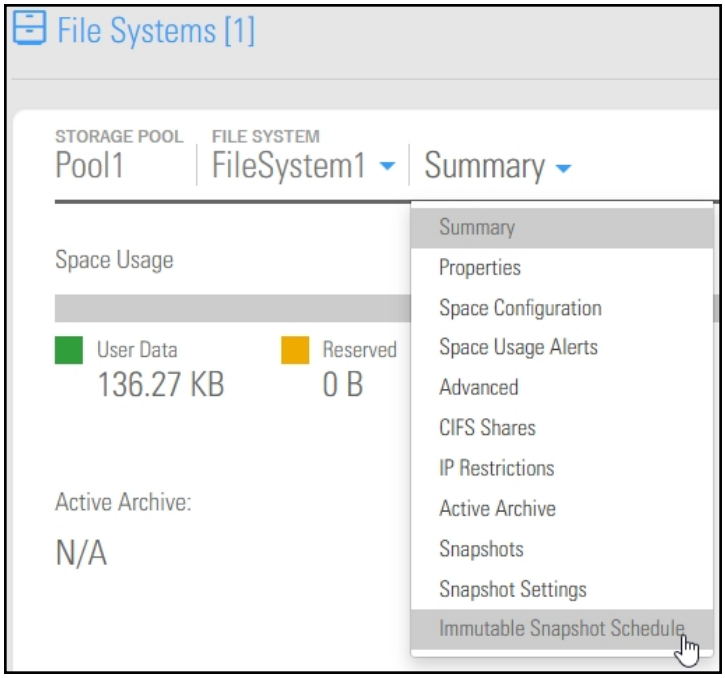
Prerequisites

To complete this procedure, you'll need a Unity Storage System set up with storage pools, file systems, LUNs, and snapshots.

► **To add an immutable snapshot schedule for a file sytem:**

1. On the **Unity navigation bar**, select **Storage > File Systems**.
2. Click the link to the File System you would like to set an immutable snapshot schedule for. **The File Systems Summary** page appears.
3. Select **Summary > Immutable Snapshot Schedule**.

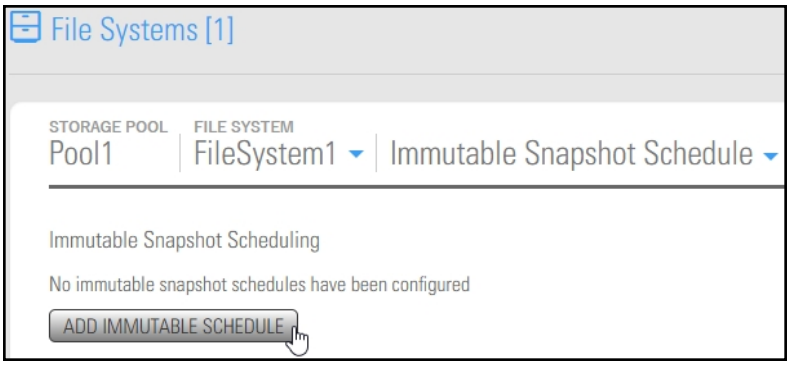
Figure 5-78: Immutable Snapshot Schedule menu selection



5

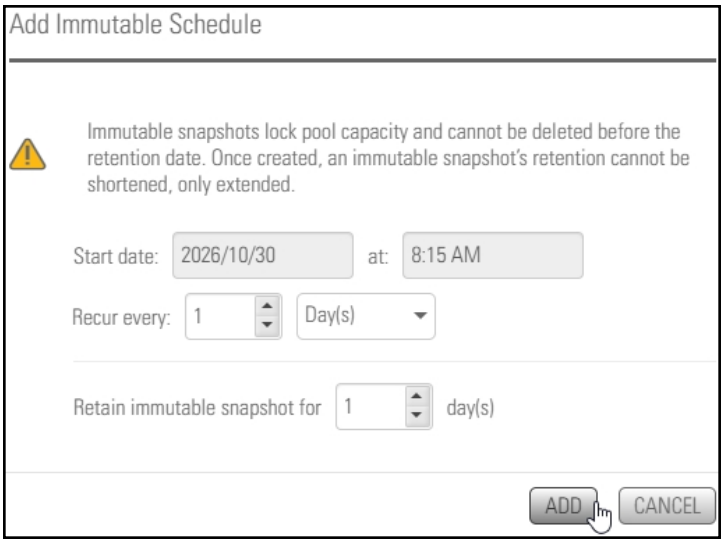
4. The **Immutable Snapshot Scheduling** panel appears . Click the **Add Immutable Schedule** button.

Figure 5-79: Immutable Snapshots Scheduling panel - Add Immutable Schedule



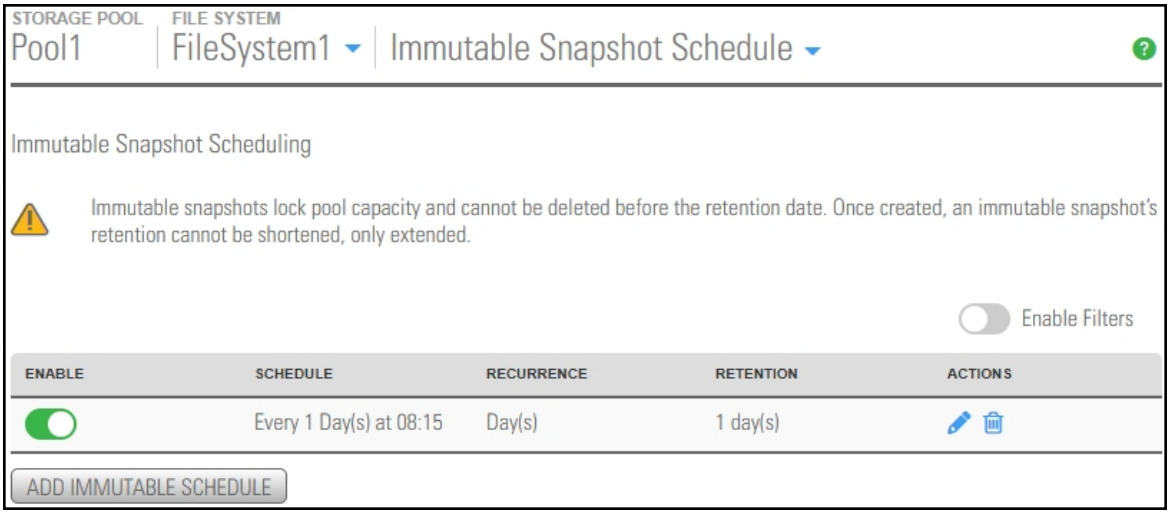
5. The **Add Immutable Schedule** pop-up appears. The fields for **Start date** and **at** time are pre-set to the time of creation. Complete the **Recur every** fields and the **Retain immutable snapshot for** (number of) **day(s)** field. When done, click the **Add** button.

Figure 5-80: Add Immutable Schedule pop-up



6. The **Immutable Snapshot Schedule** panel refreshes, with the newly created schedule listed in the chart. The columns include information for **Enable**, **Schedule**, **Recurrence**, **Retention**, and **Actions**.

Figure 5-81: Immutable snapshot schedule added

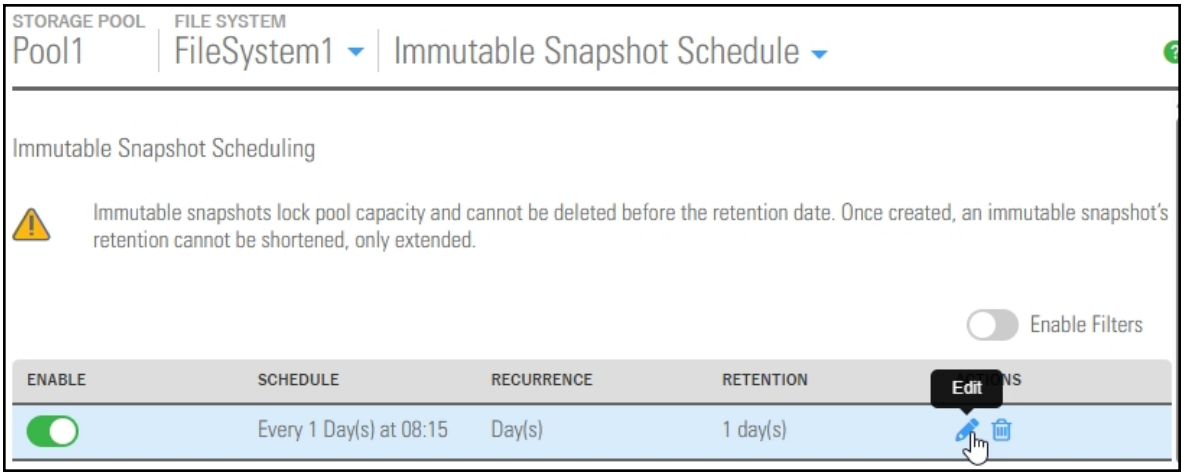


5

To edit an immutable snapshot schedule for a file sytem:

1. On the **Unity navigation bar**, select **Storage > File Systems**.
2. Click the link to the File System you would like to edit an immutable snapshot schedule for. **The File Systems Summary** page appears.
3. Select **Summary > Immutable Snapshot Schedule**.
4. The **Immutable Snapshot Scheduling** panel appears with a list of schedules. In the **Actions** column, click the **Edit icon** associated to the schedule to edit.

Figure 5-82: Immutable Snapshot Scheduling - Edit schedule



5. The **Edit Immutable Schedule** pop-up appears. The fields for **Recur every** and **Retain immutable snapshot for** (number of) **day(s)** can be modified.
   To disable or enable a snapshot schedule, use the radio button in the **Enable** column.
   When done, click the **Save** button.

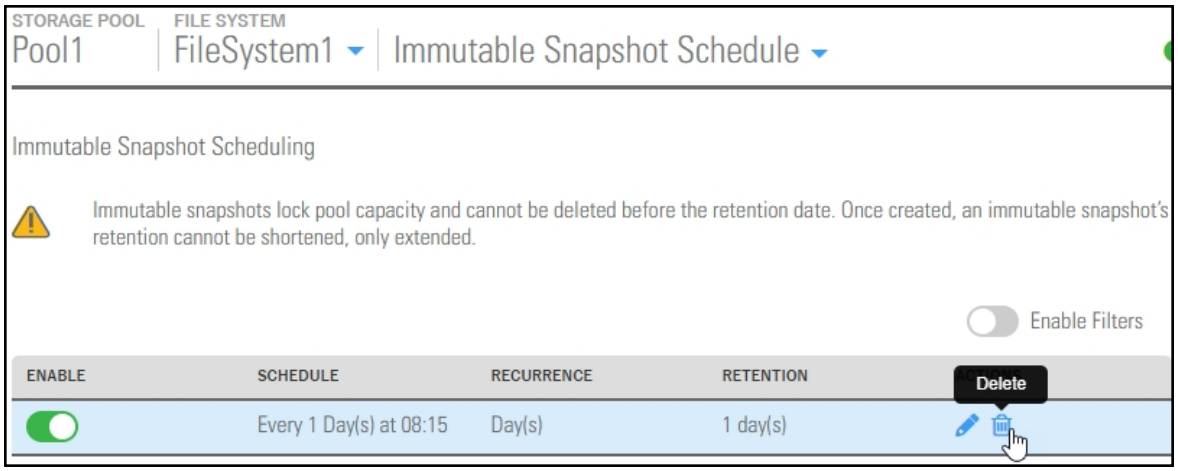
Note Immutable snapshots lock pool capacity and cannot be deleted before the retention date. Once created, an immutable snapshot's retention cannot be shortened, only extended.

5

▶ **To delete an immutable snapshot schedule for a file sytem:**

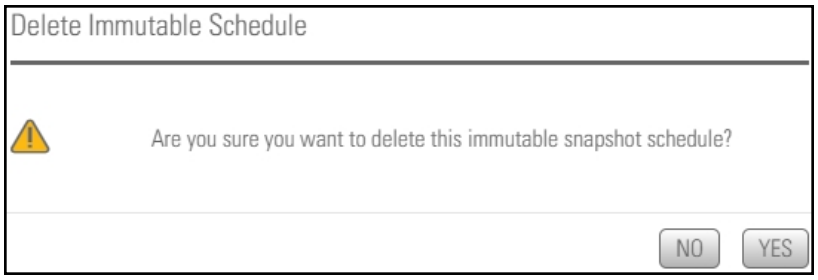
1. On the **Unity navigation bar**, select **Storage > File Systems**.
2. Click the link to the File System you would like to delete an immutable snapshot schedule for. **The File Systems Summary** page appears.
3. Select **Summary > Immutable Snapshot Schedule**.
4. The **Immutable Snapshot Scheduling** panel appears with a list of schedules. In the **Actions** column, click the **Delete icon** associated to the schedule to delete.

Figure 5-83: Immutable Snapshot Scheduling - Delete schedule



5. The **Delete Immutable Schedule** pop-up appears. To confirm, click the **Yes** button.

Figure 5-84: Delete Immutable Schedule pop-up



5

Chapter 6

LUNs

Unity supports block-level storage access using storage protocols (iSCSI and Fibre Channel). 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. When assigning a target to a LUN, you can choose to expose the LUN over iSCSI or Fibre Channel.

This section includes these topics:

Data management functions on LUNs 232
Guidelines for adding and managing LUNs 232
Understanding disk space consumption 233
Creating a LUN 236
Viewing LUNs 248
Configuring client-side (host) settings for a LUN 254
Changing LUN space configuration 256
Deleting a LUN 257
Using Windows VSS 258
Enabling ZFS Encryption for LUNs 280
Managing snapshots for LUNs 285
Immutable snapshots for LUNs 304
Managing iSCSI targets 315
Host connectivity: LUN masks and Initiator Groups 322

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 enables 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 any time. Thin provisioning allows efficient storage management since the system administrator need only monitor the storage capacity of one single Unity Storage System. 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 enables you to replicate the data contained in each LUN to a remote Unity Storage System, 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 Unity System goes down (for routine maintenance or a natural disaster), Unity enables 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 enables you to take point-in-time snapshots of the data contained in each LUN, including scheduled automatic snapshots. This enables you to maintain a set of previous versions of all files in a LUN.
- Data backups with NDMP support: Unity enables 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 Unity System-level tasks on page 437.

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 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 disk space is used when creating snapshots and replicating data. It also provides recommendations for setting up replication, especially if you are using thick LUNs. As opposed to thin-provisioned LUNs or file systems, which can use virtual space, thick LUNs use only the space allocated on disk. The amount of reserved space is the same as the disk's physical capacity.

When creating snapshots:

- When the LUN or file system is almost full, a snapshot of either uses that same amount of space, which almost doubles the space used on disk for the LUN or file system and snapshot on the storage pool. In such cases, snapshots use space outside the LUN or file system reserved space.
- When creating multiple snapshots, any changes to the data (deletions, additions, and rewrites) between snapshots create additional copies of all used space on thick LUNs, so the total amount of space may exceed the LUN size.

When creating replications:

Unity takes two snapshots:

1. A baseline snapshot that captures the data of last replication.
2. An incremental snapshot that 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 that there is enough disk space on your storage pool for the replication because snapshots and replications will use additional space, as explained above.
- Make sure data compression is turned on (the default).Open the storage pool, and click **Summary** > **Advanced Settings**.
- Use a shorter replication interval to save space and replication time.

Space comparison for Thin vs. Thick LUNs

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.)

#	Action	Data written	Data size	Baseline snapshot	Increm. 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

#	Action	Data written	Data size	Baseline snapshot	Increm. snapshot	THIN LUN	THICK LUN
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
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

[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.

#	Action	Data written	Data size	Baseline snapshot	Increm. snapshot	THIN LUN	THICK LUN
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

Creating 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 Create a LUN wizard; before starting the Create a LUN wizard, review the guidelines provided in the subsequent sections.

Note If you select the option to create a new iSCSI target during the LUN creation process (*step 1*), the Create a LUN wizard includes 7 steps. This section only describes the process for adding a LUN using the default, or an existing target. Unity provides the Target Setup wizard to guide you through the process for adding a target to a storage pool; for more information, see Adding an iSCSI target on page 315.

Before you begin:

- If you intend to use CHAP (Challenge Handshake Authentication Protocol) authentication, you must add CHAP users to the Unity System.
- You can add one or more iSCSI targets to storage pools 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 315.

  For Fibre Channel, the target is automatically created by Unity.

The Create a LUN wizard guides you through the process of adding a LUN to a storage pool.

6

Prerequisites

To add a LUN, you must first define a storage pool.

To start the Create a LUN wizard:

1. On the **Unity navigation bar**, select **LUNs**.
2. Click **Add LUN**.

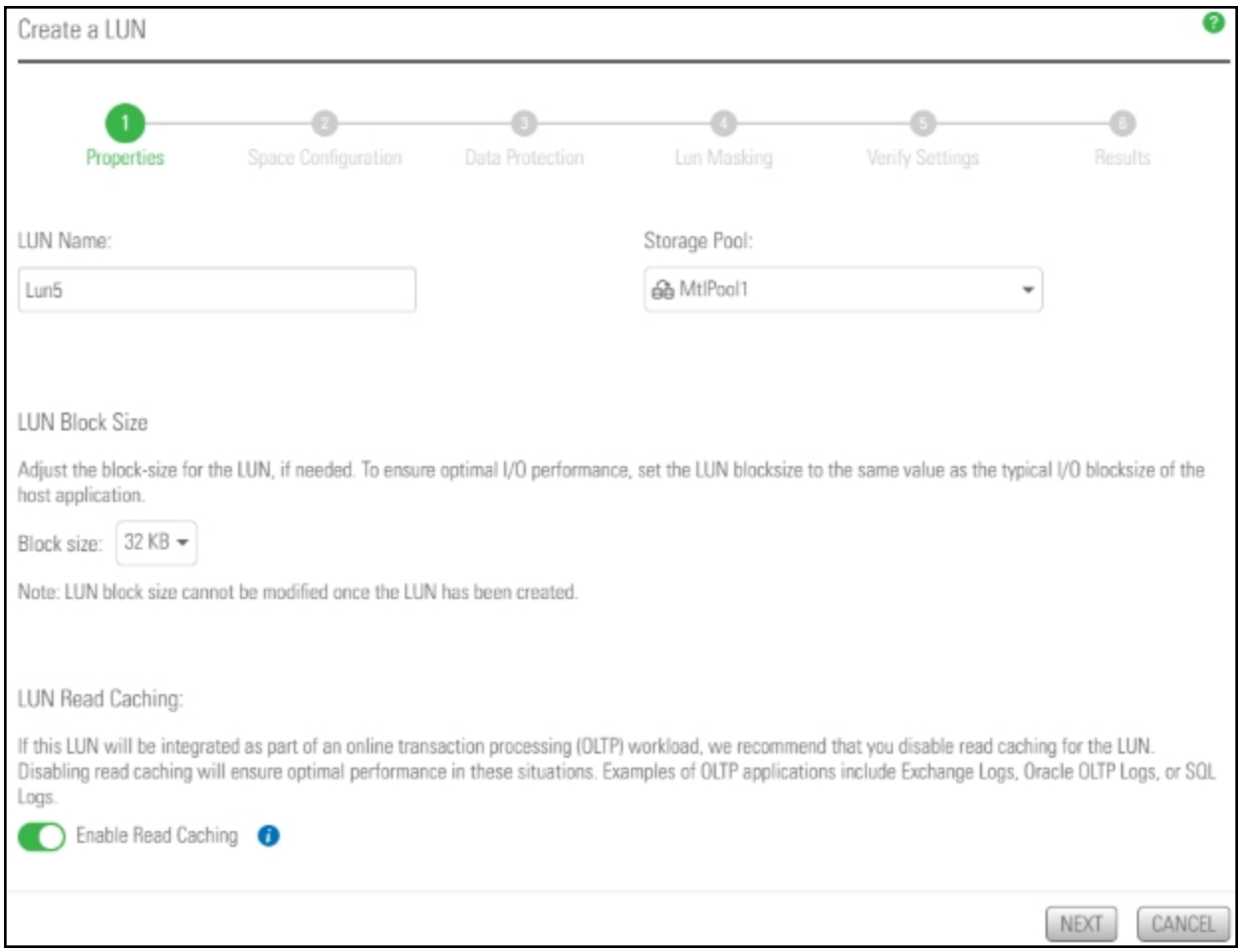
This section includes these steps:

Step 1: Setting the LUN name and block size on the facing page
Step 2: Space configuration settings for the LUN on page 239
Step 3: Enabling software encryption, data replication and snapshot scheduling on page 241
Step 4: LUN masking on page 243
Step 6: Verifying settings on page 245
Step 7: Viewing progress on page 247

Step 1: Setting the LUN name and block size

This step of the Create a LUN wizard prompts you to specify a name for the new LUN, set block size, as well as define client-specific (initiators) settings.

Figure 6-1: Create a LUN wizard, Step 1: Setting the LUN name and block size



▶ **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.

   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 6-1: Recommended block size for the application used

Application / Data type	Recommended block size
Windows / Linux Boot	64 KB
Microsoft Exchange 2019 DB	32 KB
Microsoft Exchange 2019 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.
   - The successor to Microsoft Exchange Server 2019 is Exchange Server Subscription Edition (SE) as of 2025

3. (Optionally) Disable read caching for the LUN. For database OLTP LUNs, we recommend to disable read caching to increase performance.
4. Click **Next** to continue.

Step 2: Space configuration settings for the LUN

This step of the Create a LUN wizard prompts you to specify space usage settings for the LUN.

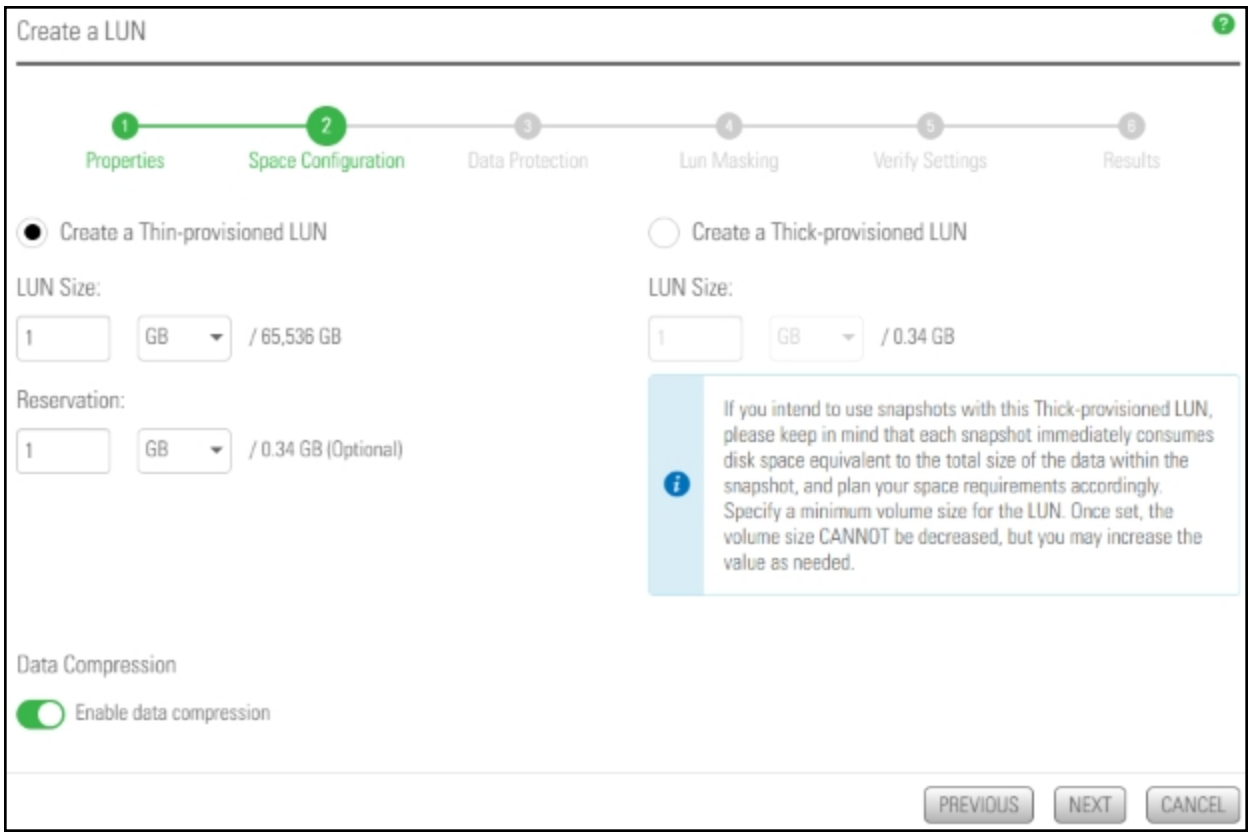
Note If you are using data replication, Nexsan recommends using thin-provisioned LUNs.

This table illustrates how Unity distributes disk space to LUNs for a storage pool of 10 TB.

Table 6-2: Distribution of disk space to LUNs

Space usage settings	Total available space in storage pool: 10 TB	
	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 6-2: Create a LUN wizard, Step 2: Space configuration



To configure space usage for the LUN:

1. To use the **Thin Provisioning** feature (enabled by default): Accept or update the **LUN Size** value.This determines the disk space that clients see when they connect to the LUN.

   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.

2. Specify the **Reservation** space for the LUN in the storage pool. This space will be reserved for the exclusive use of the LUN.

   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.

3. Optionally, select **Create a Thick-provisioned LUN**.

   Accept the default **LUN size**, or enter a value to change it. Thick Provisioning will use the specified amount of physical disk space.

   Notes:

   - The Unity graphical user interfaces do not support switching from thick to thin LUN provisioning after a LUN is created. Contact Nexsan Support if you need to perform a conversion.
   - 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.

   For LUNs hosted in a VMware environment, we recommend using Thick-provisioned LUNs.

4. Click the **Next** button to continue.

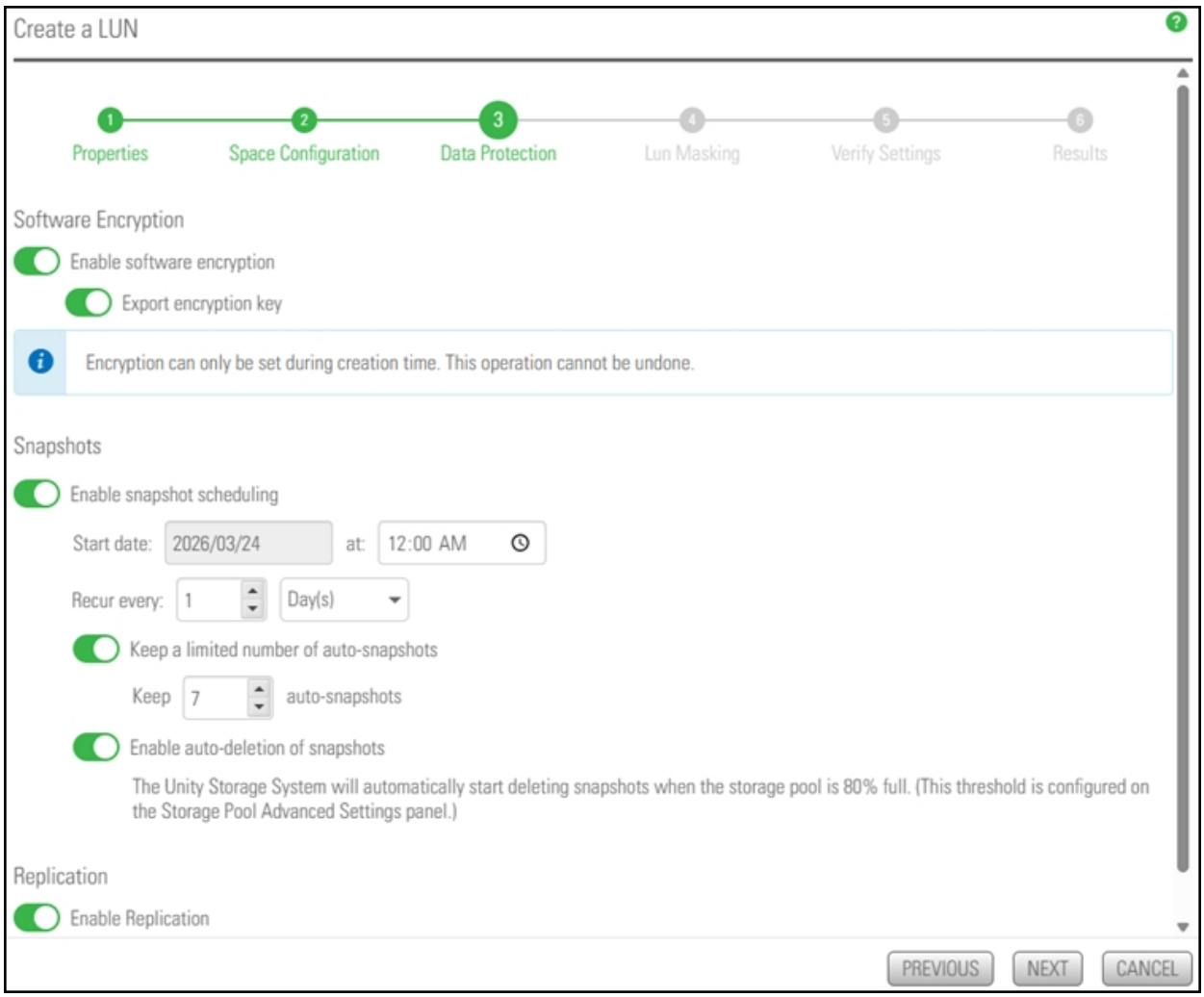
Step 3: Enabling software encryption, data replication and snapshot scheduling

This step of the Create a LUN wizard prompts you to enable software encryption and data replication for the LUN, if data replication with one or more remote sites is configured for the storage pool, and also to configure the snapshots schedule and auto-deletion settings for snapshots.

Limitations

- We do not recommend enabling snapshots scheduling when using LUNs in a Hyper-V environment. You can take manual snapshots and roll back data to a snapshot.
- We do not recommend enabling snapshot scheduling when using LUNs in a VMware environment. To take manual snapshots and roll back data to a snapshot for VMware, see the *VMware Best Practices Guide* on the Nexsan.com/support webpage.

Figure 6-3: Create a LUN wizard: Software encryption, replication, and snapshots



▶ **To enable software encryption for the LUN:**

1. To enable software encryption, select **Enable software encryption**. By default, **Export encryption key** is pre selected.

NOTE: Encryption can only be set during creation time. The operation cannot be undone.

2. Proceed to **Snapshots** and **Replication** in the same panel.

To enable data replication for the LUN:

1. Select **Enable Replication**. 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 don't need to enable snapshot scheduling, click **Next** on the wizard panel to continue.

To configure snapshot scheduling for the LUN:

Note There can only be one snapshot schedule per LUN.

1. Configure the snapshot schedule for the LUN:
   a. Select **Enable snapshot scheduling**. This option is selected by default. Clearing the check box disables snapshot scheduling.
   b. Specify a recurrence pattern for the schedule by typing a value in the **Recur every** field; then, select the recurrence period 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, then select the day or days of the week that you want Unity to take automatic snapshots on.
      - If you select **Month(s)**, 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. Select **Enable the auto-deletion of snapshots** if you want Unity to automatically delete 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 **Next** to continue.

Step 4: LUN masking

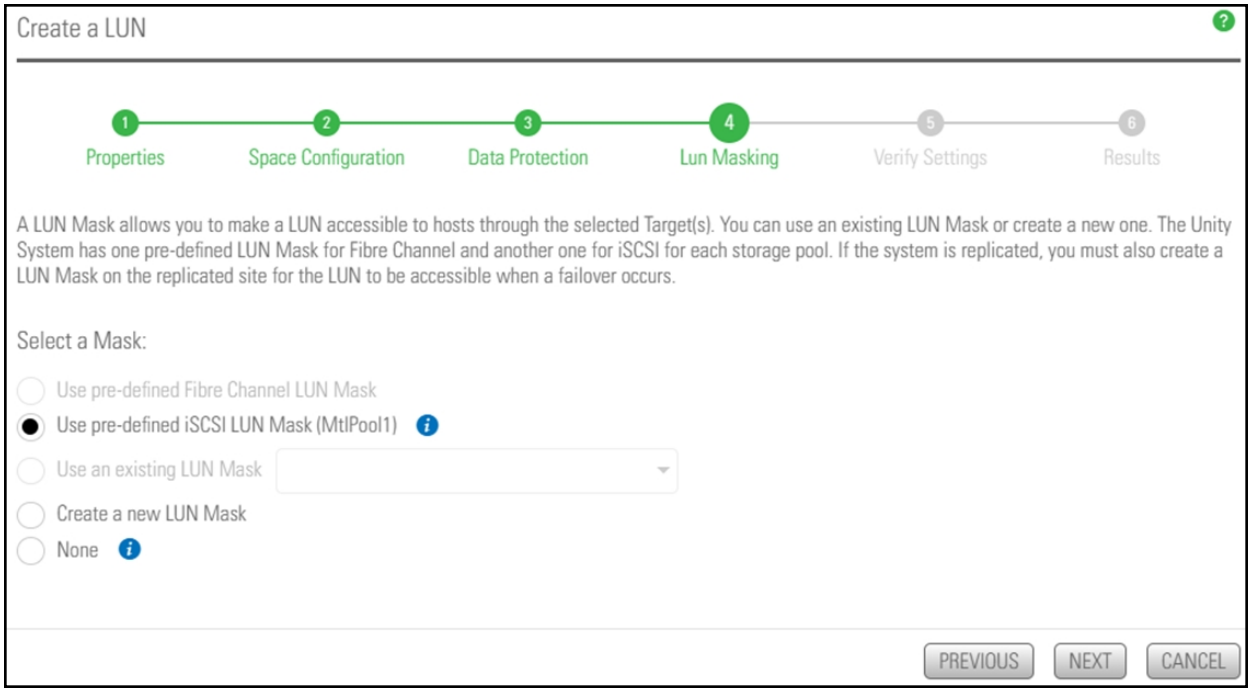
This step of the Create a LUN wizard prompts you to select a LUN mask. A LUN mask enables you to make a LUN accessible to hosts through the selected Target(s). You can use an existing LUN mask or create a new one. Unity has two types of LUN masks, one for Fibre Channel and the other one for iSCSI for 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.

To select 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**: This step adds a step to the wizard for defining a LUN mask. See the next step.
   - **None**: If you select this option, you will need to select or create a LUN mask later to make the LUN accessible to hosts .

Figure 6-4: Create a LUN wizard, Step 4: Selecting a Mask



6

2. Click **Next** to continue. If you selected to create a new LUN mask, the wizard will continue to Step 5: Create a new LUN mask below.

   If you selected an existing LUN mask, the wizard will continue to Step 6: Verifying settings on the facing page.

Step 5: Create a new LUN mask

This step of the **Create a LUN** wizard prompts you to create a new LUN mask if you selected that option in the previous step. The LUN mask is used to make the LUN visible to a host using the target you associate with the LUN.

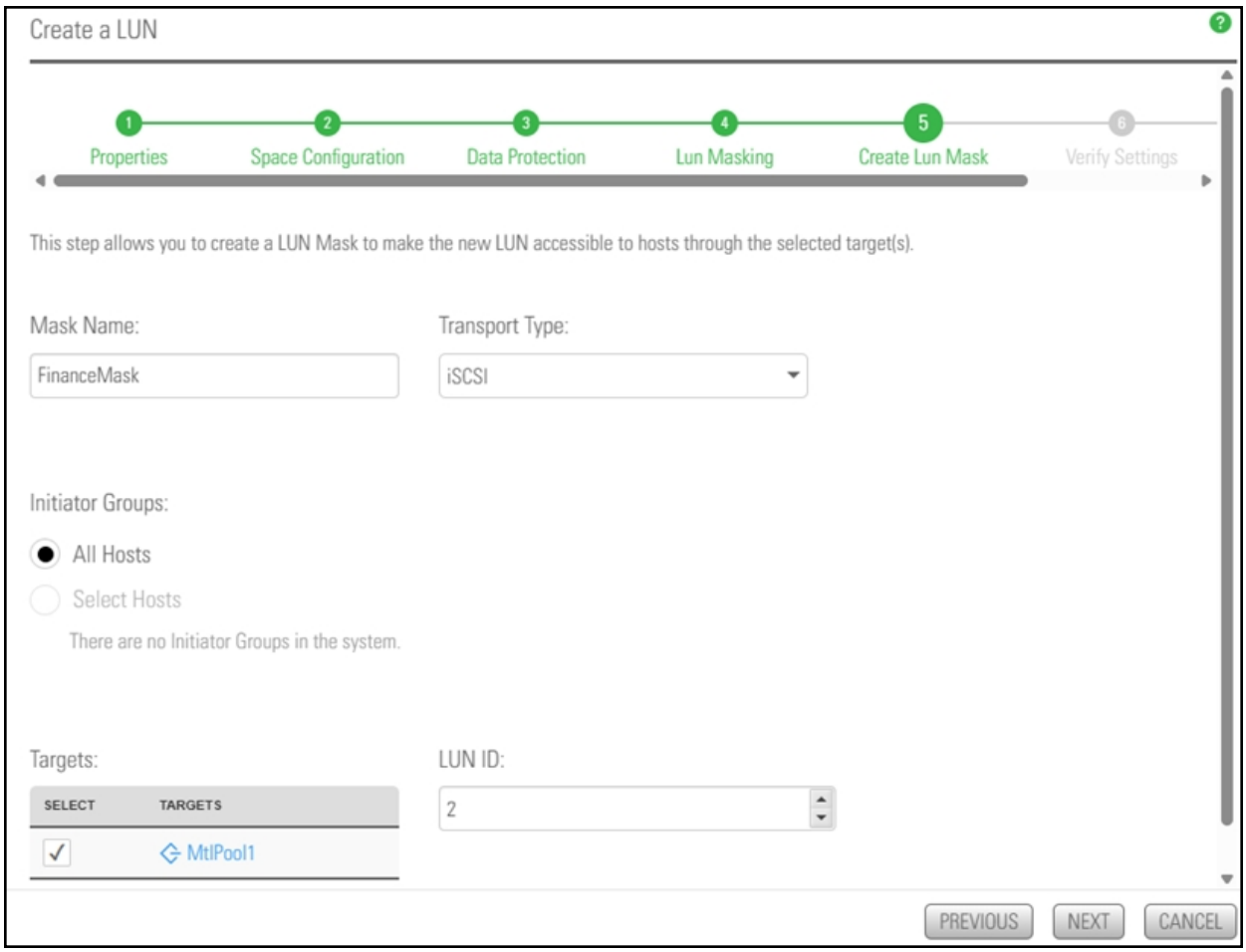
When creating an iSCSI LUN, you specify the initiators you want and assign one or more of the available iSCSI targets to the LUN. If you have not created iSCSI targets yet, you must skip this step because the wizard will not let you continue. After creating the LUN, you have the possibility to associate it to a target by following the steps in . For steps to create an iSCSI target, see Adding an iSCSI target on page 315.

When creating a Fibre Channel LUN, you specify the initiators you want and then assign the unique common Fibre Channel target to the LUN.

To add a new LUN mask:

1. Select the **Add to a new LUN mask** option.

Figure 6-5: Create a LUN wizard, Step 5: Create LUN mask



2. Enter a meaningful name in the **Name** field.
3. From the **Transport Type** drop-down list, select **iSCSI** or **Fibre Channel**. The **Target** selection is automatically updated with the existing target associated with the storage pool.
4. Select an Initiator Group. An initiator group must contain either Fibre Channel or iSCSI initiators. An initiator cannot be selected in multiple groups.
5. 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.
6. Click **Next** to continue.

Step 6: Verifying settings

This step of the Create a LUN wizard summarizes the settings you selected for your LUN. Review the summary carefully before applying the configuration settings.

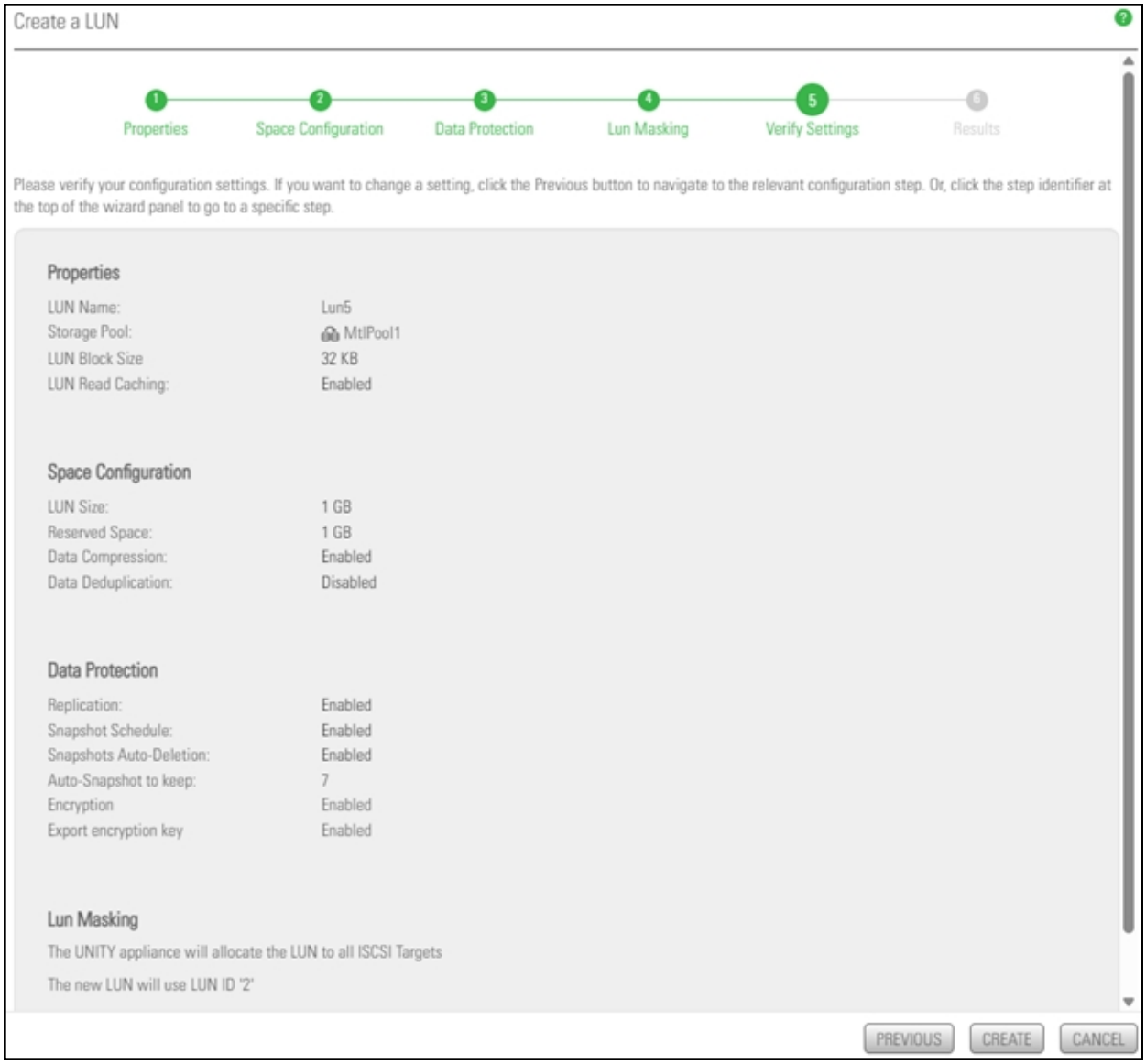
► To change a LUN configuration setting:

- Click **Previous** to go back to the corresponding configuration step.

  Or

- Click the corresponding step identifier at the top of the Create a LUN wizard panel. For example, if you want to rename the LUN, click **Properties**.

Figure 6-6: Create a LUN wizard: Verify Settings

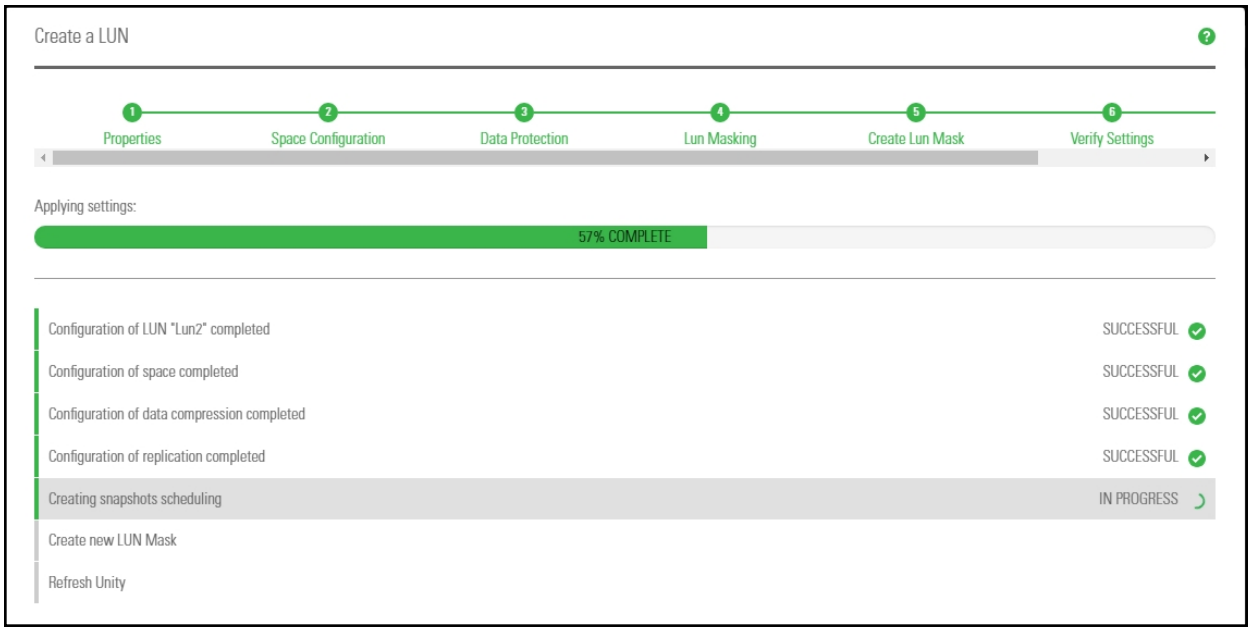


When you are satisfied with the configuration settings, click **Create** at the bottom of the panel.

Step 7: Viewing progress

In this step, the Create a LUN wizard displays progress as Unity creates the new LUN.

Figure 6-7: Create a LUN wizard: Viewing configuration results



The Create a LUN 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 **View Error** link 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.

Viewing LUNs

The LUNs panels include:

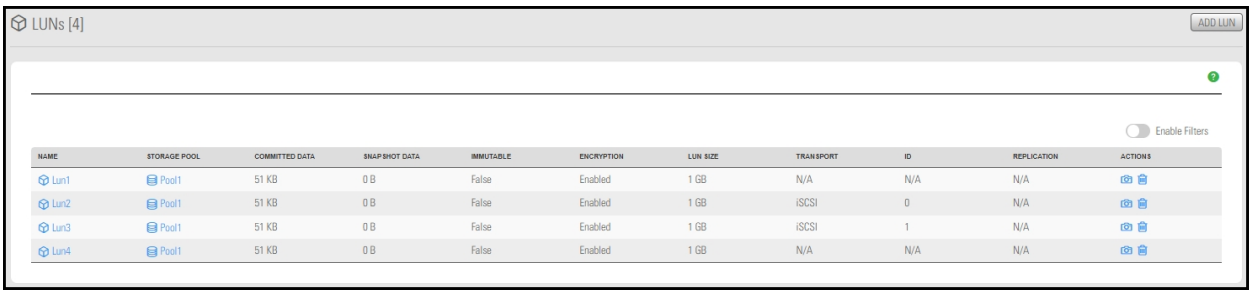
- a listing of all LUNs
- a detailed summary panel for individual LUNs
- used and available disk space details

To modify space usage settings, see Changing LUN space configuration on page 256.

To access the LUNs panels:

1. On the **Unity navigation bar**, click **Storage > LUNs**. The LUNs panel opens, showing all existing LUNs.

Figure 6-8: LUNs panel



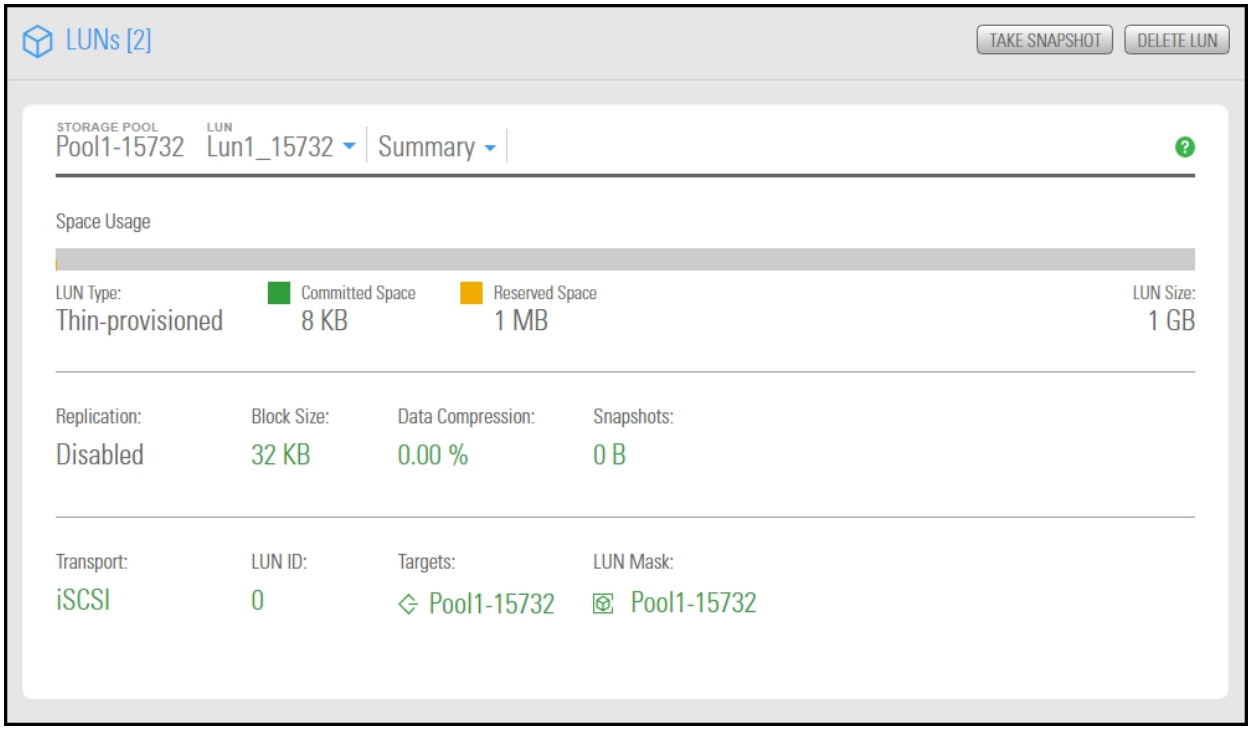
2. Optionally, select **Enable Filters** to filter based on any column's data type.

Table 6-3: LUN space usage data

Column	Description
Committed data	The amount of space that is currently consumed by the host, excluding snapshots and reservation.
Snapshot data	The amount of the space consumed by snapshots, including the reservation added for snapshots.
LUN size	The size of the LUN.

3. Click the link to a LUN to open the **LUN properties** panel.

Figure 6-9: LUNs Summary panel



6

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.

Renaming a LUN

Use this topic for renaming a LUN. If the LUN is replicated, Unity also renames the LUN's replica on the remote Unity.

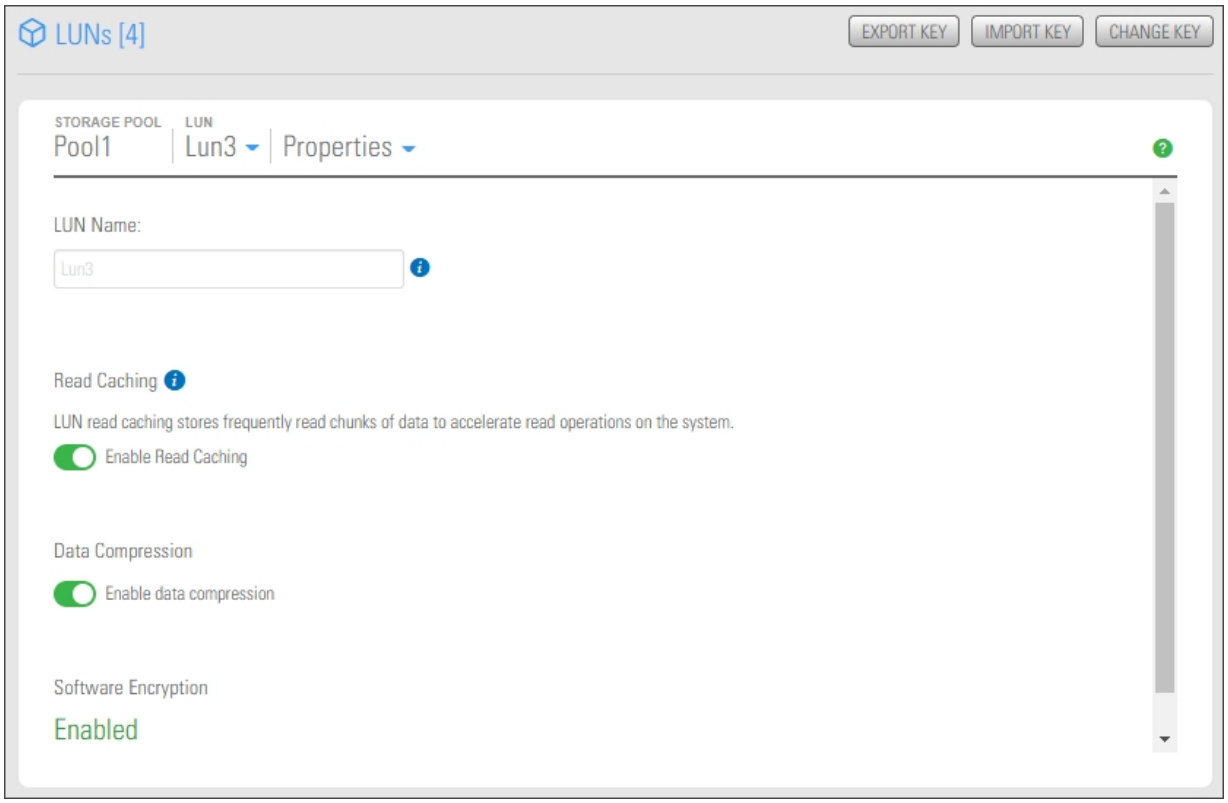
CAUTION: An encrypted dataset cannot be renamed. If you rename a LUN, client systems on the network will be disconnected from the LUN; this could result in data loss. Before renaming a LUN, make sure that active client systems disconnect from the LUN.

After renaming the LUN, you will need to update the host connection to the LUN using the new name.

To rename a LUN:

1. On the **Unity navigation bar**, click **Storage > LUNs**.
2. Select the LUN you want to rename.
3. Click **Summary > Properties**.

Figure 6-10: LUNs properties panel



4. 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 hyphen (-) and period (.), the name can only contain alphanumeric characters, without spaces.

   These characters are NOT allowed:

   ″ / \ _ [ ] : ; | = , + * ? < >

5. Click the **Apply** button.

Configuring 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 Configuring data compression on a storage pool on page 102. If you choose to disable data compression on the LUN, only that LUN will be affected.

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.

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.



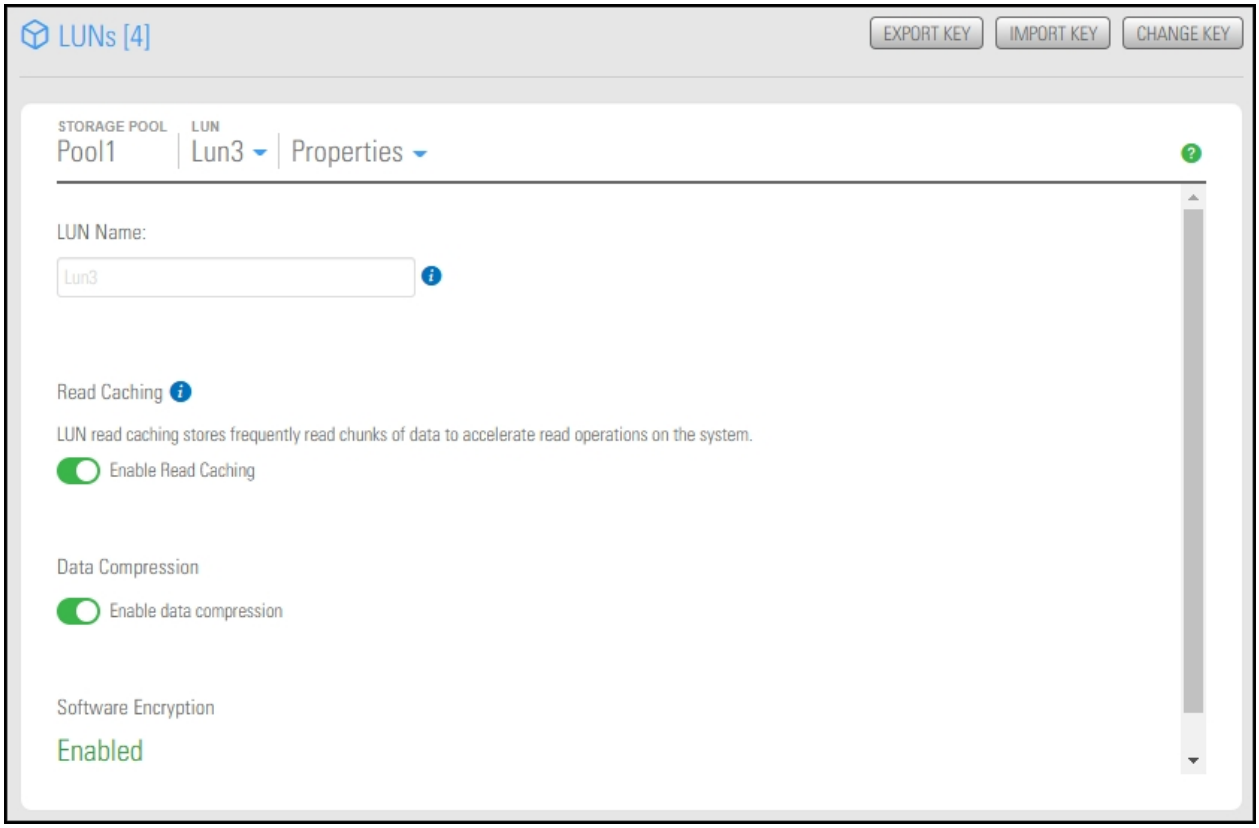
CAUTION: If you turn on data compression for a LUN, and then you turn it off before you set up replication for the LUN, part of the data will be decompressed and the other part will not. Since the LUN has not been replicated yet, the compression settings are not inherited and data compression is off 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. On the **Unity navigation bar**, click **Storage > LUNs**.
2. Click the link to a LUN to open the **LUN properties** panel.
3. Select **Summary > Properties**.

Figure 6-11: LUNs Properties panel



4. Select **Enable data compression**.
5. Click the **Apply** button.

Disabling Read caching

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 afterward using the LUNs properties panel.

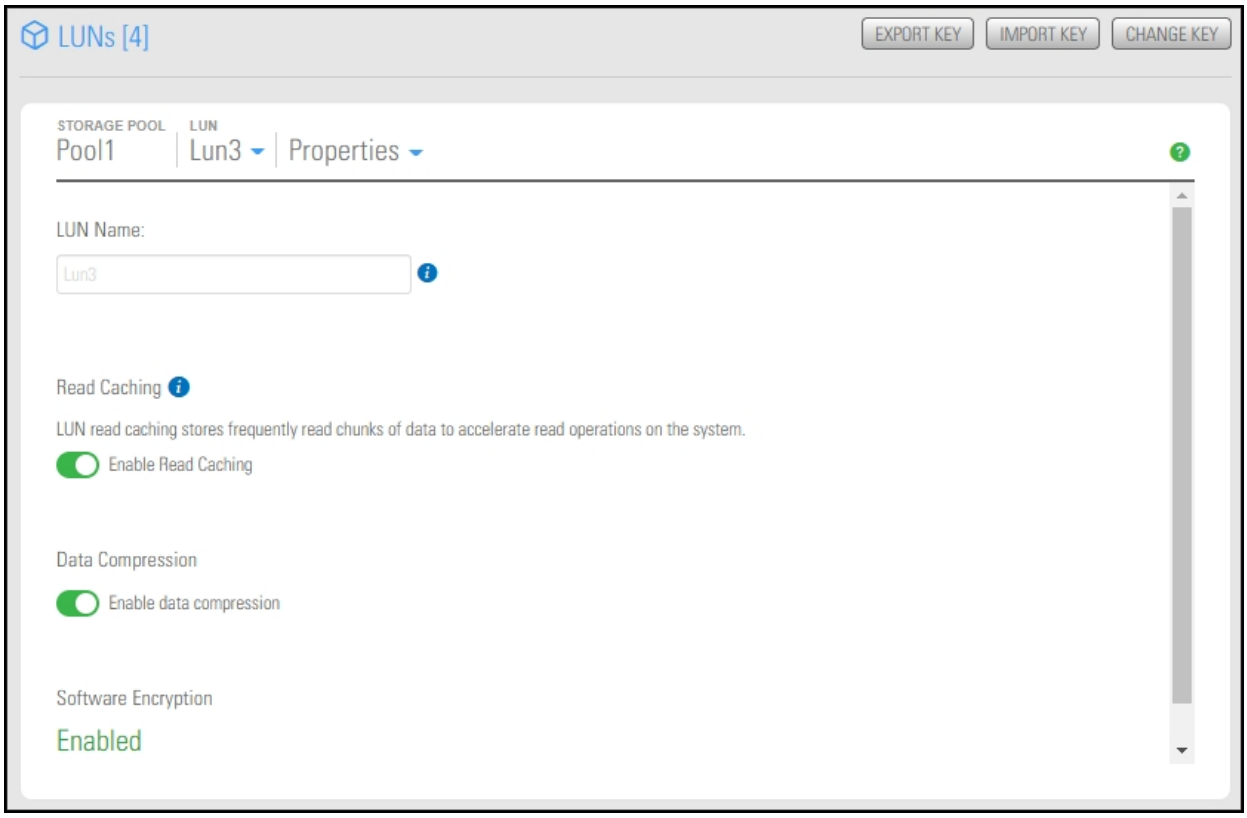
LUN read caching stores frequently read chunks of data to accelerate read operations on the system.

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 disabling read caching to increase performance.

▶ **To disable Read caching:**

1. On the **Unity navigation bar**, select **Storage > LUNs**.
2. Click the link to a LUN to open the **LUN properties** panel.
3. Select **Summary > Properties**.

Figure 6-12: LUNs Properties panel



4. Select **Enable Read Caching**.
5. Click the **Apply** button.

Configuring client-side (host) settings for a LUN

Unity provides two configuration options that allow you to set client-specific (iSCSI 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

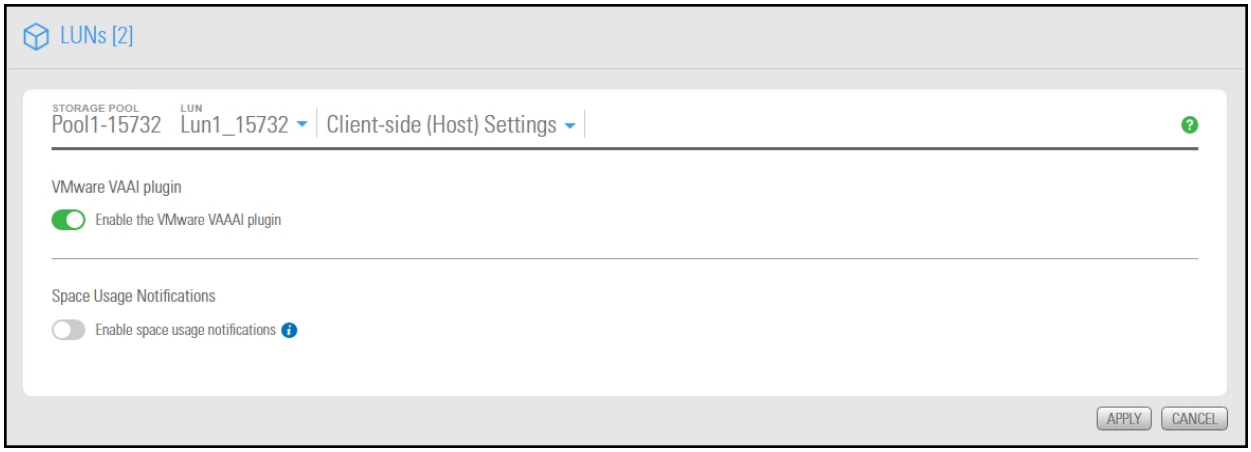
You must configure and enable VAAI hardware acceleration functionality on your VMware ESX/ESXi support for the VAAI plug-in on Unity to work; for more information, please refer to the VMware documentation. If you already created LUNs but the VAAI plugin is not enabled for these LUNs, follow the steps mentioned in this section.

Note The VMware VAAI plug-in is always disabled by default when you create a LUN.

To enable the VAAI plug-in for a LUN:

1. On the **Unity navigation bar**, click **Storage > LUNs**.
2. Click the LUN that you want to enable the VAAI plug-in for.
3. Click **Summary > Client-side (Host) Settings**.
4. Click the **Enable the VMware VAAI plugin** button.

Figure 6-13: LUN Client-side (Host) Settings



5. Click the **Apply** button.

Enabling client-side space usage notifications for a LUN

Unity provides a notification mechanism that automatically notifies client systems (iSCSI or Fibre Channel 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.

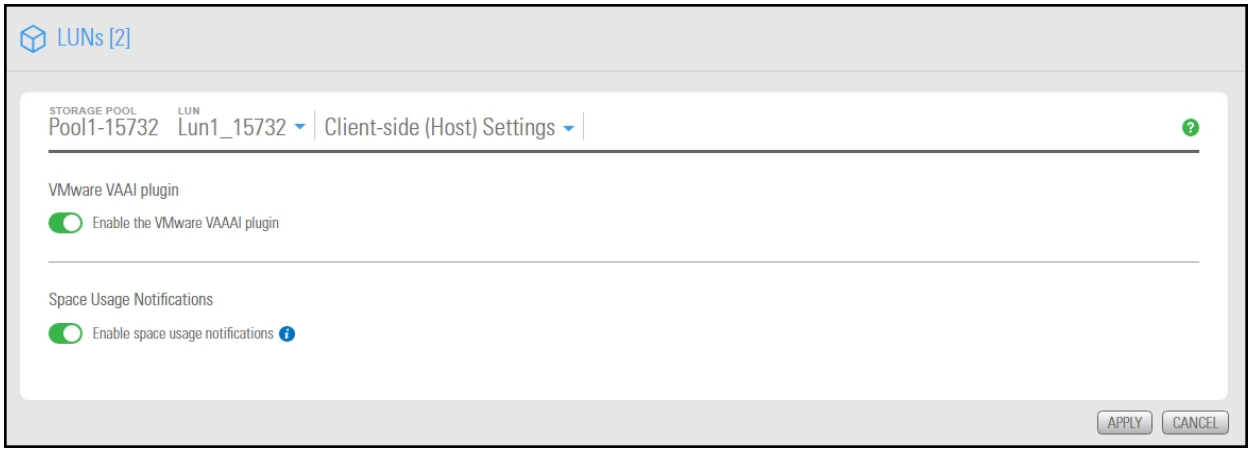
Before enabling this option, it is recommended that you:

- remove the mask at the target level; see Deleting a LUN mask on page 329.
- disconnect the LUN at the client level.

To enable client-side space usage notifications for a LUN:

1. On the **Unity navigation bar**, click **Storage > LUNs**.
2. Click the LUN that you want to enable the VAAI plug-in for.
3. Click **Summary > Client-side (Host) Settings**.
4. Click the **Enable Space Usage Notifications** button.

Figure 6-14: LUN Client-side (Host) Settings



5. Click the **Apply** button.

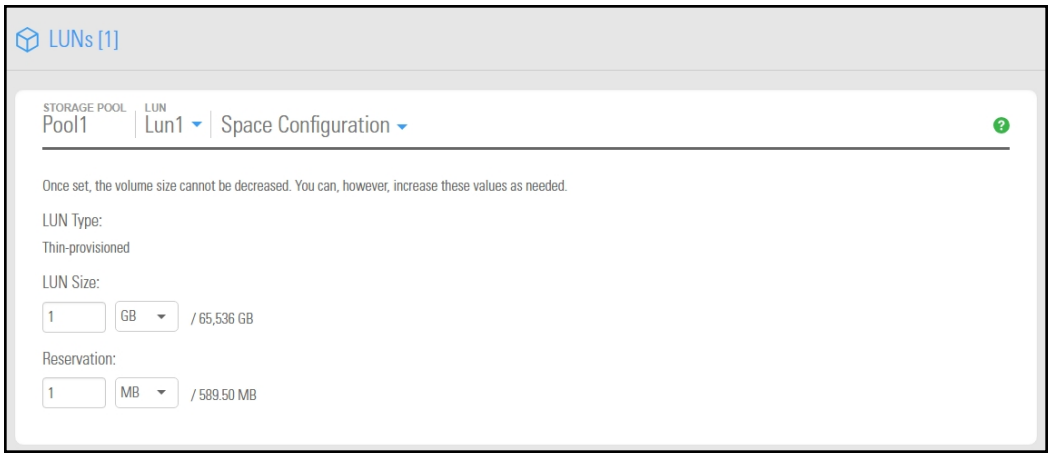
Changing LUN space configuration

Once 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 Step 2: Space configuration settings for the LUN on page 239.

To change LUN space configuration:

1. On the **Unity navigation bar**, click **Storage > LUNs**.
2. Click the link to the LUN that you want to reconfigure.
3. Select **Summary > Space Configuration**.

Figure 6-15: LUN Space Configuration panel



4. Perform one of these actions:

For a...	Do this
Thick-provisioned LUN	• To change the LUN size, select the relevant capacity unit from the drop-down list and type a value in the box. 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.
Thin-provisioned LUN	• 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. **Note** The virtual volume size cannot be less than the reserved space.

5. Click the **Apply** button.

Deleting a LUN

Use this procedure for instructions about how to delete 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 Storage System, the replicated LUN, including all the data in the replicated LUN is permanently removed as well.

To delete a LUN:

1. On the **Unity navigation bar**, select **Storage > LUNs**.
2. Click the **Delete LUN** icon.
3. In the **Delete LUN** popup window, review the warning text, and when you are ready to proceed, type the word "Delete" (non case sensitive) in the box.

Figure 6-16: Delete LUN popup



4. Click the **Delete** button.

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.

Supported Windows Server versions:

- Windows Server 2025
- Windows Server 2022
- Windows Server 2019
- Legacy Support:
  - Windows Server 2016
  - Windows Server 2012 R2

This section includes these steps:

Adding a CHAP user to the Management target 258
Installing the VSS Hardware Provider 258
Enabling the Microsoft VSS client for LUNs 262
Discovering your LUNs with the Windows iSCSI Initiator 263
Configuring the LUNs in Disk Management 267
Creating a VSS snapshot 269
Browsing a VSS snapshot 273
Viewing VSS client information 276
Rolling back data to a VSS snapshot 276
Deleting a VSS snapshot 278

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.

See "Users and Access Rights".

Installing the VSS Hardware Provider

The installation of the VSS Hardware Provider is available on Unity Discovery CD.

Before you begin:

Make sure to review the list of supported operating systems in Using Windows VSS above.

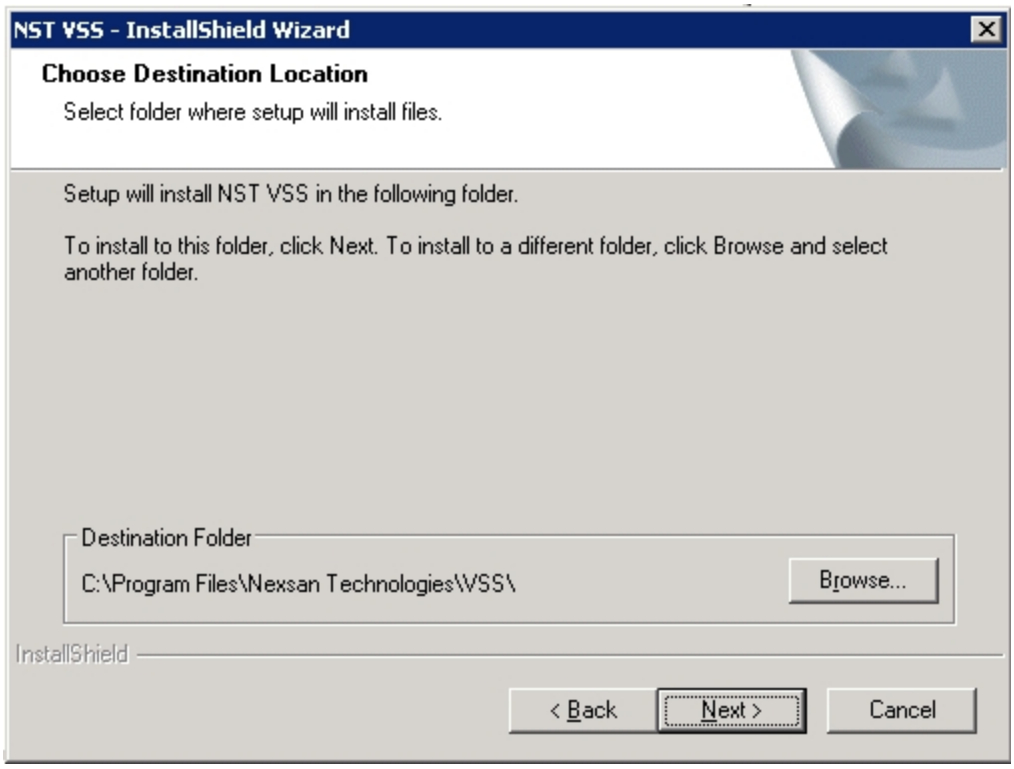
If you install the VSS Hardware Provider on Windows Server 2003 R2, you will see several warning messages:

- 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 Unity Discovery CD, 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**.

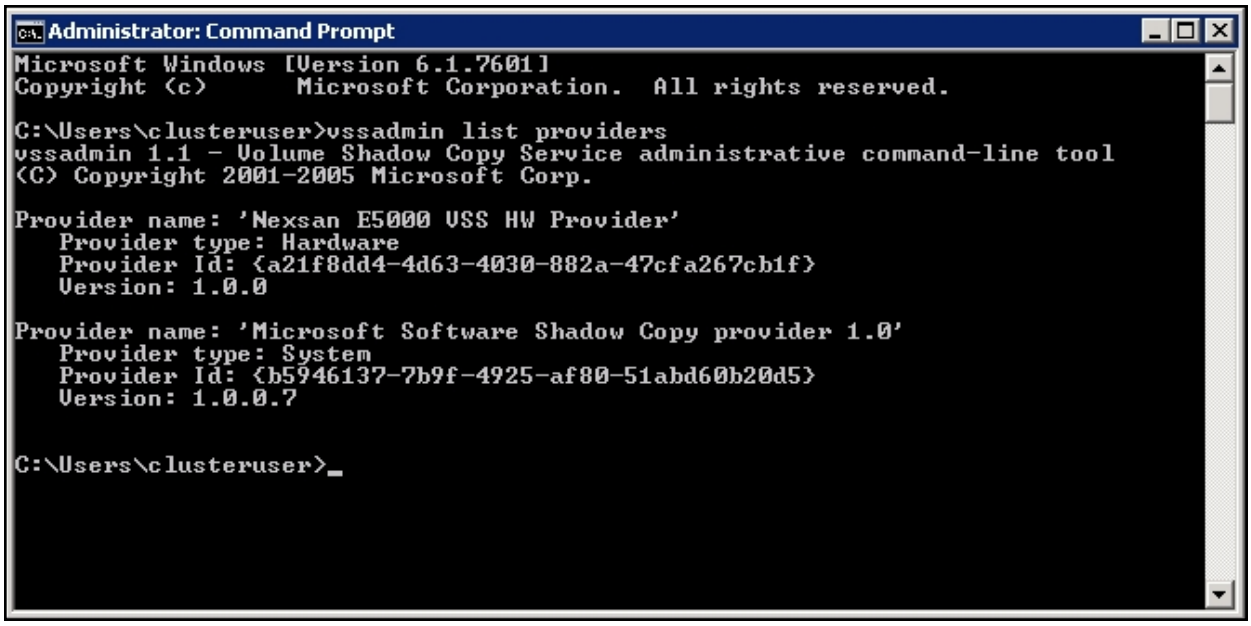
Figure 6-17: Installing VSS Hardware Provider



4. On the Ready to Install page, click **Install**.
5. On the Installation Complete page, click **Finish** to exit the wizard.

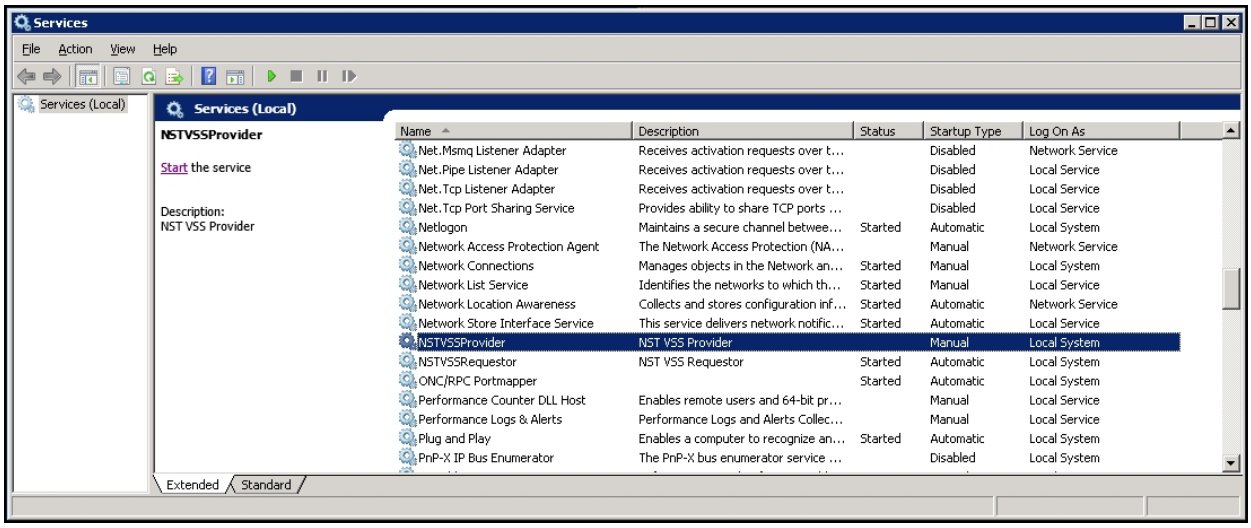
6. Verify the VSS Hardware Provider installation:
   a. Open a command prompt.
   b. Type this command: `vssadmin list providers`
   c. If the installation was successful, the list should display an entry for Nexsan VSS Hardware provider.

Figure 6-18: Verifying the VSS Hardware Provider installation



7. Start the VSS Hardware Provider service:
   a. Open the *Services* application.
   b. Locate and right-click the **NSTVSSProvider** service.

Figure 6-19: 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 on the next page

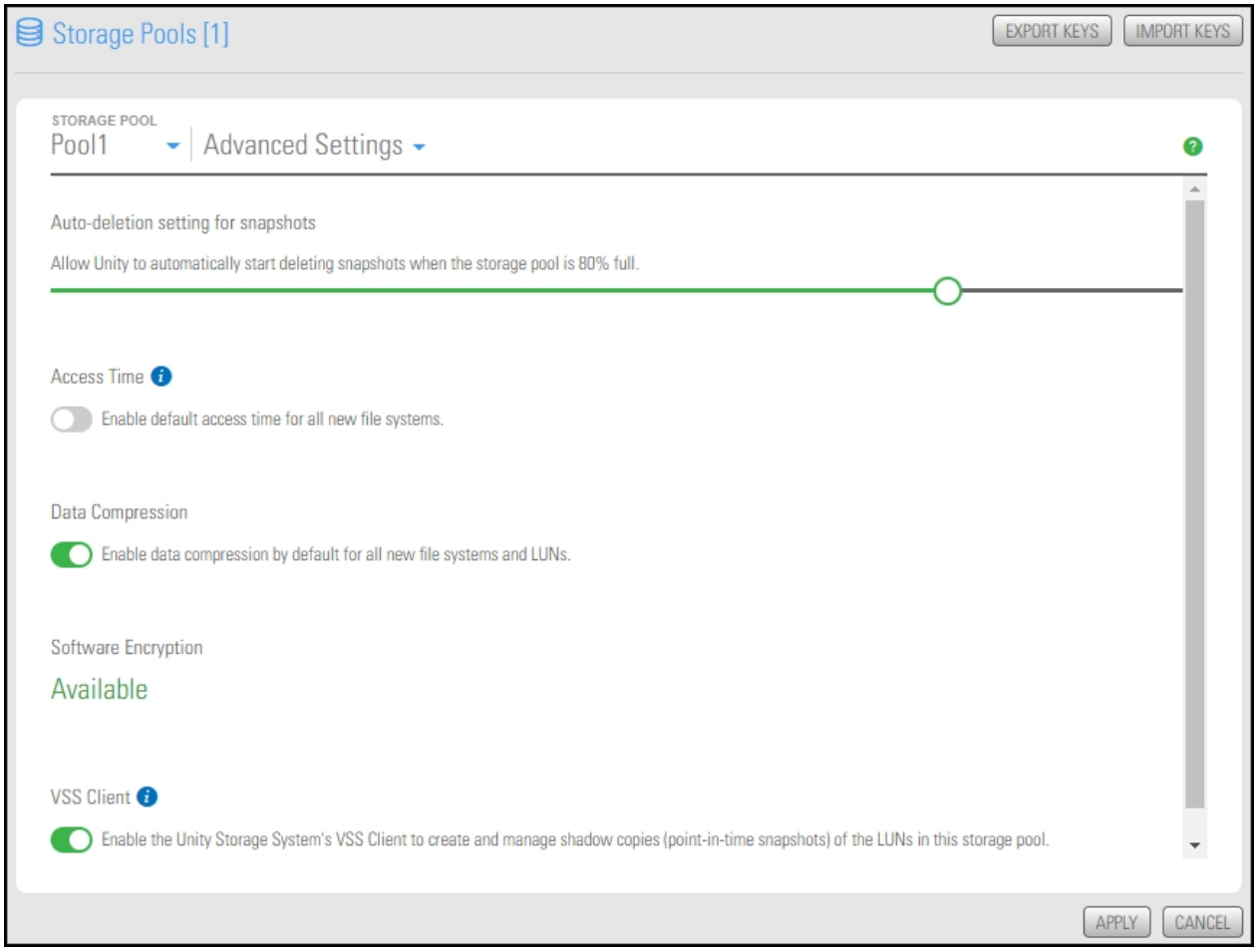
Enabling the Microsoft VSS client for LUNs

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. On the **Unity navigation bar**, select **Storage > Storage Pools**.
2. Select the storage pool that you need to enable Microsoft VSS for. The **Pool Summary** panel opens.
3. Select **Summary > Advanced Settings**.
4. Click the Enable VSS client button to permit Unity's VSS Client to manage snapshots for LUNs hosted on this pool.

Figure 6-20: Storage Pool panel, Advanced Settings



5. Click the **Apply** button.

▶ **Related topics:**

Installing the VSS Hardware Provider on page 258

Discovering your LUNs with the Windows iSCSI Initiator on the facing page

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 Windows *Disk Management* and *Explorer*.

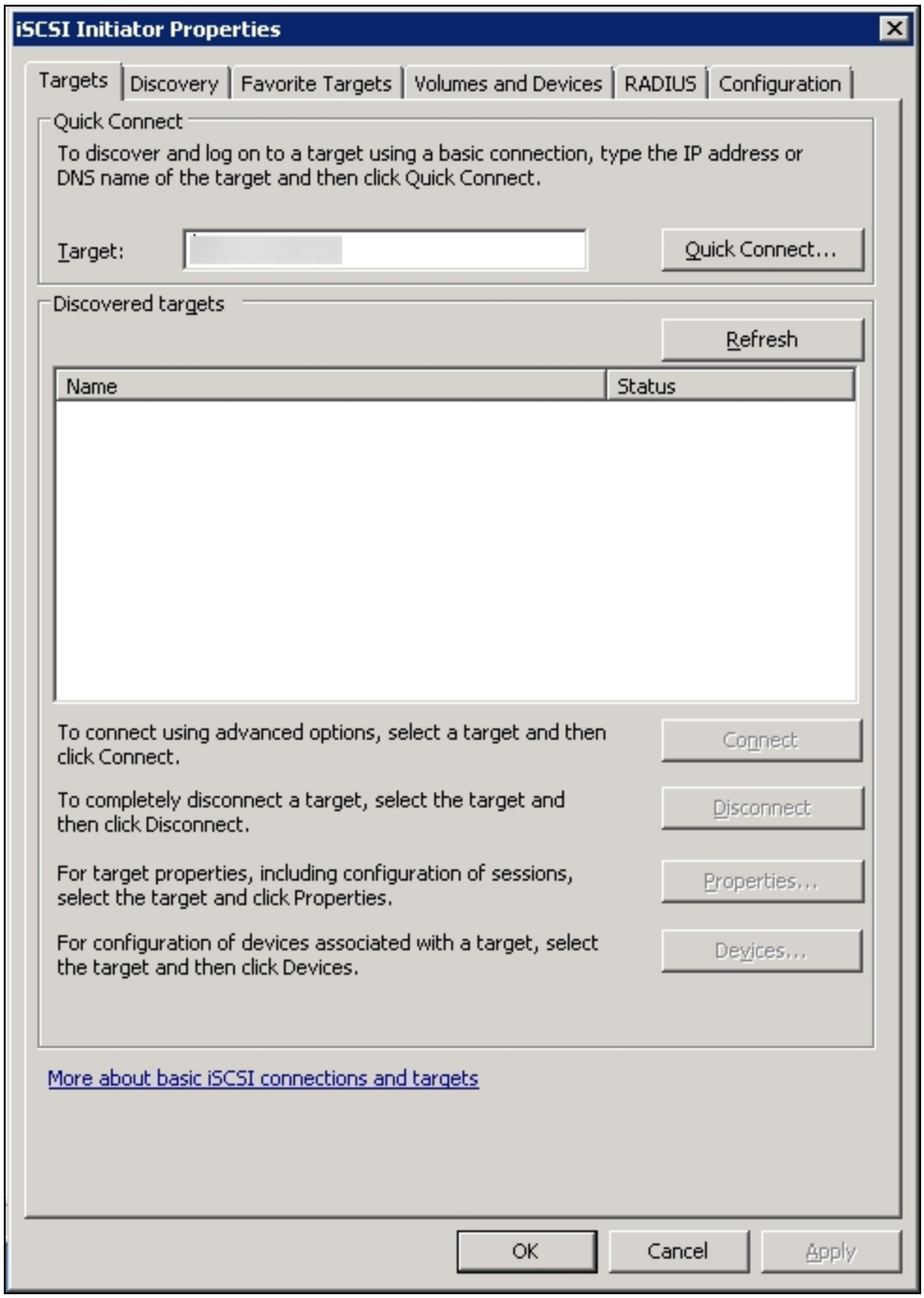
The VSS Hardware Provider connects to a storage pool's Management target via iSCSI to view, create, and manage snapshots of all LUNs in the storage pool. To discover the Management target, you must first enable the VSS feature in Unity; see Enabling the Microsoft VSS client for LUNs on the previous page.

You can discover Unity targets using the **Targets** tab or the **Discovery** tab of the Windows iSCSI Initiator Properties dialog box.

To discover the LUNs using the Targets tab:

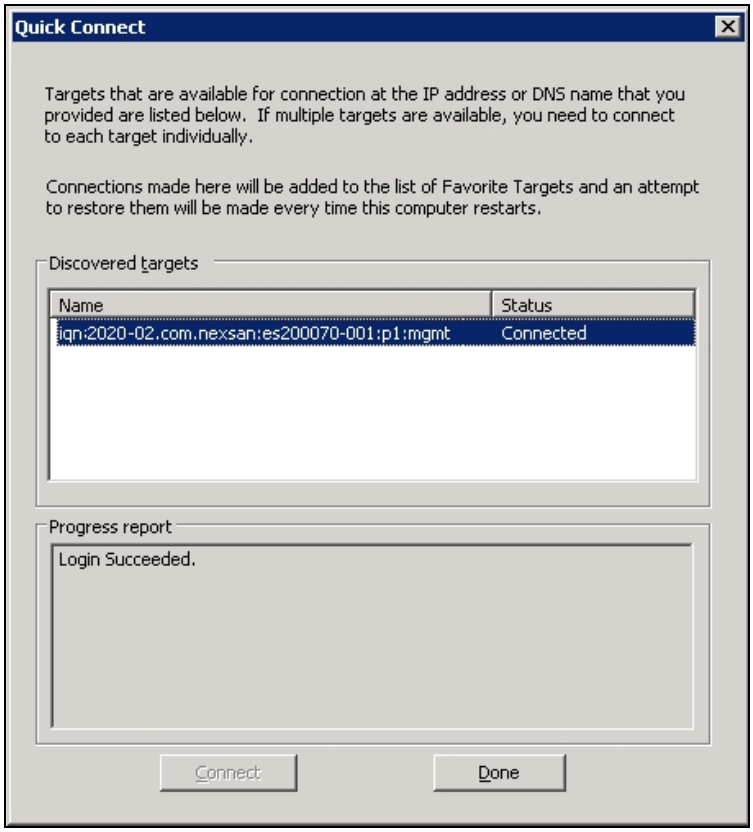
1. On the Windows server, select **Start > All Programs > iSCSI Initiator**.
2. In the **Target** field, type the Management virtual IP address of Unity.

Figure 6-21: iSCSI Initiator—Targets tab



3. Click **Quick Connect**. The discovered targets appear in the list.

Figure 6-22: iSCSI Initiator—Targets tab: Discovering targets



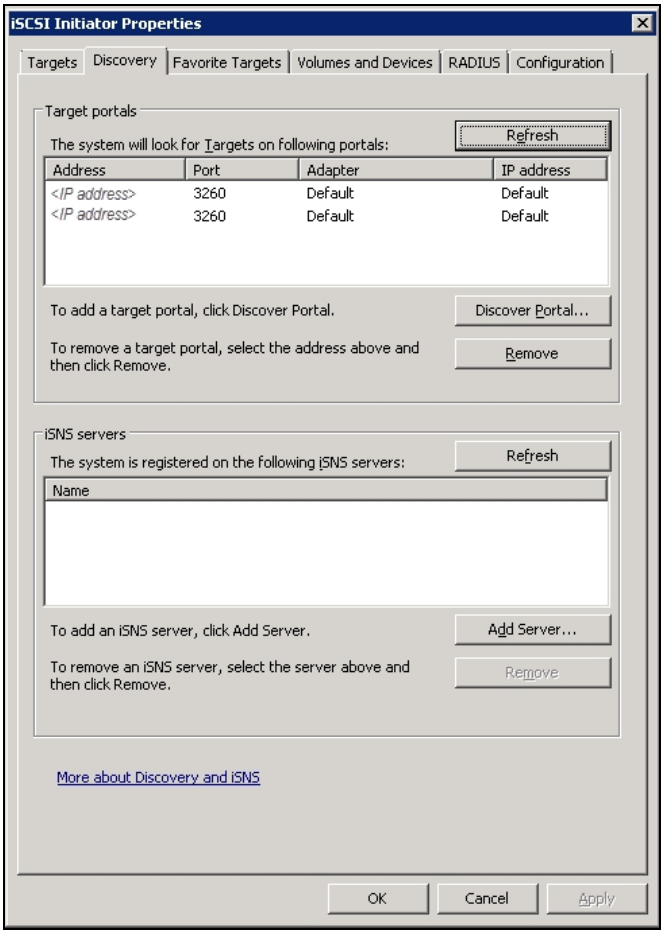
4. Click **Done** to close the Quick Connect dialog box.
5. The discovered target appears in the list. Click **OK** to exit the iSCSI Initiator.

► To discover the LUNs using the Discovery tab:

1. On the Windows server, select **Start > All Programs > iSCSI Initiator**.
2. Select the **Discovery** tab.

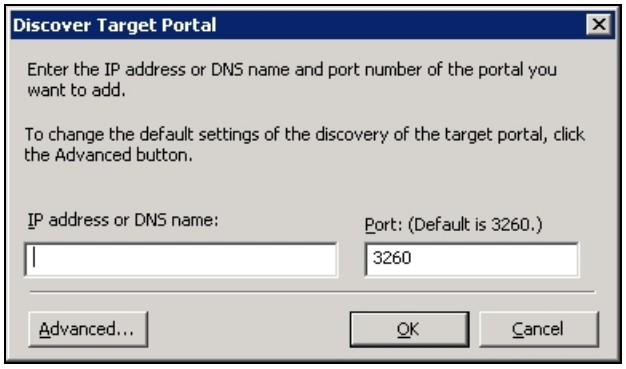
3. Click **Discover Portal**.

Figure 6-23: 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 6-24: iSCSI Initiator—Discovery tab: Discovering targets



5. The discovered targets appears in the list. Click **OK** to exit the iSCSI Initiator.

Related topics:

Configuring the LUNs in Disk Management on the facing page

Configuring the LUNs in Disk Management

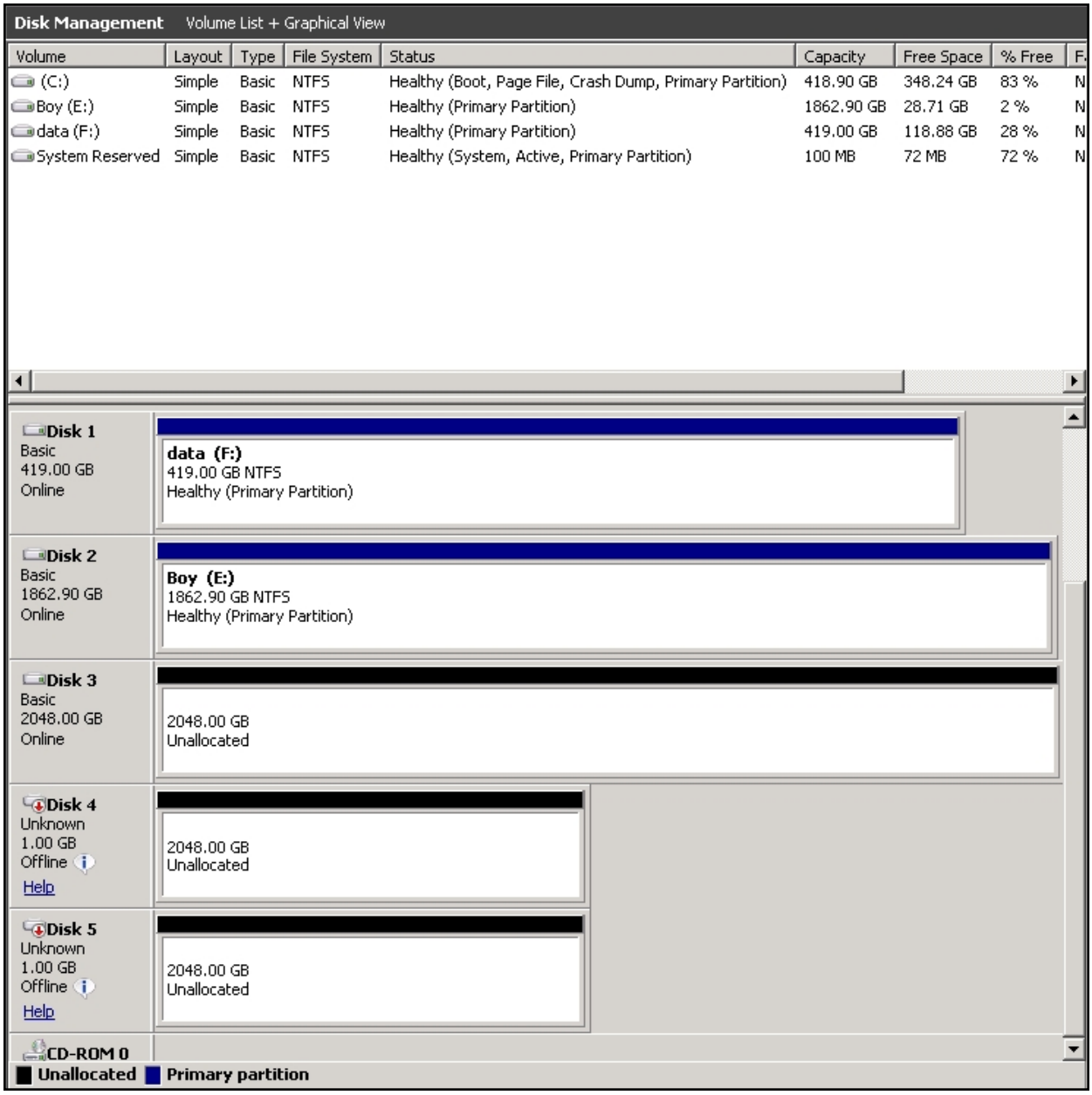
After discovering your LUNs with the Windows iSCSI Initiator, the LUNs appear as new disks, which you need to initialize and configure before you can use them.

▶ **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 6-25: Discovered targets in Disk Management

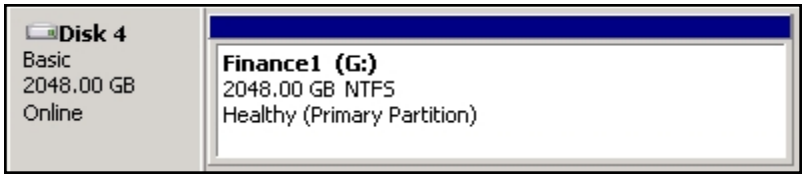


2. Right-click a disk on the left-hand side and select **Online**. The status changes to *Not Initialized* and *Online*.

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 6-26: Configured volume in Disk Management

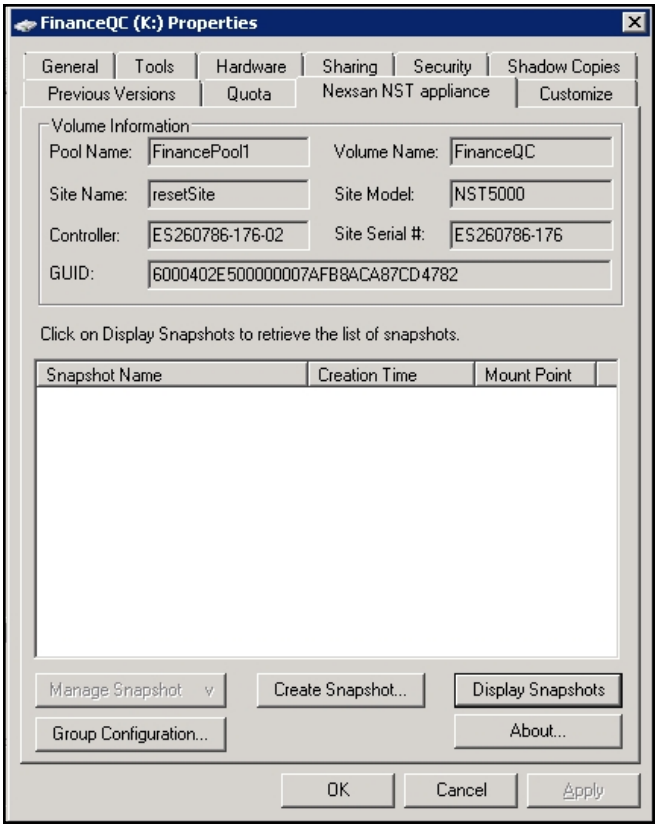


7. Repeat steps 2 to 5 for each discovered target disk.

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 6-27: Disk Properties—Nexsan Unity tab



Creating a VSS snapshot

Unity's VSS Hardware Provider enables you to take snapshots of one or more LUNs. As opposed to Unity, the VSS Hardware Provider enables you to create groups of multiple LUNs and to take snapshots of these groups.

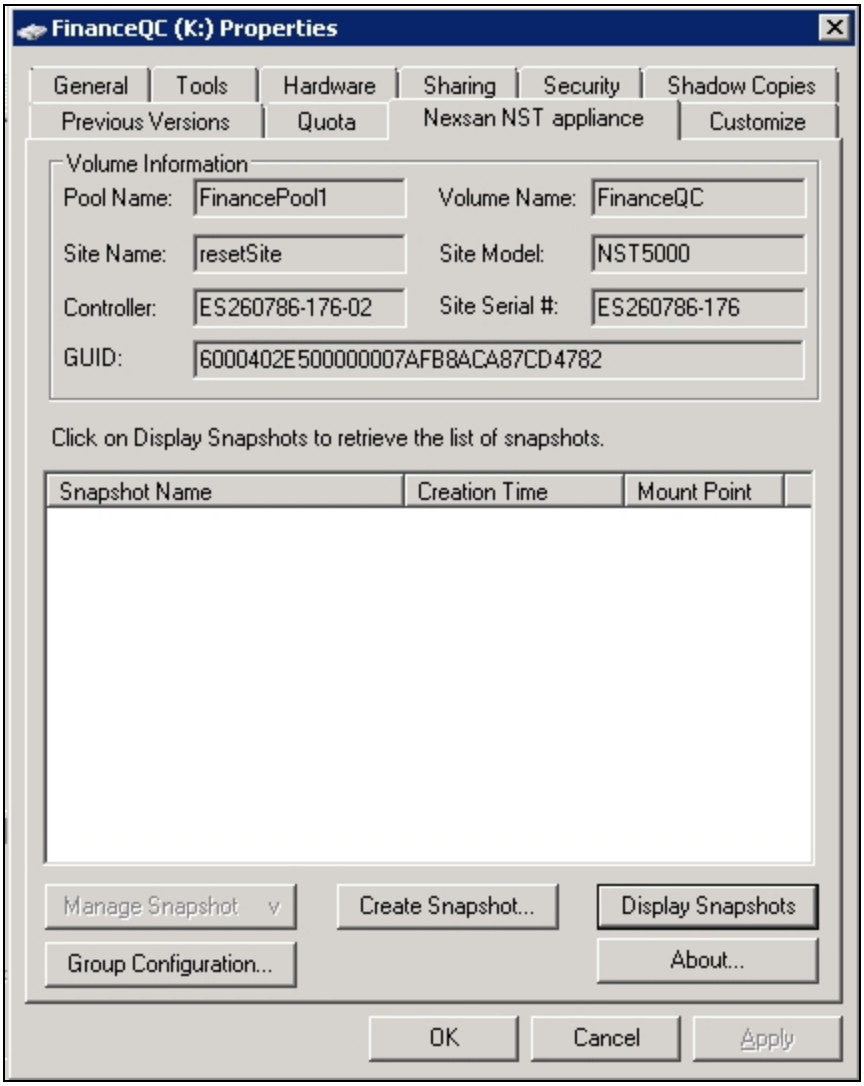
For applications running on multiple LUNs, such as an SQL Server database, you can create a snapshot of all the LUNs that are being used for the database. This enables you to restore the data residing on multiple LUNs at the same time, and not lose data integrity, such as database links.

▶ **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**.

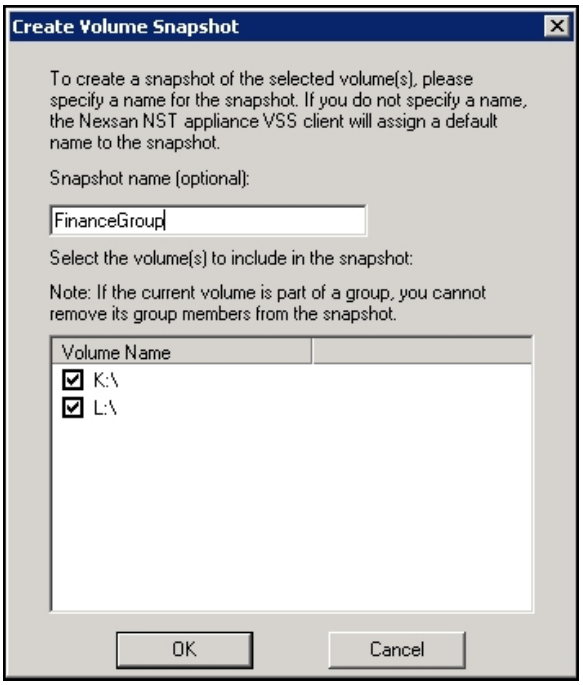
Figure 6-28: Creating VSS snapshots on the Windows host



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.

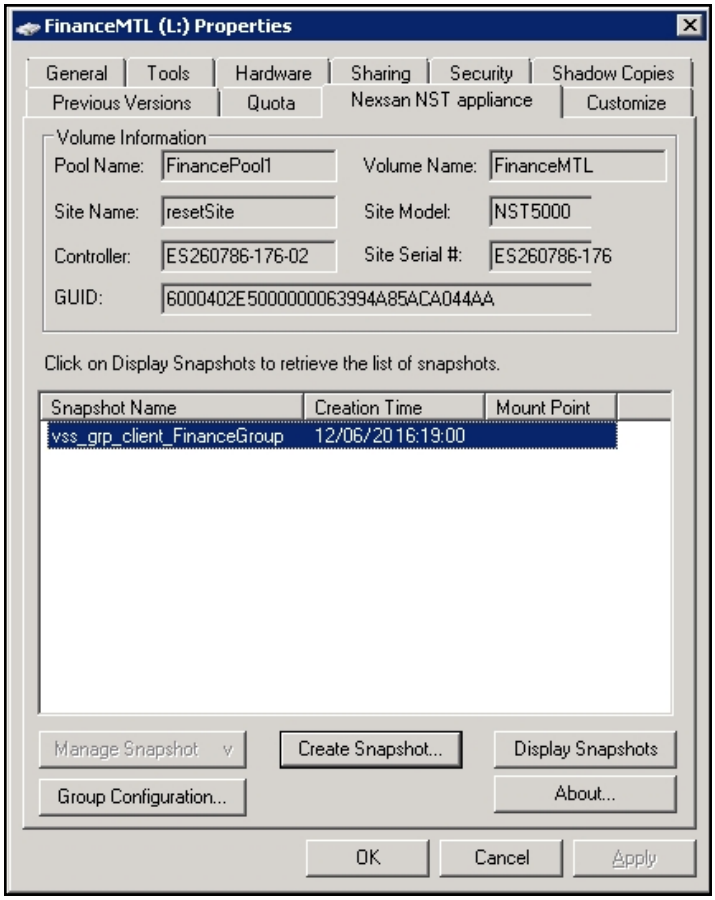
Figure 6-29: Creating a VSS group snapshot



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 6-30: Viewing a VSS snapshot on the Properties page



You can also view the VSS snapshot from 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.

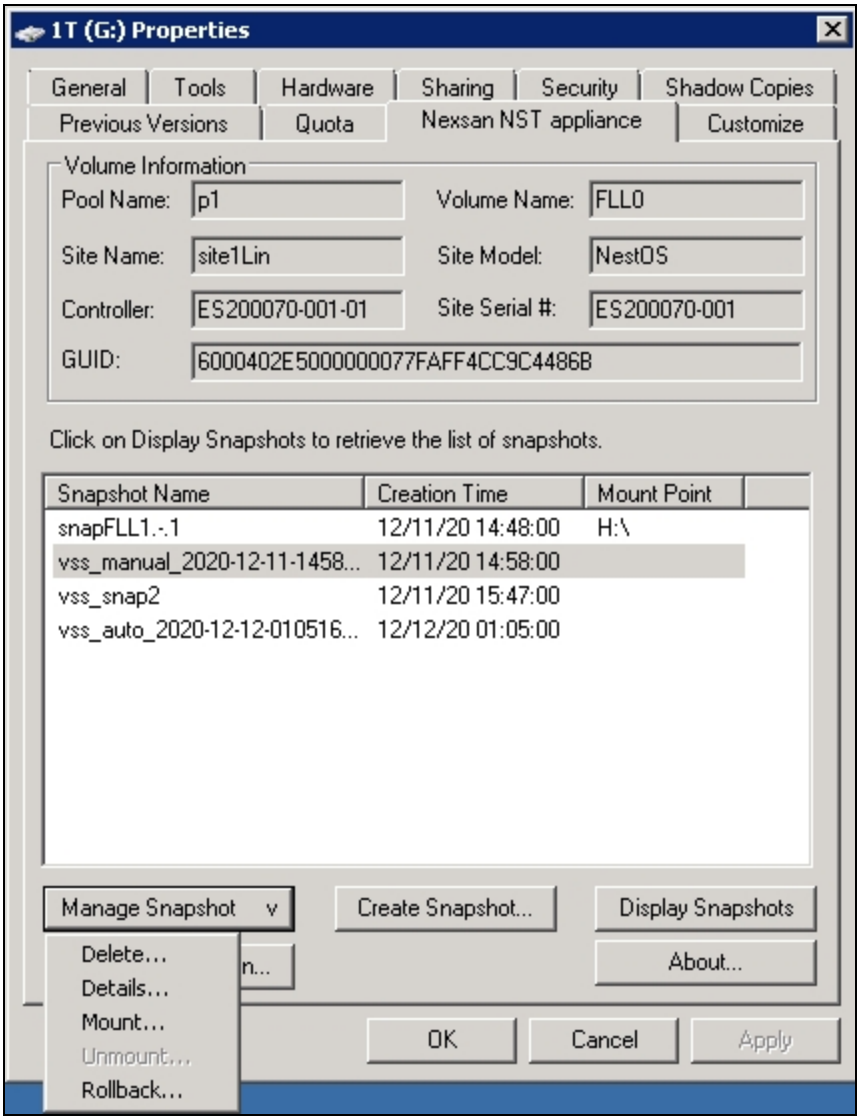
Note When browsing or mounting a LUN snapshot using the VSS Hardware Provider on Windows hosts, the disk is read-only. This applies to both iSCSI and Fibre Channel LUNs.

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.

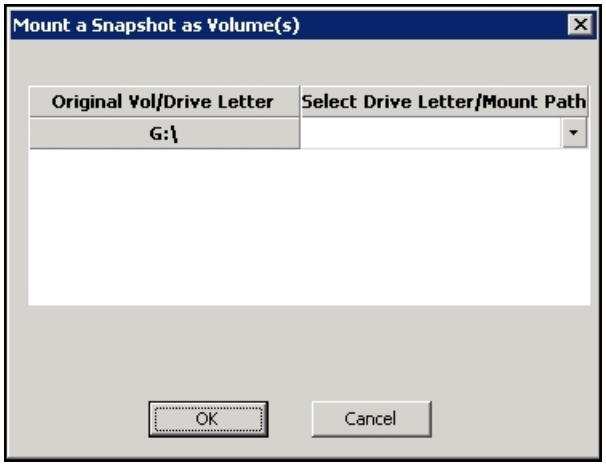
6. From the **Manage Snapshot** drop-down list, select **Mount**.

Figure 6-31: Browsing a VSS snapshot



7. A new window opens where you assign drive letter/mount path from the drop-down list. Click **OK**.

Figure 6-32: Assigning a drive letter to the VSS snapshot



8. Yo 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 269

Rolling back data to a VSS snapshot on the next page

Deleting a VSS snapshot on page 278

Viewing VSS client information

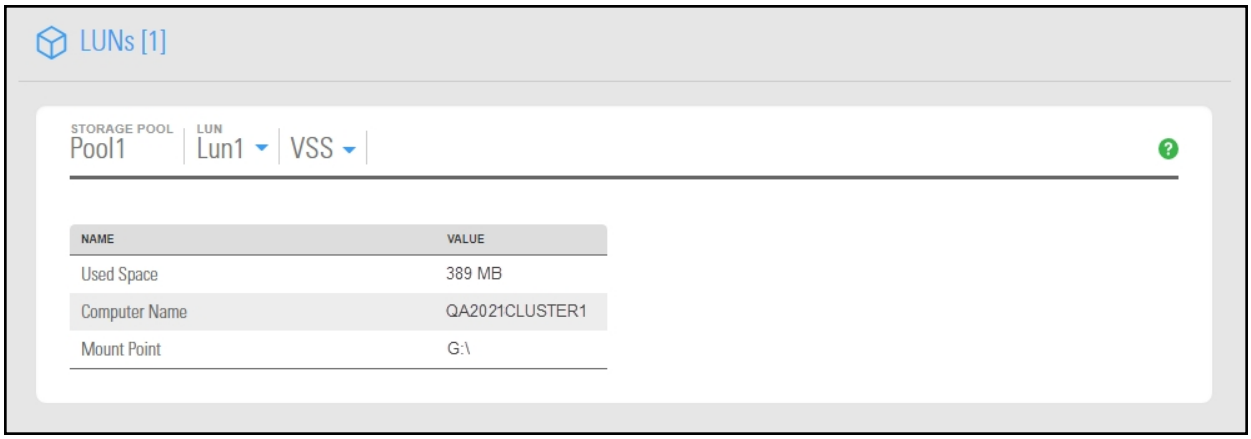
This section describes how to view the space currently used by LUN snapshots managed by the VSS Hardware Provider.

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. On the **Unity navigation bar**, select **Storage > LUNs**.
2. Click the link to the LUN you want to view VSS Information for.
3. Select **Summary > VSS**.

Figure 6-33: LUNs VSS panel



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 enables 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:

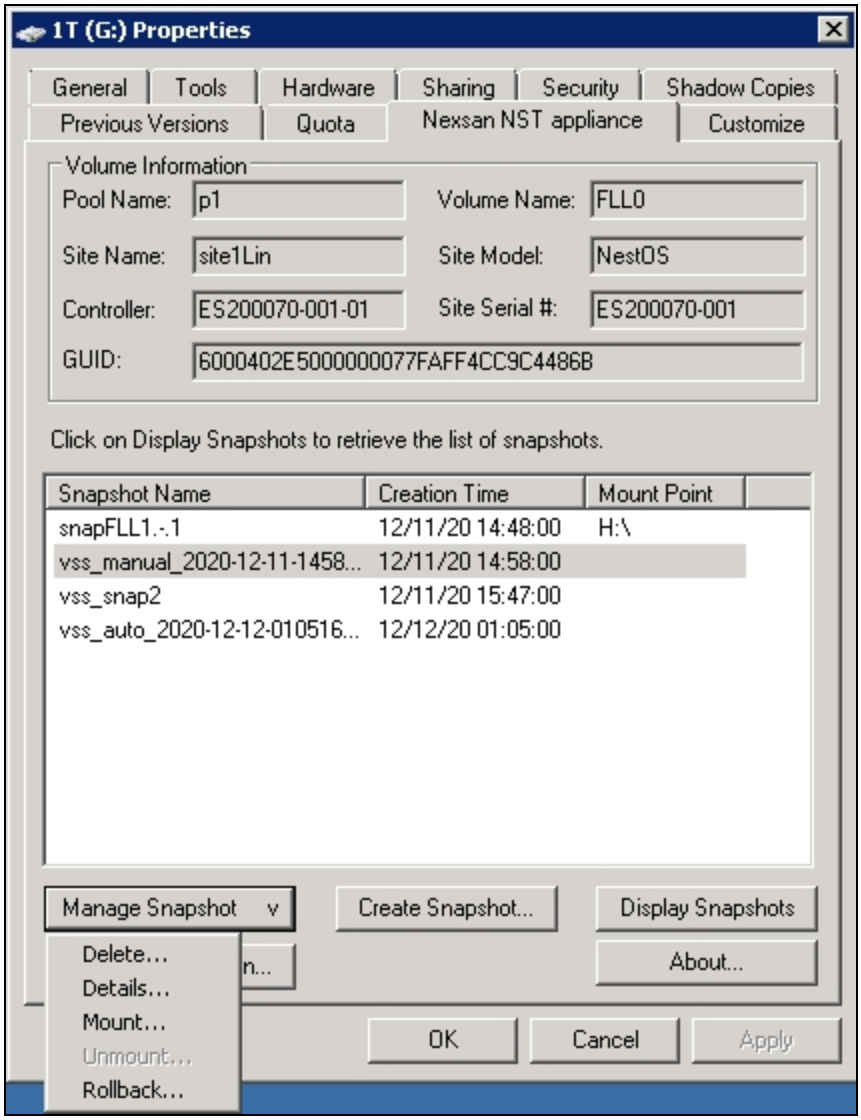
- The Management (mgmt) target must be connected for the **Manage Snapshot** button to be available and thus perform the rollback.
- The VSS feature must be enabled for the storage pool in Unity.

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**.

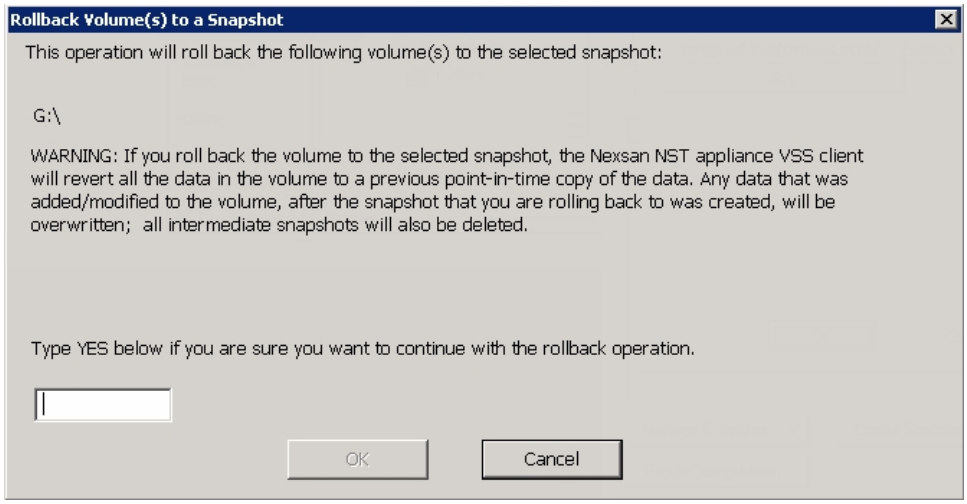
5. Select the snapshot that you wish to use for data restore.
6. From the **Manage Snapshot** drop-down list, select **Rollback**.

Figure 6-34: Rolling back data to a VSS snapshot



7. You will be prompted to confirm the restore operation. Type **Yes** in the field and click **OK**.

Figure 6-35: Confirming the VSS snapshot rollback



8. Restart these services:
   - Volume Shadow Copy
   - NSTVSSProvider
   - NSTVSSRequestor
9. 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:

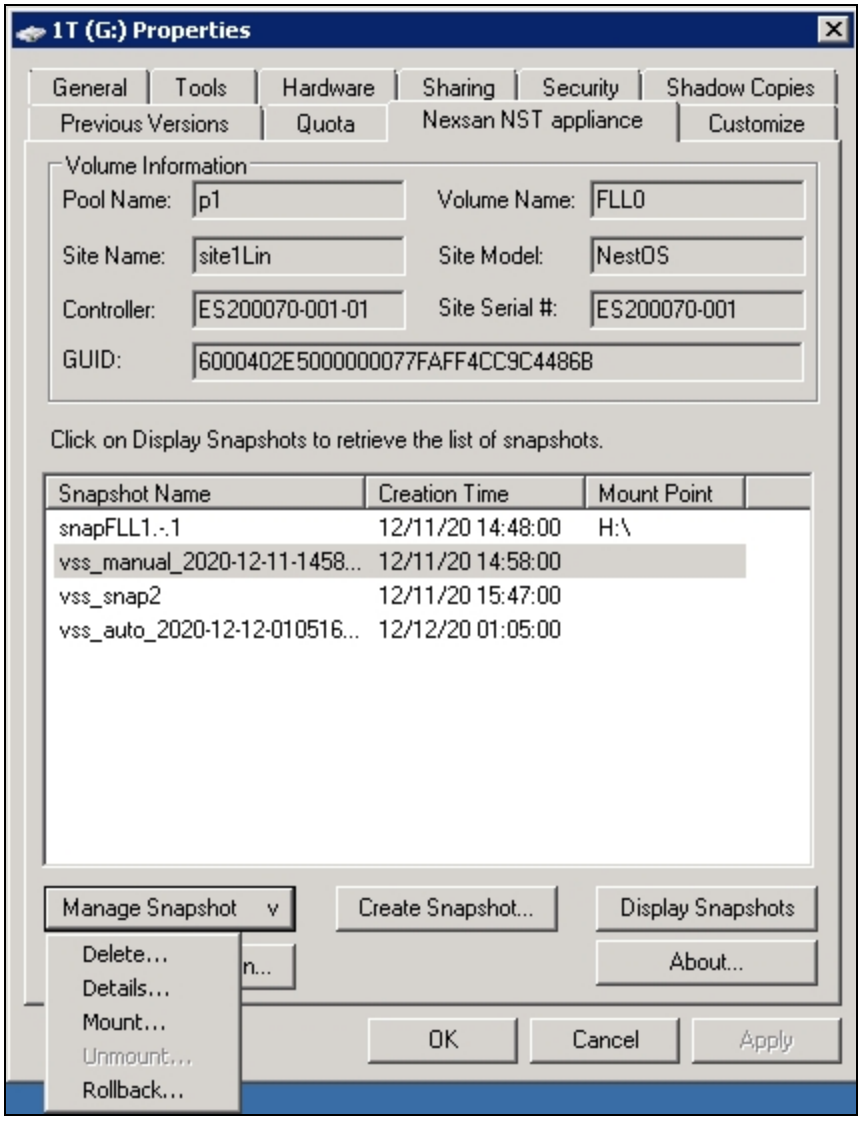
- The Management (mgmt) target must be connected for the **Manage Snapshot** button to be available and thus perform a deletion.
- The snapshot must be unmounted before it can be deleted; for steps to unmount a snapshot, see Browsing a VSS snapshot on page 273.
- The VSS feature must be enabled for the storage pool in Unity.
- You can also delete a LUN snapshot created by the VSS Hardware Provider from Unity.

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.

6. From the **Manage Snapshot** drop-down list, select **Delete**.

Figure 6-36: Deleting a VSS snapshot



7. 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 262

Enabling ZFS Encryption for LUNs

Use the topics in this section to enable ZFS encryption on a LUN, as well as to export, import, or change encryption keys for a LUN.

Enabling the encryption feature allows for the creation of encrypted file systems and volumes. This will encrypt file and volume data as well as the metadata.

This section includes these steps:

Enable ZFS encryption on a LUN 280
Export encryption key for a LUN 281
Import encryption key for a LUN 282
Change encryption key for a LUN 283

Enable ZFS encryption on a LUN

Use this topic to enable ZFS encryption on a LUN.

Prerequisites

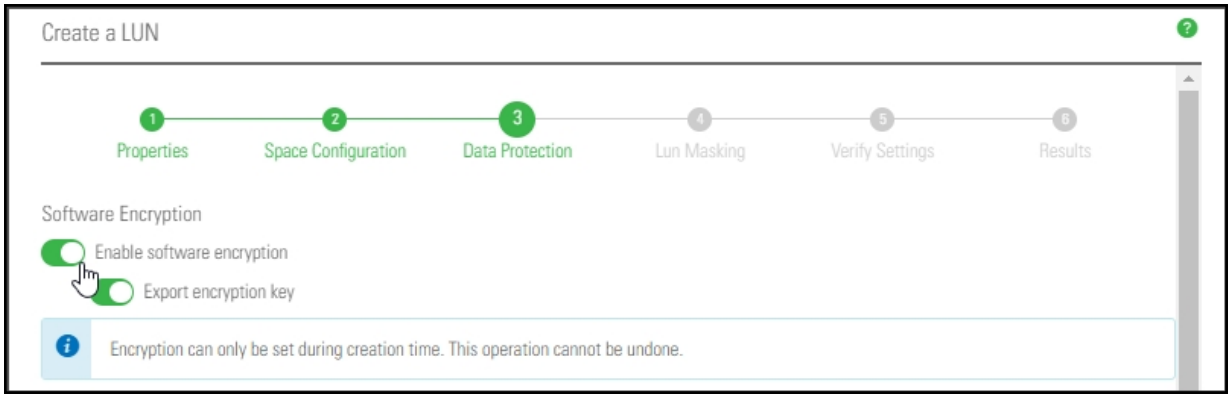
To complete this procedure, you'll need to have completed the first two of six steps using the Unity Create a LUN wizard.

To enable ZFS encryption:

1. On the **Unity navigation bar**, select **Storage > LUNS**.
2. On the upper right of the page, click the **Add LUN** button. The Create a LUN wizard pop-up appears.
3. Complete Steps 1 to 2 (Properties, Space Configuration).
4. At **Step 3**, Data Protection, click the **Enable software encryption** as well as the **Export encryption key** slider buttons in the top section of the window. Complete the remaining settings in this step and then click the **Next** button at the bottom right.

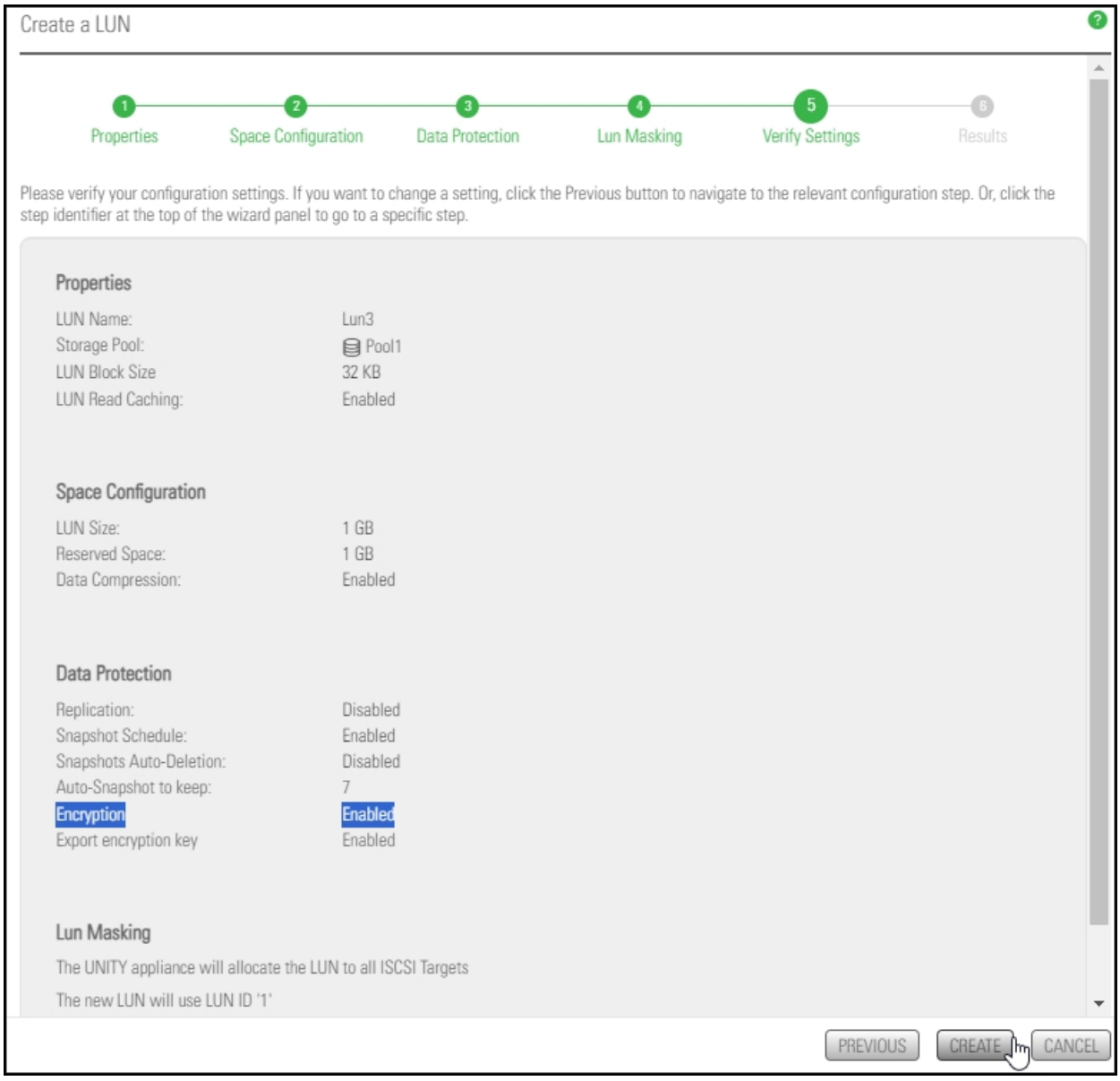
   CAUTION: Encryption can only be set during creation time. This operation cannot be undone.

Figure 6-37: Enable software encryption settings



5. In **Step 5**, Verify Settings, in the Data Protection section, ensure that Encryption indicates Enabled. After all settings have been verified, click the **Create** button on the bottom right.

Figure 6-38: Verify configuration settings for Encryption Enabled



6. **Step 6**, Results, indicates the successful creation of a LUN including encryption.

Export encryption key for a LUN

Use this topic to export an encryption key for a LUN.

Prerequisites

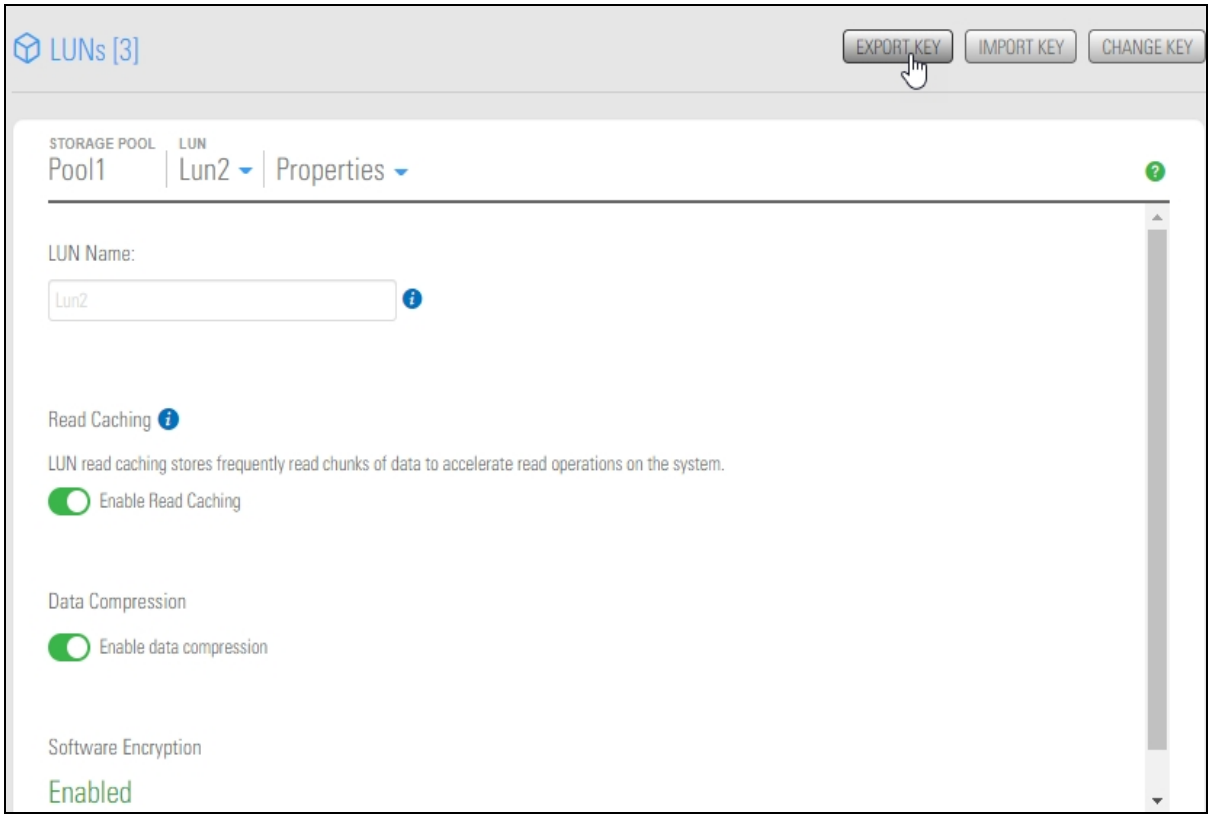
To complete this procedure, you'll need an existing LUN.

► **To export an encryption key:**

1. On the **Unity navigation bar**, select **Storage > LUN**.
2. Click the link to the LUN you would like to export the encryption key for. The **LUNs Summary** page appears.

3. Select **Summary > Properties**.The **LUN Properties** panel appears.

Figure 6-39: selected LUN Properties panel



4. Click the **Export Key** button on the upper right. A pop-up window appears indicating that the key export was successful.

Figure 6-40: Export Encryption Key for LUN - success confirmation dialog



Import encryption key for a LUN

Use this topic to import an encryption key for a LUN.

Prerequisites

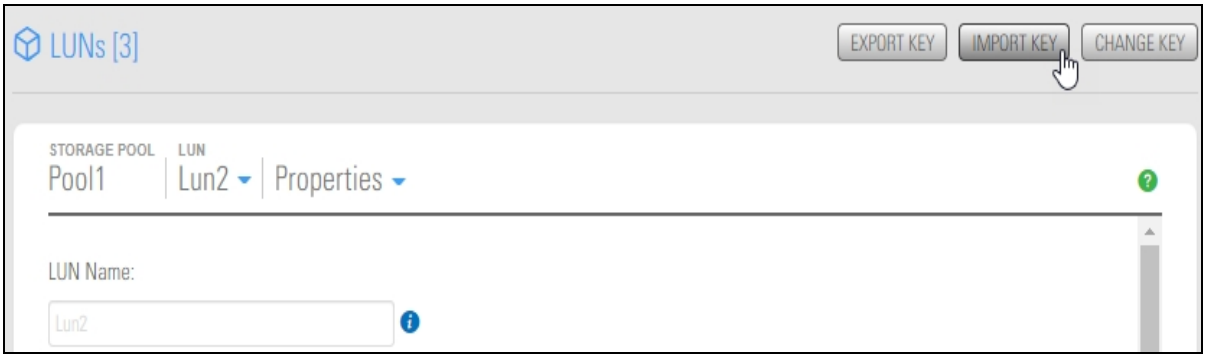
To complete this procedure, you'll need an existing LUN.

► **To import an encryption key:**

1. On the **Unity navigation bar**, select **Storage > LUNS**.
2. Click the link to the LUN you would like to import a key for. The **LUNs Summary** page appears.

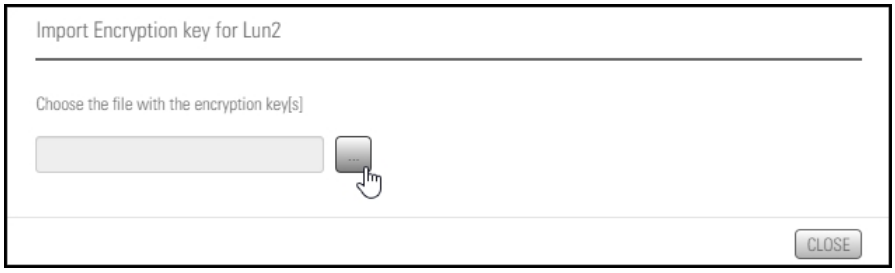
3. Select **Summary > Properties**.The **LUN Properties** panel appears.

Figure 6-41: selected LUN Properties panel



4. Click the **Import Key** button on the upper right. An Import Encryption Key pop-up window appears for the selected LUN. Select the key file using the blank field, or the browse button just beside it.

Figure 6-42: Import Encryption Key pop-up window - select file



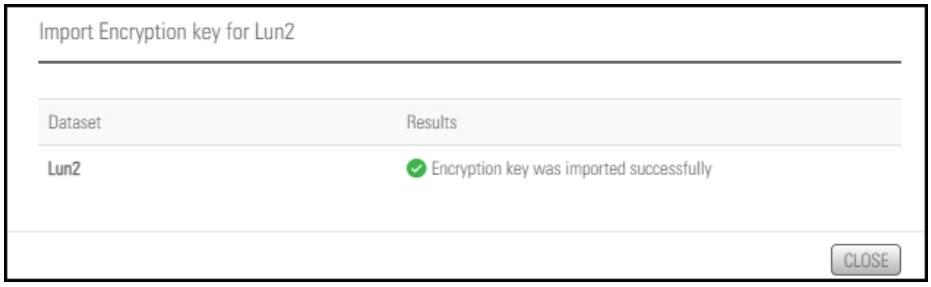
5. An Import Encryption Key pop-up window appears, confirming the date and time which the encryption key file was exported. Click the **Import** button on the bottom right.

Figure 6-43: Import Encryption Key pop-up window - import file



6. An Import Encryption Key pop-up window appears, indicating that the import was successful.

Figure 6-44: Import Encryption Key pop-up window - import successful



Change encryption key for a LUN

Use this topic to change an encryption key for a LUN.

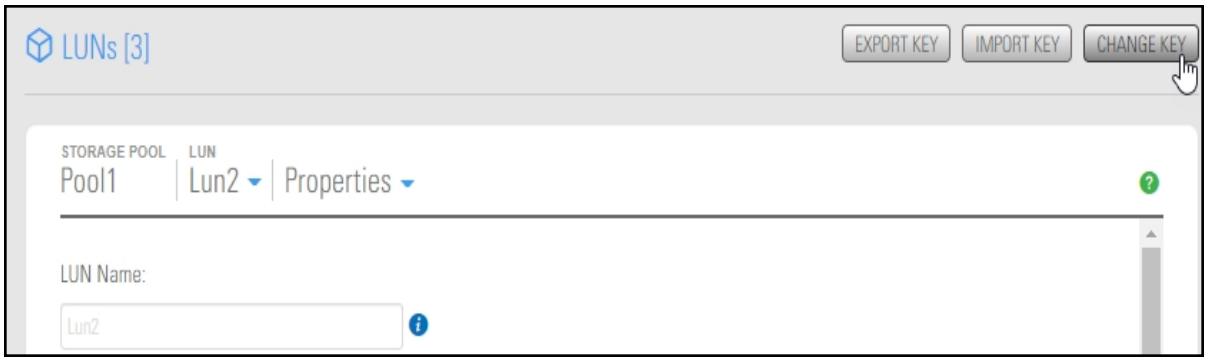
Prerequisites

To complete this procedure, you'll need an existing LUN.

To change an encryption key:

1. On the **Unity navigation bar**, select **Storage > LUNS**.
2. Click the link to the LUN you would like to change a key for. The **LUNs Summary** page appears.
3. Select **Summary > Properties**.The **LUN Properties** panel appears.

Figure 6-45: selected LUN Properties panel



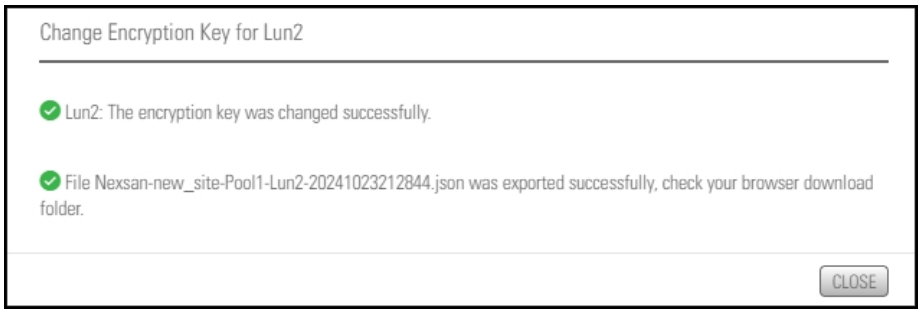
4. Click the **CHANGE KEY** button on the upper right. A Change Encryption Key pop-up window appears for the selected LUN. Ensure the **Export the new encryption key** check box is selected. Then click the **CHANGE** button on the lower right to complete the operation.

Figure 6-46: Change Encryption Key pop-up window



5. A Change Encryption Key pop-up window appears, indicating the change and the export was successful.

Figure 6-47: Change Encryption Key pop-up window - change and export successful



Managing snapshots for LUNs

Unity provides continuous data protection with the Snapshots feature, which enables you to capture, store, and access point-in-time copies of the data in your LUNs. Unity provides these methods of managing snapshots for LUNs:

- **Using the LUN Snapshots panel or Data Protection Snapshots panel:**

  You can enable browsing for a LUN 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 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 258.

  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 the Unity 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).

See also: Understanding LUN snapshots on page 289

This section includes these topics:

Introduction to snapshots

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 enables 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.

Snapshot concepts and terminology

This table describes snapshots concepts and terminology used in Unity.

Table 6-4: Snapshot concepts and terminology

Snapshot terminology	Description
Snapshot	A snapshot is a read-only copy of a file system/LUN at a specific point in time. 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. 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. The Unity Storage System protects the file's original data blocks from being overwritten; it stores the new updates in a new location. The Unity Storage System 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.
Automatic snapshot, or scheduled snapshots	Unity takes periodic snapshots according to the schedule you define. Typically, you set a snapshot schedule when you initially create the file system or LUN. You can then modify or disable the schedule in Unity. ▶ **Related topics:** ● Setting a schedule for automatic file system snapshots on page 208 ● Setting a schedule for automatic LUN snapshots on page 302
Manual snapshot	You can take manual snapshots of a file system or LUN at any time, even if you have automatic snapshots enabled. Manual snapshots allow you to record a copy of the dataset contents at any point in time. ▶ **Related topics:** ● Taking a manual file system snapshot on page 211 ● Taking a manual LUN snapshot on page 296
Immutable snapshot	You can make a snapshot immutable, meaning it cannot be modified or deleted once set to immutable status, until the selected expiry date. ▶ **Related topics:** ● Taking an immutable snapshot for a file system on page 221 ● Taking an immutable LUN snapshot on page 305

Snapshot terminology	Description
Browsing a snapshot, or mounting a snapshot	Unity provides a mechanism that enables 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 or LUN 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 or LUN 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. ▶ **Related topics:** • Browsing a file system snapshot on page 212 • Browsing a LUN snapshot on page 297 • Browsing a VSS snapshot on page 273 • Browsing replicated datasets and snapshots on page 290
Rollback	The Unity Storage System enables 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 or LUN 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. ▶ **Related topics:** • Rolling back to a snapshot on page 215 • Rolling back data in a LUN to a snapshot on page 300 • Rolling back data to a VSS snapshot on page 276

Snapshot terminology	Description
VSS, or Microsoft Volume Shadow Copy Service, Volume Snapshot Service, Volume Shadow Copy Service	Microsoft Volume Shadow Copy is a technology included in Microsoft Windows that enables you to take manual or automatic backup copies or snapshots of data. If the Unity Storage System is joined to a Microsoft Active Directory domain, Unity automatically exposes all the snapshots for each file system/LUN on the Unity Storage System 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. ▶ **Related topics:** ● Using Windows VSS on page 258

Understanding LUN snapshots

A snapshot is a read-only copy of a LUN at a specific point in time. Think of a snapshot as a frozen image of the data in a LUN at the time the snapshot is recorded.

Snapshots browsing

Unity provides a mechanism that enables 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.

Rollback function

Unity enables 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.

Microsoft Volume Shadow Copy Service

Microsoft Volume Shadow Copy (also referred to as Volume Snapshot Service or VSS), is a technology included in Microsoft Windows that enables you to take manual or automatic backup copies or snapshots of data.

If Unity is joined to a Microsoft Active Directory domain, Unity automatically exposes all the snapshots for each file system/LUN on 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.

Browsing replicated datasets and snapshots

Once you set up data replication for a storage pool on the primary Unity System, you can view and browse the storage pool's replicated datasets (file systems and LUNs) and snapshots on the remote Unity System, under the storage pool replica.

Using Unity and VSS to manage LUN snapshots

Unity provides two ways for managing snapshots for LUNs:

- Using Unity—see Viewing LUN snapshots on the facing page
- Using the VSS Hardware Provider—see Using Windows VSS on page 258

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 6-5: Managing LUN snapshots using both Nexsan Unity and the 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: 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 **LUN Snapshots** panel or **Data Protection Snapshots** panel.	You cannot filter snapshots on the Windows host.
Search for a snapshot	Use the **LUN Snapshots** panel or **Data Protection Snapshots** panel.	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 *Browsing Enabled*.

Action performed	... in Nexsan Unity	... using VSS Hardware Provider on the Windows host
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 *Explorer* and *Disk Management*.	In Unity, the snapshot disappears from the grid in the **Snapshots** tab.

Viewing LUN snapshots

The **Snapshots** 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.

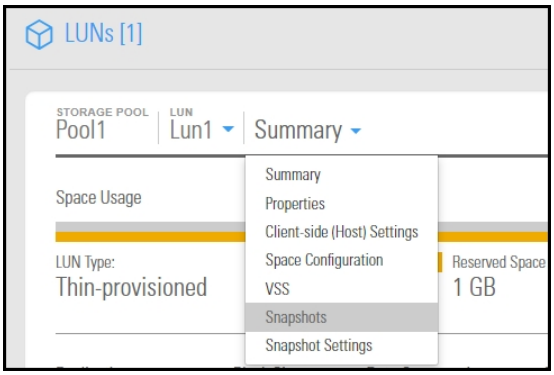
In the **LUN Snapshots** panel you can:

- Take a snapshot
- Delete all snapshots
- Manage the snapshot browsing method
- Make the snapshot immutable
- Delete snapshots
- Roll back a snapshot

To access LUN Snapshots from the LUNs panel:

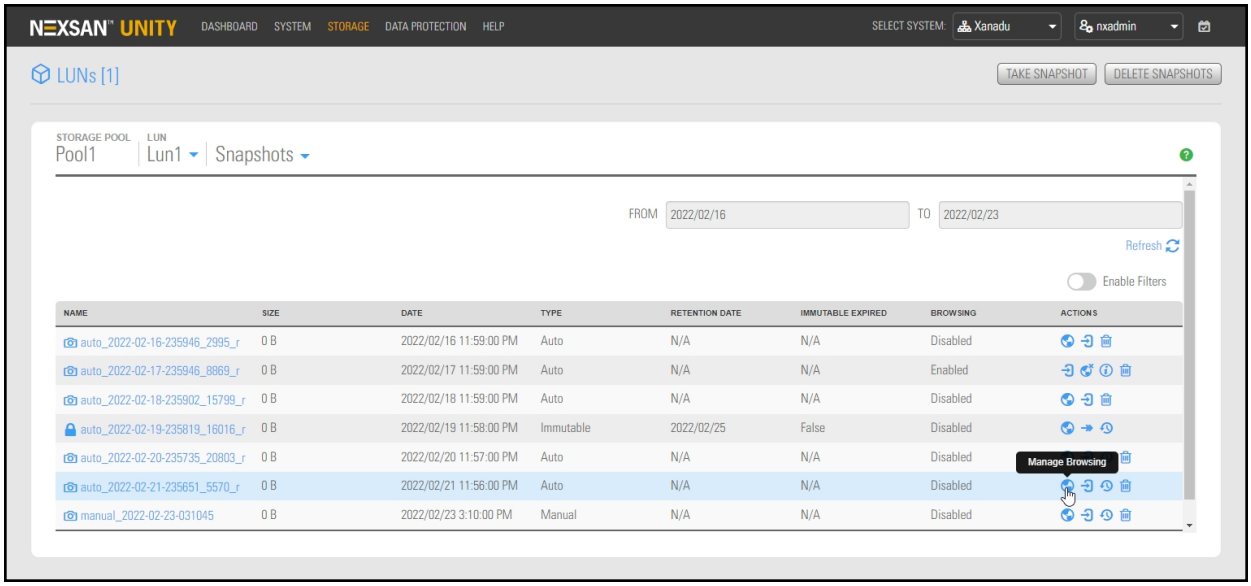
1. On the **Unity navigation bar**, select **Storage > LUNs**.
2. Click the link to the LUN that you want to access.
3. Select **Summary > Snapshots**.

Figure 6-48: LUNs Summary panel menu



The **LUN Snapshots** panel opens.

Figure 6-49: LUN Snapshots panel - Manage Browsing



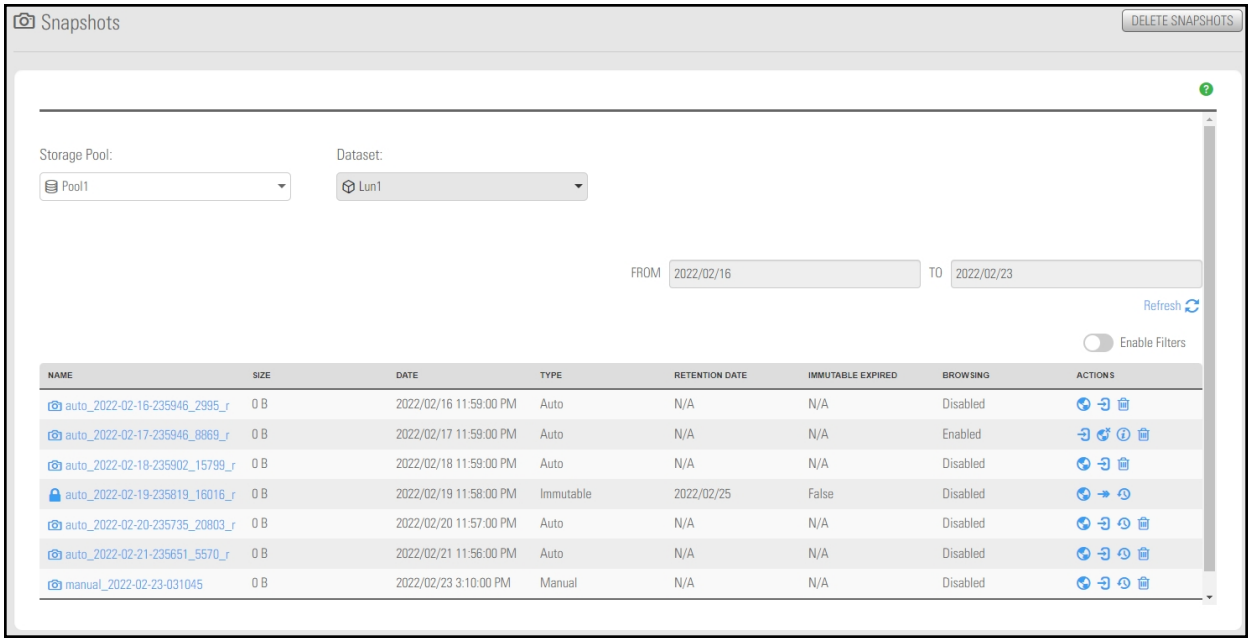
6

To manage LUN snapshots from the Snapshots panel:

1. On the **Unity navigation bar**, select **Data Protection > Snapshots**.
2. Select a **Storage Pool** and then select **Dataset > LUN**.
3. Click **Manage Browsing** to enable viewing of LUN Snapshots.

   You can also click **Change to Immutable**, **Roll back**, or **Delete** snapshots.

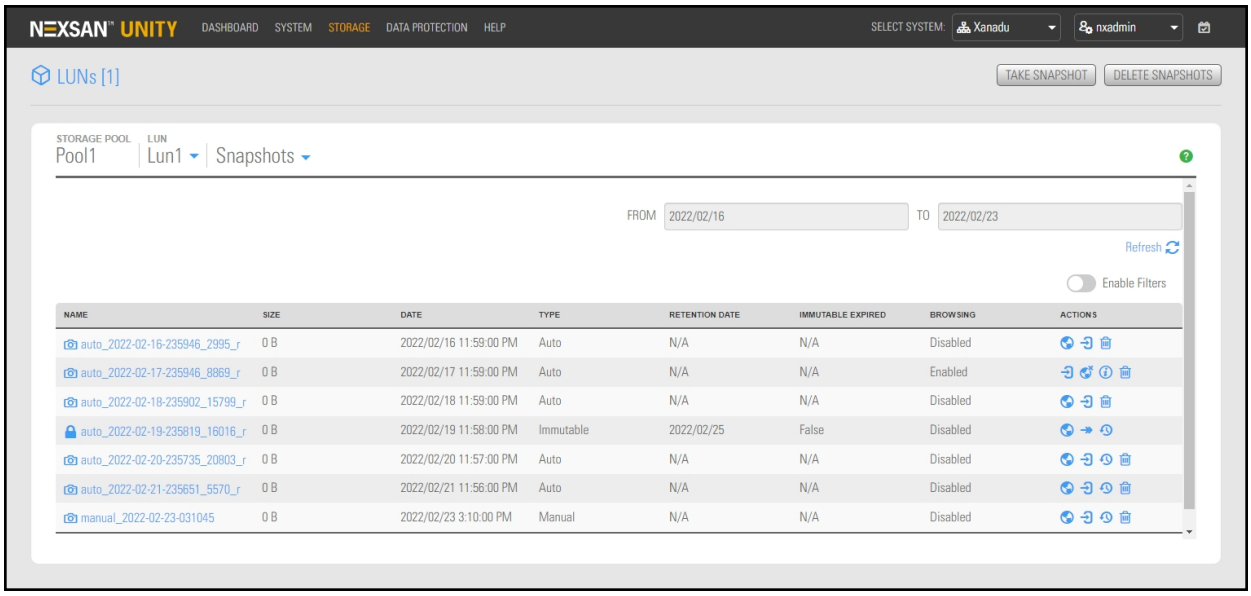
Figure 6-50: Snapshots panel with LUNs selected



LUNs Snapshots panel

The **LUNs Snapshots** panel displays a grid that lists all the snapshots recorded for the corresponding LUN.

Figure 6-51: LUNs Snapshots panel



The grid shows this information for each snapshot:

- 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 February 16, 2022 at 11:59 PM: `auto_2022-02-16-115900`.
  - 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 February 23, 2022 at 3:10 PM and you use the default snapshots naming convention, Unity assigns this name to the snapshot: `manual_2022-02-23-151001`.

    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 258.
- 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.
- Date: this column displays the date and 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.
- Type: this column indicates whether the snapshot is an **Auto** (scheduled), **Manual**, or **Immutable** snapshot.
- Retention Date: this column displays the date until an immutable snapshot is retained.

- Immutable Expired: this column indicates whether the immutable snapshot retention date is expired.
- Browsing: this column indicates whether or not browsing is enabled for the snapshot.

Sorting the list of snapshots

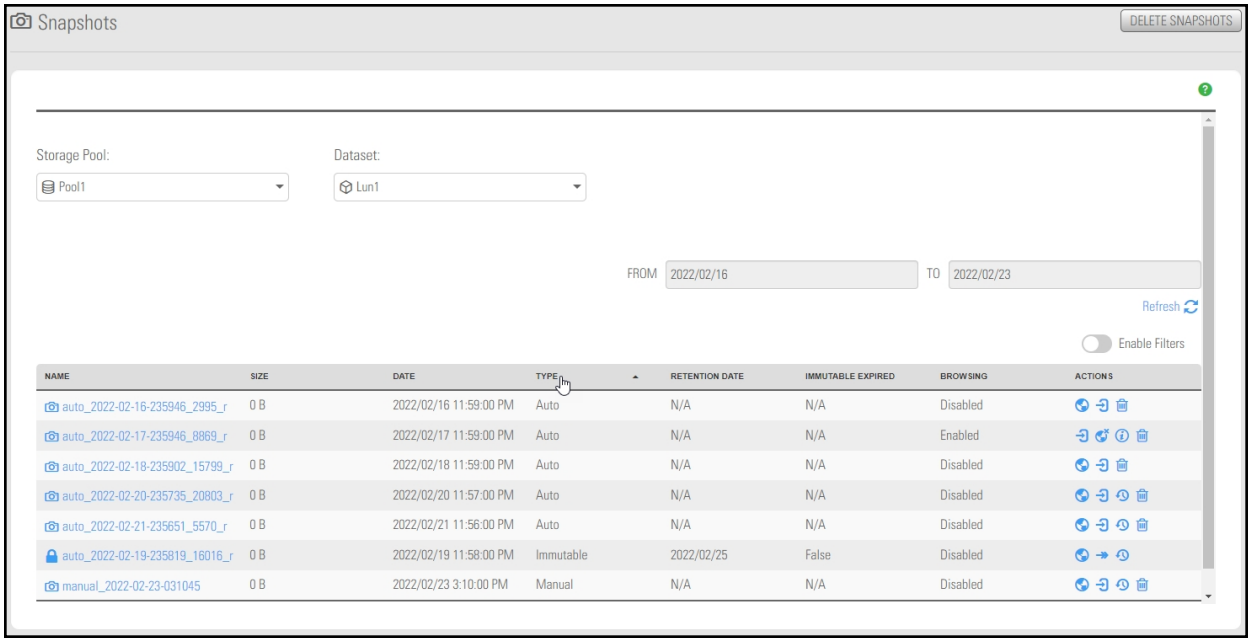
You can sort the list of snapshots displayed in the grid in either ascending or descending (alphabetical) order by clicking any of the column headings.

See also LUNs Snapshots panel on the previous page

To sort the list of snapshots:

1. On the **Unity navigation bar**, select **Data Protection > Snapshots**.
2. In the **Snapshots** list, click a column header to sort by that data type. For example, this list of snapshots is sorted by column 4, **Type**.

Figure 6-52: Snapshot sorting



Searching for a specific snapshot in the grid

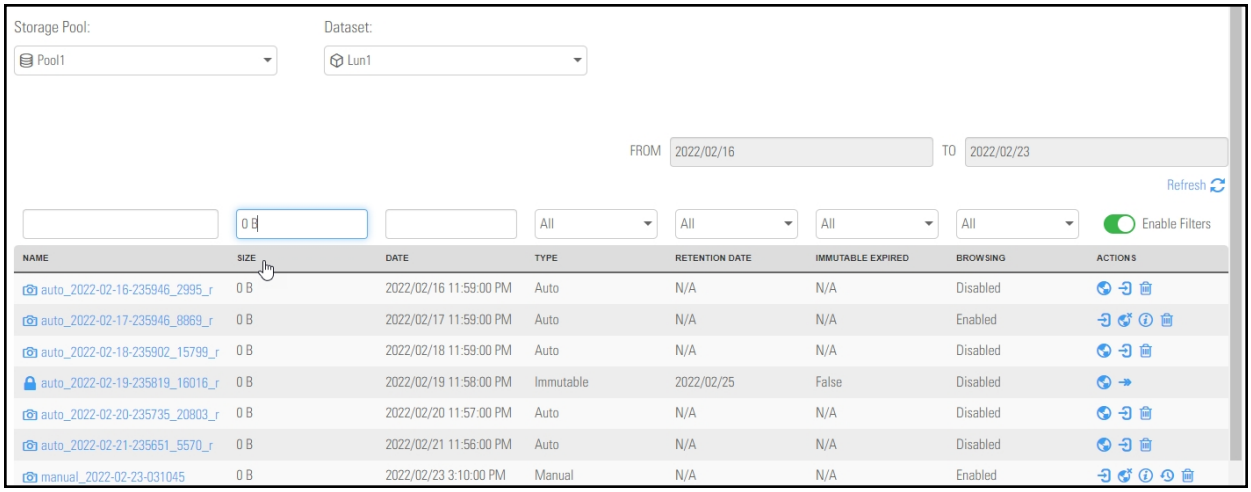
You can search for a specific snapshot in the LUN snapshots grid by **Name**, **Size**, or **Date**, by entering a search string in the text boxes above the corresponding column headings.

To search for a specific snapshot in the grid:

1. On the **Unity navigation bar**, select **Storage > LUNs**.
2. Click the link to the LUN that you want to search about.
3. Click **Summary > Snapshots**.
4. Click the **Enable Filters** button.
5. Enter a search string in the text boxes above the **Name**, **Size**, or **Date** 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 6-53: LUNs Snapshots panel - searching



Filtering snapshots in the grid

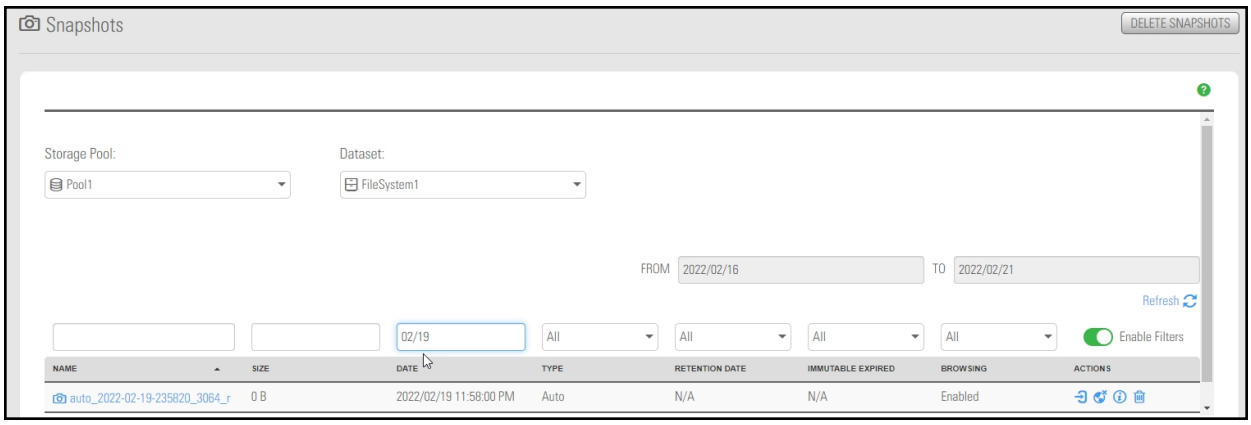
You can filter the snapshots displayed in the grid by **Date**, **Type**, **Retention Date**, **Immutable Expired**, and **Browsing** status. You can also filter the snapshots to only display snapshots recorded within a specific time period.

6

► To enable filtering:

1. On the **Unity navigation bar**, select **Data Protection > Snapshots**.
2. Click the **Enable Filters** button 

Figure 6-54: Snapshot filtering



► To display only snapshots recorded within a specific time period:

1. Select the **From** date field above the snapshots grid, and select a starting date for the time period that you want to display snapshots from.
2. Select the **To** date field, and select an end date for the time period.

Unity filters the grid to display only snapshots recorded within the specified time period.

To display only snapshots with a specific Browsing status:

1. Open the drop-down list above the **Browsing** 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**.

Unity filters the grid to display only snapshots that have either browsing enabled or disabled, depending on your selection.

To display only snapshots of a specific type:

1. Open the drop-down list above the **Type** column heading in the grid.
2. Select the type (**Auto**, **Immutable**, or **Manual**) that you want to display snapshots for in the grid. The default filter setting is **All**.

Unity filters the grid to display only **Auto**, **Immutable**, or **Manual** snapshots, depending on your selection.

To filter snapshots further:

You can further filter snapshots in the grid by combining filter settings. For example, to display snapshots that have **Browsing Enabled**, of type **Automatic**, and which were recorded between February 16, 2022 and February 22, 2022, set these filter settings in the grid:

1. Click the **From** date field above the snapshots grid, and select February 16 in the calendar.
2. Click the **To** date field, and select February 22 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** 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 **Auto**. Unity filters the grid again to only display scheduled (automatic) snapshots.

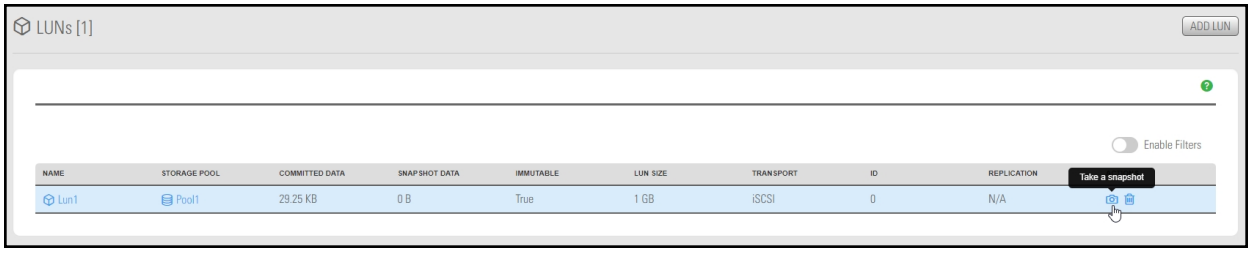
Taking a manual LUN snapshot

You can take manual snapshots of a LUN at any time, even if you have scheduled snapshots enabled. This mechanism enables you to record a copy of the contents of a LUN at any point in time.

To take a manual snapshot:

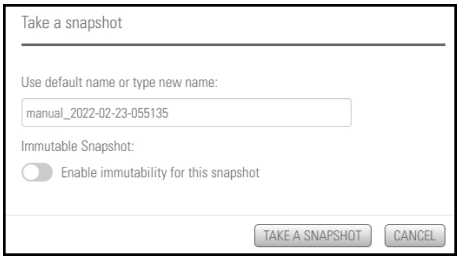
1. On the **Unity navigation bar**, select **Storage > LUNs**.
2. Under **Actions**, click the **Take a Snapshot** button in the row associated with the LUN you need the snapshot for.

Figure 6-55: LUN panel - Take a Snapshot button



3. The **Take a Snapshot** popup window opens.

Figure 6-56: Take a snapshot popup



Do one of the following:

To...	Do this
specify a name for the manual snapshot	a. Clear the **Automatically assign a name** option (selected by default). b. 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. c. Click the **Take a Snapshot** button to set the name and close the window. Unity immediately takes a snapshot and adds it to the snapshots grid.
allow Unity to automatically assign a name to the manual snapshot	a. Use the default name. b. Click the **Take Snapshot** button to close the window. 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 `manual_` and includes the date and time the manual snapshot is recorded; for example: if you take a manual snapshot on March 1, 2022 at 7:35PM, Unity assigns this name to the snapshot: `manual_2022-03-01-193501`
make the snapshot immutable	a. Click the **Enable immutability for this snapshot** button. b. Click the **Take Snapshot** button to close the window.

Browsing a LUN snapshot

Setting browsing for a snapshot enables you to access the snapshot from a LUN and browse its contents in the same way that you access a LUN.

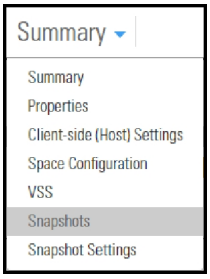
You can use Unity's snapshot browsing mechanism to recover individual files from a snapshot in case the files are accidentally deleted or overwritten, or corrupted in the snapshot's parent LUN. Unity maintains all of the parent LUN's access-level attributes with the snapshot to ensure any recovery is 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 snapshot for a LUN, Unity makes the snapshot available to host systems of the LUN as a read/write clone. The host system can then both read from and write data to the clone, however Unity will NOT preserve direct changes to the clone. 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.

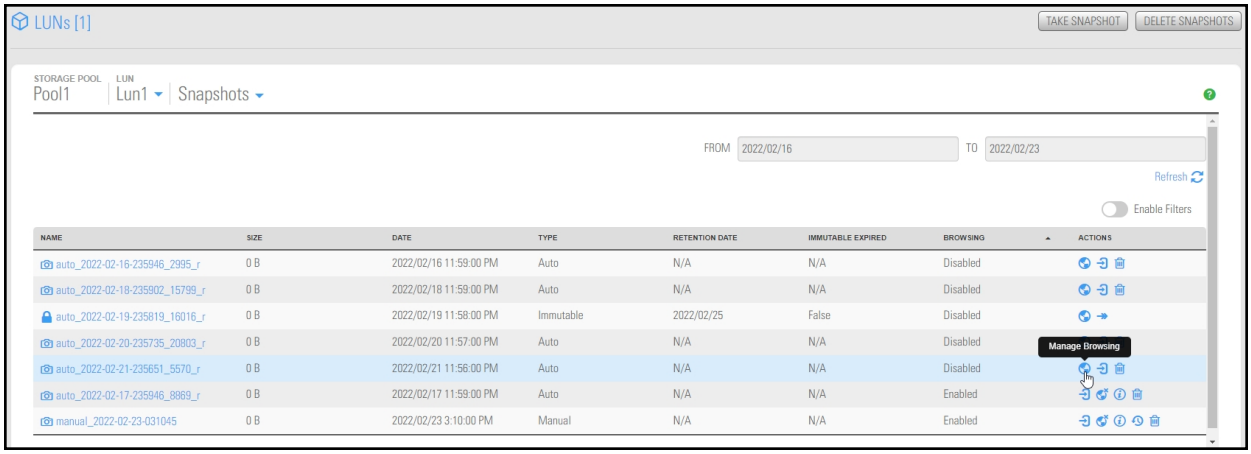
To set browsing for a snapshot:

1. On the **Unity navigation bar**, select **Storage > LUNs**.
2. Click the link to the LUN that you want to browse snapshots for.
3. Click **Summary > Snapshots**.



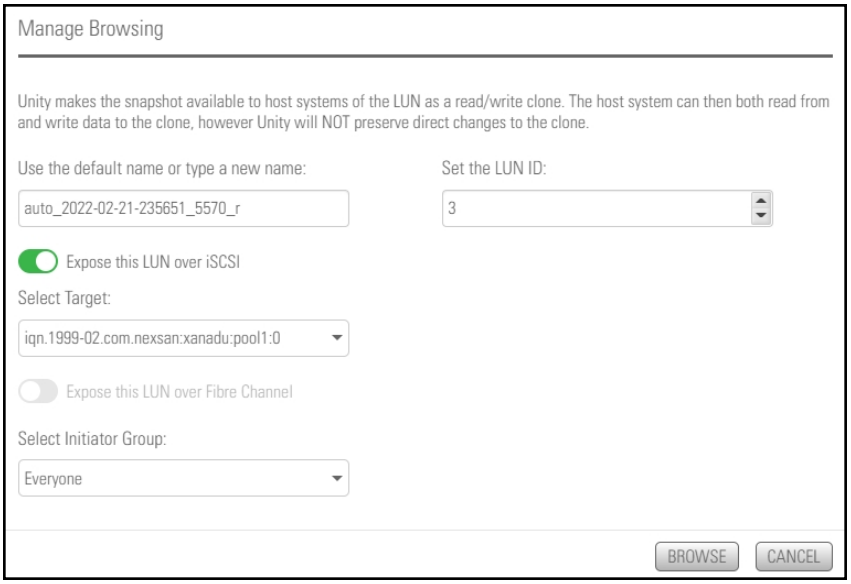
The **LUN Snapshots** panel opens.

Figure 6-57: LUN Snapshots panel - Manage Browsing



4. In the grid, click the **Manage Browsing** icon for the applicable snapshot. The Manage Browsing window opens.

Figure 6-58: LUN Snapshots - Manage Browsing window



5. Use the default or specify a new browsing name for the snapshot.
6. Review the other options displayed:
   a. Choose **Expose this LUN over iSCSI** or **Expose this LUN over Fibre Channel** as required.
   b. **Select Target**: Unity displays existing targets.
   c. **Select Initiator Group**: The default is **Everyone**, but you can choose others if defined.
   d. **Set LUN ID**: Choose another **LUN ID** if necessary.
   e. Click the **Browse** button to save your settings and close the **Browse Snapshot** window.

Unity enables browsing for the snapshot. The **Actions** column in the snapshots grid displays the following additional icons:

Icon	Description
	Browsing Properties icon: Browsing is enabled for the snapshot. Click the icon to stop browsing the snapshot.
	View Properties icon: Click to view the **Browsed Snapshot** properties.

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:

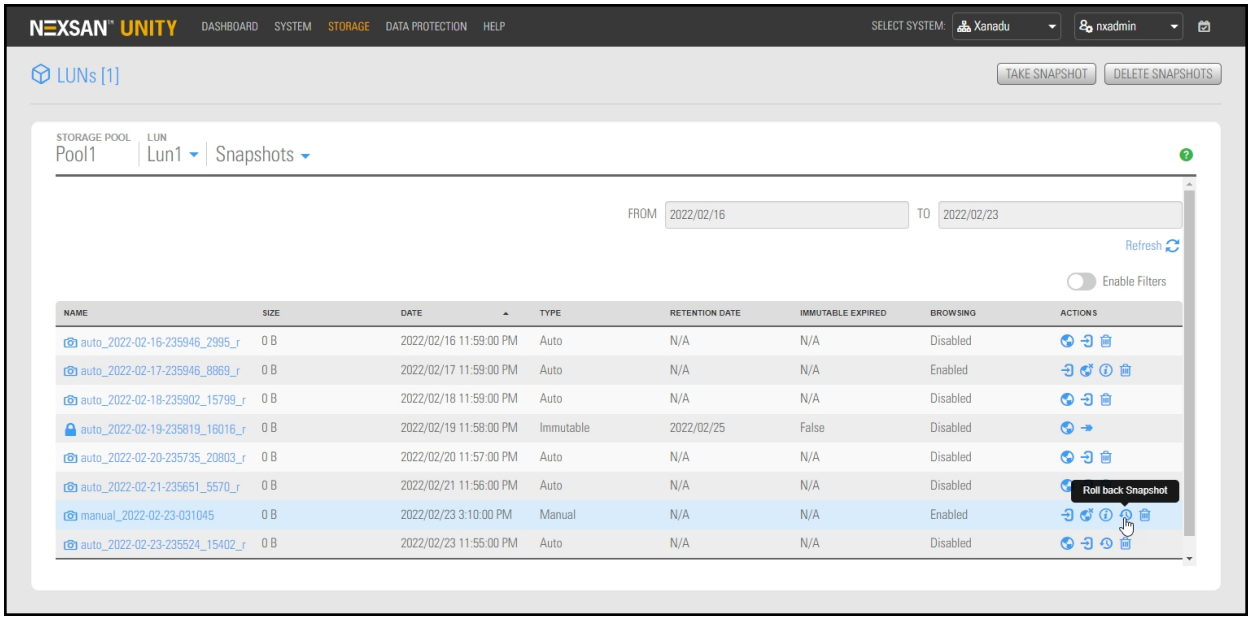
1. Power off all virtual machines hosted on the LUN.
2. Roll back the snapshot.
3. Rescan the datastores.
4. Power on the virtual machines hosted on the LUN.

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. On the **Unity navigation bar**, select **Storage > LUNs**.
2. Click the link to the LUN that you want to roll back a snapshot for.
3. Click **Summary > Snapshots**. The **LUN Snapshots** panel opens.

Figure 6-59: LUN Snapshots panel - Roll back snapshot



4. In the grid, click the **Roll back Snapshot** icon for the applicable snapshot. The **Roll back Snapshot** window opens.
5. When you are ready to proceed, type **Roll back** in the text box and click the **Roll back** button.

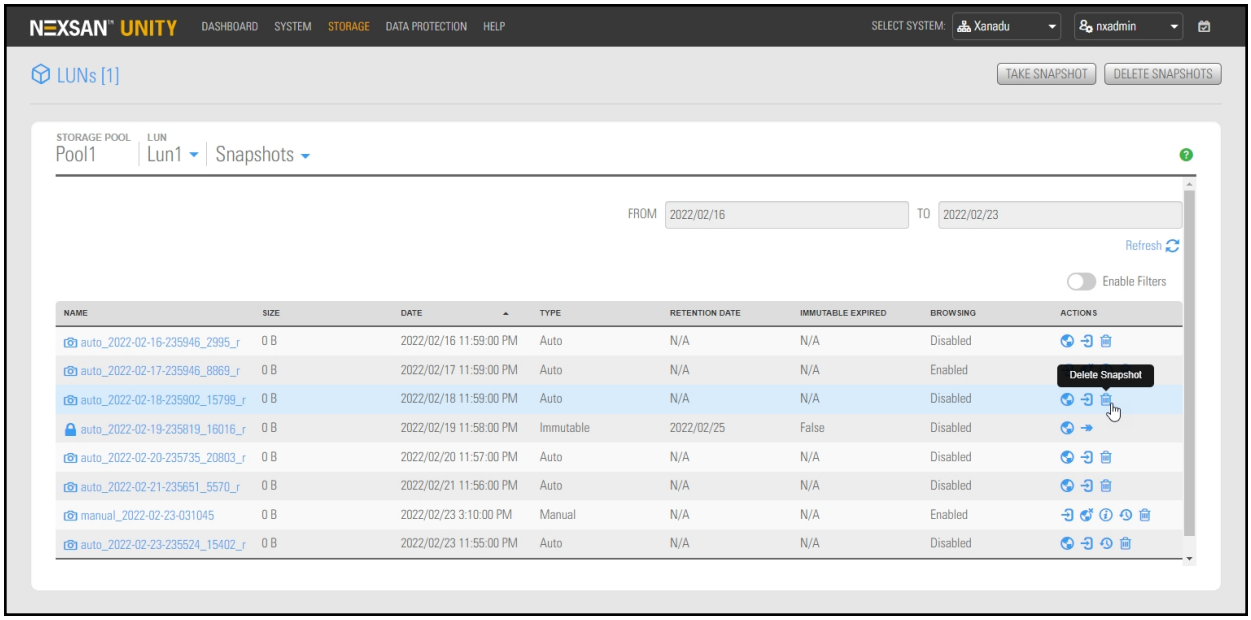
Deleting LUN snapshots manually

This section describes how to delete snapshots for a LUN. You can delete both manual snapshots and automatic snapshots. For instructions to delete snapshots automatically, see Setting a schedule for automatic LUN snapshots on the next page.

To manually delete snapshots for a LUN:

1. On the **Unity navigation bar**, select **Storage > LUNs**.
2. Click the **LUN** you want to delete snapshots for. The **LUN Summary** panel opens.
3. Click **Summary > Snapshots**. The **LUN Snapshots** panel opens.

Figure 6-60: LUN Snapshots panel - Delete Snapshot



4. In the grid, click the **Delete Snapshot** icon for the applicable snapshot.
5. In the **Delete Snapshot** popup window, type **Delete** to complete the operation.

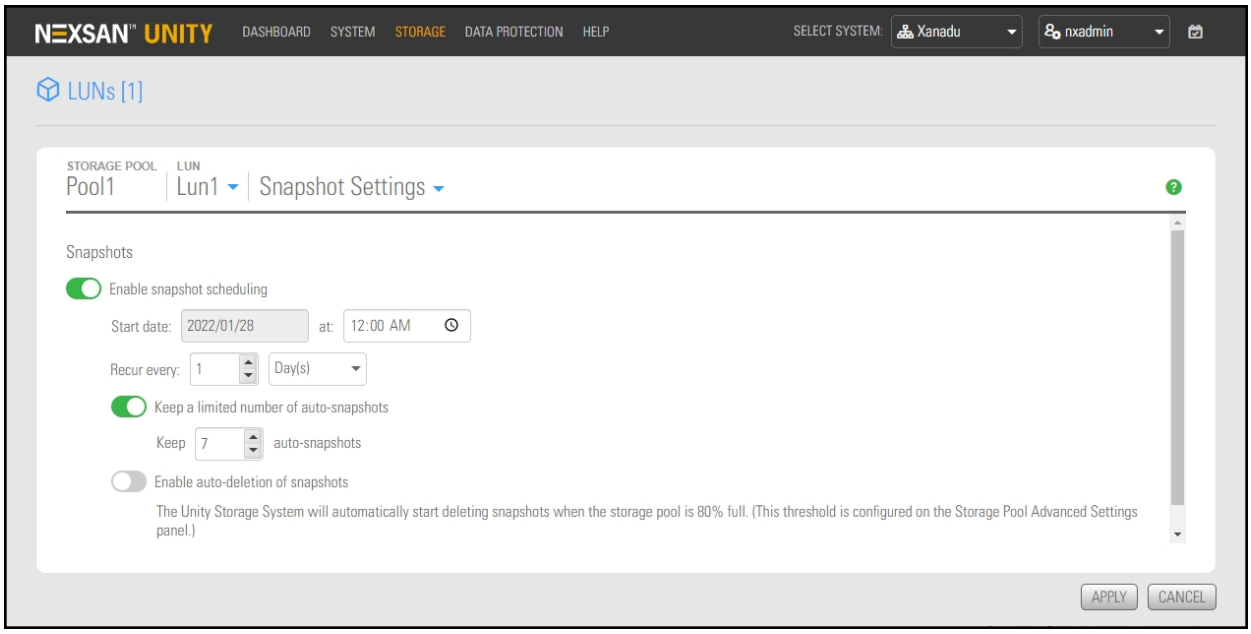
Managing LUN Snapshot scheduling

The **LUN Snapshot Settings** panel 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 below.

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.

Figure 6-61: LUN Snapshot Settings panel



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 page 296.

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.

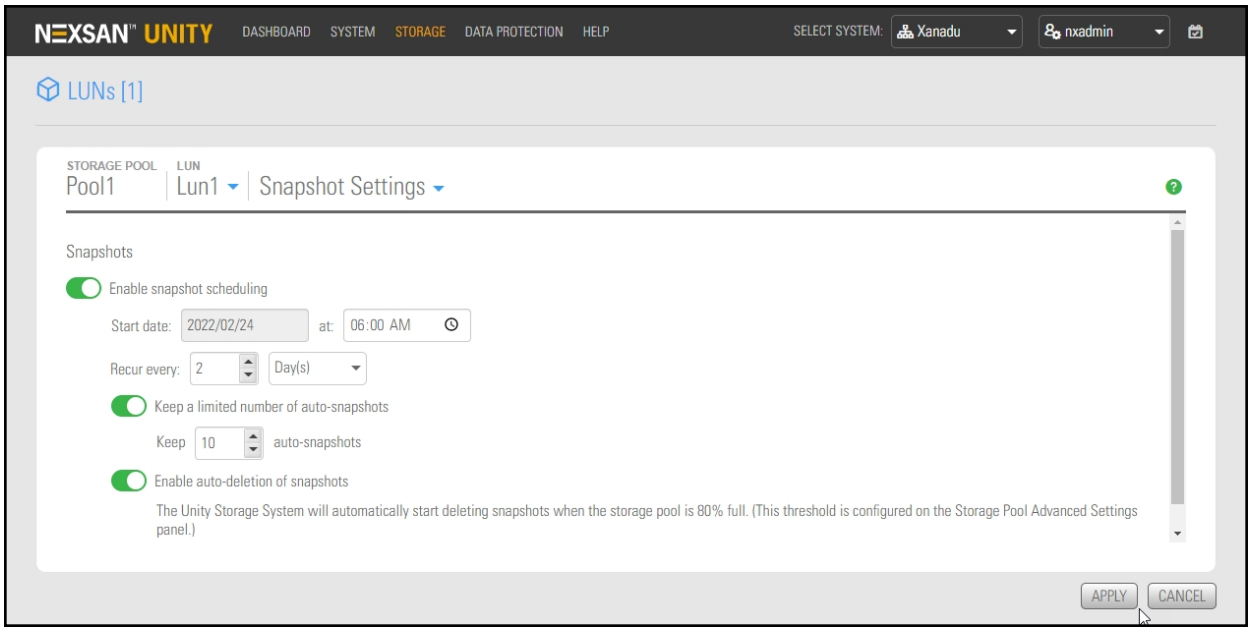
▶ **To set or modify a schedule for automatic snapshots:**

1. On the **Unity navigation bar**, select **Storage > LUNs**.
2. Click the link to the LUN that you want to schedule automatic snapshots for.
3. Select **Summary > Snapshot Settings**.

4. In the **Snapshot Settings** panel, configure the snapshots schedule for the LUN:
   a. **Enable snapshot scheduling** 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 12 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. Accept or change the value for the number of auto-snapshots to be kept. The default is 7.
   d. Select the **Enable auto-deletion of snapshots** button if you want Unity to start deleting snapshots when the storage pool is 80% full.
   e. 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.

Figure 6-62: LUN Snapshot Settings panel - set a schedule



Note By default, Unity Storage System information refreshes every 5 minutes; as a result, a scheduled snapshot that Unity records may not be immediately visible in the snapshots grid. To force a refresh, click Refresh in the grid.

Immutable snapshots for LUNs

Use the topics in this section to create immutable LUN snapshots, to make existing LUN snapshots immutable, to change the retention date of a LUN snapshot, or to make an immutable snapshot schedule.

A snapshot is immutable when it is locked for a specified period of time, and protected from modification or deletion. Having immutable snapshots ensures

- availability of snapshot data for disaster recovery, and,
- faster recovery compared to traditional recovery using backups

The LUNs Snapshots panel lists all snapshots for the corresponding LUN, and provides options for the tasks you can perform with immutable snapshots.

This section includes these topics:

Taking an immutable LUN snapshot 305
Making an existing LUN snapshot immutable 307
Extending the retention date of an immutable LUN snapshot 309
Scheduling immutable snapshots for LUNs 311

Taking an immutable LUN snapshot

Use this topic to take an immutable LUN snapshot.

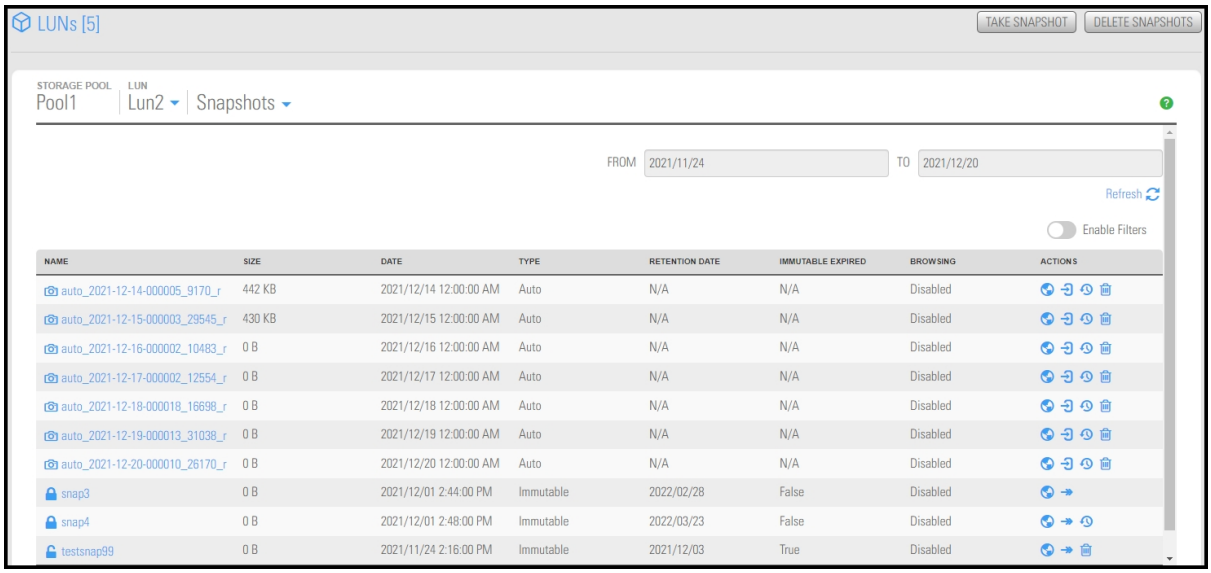
Prerequisites

To complete this procedure, you'll need a Unity Storage System set up with storage pools, file systems, LUNs, and snapshots.

To take an immutable LUN snapshot:

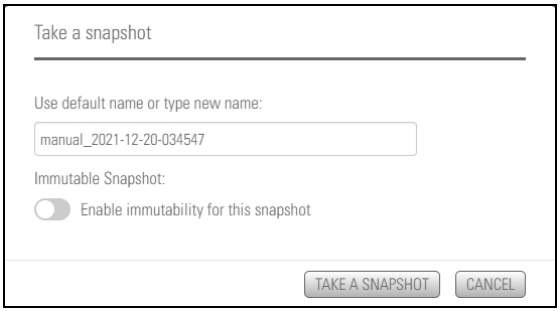
1. On the **Unity navigation bar**, select **Storage > LUNs**.
2. Click the link to the LUN you would like to view snapshots for. The **LUNs Summary** page appears.
3. Select **Summary > Snapshots**.The **LUNs Snapshots** panel appears.

Figure 6-63: The LUNs Snapshots panel



4. Click the **Take Snapshot** button on the upper right. The **Take a Snapshot** pop-up appears.

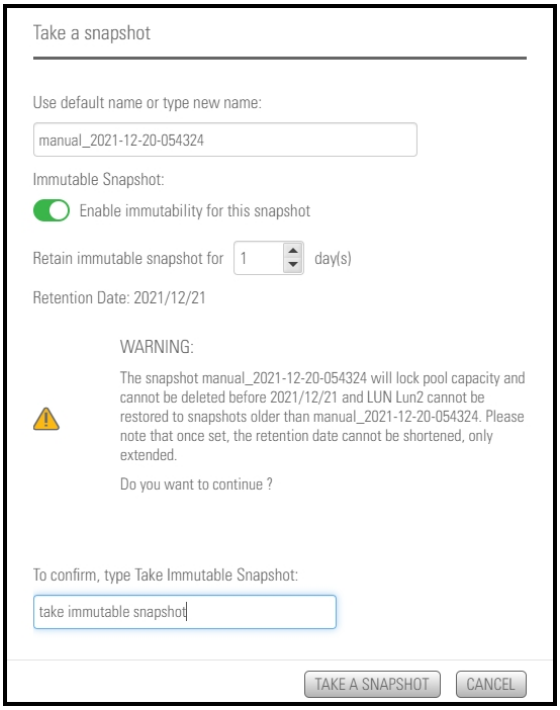
Figure 6-64: Take a snapshot pop-up window



5. Click the **Enable immutability for this snapshot** slider button . The subsequent **Take a snapshot** pop-up appears.
6. Use the default name or type a new name. The **Enable immutability for this snapshot** slider button appears green . Select the number of days to retain the immutable snapshot. The minimum number of days is one and the maximum number of days is 365. To confirm, type 'take immutable snapshot' and click the **Take a Snapshot** button.

CAUTION: Immutable snapshots lock pool capacity, cannot be deleted before the retention date, and the associated file system cannot be restored to a time before the immutable snapshot is created.

Figure 6-65: Take Immutable Snapshot confirmation pop-up window



Making an existing LUN snapshot immutable

Use this topic to make a LUN snapshot immutable.

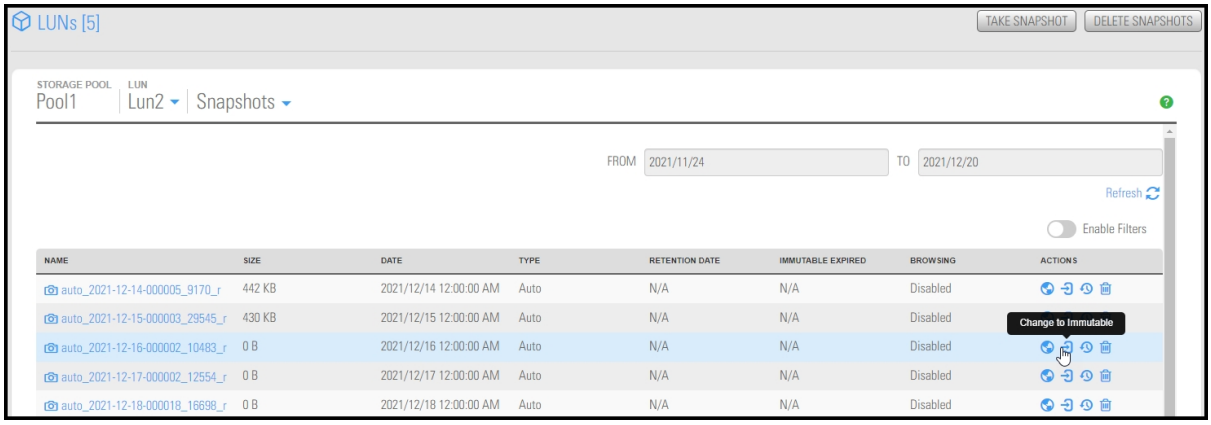
Prerequisites

To complete this procedure, you'll need a Unity Storage System set up with storage pools, file systems, LUNs, and snapshots.

To make a LUN snapshot immutable:

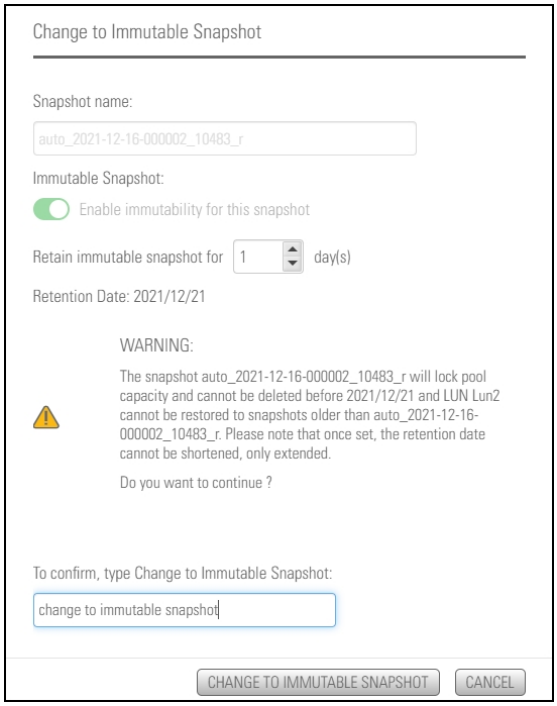
1. On the **Unity navigation bar**, select **Storage > LUNs**.
2. Click the link to the LUN you would like to view snapshots for. **LUNs Summary** page appears.
3. Select **Summary > Snapshots**. The **LUNs Snapshots** panel appears.
4. For the target snapshot, click the **Change to Immutable** icon . The **Change to Immutable Snapshot** pop-up appears.

Figure 6-66: Change to immutable action icon in LUNs panel



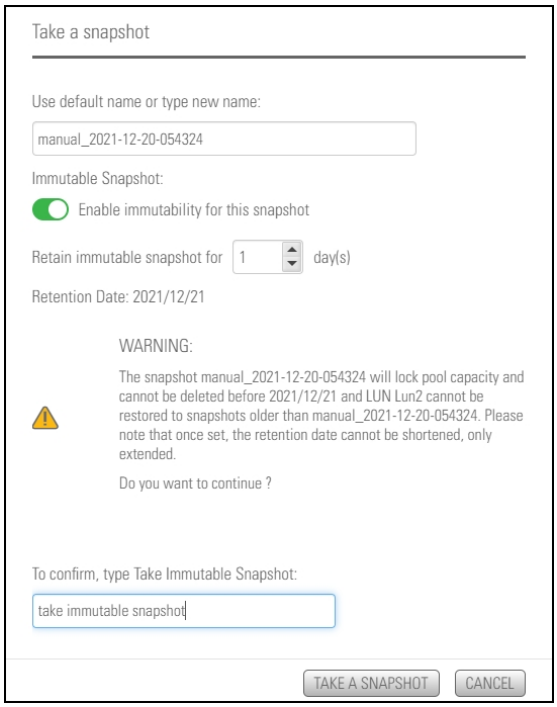
5. Select the number of days to retain the immutable snapshot. The minimum number of days is one and the maximum number of days is 365. To confirm, type 'change to immutable snapshot' in the confirmation field, then click the **Change to Immutable Snapshot** button.

Figure 6-67: Change to Immutable Snapshot pop-up window



CAUTION: Immutable snapshots lock pool capacity, cannot be deleted before the retention date, and the associated file system cannot be restored to a time before the immutable snapshot is created.

Figure 6-68: Take Immutable Snapshot confirmation pop-up window



Extending the retention date of an immutable LUN snapshot

Use this topic to extend the retention date of an immutable LUN snapshot.

Prerequisites

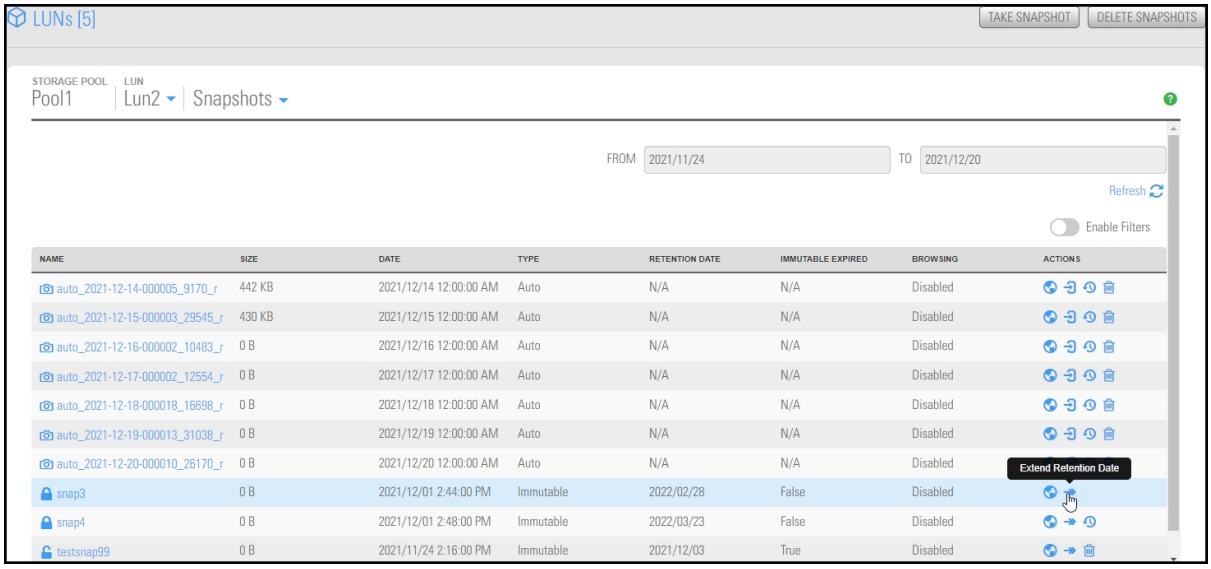
To complete this procedure, you'll need a Unity Storage System set up with storage pools, file systems, LUNs, and snapshots.

► **To extend the retention date of an immutable LUN snapshot:**

1. On the **Unity navigation bar**, select **Storage > LUNs**.
2. Click the link to the LUN you would like to view snapshots for. The **LUNs Summary** page appears.
3. Select **Summary > Snapshots**.The **LUNs Snapshots** panel appears.

4. For the target snapshot, click the **Extend Retention Date** icon . The **Extend Retention Date** pop-up appears.

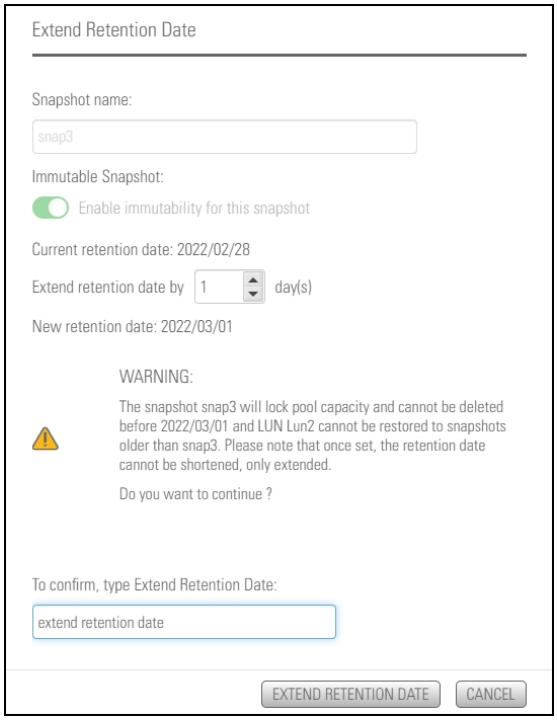
Figure 6-69: Extend Retention Date action icon in LUN Snapshots panel



5. Select the number of days to extend the retention date. The minimum number of days is one and the maximum number of days is 365. Type 'extend retention date' in the confirmation field, then click the **Extend Retention Date** button.

CAUTION: Immutable snapshots lock pool capacity, cannot be deleted before the retention date, and the associated file system cannot be restored to a time before the immutable snapshot is created.

Figure 6-70: Extend Retention Date pop-up window



Scheduling immutable snapshots for LUNs

Use this topic to add, edit, or delete an immutable snapshot schedule for a LUN.

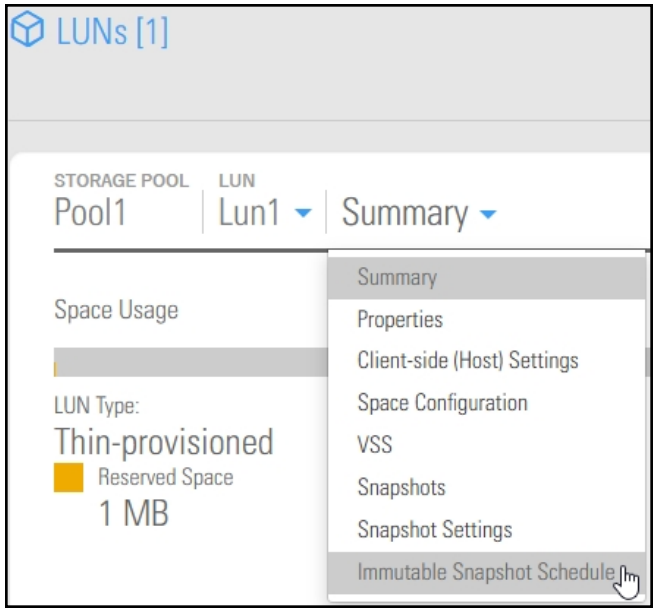
Prerequisites

To complete this procedure, you'll need a Unity Storage System set up with storage pools, file systems, LUNs, and snapshots.

► **To add an immutable snapshot schedule for a LUN:**

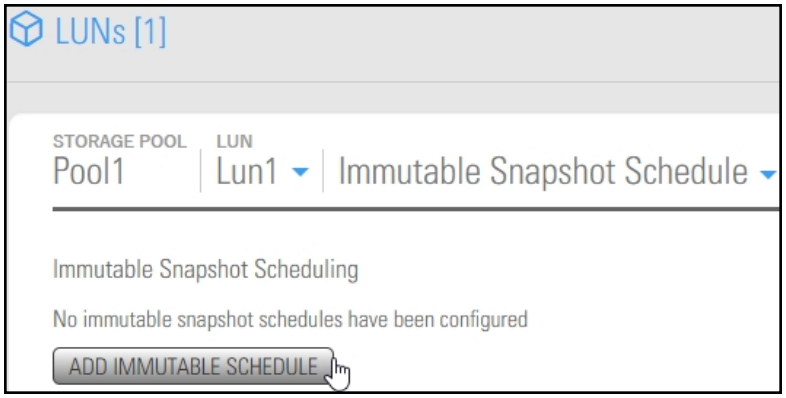
1. On the **Unity navigation bar**, select **Storage > LUNs**.
2. Click the link to the LUN you would like to set an immutable snapshot schedule for. **The LUNs Summary** page appears.
3. Select **Summary > Immutable Snapshot Schedule**.

Figure 6-71: Immutable Snapshot Schedule menu selection



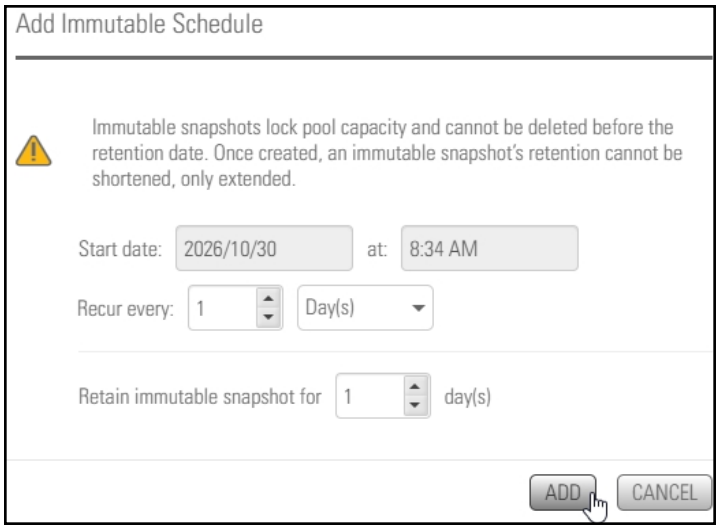
4. The **Immutable Snapshot Scheduling** panel appears . Click the **Add Immutable Schedule** button.

Figure 6-72: Immutable Snapshots Scheduling panel - Add Immutable Schedule



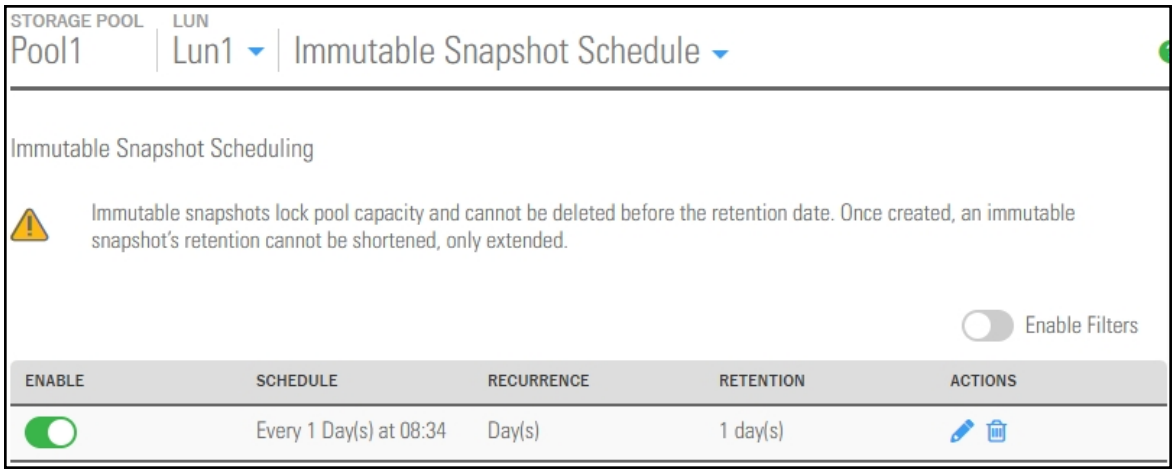
5. The **Add Immutable Schedule** pop-up appears. The fields for **Start date** and **at** time are pre-set to the time of creation. Complete the **Recur every** fields and the **Retain immutable snapshot for** (number of) **day(s)** field. When done, click the **Add** button.

Figure 6-73: Add Immutable Schedule pop-up



6. The **Immutable Snapshot Schedule** panel refreshes, with the newly created schedule listed in the chart. The columns include information for **Enable**, **Schedule**, **Recurrence**, **Retention**, and **Actions**.

Figure 6-74: Immutable snapshot schedule added

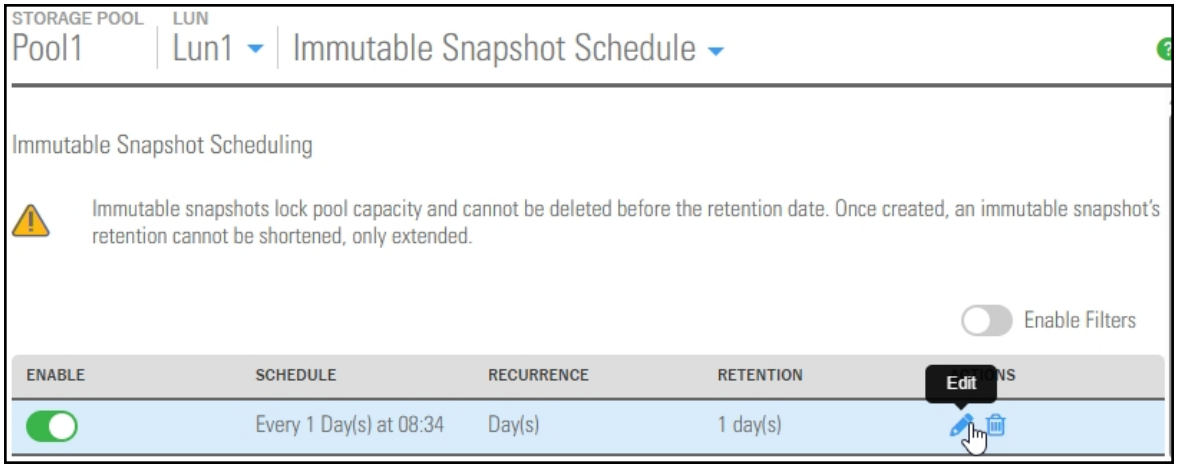


6

► To edit an immutable snapshot schedule for a LUN:

1. On the **Unity navigation bar**, select **Storage > LUNs**.
2. Click the link to the LUN you would like to edit an immutable snapshot schedule for. **The LUN Summary** page appears.
3. Select **Summary > Immutable Snapshot Schedule**.
4. The **Immutable Snapshot Scheduling** panel appears with a list of schedules. In the **Actions** column, click the **Edit icon** associated to the schedule to edit.

Figure 6-75: Immutable Snapshot Scheduling - Edit schedule



5. The **Edit Immutable Schedule** pop-up appears. The fields for **Recur every** and **Retain immutable snapshot for** (number of) **day(s)** can be modified.
   To disable or enable a snapshot schedule, use the radio button in the **Enable** column.
   When done, click the **Save** button.

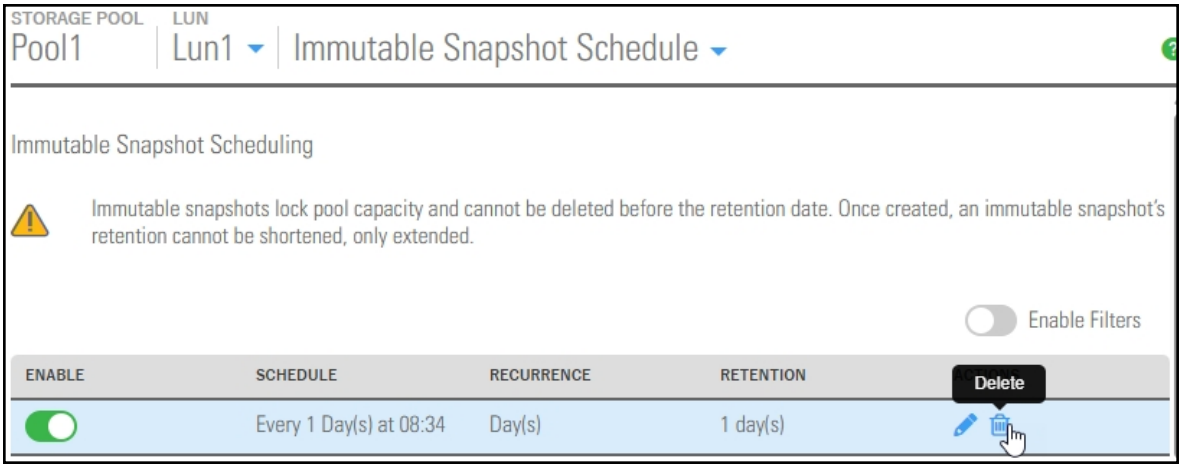
Note Immutable snapshots lock pool capacity and cannot be deleted before the retention date. Once created, an immutable snapshot's retention cannot be shortened, only extended.

6

► To delete an immutable snapshot schedule for a LUN:

1. On the **Unity navigation bar**, select **Storage > LUNs**.
2. Click the link to the LUN you would like to delete an immutable snapshot schedule for. **The LUNs Summary** page appears.
3. Select **Summary > Immutable Snapshot Schedule**.
4. The **Immutable Snapshot Scheduling** panel appears with a list of schedules. In the **Actions** column, click the **Delete icon** associated to the schedule to delete.

Figure 6-76: Immutable Snapshot Scheduling - Delete schedule



5. The **Delete Immutable Schedule** pop-up appears. To confirm, click the **Yes** button.

Managing iSCSI targets

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.

Note This section does not apply to Fibre Channel targets.

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 on page 82

Adding an iSCSI target below

Connecting to an iSCSI LUN from Windows on page 318

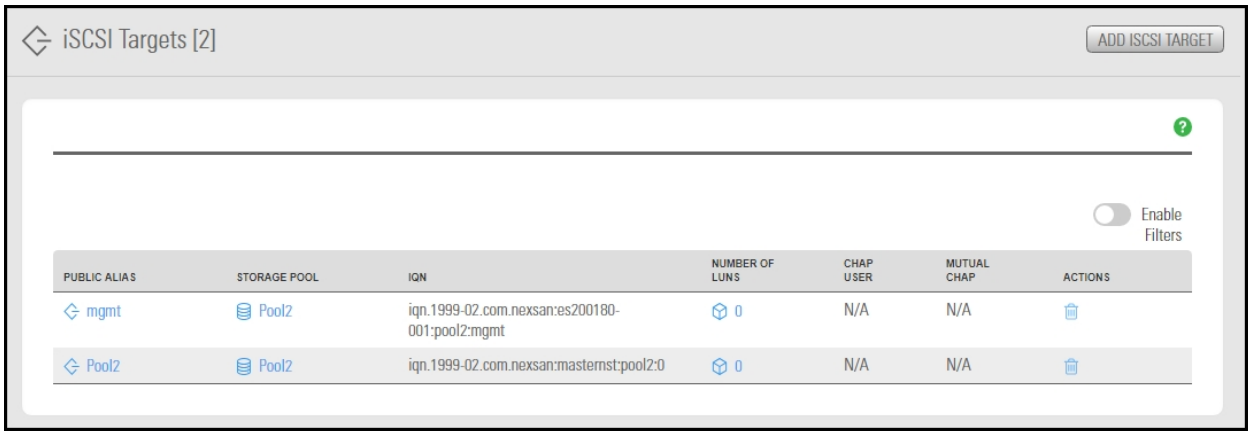
Adding an iSCSI target

Unity provides the **Create an iSCSI Target** wizard to guide you through the process of adding a target to a storage pool.

▶ **To add an iSCSI target:**

1. On the **Unity navigation bar**, select **Storage > iSCSI targets**.

Figure 6-77: iSCSI targets panel



2. Click the **Add iSCSI Target** button.

The **Create an iSCSI Target** wizard guides you through the process of adding a target to a storage pool.

This section includes these steps:

Step 1: Setting iSCSI target properties on the next page

Step 2: Verifying settings on the facing page
Step 3: Viewing results on page 318

Step 1: Setting iSCSI target properties

Step 1 of the **Create an iSCSI target** wizard prompts you to select a pool, public alias, and target IQN.

- 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:

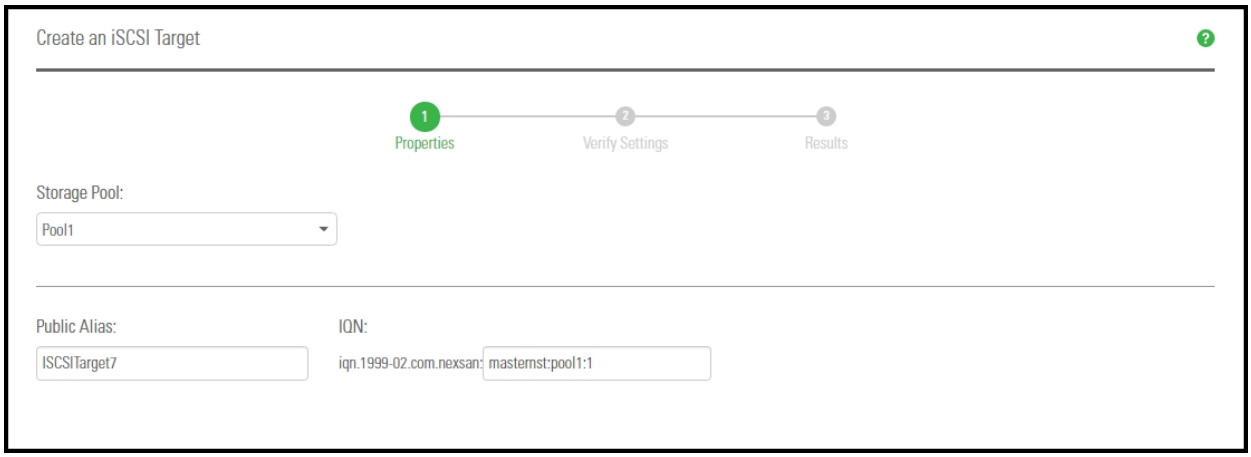
  `iqn.1999-02.com.nexsan:<site name>:<pool name>:<unique ID>`

  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 Unity Storage System (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 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 6-78: Create an iSCSI target wizard, Step 1: Specifying properties



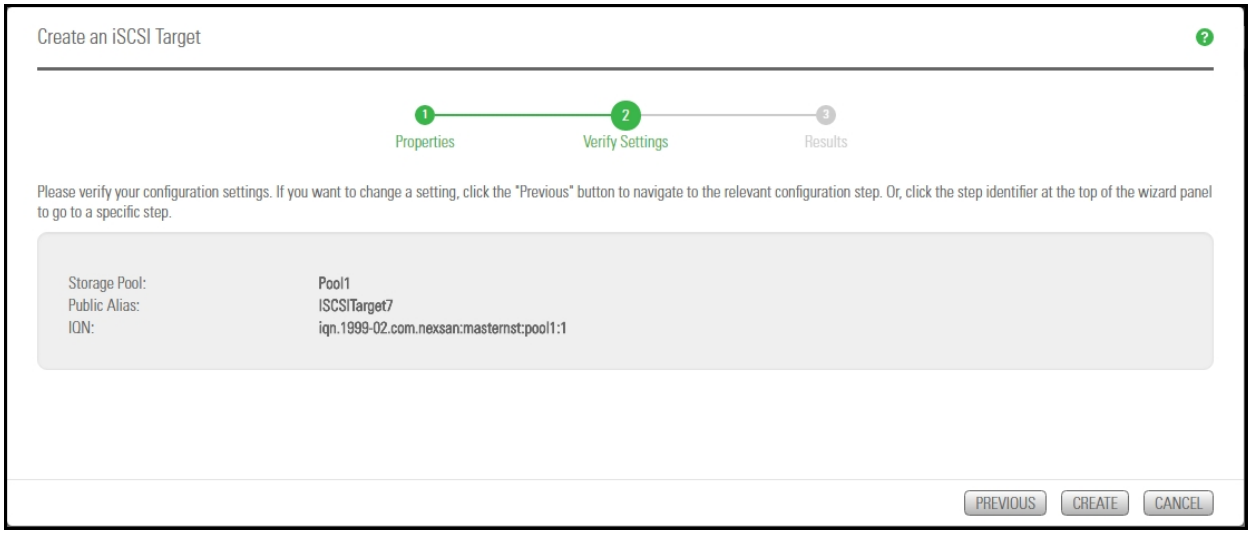
To specify the Storage Pool, IQN and public alias for the iSCSI target:

1. Select an available pool from the **Storage Pool** list.
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. 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.
4. Once you specify the IQN and public alias for the target, click **Next** to continue to Step 2: Verifying settings on the facing page to Step 3: Viewing results on page 318.

Step 2: Verifying settings

Step 2 of the **Create an iSCSI target** wizard prompts you to verify your settings before you create the target..

Figure 6-79: Create an iSCSI target wizard: Verifying Settings



To verify settings for the target:

1. Review your settings from the wizard step 1.
2. Do one of the following:
   a. Click **Previous** to make changes.
   b. Click **Create** to begin the creation process. See Step 3: Viewing results on the next page

Step 3: Viewing results

The last step of the **Create an iSCSI target** wizard displays progress as Unity creates the new iSCSI target.

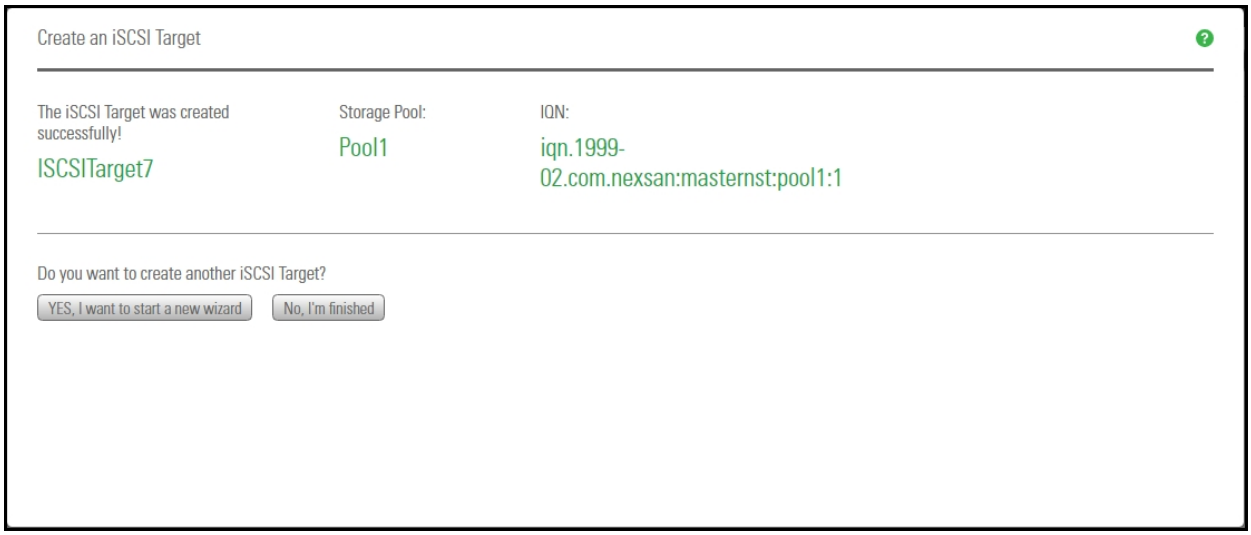
To view more details for an error event:

- Click the **View Error** link next to the error in the **Results** panel.

Figure 6-80: Create an iSCSI target wizard, Step 3: Viewing progress



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



Connecting to an iSCSI LUN from Windows

Use this section for instructions about connecting to an iSCSI LUN from a Windows-based initiator.

Notes:

- The procedures provided here are specific to Microsoft Windows 11; the process for connecting to an iSCSI LUN on Unity may differ to some extent depending on the version of Windows you are initiating the connection from.
- In addition, some iterations of Microsoft Windows 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** > **Windows Administrative Tools** > **iSCSI Initiator**.
2. 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.
3. The Microsoft iSCSI Initiator Properties dialog box opens, and the **Targets** tab displays. Click the **Discovery** tab.
4. To add Unity as a target portal, click **Discover Portal**.
5. In the Discover Portal dialog box, type the virtual IP address of the Pool Resource Group where the LUN exists. (To identify the Pool Resource Group IP address, on the Unity Dashboard, click **Cluster Status**, then **Status** > **IP Configuration**.)
6. Click the **Targets** tab, select the discovered targets (LUNs) that you want to connect to, and click **Connect**.
7. In the **Connect to Target** popup, choose from the following:
   a. Add this connection to the list of Favorite Targets. This default setting ensures that Windows automatically attempts to restore the connection every time the computer restarts.
   b. Click **Enable multi-path**. Multipathing is recommended
   c. Optionally, click **Advanced** to specify additional or edit connection settings such as local adaptor, initiator and target IP address, or CRC/Checksum or spChap logon. You can also click the **IPsec** tab to change the security protocol settings.
   d. Click **OK**.

   The initiator adds the iSCSI LUN to Windows, but must still be initialized, as described in step 2, below.
8. Click **OK** to close the **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** > **Windows Administrative Tools** > **Computer Management**.
2. Click **Disk Management**.
3. The *Disk Management* app 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 Disk Management 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.

Adding an iSNS server

You can configure iSCSI targets on Unity to use 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.

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.

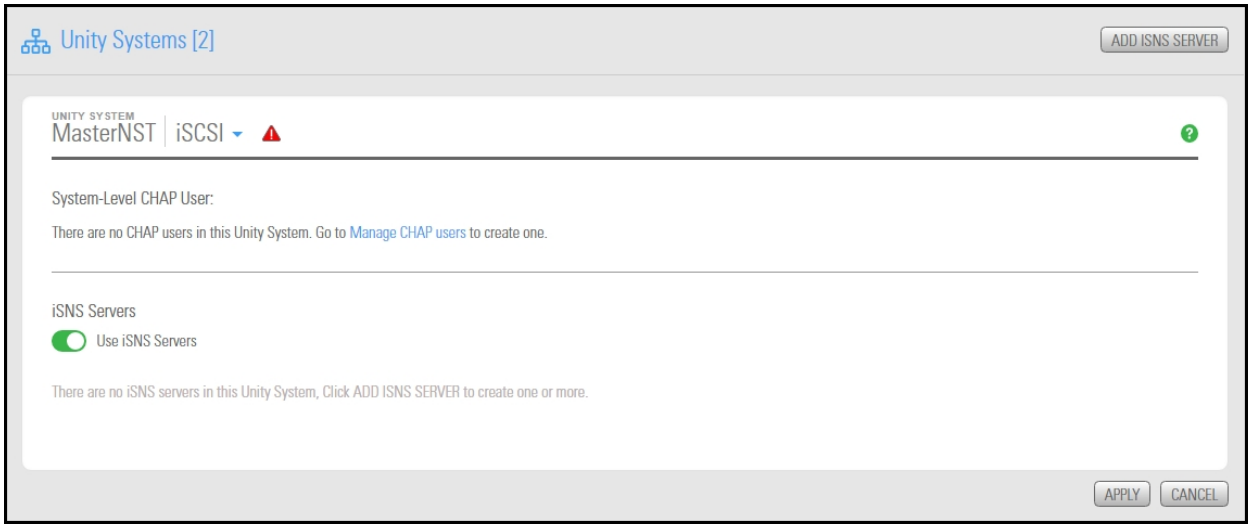
Note An iSNS server must already be set up and available on the network in order for Unity to access it.

Unity does not support the use of iSNS servers for Fibre Channel targets.

▶ **To add an iSNS server:**

1. On the **Unity navigation bar**, select **System > Unity Systems**.
2. Open the Unity Storage System that you want to connect to.
3. Select **Summary > iSCSI**.
4. Click the **Use iSNS servers** button.

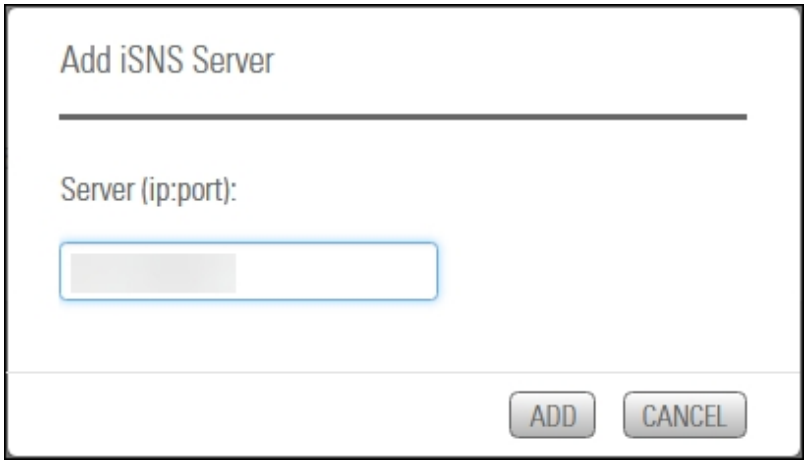
Figure 6-81: Unity Systems, iSCSI panel



5. Click the **Add iSNS Server** button.

6. Enter the IP address of the iSNS server in the window and click **Add**.

Figure 6-82: Add iSNS server window



7. Click the **Apply** button. All iSCSI targets on Unity will be managed by the specified iSNS server. For large networks, you can add additional iSNS servers.

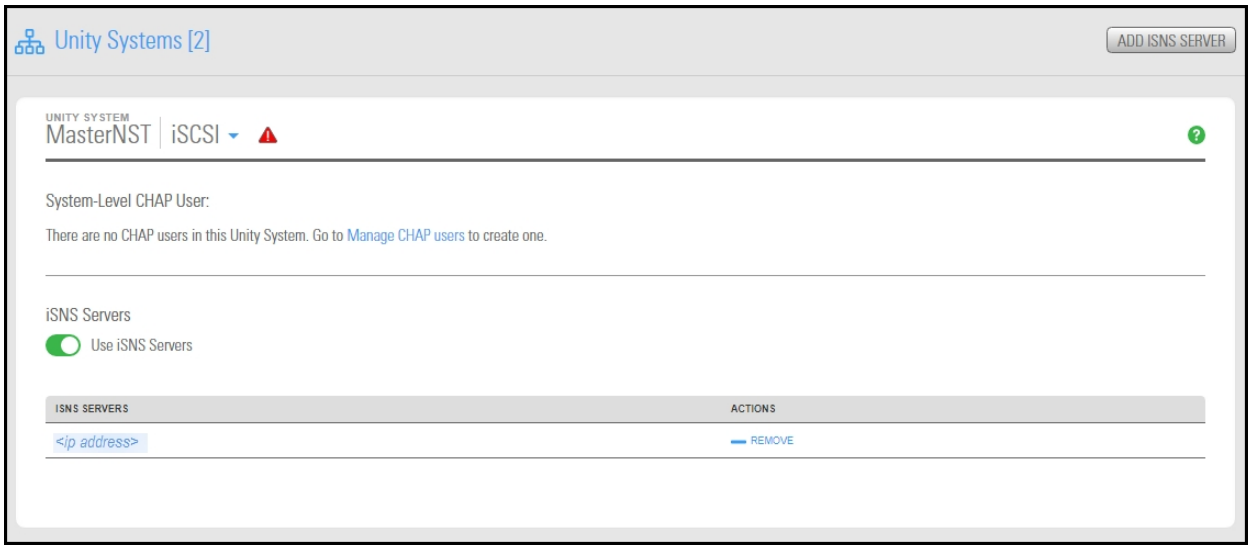
Removing an iSNS server

Use this topic for help with removing an iSNS server.

▶ **To remove an iSNS server:**

1. On the **Unity navigation bar**, select **System > Unity Systems**.
2. Open the Unity Storage System that you want to remove the connection from.
3. Select **Summary > iSCSI**.

Figure 6-83: Unity Systems, iSCSI panel



4. Click **Remove**.
5. Click the **Apply** button. The iSNS server is removed from Unity.

Host connectivity: LUN masks and Initiator Groups

LUN masks enable you to restrict access to LUNs on the Unity Storage System based on initiator name and type–iSCSI or Fibre Channel. 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.

Topics in this section:

About LUN masks 323
Viewing LUN masking information 323
Creating a LUN mask 324
Editing a LUN mask 326
Deleting a LUN mask 329
Viewing initiator group information 330
Adding an initiator group 330
Editing an initiator Group 331
Deleting an initiator group 333

6

About LUN masks

LUN masks enable you to organize LUNs according to your storage and access needs. LUN masks use authentication to make a Logical Unit Number accessible to selected storage targets. For a LUN to be visible to a host, you must create a LUN mask and add the LUN to the mask.

A LUN mask also enables 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.

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 in initiator groups.

When you create LUN masks, they are created on both controllers by default. Upon cluster failover, the LUN masks are still available on Unity. See Creating a LUN mask on the next page

CAUTION: Replication and LUN masking

LUN masks are not replicated on secondary Unity Systems. If you ever need to make a pool on the secondary Unity System of the primary pool, you must create one or more LUN masks on the secondary system for that pool so that it can be accessed by the same hosts as the current primary pool.

Initiator Groups

An Initiator Group is a group of iSCSI or Fibre Channel target ports through which the application will access storage. You must create an Initiator Group before you can add initiators to a LUN mask. See Adding an initiator group on page 330

Viewing LUN masking information

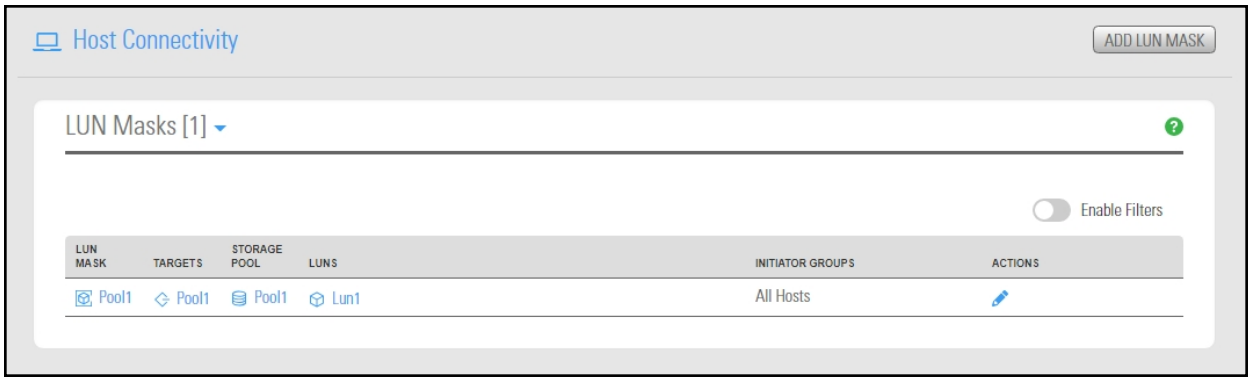
The LUN Mask panel displays LUN masks and their associated targets, storage pools, and LUNs. A LUN can be accessed by multiple initiators. A LUN can also be associated to multiple targets. However, a LUN can only be selected in one LUN mask, as opposed to initiators with targets. See also Host connectivity: LUN masks and Initiator Groups on the previous page.

The LUN Masks panel enables you to add, edit, or delete LUN masks. For procedural steps, see Creating a LUN mask on the next page, Editing a LUN mask on page 326, and Deleting a LUN mask on page 329.

To view LUN mask information:

- On the **Unity navigation bar**, select **System > Host Connectivity**.

Figure 6-84: LUN masks panel



Creating 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 enables 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.

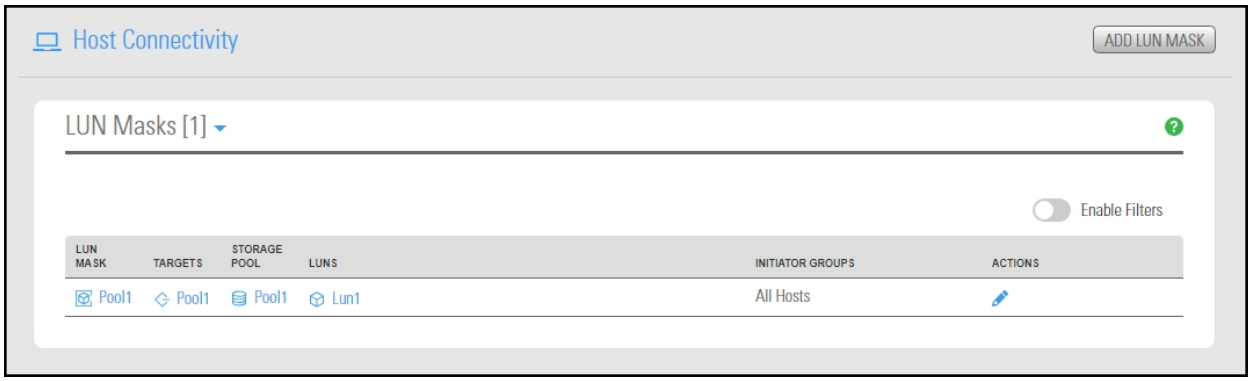
Notes:

- 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 315.
- LUN masks are managed per Unity System. If your storage pool is replicated, you must create corresponding LUN masks on the remote system for the replica. This is so that the LUNs remain accessible in case of a failover.

To create a LUN mask:

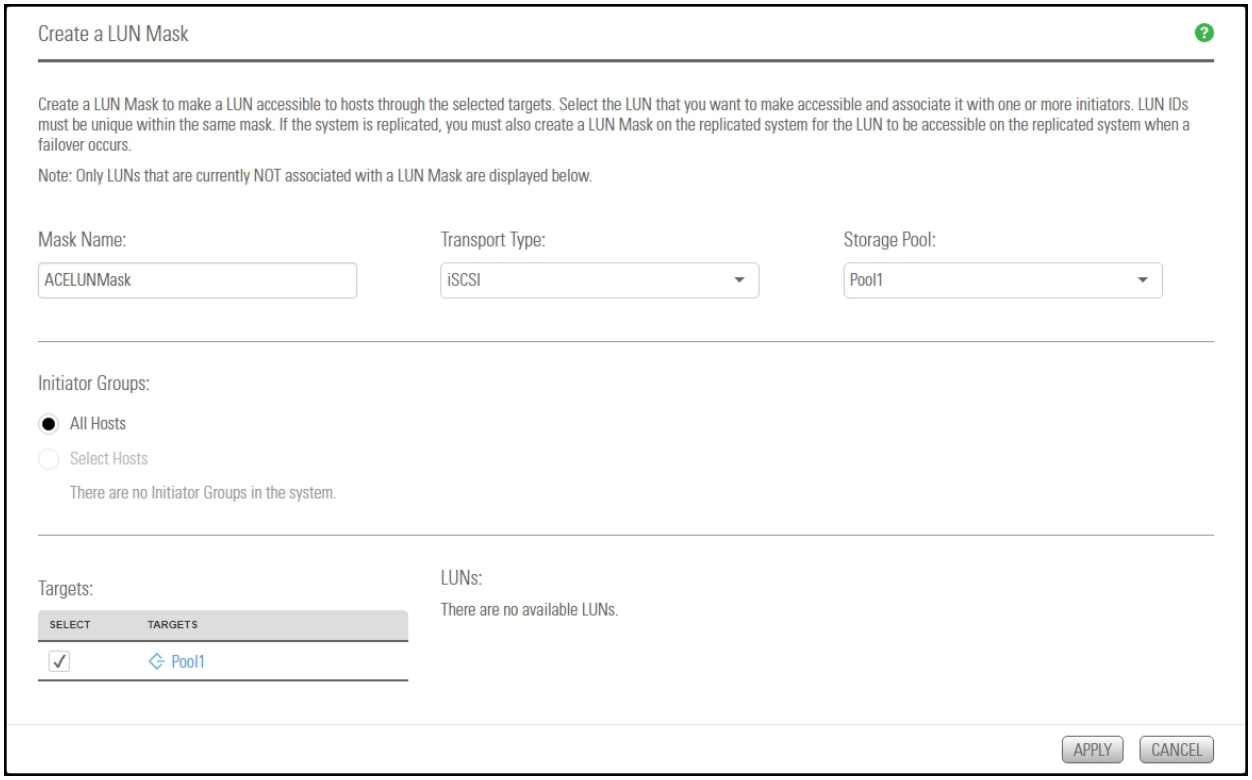
1. On the **Unity navigation bar**, select **System > Host Connectivity**.

Figure 6-85: LUN masks panel



2. Click the **Add LUN mask** button. The **Create a LUN mask** popup window opens.

Figure 6-86: Creating a LUN mask popup



3. Enter a meaningful name in the **Name** field.
4. From the **Storage Pool** drop-down list, select the name of the pool hosting the LUNs you will add to the mask. The list of targets in the **Targets** column gets automatically updated for the selected pool.
5. From the **Transport Type** drop-down list, select **iSCSI** or **Fibre Channel**.
6. Under the **Initiators** list, **All hosts** is selected by default. You can uncheck that option if you want to provide access to only selected initiators. To add an Initiator Group, see Adding an initiator group on page 330.
7. Click **OK** to return to the **Create a LUN mask** dialog box.
8. In the **Targets** section, 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 LUNs that you want to make visible to the host.
10. Click the **Apply** button to save your changes.

Editing a LUN mask

You can modify the settings listed below in user-defined LUN masks.

- add new LUNs, if available. A LUN must be available in target pool.
- rename LUN masks
- assign new storage pools to the LUN mask
- assign initiator groups
- 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.

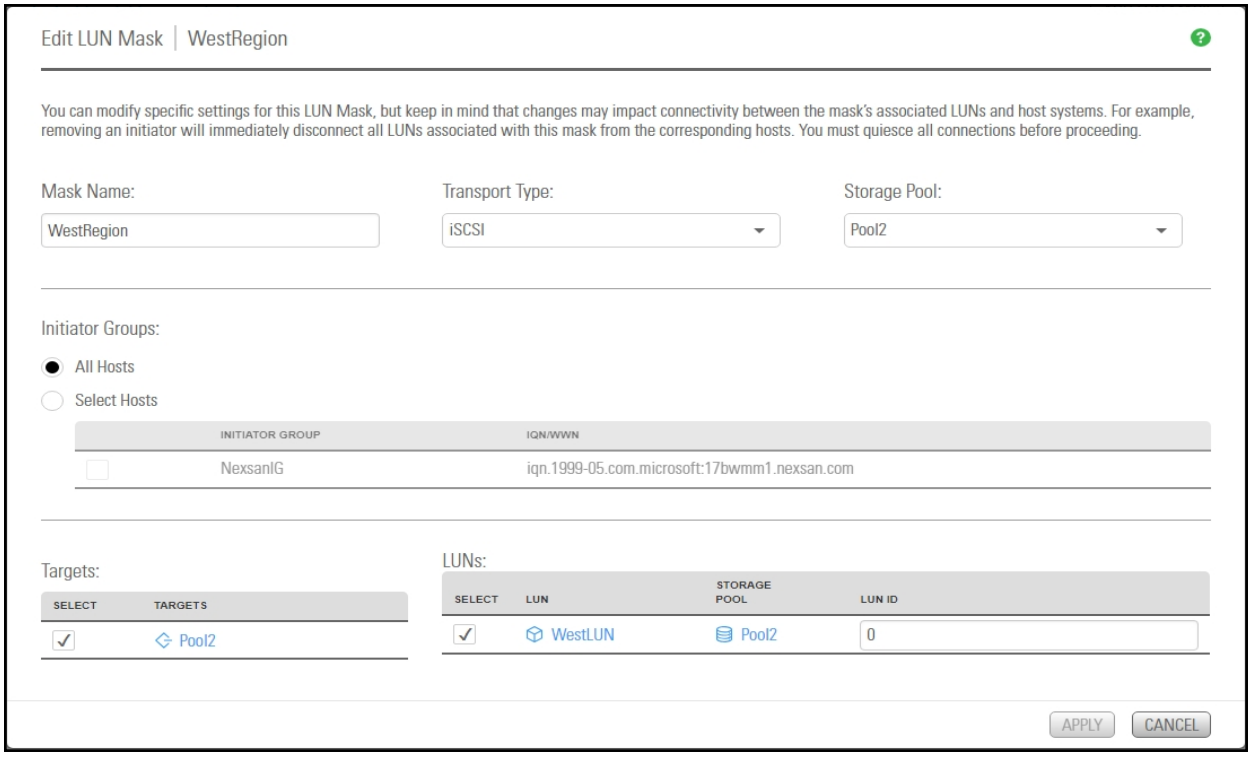
Notes:

- The mask will only display LUNs that have not been assigned to a target.
- Editing options for predefined LUN masks are limited to changing their pool association and editing LUN IDs. Predefined LUN masks are preinstalled with Unity and have many presets to save configuration steps.
- Before editing a mask for iSCSI LUNs, make sure all storage pools have iSCSI targets created; see Adding an iSCSI target on page 315.

To edit a LUN mask:

1. On the **Unity navigation bar**, select **System > Host Connectivity**.
2. Click the **Edit LUN mask** icon . The **Edit the LUN mask** popup window opens.

Figure 6-87: Edit LUN mask popup



3. 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 Transport Type	a. From the **Transport Type** drop-down list, select **iSCSI** or **Fibre Channel**. b. Add initiators (see the procedure in the row below). c. Select targets from the **Targets** column. The LUNs present in the pool become available for selection in the **LUN Names** column. d. Select the desired LUNs from the **LUN Names** column. e. Enter the LUN ID. **Note** LUN IDs must be unique within the same mask.
select Initiator Groups	Do either of the following: a. Use the default selection of **All Hosts**. b. Select another available Initiator Group, if available. See Adding an iSCSI target on page 315
change the LUN ID	Enter a new LUN ID for the selected LUN. **Note** LUN IDs must be unique within the same mask.

4. Click the **Apply** button to save your changes.

Deleting a LUN mask

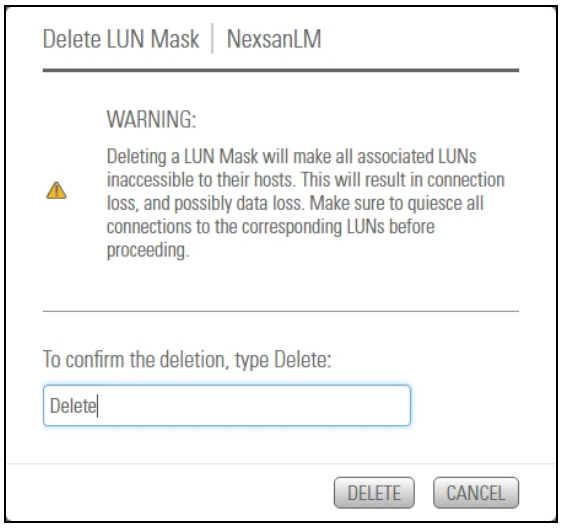
Use this procedure to delete user-defined LUN masks. Predefined LUN masks, which are pre-installed with Unity and have many presets to simplify configuration, cannot be deleted.

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. On the **Unity navigation bar**, select **System > Host Connectivity**.
2. In the LUN Masks table, click the **Delete LUN Mask** icon next to the LUN mask that you want to delete. The **Delete LUN Mask** popup window opens.

Figure 6-88: Delete LUN Mask popup window



3. Type **Delete** in the text field.
4. Click the **Delete** button to confirm.

Viewing initiator group information

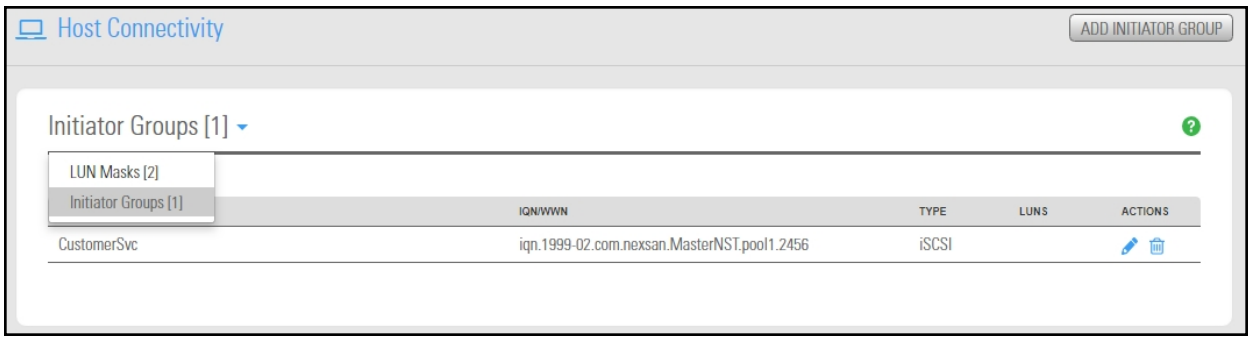
The Initiator Groups panel displays the initiators and their associated targets and LUNs. The same initiator can be used by multiple LUNs. Likewise, a LUN can be accessed by multiple initiators. A LUN can also be associated to multiple targets. However, a LUN can only be selected in one LUN mask, as opposed to initiators and targets. See also Host connectivity: LUN masks and Initiator Groups on page 322

The Initiator Groups panel also enables you to add, edit, or delete Initiator Groups. For procedural steps, see Adding an initiator group below, Editing an initiator Group on the facing page, and Deleting an initiator group on page 333.

To view LUN mask information on a specific LUN:

1. On the **Unity navigation bar**, select **System > Host Connectivity**.
2. Select **LUN Masks > Initiator Groups**.

Figure 6-89: Initiator Groups panel



Adding an initiator group

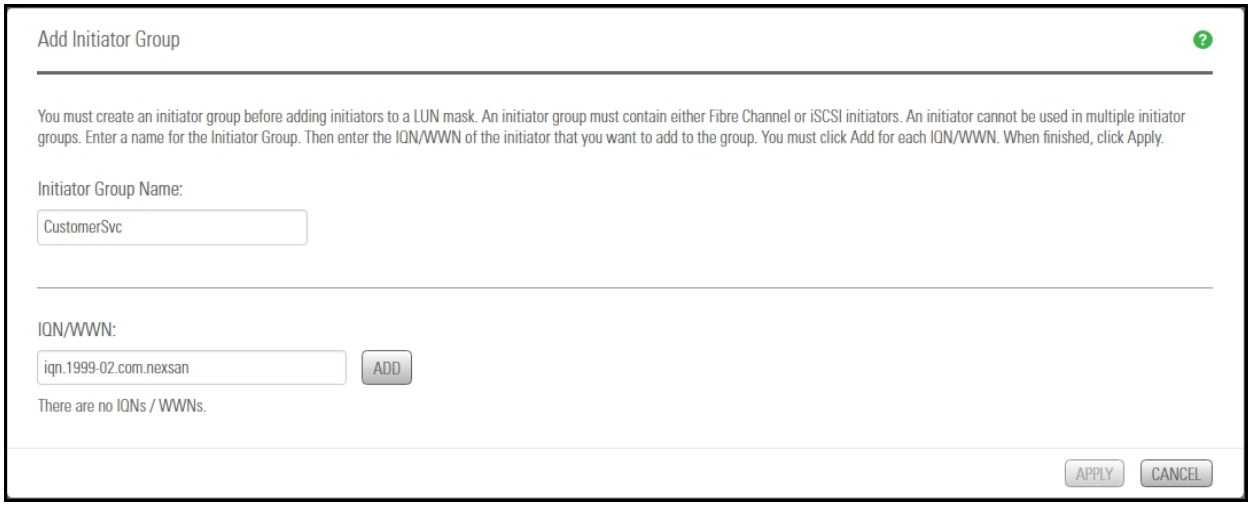
You must add a group of initiators before adding them to a LUN mask. An initiator group must contain either Fibre Channel or iSCSI initiators. An initiator cannot be part of multiple groups.

To add an Initiator group:

1. On the **Unity navigation bar**, select **System > Host Connectivity**.
2. Select **LUN masks > Initiator Groups**.

3. Click the **Add Initiator Group** button.

Figure 6-90: Add Initiator Group window



4. Enter a friendly name in the **Initiator Group Name** field.
5. Enter an Initiator IQN or WWN number:

   IQN format: `iqn.1999-05.com.microsoft:17bwmm1.nexsan.com`.

   WWN format: `wwn.50003a4ff000681a`.

   Existing IQN numbers display in the iSCSI Targets properties panel. For targets that are connected but not defined on Unity, use the CLI command, `wwn`. This command will display all iSCSI and Fibre Channel targets connected to Unity.
6. Click **Add** again and repeat the previous two steps to add more initiator groups.
7. Click the **Apply** button to save your changes.

Editing an initiator Group

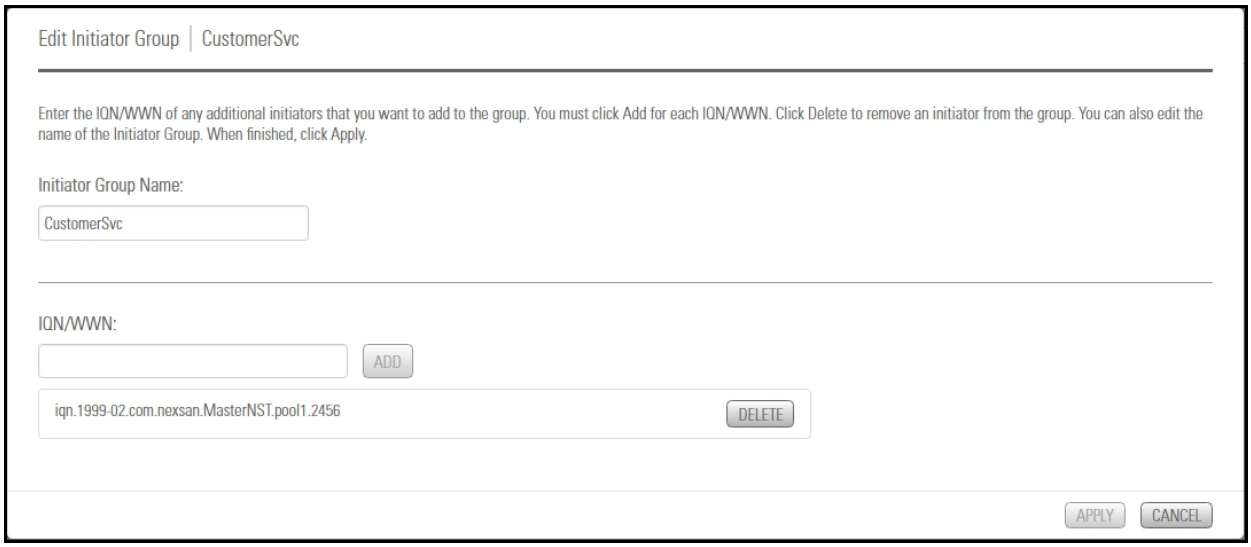
An **Initiator Group** must contain either Fibre Channel or iSCSI initiators. An initiator cannot be selected in multiple groups.

▶ **To modify an Initiator Group:**

1. On the **Unity navigation bar**, select **System > Host Connectivity**.
2. Select **LUN masks > Initiator Groups**. The **Initiator Groups** panel displays all initiators currently added to Unity, their IQN/WWN name, type, and associated LUNs.
3. Select the **Initiator Group** that you want to modify.

4. Click the **Edit Initiator Group** icon .

Figure 6-91: Edit Initiator Group popup window



5. 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	1. Click **Add** to add an Initiator to the group. 2. Enter the Initiator IQN or WWN number: IQN format: `iqn.1999-05.com.microsoft:17bwmm1.nexsan.com`. WWN format: `wwn.50003a4ff000681a`. **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 and Fibre Channel targets connected to Unity. 3. Click **Add**. 4. Repeat these steps for each Initiator to add to the group.
remove initiators	1. Select the IQN/WNN number of the Initiator to remove. 2. Click **Delete**. 3. Repeat these steps for each Initiator to remove from the group.

6. Click the **Apply** button to save your changes.

Deleting an initiator group

Before you begin:

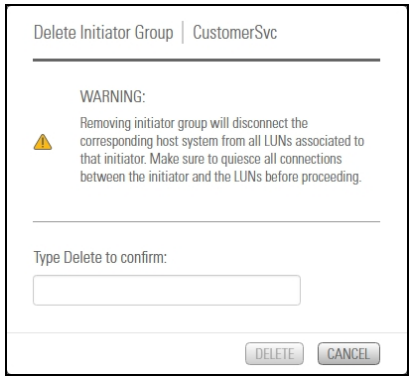
You must remove the Initiator group from all LUN masks where it is used; see Editing a LUN mask on page 326. Removing an initiator group will disconnect the corresponding host systems from all LUNs associated to these initiators.

CAUTION: Removing the initiator group will disconnect the corresponding host system from all LUNs associated with that initiator. Make sure to quiesce all connections between the initiator and the LUNs before proceeding.

To delete an Initiator group:

1. On the **Unity navigation bar**, select **System > Host Connectivity**.
2. Select **LUN masks > Initiator Groups**. The **Initiator Groups** panel displays all initiators currently added to Unity, their IQN/WWN name, type, and their associated LUNs.
3. Select the Initiator Group that you want to delete.
4. Click the **Delete Initiator Group** icon

Figure 6-92: Delete Initiator Group popup



5. Type **Delete** in the text field to confirm.

6

Chapter 7

Object Stores

Unity's Object Store is based on the S3 protocol, as well as object locking support, enabling bucket or object level protection for a specified retention period, thereby creating immutable copies of data. These capabilities enable enterprises to address compliance, regulatory, and other data protection requirements.

Within the Unity storage system, an object store is created within a storage pool. The storage pool MUST be empty, therefore one without any file systems or LUNs. Since a storage pool can have multiple object stores, it is possible to add object stores once the first one is created.

Unity includes wizard-based configuration tools to help you create object stores. For methods of working with object stores using the Unity CLI, refer to the procedures in the *nxcmd Command Line Interface Reference Guide*.

This section includes these topics:

Creating an object store 336
Viewing object store system information 342
Enabling or disabling TLS on the object store 343
Increasing storage capacity for object stores 344
Starting the service for an object store 346
Stopping the service for an object store 347
Deleting an object store 347
Resetting object store keys 349
Accessing the NexObject Web client 349
Creating a data bucket using the Web client 353
Adding data to an object store bucket 355
Creating an object store S3 Table Bucket 357
Creating an object store user 360
Managing object store users 362
Creating and managing object store groups 366
Creating and managing object store service accounts 369
Creating and managing object store policies 371

Creating an object store

Use this procedure to create an object store in the Unity system.

To create an object store:

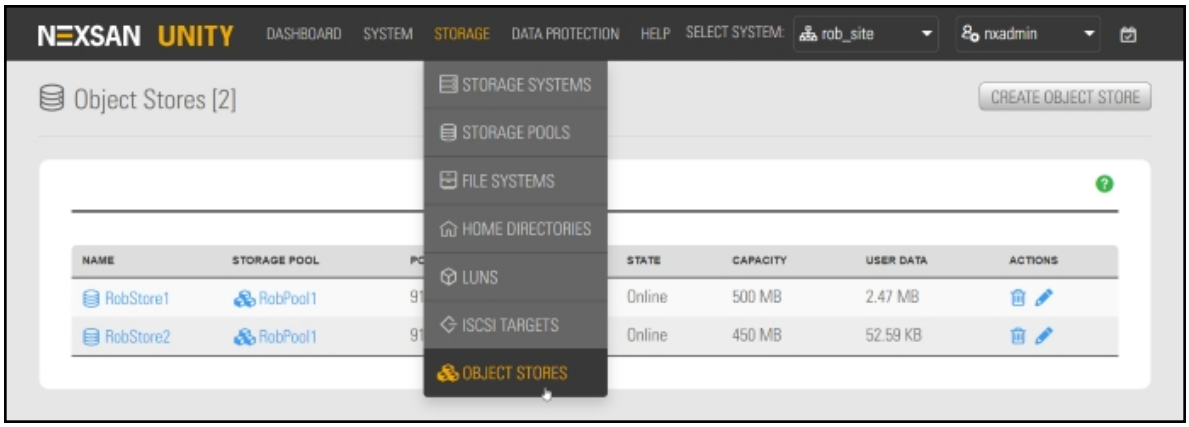
Note Creating an object store requires a storage pool with no file systems or LUNs assigned to it.

1. On the **Unity navigation bar**, click **Storage > Object Stores**.

   The **Object Stores** page displays the available object stores. If an object store has not yet been configured, the status will indicate it.

   Click **Create Object Store** on the top right to create a new object store.

Figure 7-1: Object Stores page



2. The **Create an Object Store** wizard opens, starting with step **1**, **Properties**. Under **Object Store Name**, enter a name for the new object store.

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

   These characters are NOT allowed:

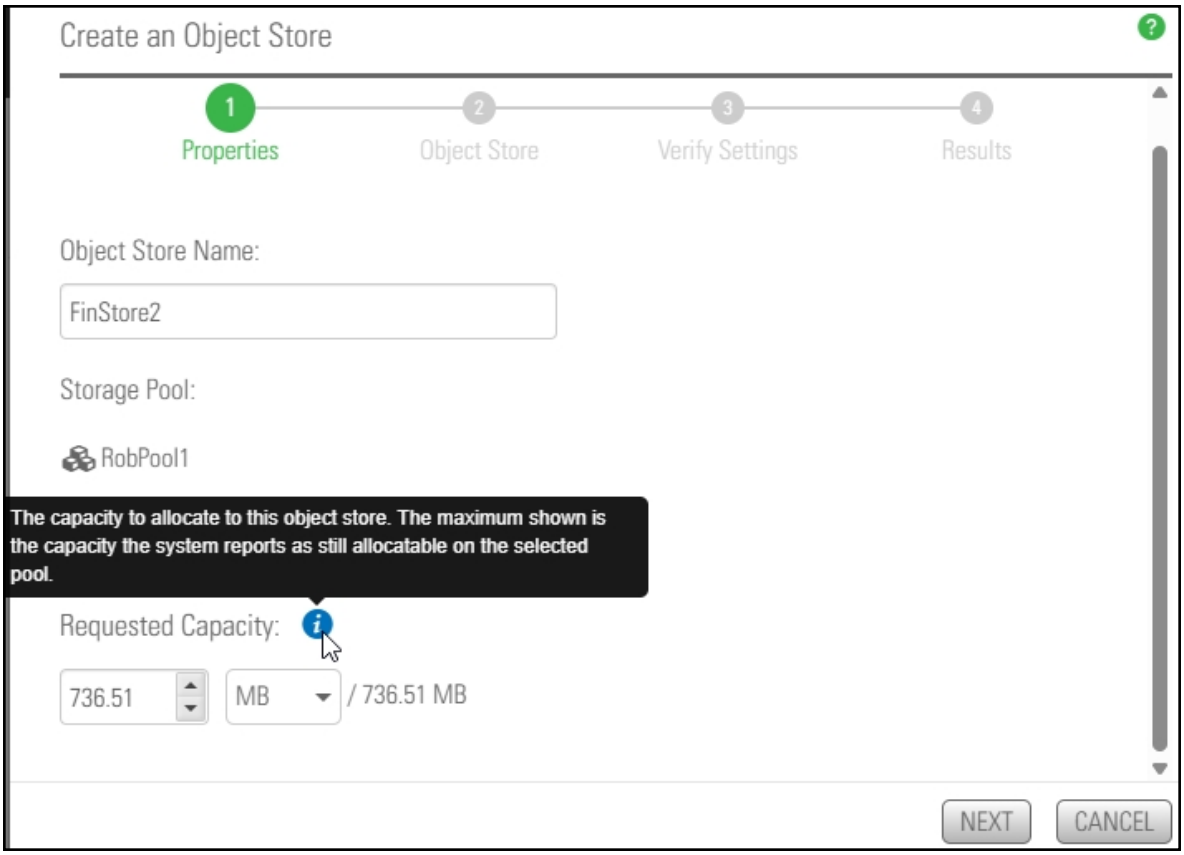
   ” / \ _ [ ] : ; | = , + * ? < >

   Under **Storage Pool**, click the drop-down arrow to select the pool for the object store (if there is more than one).

   Under **Requested Capacity**, enter a value equal to or greater than the 400 MB minimum. The maximum shown is the capacity the system reports as still allocatable on the selected pool.

   Click the **Next** button.

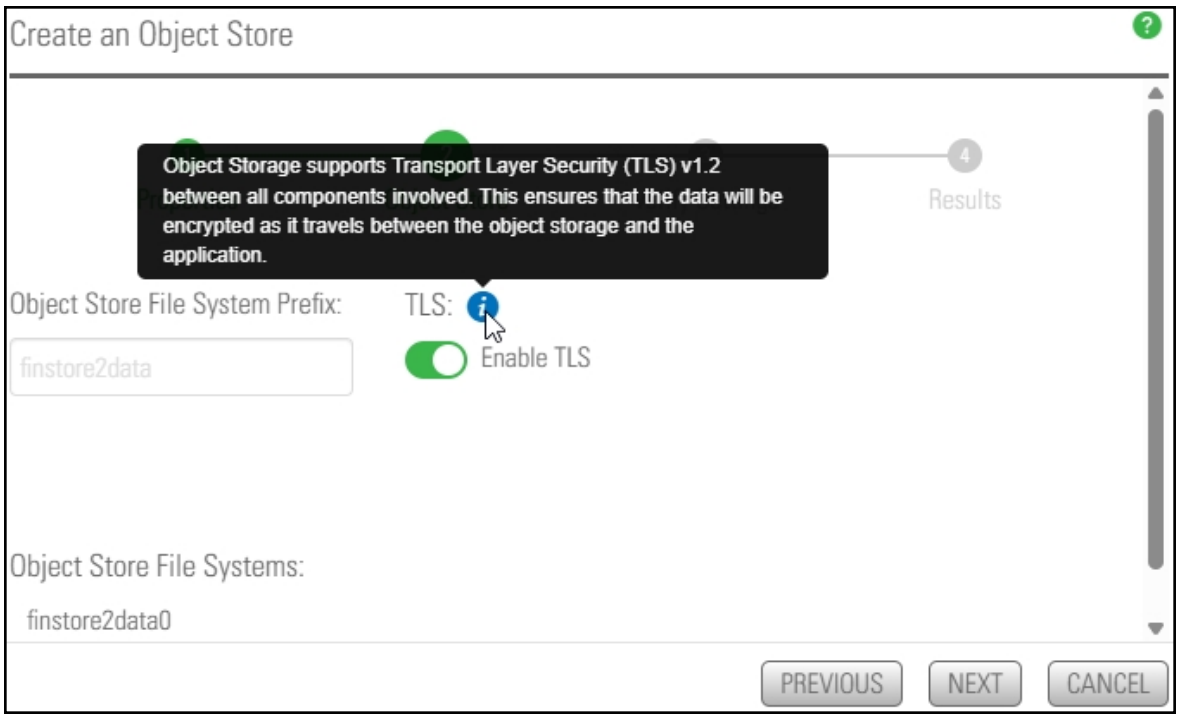
Figure 7-2: Create an Object Store wizard: Properties



3. In step **2** of the wizard, **Object Store**, the user can turn on End-to-End Transport Layer Security (TLS) between the object store and the application. Select **Enable TLS** (default) to activate this option.

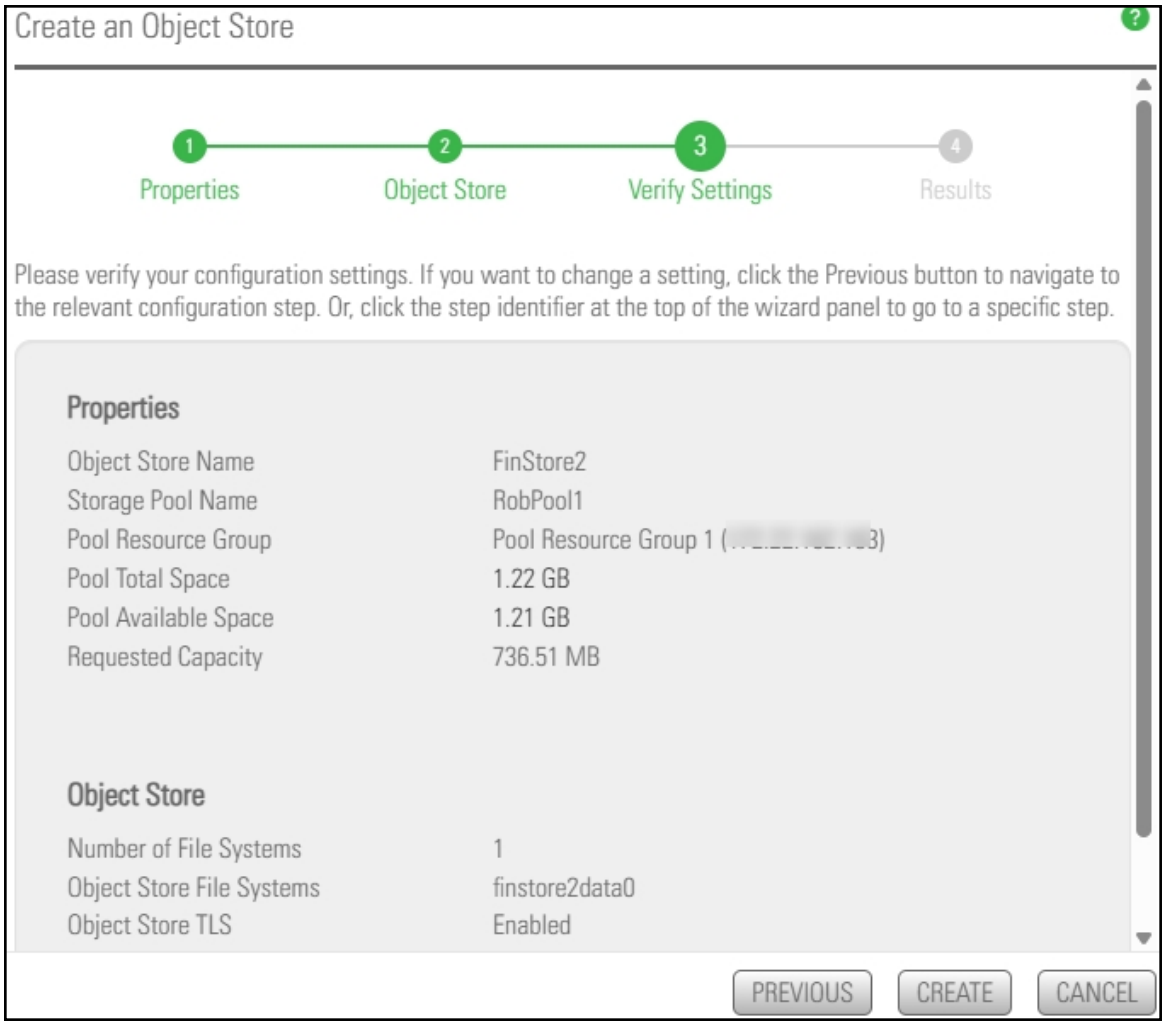
   Click the **Next** button.

Figure 7-3: Create an Object Store wizard:Transport Layer Security



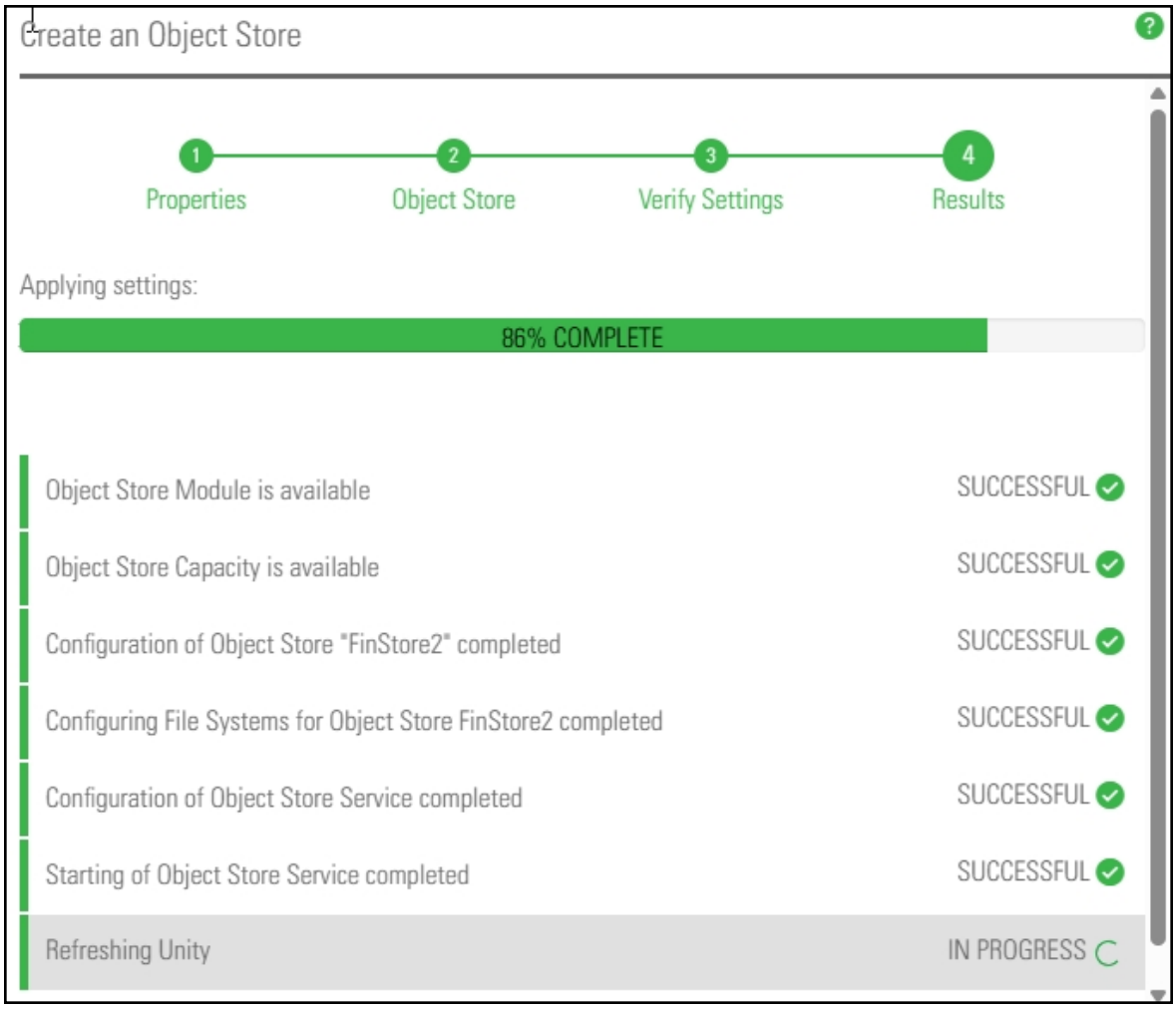
4. In step **3** of the wizard, **Verify Settings**, verify the configuration settings. To complete the process of creating a new object store, click the **Create** button. Unity will now start creating the object store as per the parameters set in the above steps.

Figure 7-4: Create an Object Store wizard: Verify Settings



5. In step **4** of the wizard, **Results**, all criteria within the configuration stages of the process should be marked **Successful**, indicated on the right. During the creation of the new object store, Unity creates four file systems. These file systems are available to store the user data objects. However, the user cannot edit the configuration and settings of these four file systems. The Unity object store manages how the user data is saved across these file systems.

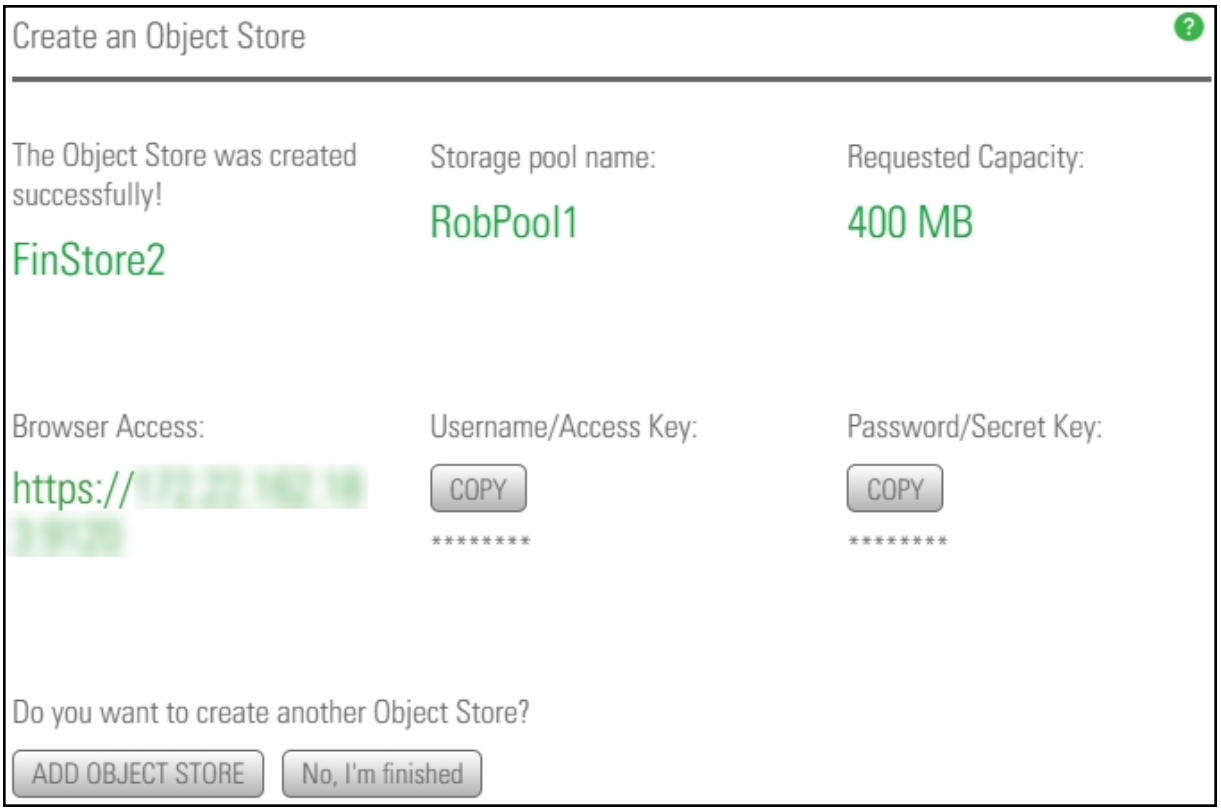
Figure 7-5: Create an Object Store wizard: Results



6. The Create an Object Store page will appear with an indiciation of successful creation, including relevant details for name, capacity, and browser access. If an error message appears, follow the directions to resolve.
   To create another object store, select **Add Object Store**. Otherwise select **No I'm finished**.

Note Click **Copy** for the **Username** and paste it to a safe place for reference. Do the same for **Password**.

Figure 7-6: Create an Object Store wizard: Successful creation



Viewing object store system information

Use this procedure to view object store information.

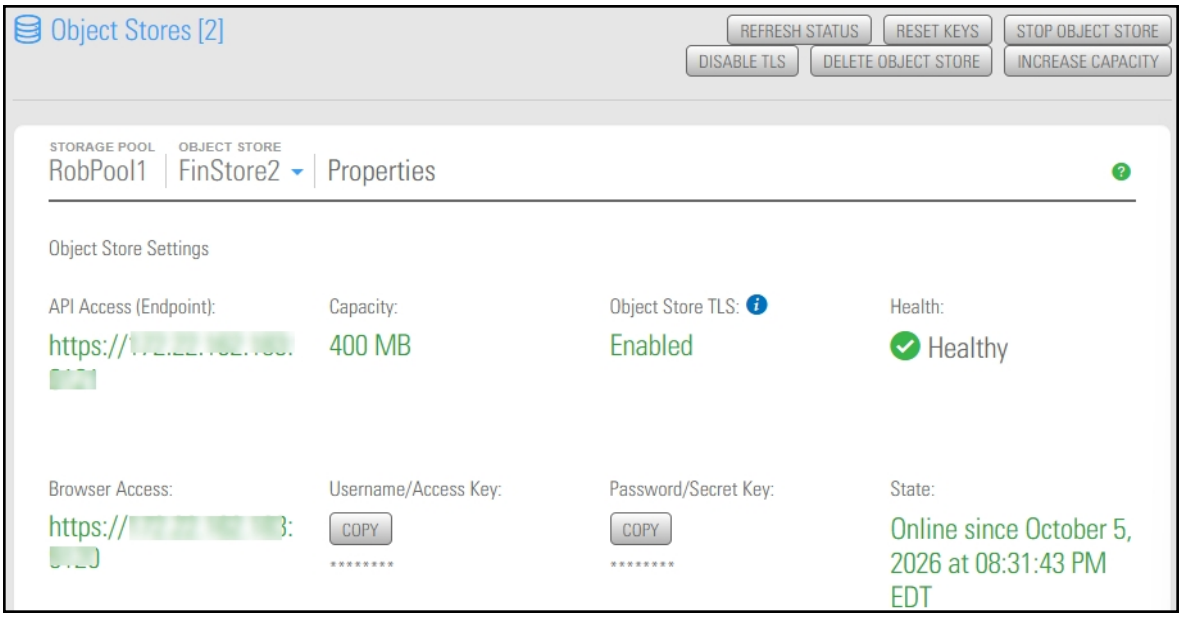
To view the properties of the object store:

1. On the **Unity navigation bar**, click **Storage > Object Stores**.The **Object Stores** page appears.
2. On the left side, under **Name**, select the object store by its name. The selected **Object Store Properties** page appears, displaying the properties of the object store.
3. On the top right, there are six buttons for the user to perform operations on the object store:
   a. **Refresh Status**
   b. **Reset Keys**
   c. **Stop Object Store**
   d. **Disable TLS**
   e. **Delete Object Store**
   f. **Increase Capacity**

   These six operations are further detailed in their appropriate sections in this manual.

   To the right of the name of the current object store, a **blue drop down arrow** appears. Click to select any other available object store.

Figure 7-7: Object store Summary information in Storage Pools



Enabling or disabling TLS on the object store

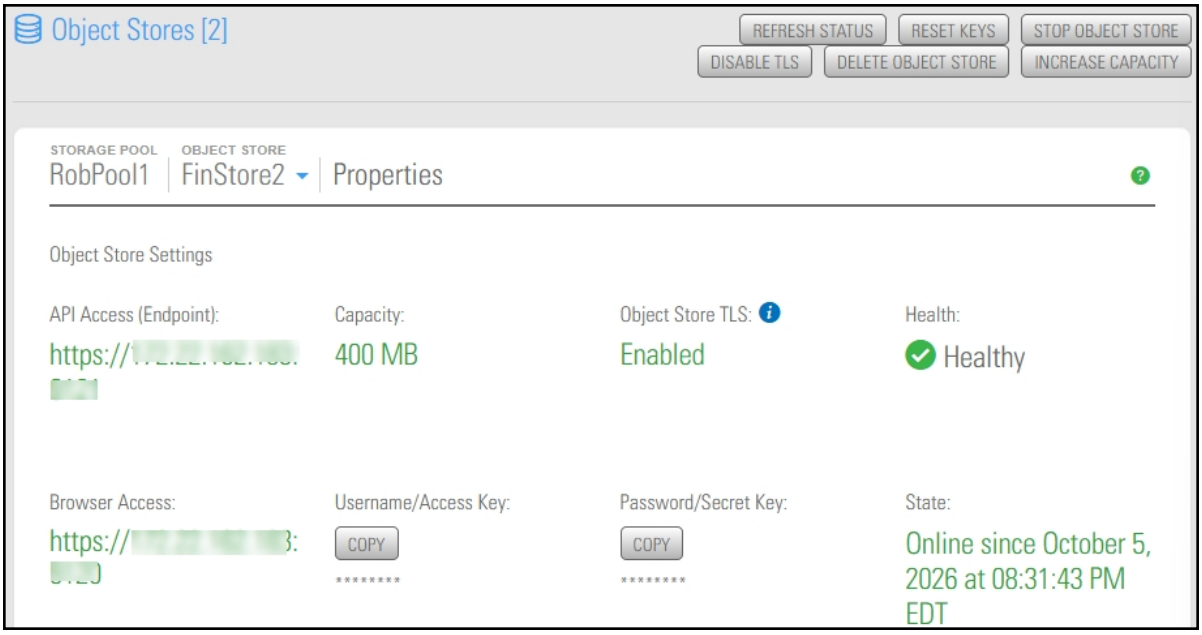
Use this procedure to enable or disable Transport Layer Security (TLS) on the object store.

Select TLS on an object store to set encryption of object data upload and download between the object store and the application.

▶ **To enable or disable Transport Layer Security (TLS) on the object store:**

1. On the **Unity navigation bar**, click **Storage > Object Stores**.The **Object Stores** page appears. In the Name column, click the name of the target object store.
2. The **Properties** page appears for the target object store. Click the **Enable** (or **Disable**) **TLS** button. Current status is indicated under the **Object Store TLS** heading.

Figure 7-8: Enable or Disable TLS



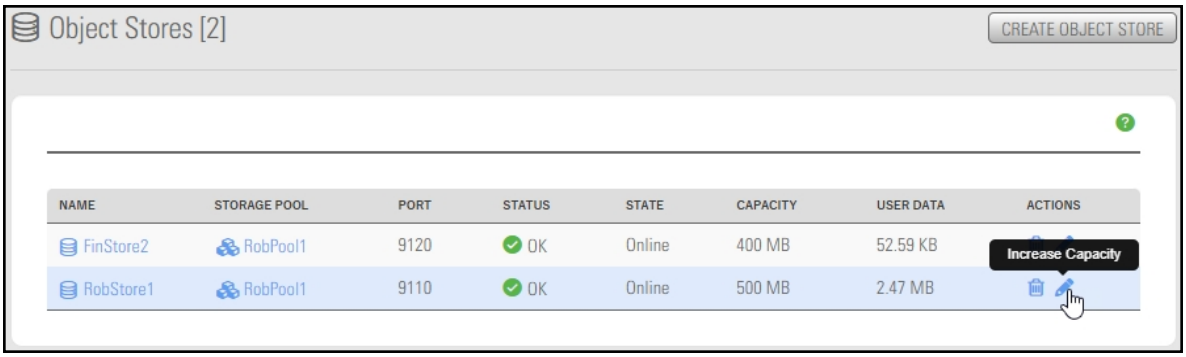
Increasing storage capacity for object stores

Use this procedure to increase the storage capacity for object stores.

To increase the storage capacity of an object store:

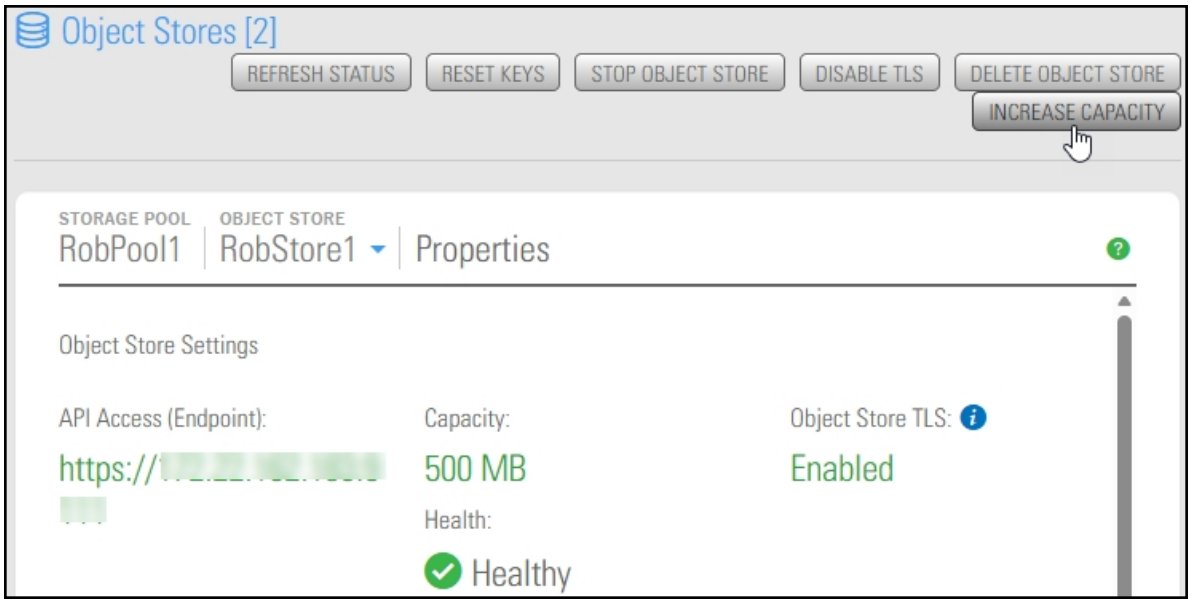
1. On the **Unity navigation bar**, click **Storage > Object Stores**.The **Object Stores** page appears.
2. In the **Actions** column, for the target object store, click the **Increase Capacity** icon, as shown.

Figure 7-9: Increase capacity for an object store, Actions on summary page



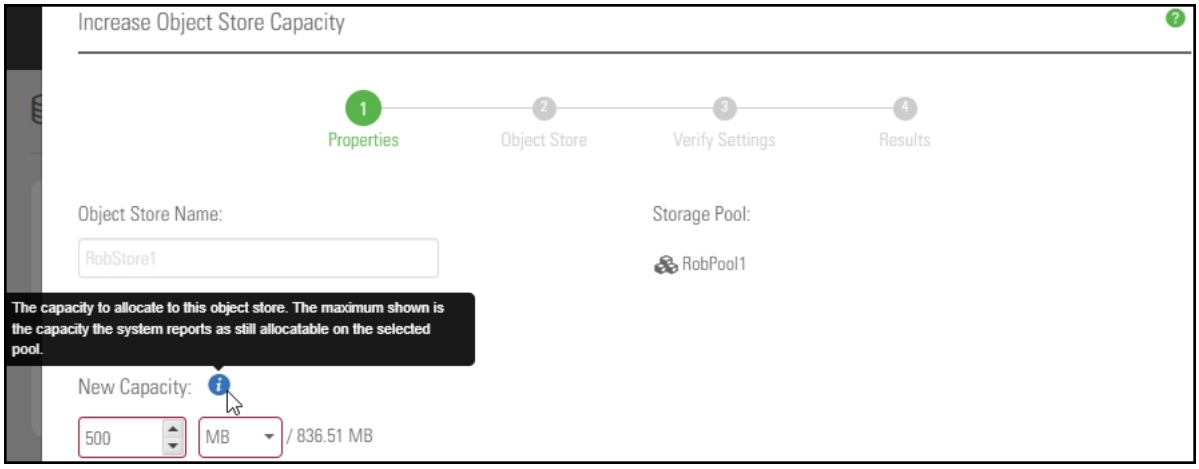
Alternately, from the **Object Store Properties** page, click the **Increase Capacity** button on the top right, as shown.

Figure 7-10: Increase capacity for an object store, button on Object Store properties page



3. The Object Store Wizard launches to step **1**, **Increase Object Store Capacity**.

Figure 7-11: Object Store wizard - Increase object store capacity



4. Under **New Capacity**, enter a new value to increase the existing capacity. The maximum shown is the capacity the system reports as still allocatable on the selected pool.
5. Click **Next** for steps **1** and **2**. In step **3**, click **Increase** to confirm the increase. In step **4**, **Results**, the new setting applies and a confirmation screen appears with the new capacity. Click **Close**.

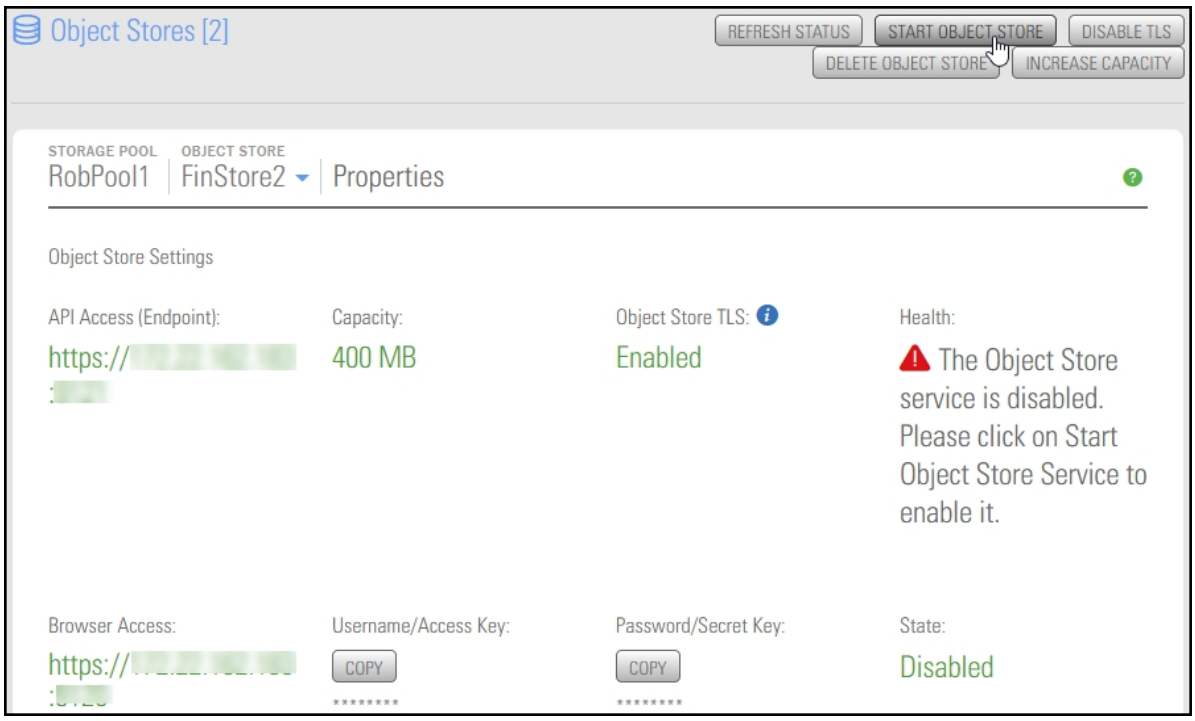
Starting the service for an object store

Use this procedure in Unity to enable the service for an object store.

To start the service for an object store:

1. On the **Unity navigation bar**, click **Storage > Object Stores**.The **Object Stores** page appears. In the **Name** column, click the name of the target object store.
2. The **Properties** page appears for the target object store. Under the **Health** heading, the status of the object store service is disabled. Click **Start Object Store** on the top right of the page to enable the service.

Figure 7-12: Object Store properties page



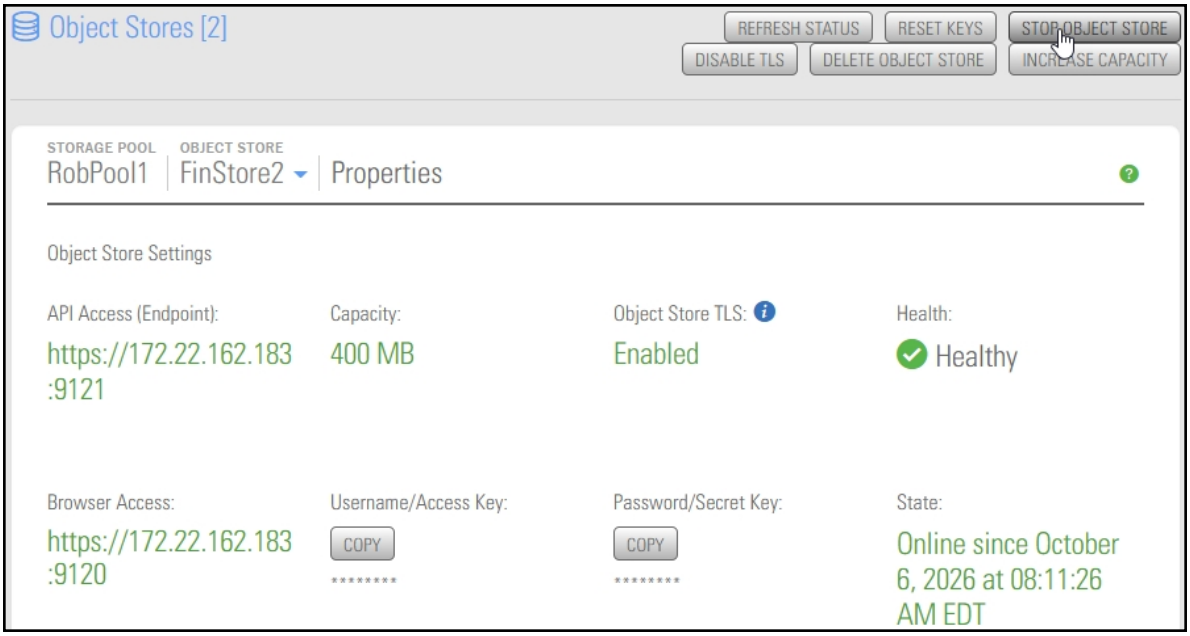
Stopping the service for an object store

Use this procedure in Unity to disable the service for an object store.

To stop the service for an object store:

1. On the **Unity navigation bar**, click **Storage > Object Stores**.The **Object Stores** page appears. In the **Name** column, click the name of the target object store.
2. The **Properties** page appears for the target object store. Under the **Health** heading, the status of the object store service indicates Healthy. Click **Stop Object Store** on the top right of the page to disable the service.

Figure 7-13: Object Store properties page



Deleting an object store

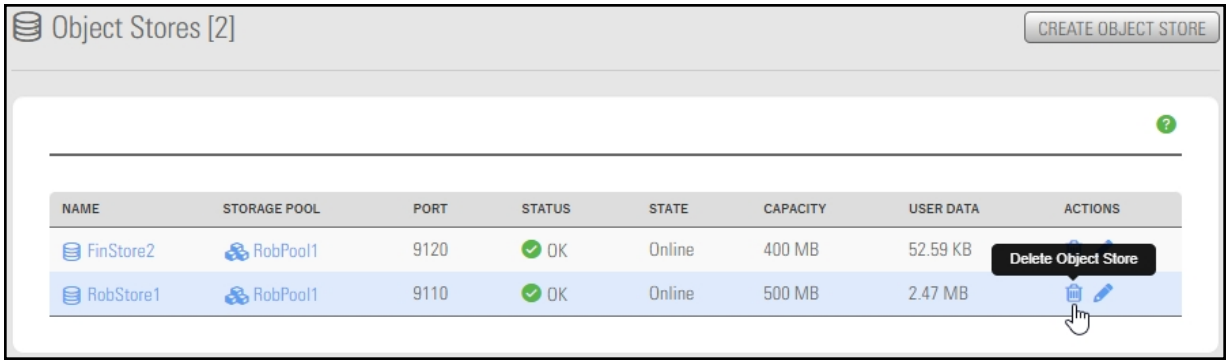
Use this procedure to delete an object store in Unity.

To delete an object store:

On the **Unity navigation bar**, click **Storage > Object Stores**. The **Object Stores** page appears.

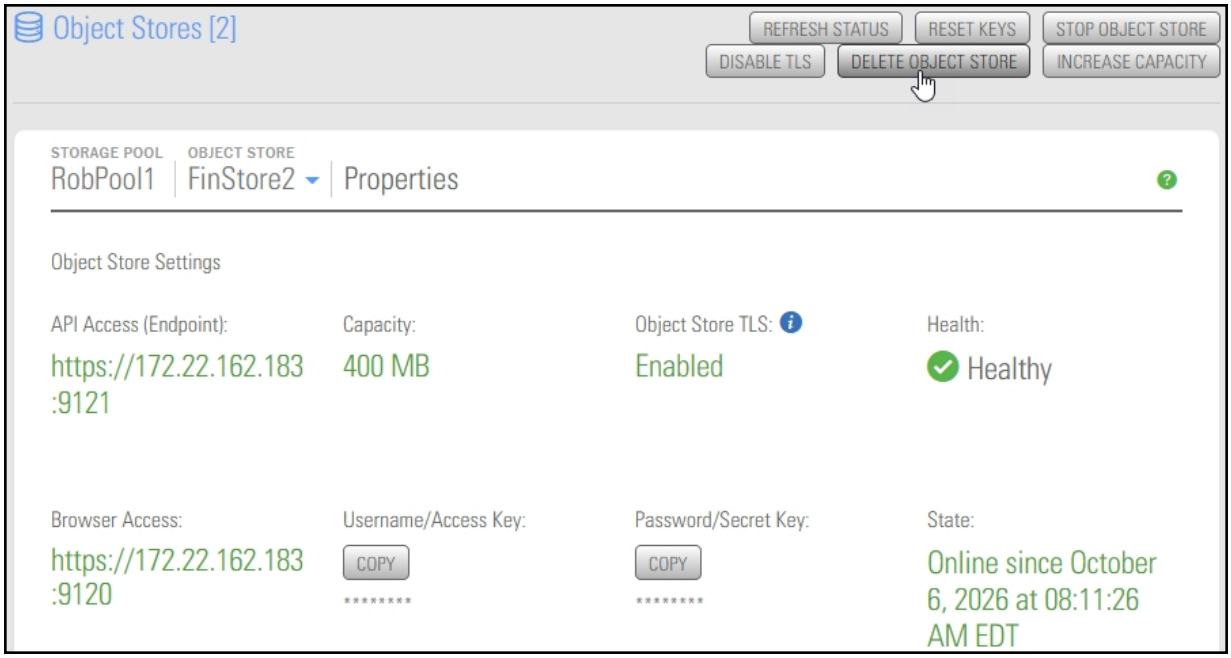
In the **Actions** column, for the target object store, click the **Delete Object Store** icon, as shown.

Figure 7-14: Deleting an object store from Object Stores page



Alternately, from the **Object Store Properties** page, click the **Delete Object Store** button on the top right, as shown.

Figure 7-15: Deleting an object store from Object Store Properties page



Resetting object store keys

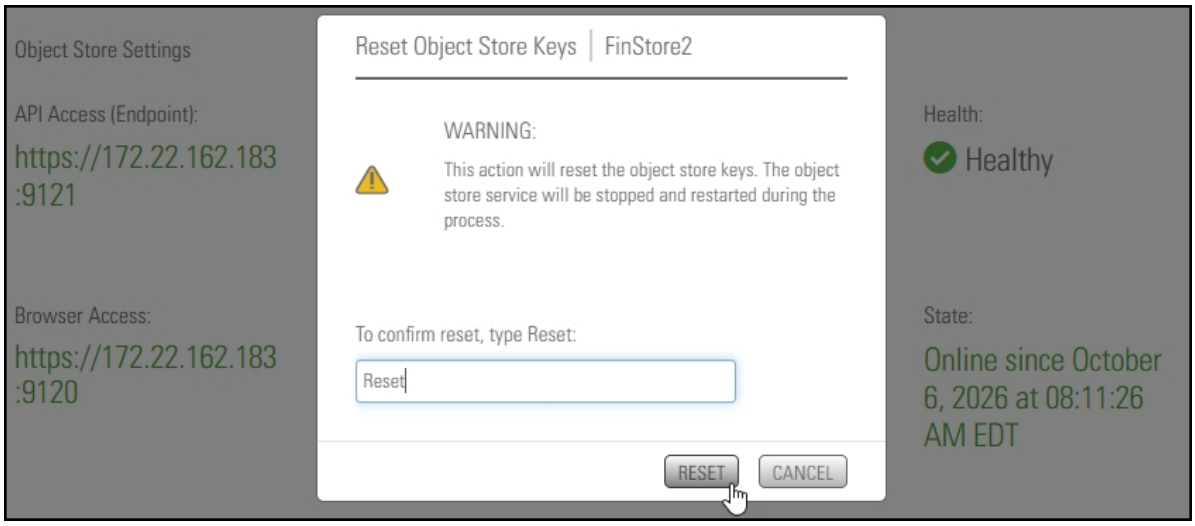
Use this procedure to reset keys for an object store.

To reset keys for an object store:

1. On the **Unity navigation bar**, click **Storage > Object Stores**.The **Object Stores** page appears. In the **Name** column, click the name of the target object store.
2. Click the **Reset Keys** button on the top right.

   The **Reset Object Store Keys** dialog box appears. To perform the reset, type in 'Reset', then click the **Reset** button.

Figure 7-16: Resetting keys for an object store



Accessing the NexObject Web client

Access a Unity Object Store using the Nexsan NexObject Web-based client interface. Two keys are required by the user to access the object store, the Access Key (or Username) and the Secret Key (or Password).

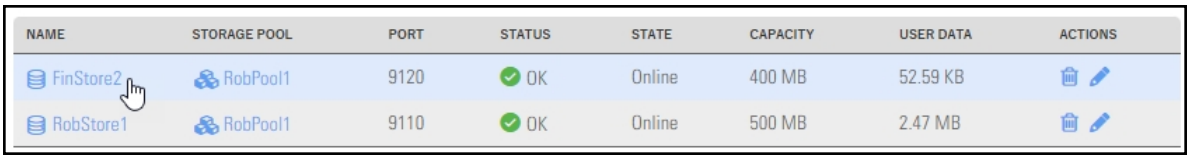
Note Each object store has a Web client that is unique. Object store Web clients are independent of each other.

Use this procedure to enable user access to the object store by the system administrator.

To provide access to the object store client:

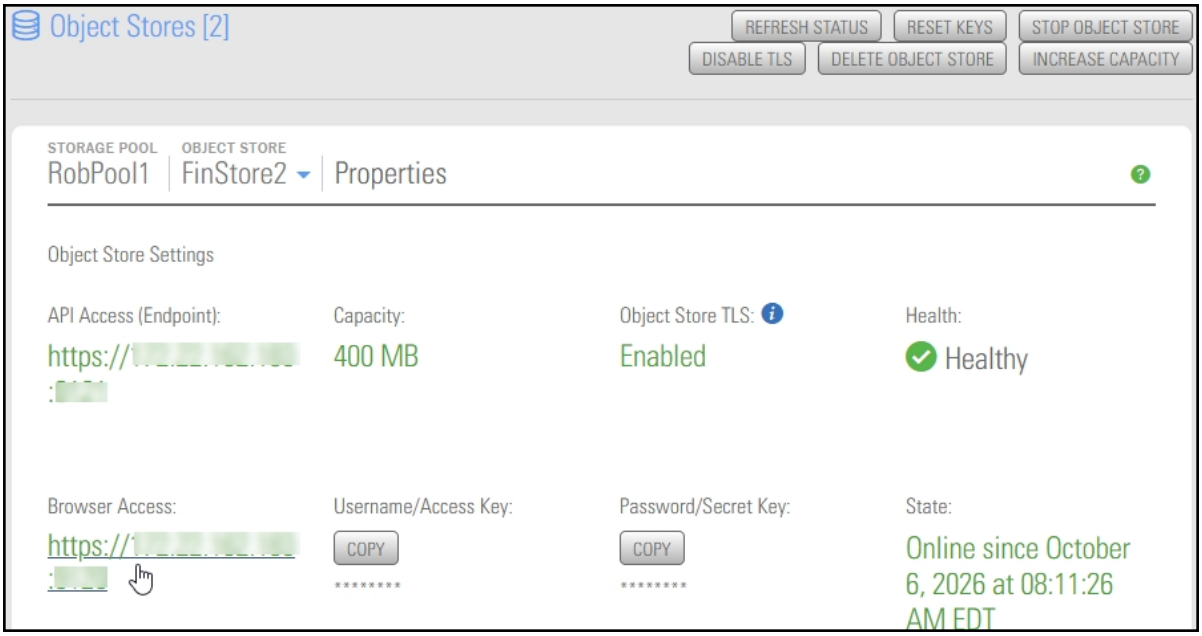
1. On the **Unity navigation bar**, click **Storage > Object Stores**.
2. The **Object Stores** page appears. In the **Name** column, click the name of the target object store.

Figure 7-17: Object Stores page



3. The selected object store **Properties** page appears. On the left side, under **Browser Access**, click the URL for the object store.

Figure 7-18: Object Store Properties page



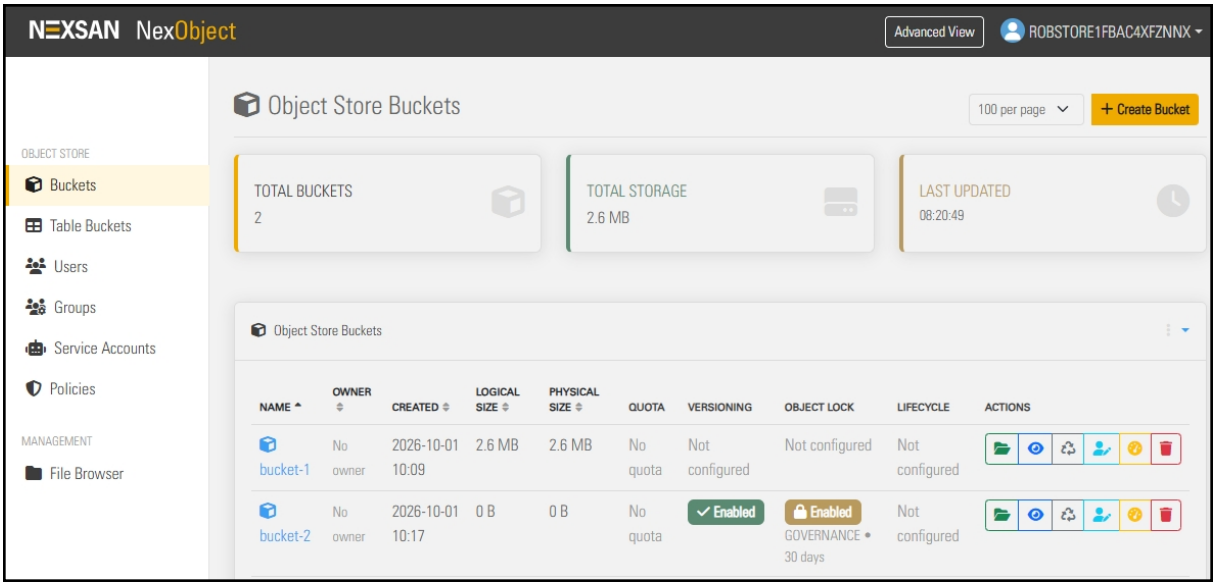
4. A separate browser tab or window launches the client access page with the selected IP address, along with a field for the object store **Username** and **Password**.
   A. From the Unity **Object Store** page, click the **Copy** button under **Username/Access Key**. In the NexObject client access page, click paste in the **Username** field.
   B. From the Unity **Object Store** page, click the **Copy** button under **Password/Secret Key**. In the NexObject client access page, click paste in the **Password** field.
   C. Click **Sign in** on the NexObject client access page.

Figure 7-19: NexObject Web client sign-in panel



5. The **NexObject** default home page appears, with a list of the current Object Store Buckets.

Figure 7-20: NexObject home page



On the left side panel under **Object Store**, several Administrative functions are available: **Buckets** (default view), **Table Buckets**, **Users**, **Groups**, **Service Accounts**, and **Policies**. Under **Management**, a **File Browser** function is available to manage content assets. Each of these functions is detailed in a separate section of this guide.
Close the session by selecting the object store name on the top navigation bar far right, then click **Logout**.

Creating a data bucket using the Web client

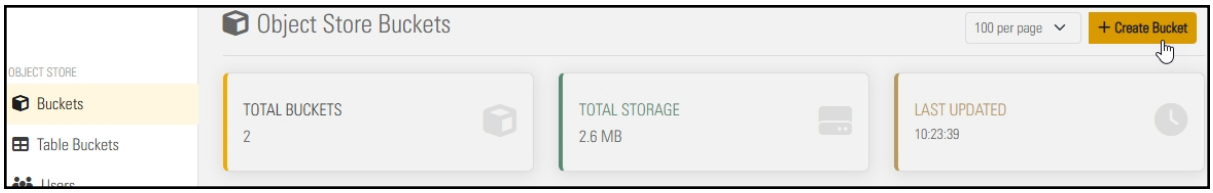
Use this procedure to create a new object store data bucket using the NexObject Web client. The data is typically unstructured, and can include text files, images, and audio or video files.

Note Each object store has a Web client that is unique. Object store Web clients are independent of each other.

▶ **To create an object store bucket:**

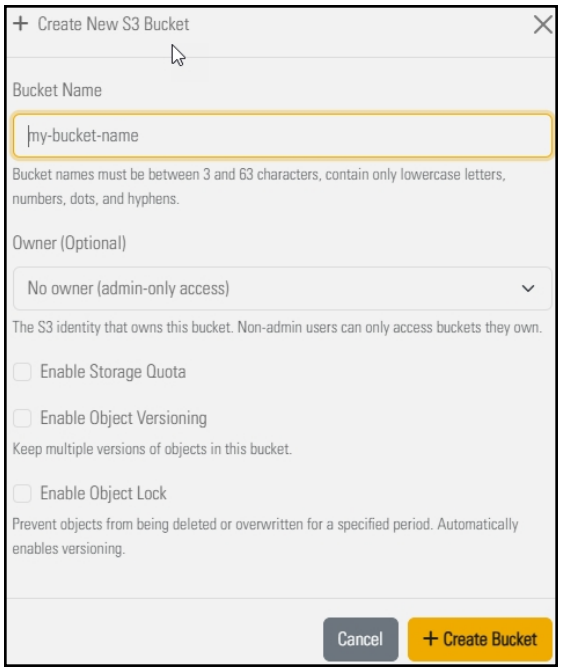
1. From the **NexObject Browser** default home page, click the link to get started, **Create Bucket**.

Figure 7-21: NexObject home page select Create Bucket



2. The **Create New S3 Bucket** pop-up appears. Enter a **Bucket Name** in the field, which must be between 3 and 63 characters, contain only lowercase letters, dots, numbers, and hyphens.
3. Select **Owner** and choose from the available options. Optionally, click any or all of the check boxes to **Enable Storage Quota**, **Enable Object Versioning**, and/or **Enable Object Lock**.
   When done, click **Create Bucket**.

Figure 7-22: Create New S3 Bucket pop-up



4. The Object Store Buckets page appears, with a list that includes the newly created bucket and associated properties in the table: **Name**, **Owner**, **Created**, **Logical Size**, **Physical Size**, **Quota**, **Versioning**, **Object Lock**, **Lifecycle**, and **Actions**.

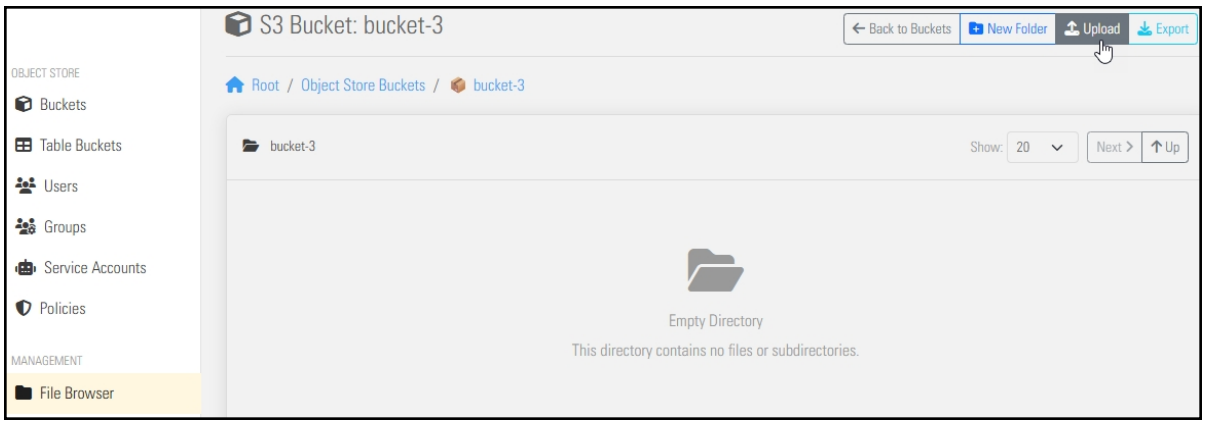
5. From the Actions (Browse Files, View Details, Lifecycle Rules, Manage Owner, Manage Quota, Delete Bucket) column, select the first icon, **Browse Files**.

Figure 7-23: Browse Files icon from Actions column of Object Store Buckets page



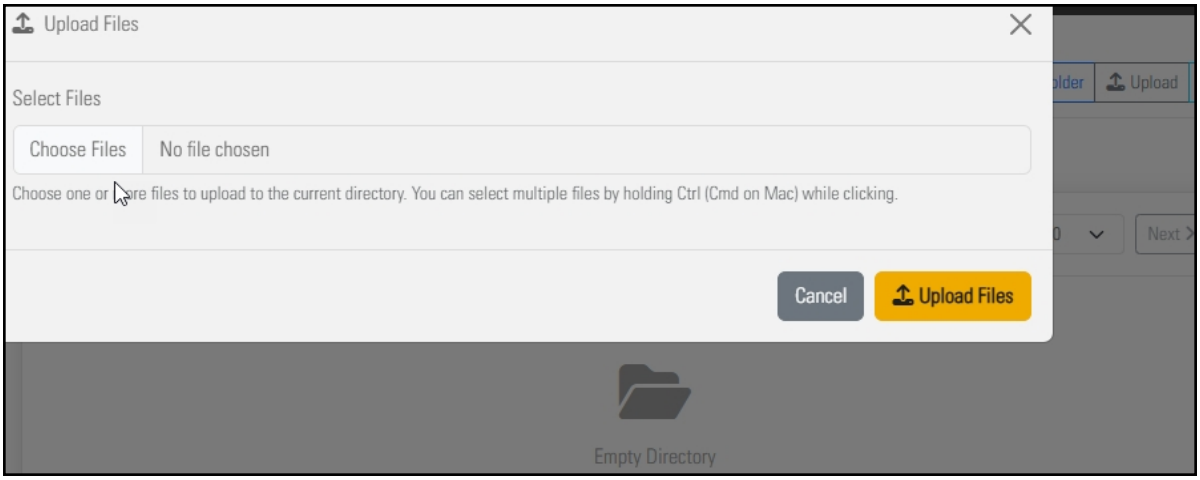
6. The S3 Bucket page appears, with the name of the newly created bucket. To add files, click the **Upload** button on the top right.

Figure 7-24: Upload files to a Bucket in the object store



7. Click **Choose Files** to launch your operating system file manager, then select files or folders for upload. When done, click the **Upload Files** button. The system displays a progress bar for each upload item, and when completed renders the file details on the bucket content page.

Figure 7-25: Upload Files page, select Choose Files



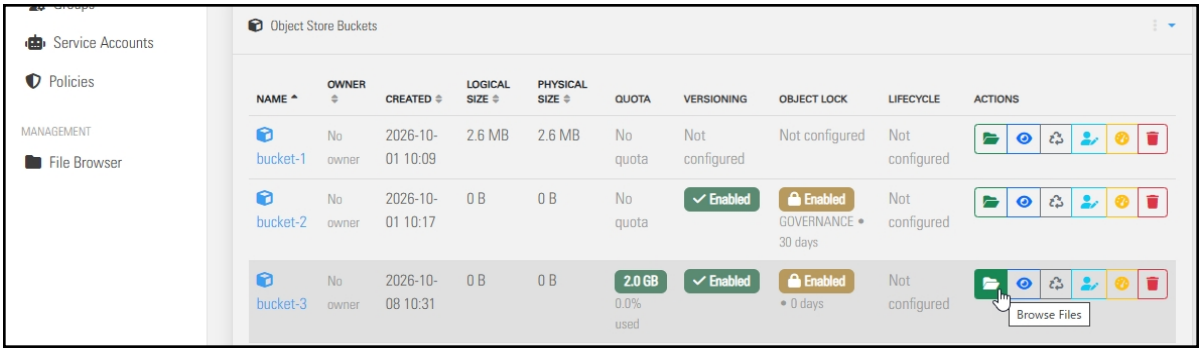
Adding data to an object store bucket

Use this procedure to add data to a newly created or to an existing object store bucket.

To add data to an object store bucket:

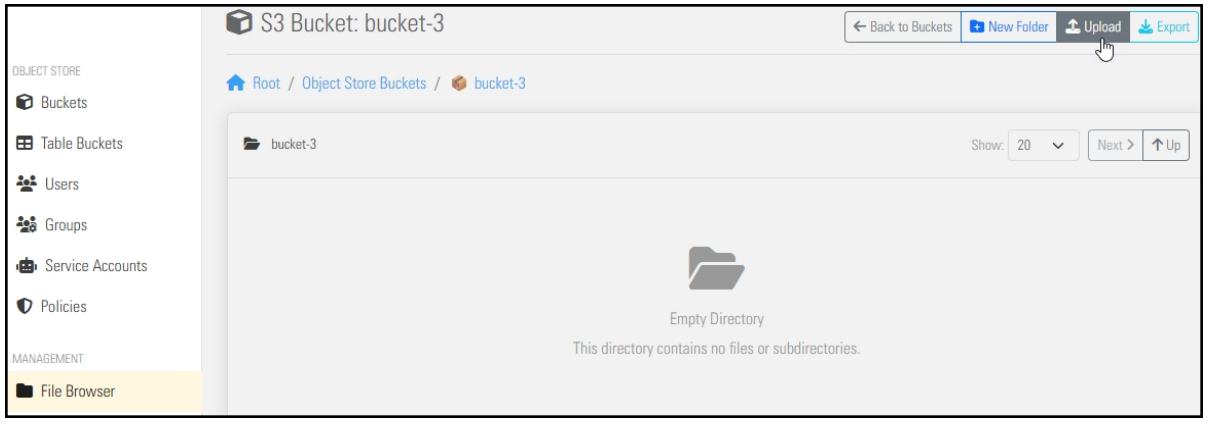
1. From the **Actions** (Browse Files, View Details, Lifecycle Rules, Manage Owner, Manage Quota, Delete Bucket) column, select the first icon, **Browse Files**.

Figure 7-26: Object Store Buckets page - Browse Files icon



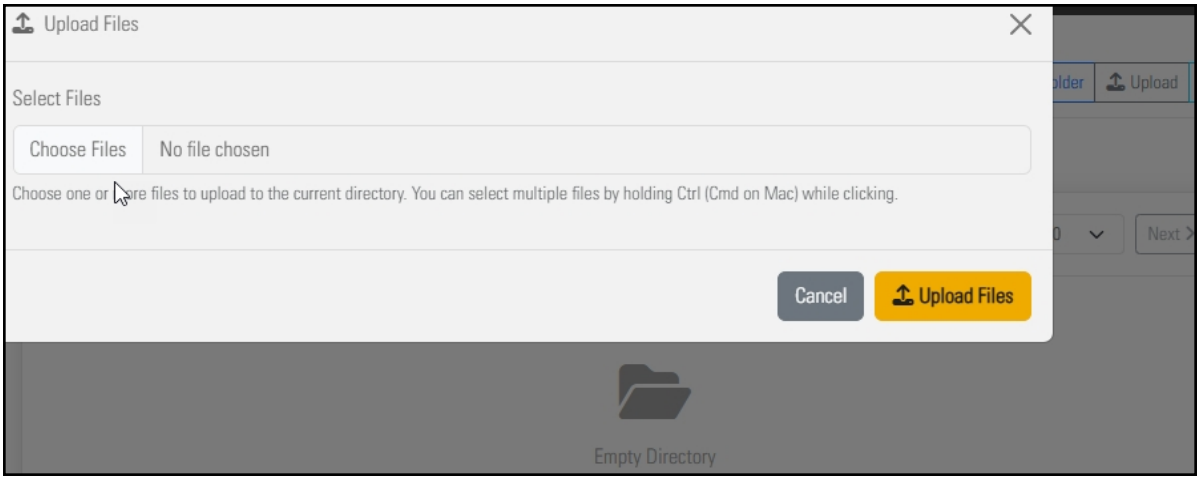
2. The S3 Bucket page appears with the newly created bucket name. Click the **Upload** button on the top right .

Figure 7-27: Upload files to a bucket in the object store



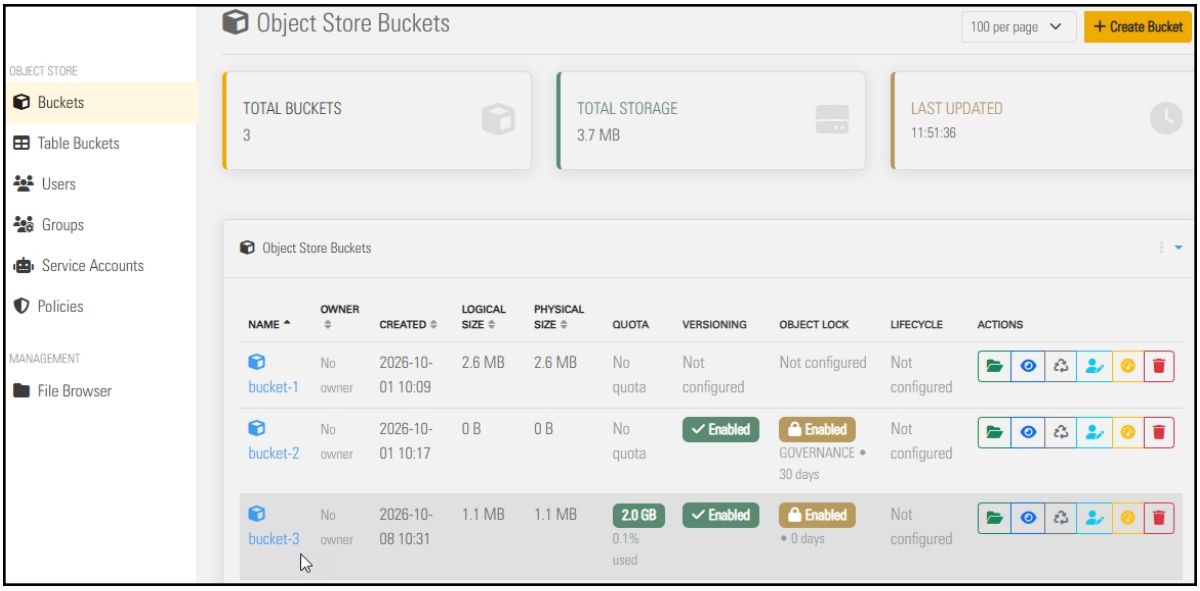
3. Click **Choose Files** to launch your operating system file manager, then select files or folders for upload. Chosen files or folders appear on the page. When done, click the **Upload Files** button.

Figure 7-28: Upload Files page, select Choose Files



4. The Object Store Buckets page reappears, with the newly created bucket and its associated details in a new row of the table.

Figure 7-29: Object Store Buckets page with newly created bucket listed



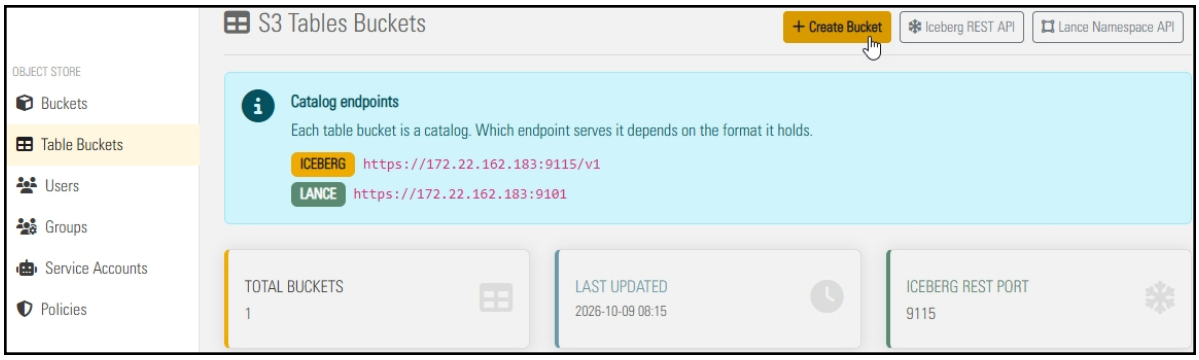
Creating an object store S3 Table Bucket

An S3 Table Bucket is a specialized type of container designed to specifically store and manage structured, tabular data using an open-source table format. While traditional general-purpose S3 buckets store raw, standalone files or objects, an S3 table bucket acts as a built-in analytics database and catalog. Nexsan's NexObject supports two different open-standard access protocols used to interact with data stored inside an S3 table bucket: Iceberg REST API and Lance Namespace API.

To create an S3 table bucket:

1. From the object store main page, select **Table Buckets** on the left side menu. Click the **Create Bucket** button on the top right.

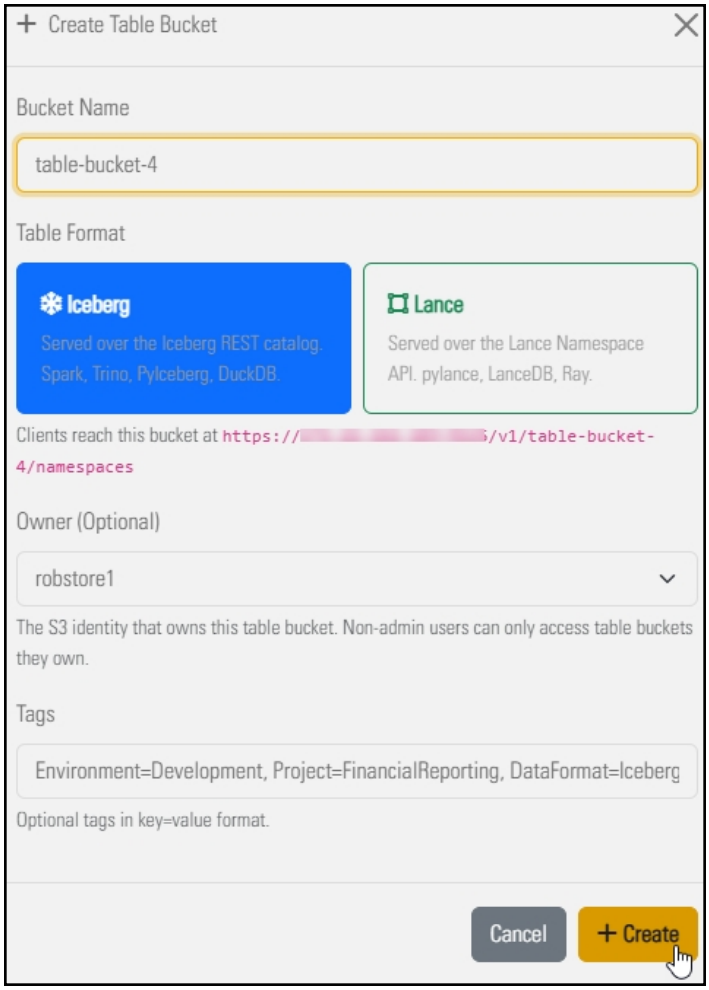
Figure 7-30: S3 Tables Buckets page, click Create Bucket



2. The **Create Table Bucket** pop-up appears. Enter a **Bucket Name** in the field, which must be between 3 and 63 characters, contain only lowercase letters, dots, numbers, and hyphens.

3. Select the **Table Format**, **Iceberg** (default) or **Lance**. Iceberg is served over the Iceberg REST catalog. Spark, Trinio, Pylceberg, DuckDB. Lance is served over the Lance Namespace API. Pylance, LanceDB, Ray. Note the IP Address at which Clients can reach the bucket.

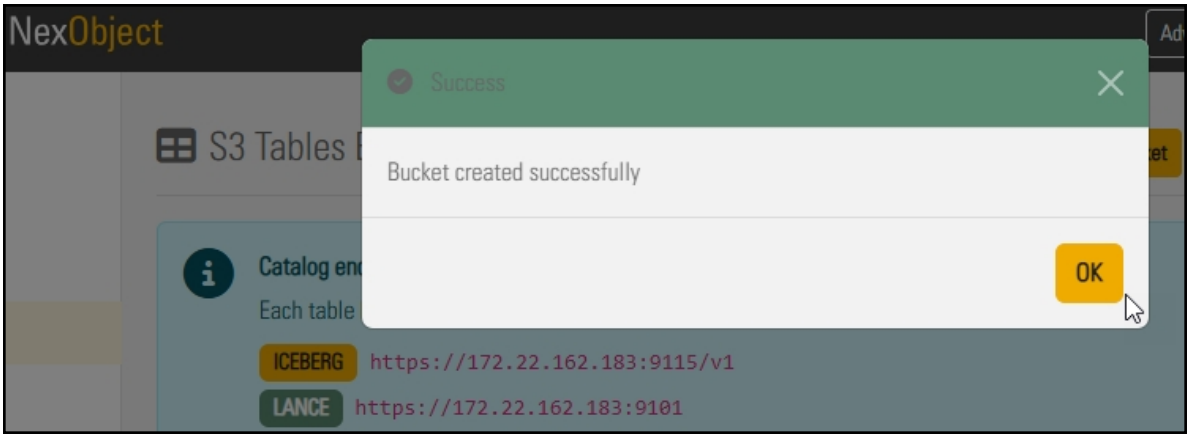
Figure 7-31: Create Table Bucket pop-up



4. Select the **Owner** (Optional) using the drop-down arrow in the field. This is the S3 identity that owns the table bucket. Non-admin users can only access table buckets they own. The default value is No owner (admin-only access). Other selections include previously created user names.
5. Create **Tags** (optional). The format is **key=value**.
   For example: Environment=Development, Project=FinancialReporting, DataFormat=Iceberg, Component=DataWarehouse, Owner=JaneDoe, Compliance=SOX.
6. When done, click the **Create** button.

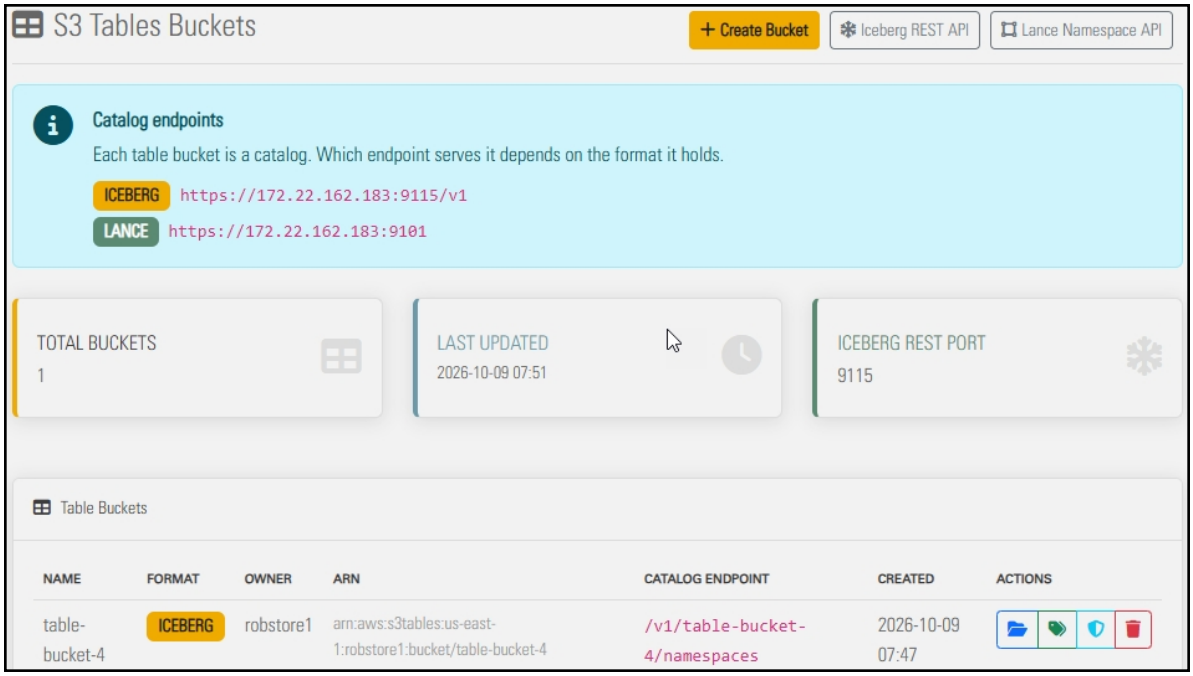
7. A pop-up appears, **Bucket created successfully**. Click **OK**.

Figure 7-32: Bucket created successfully pop-up



8. The S3 Tables Buckets page reappears, with the newly created table bucket in a new row. The columns provide information on the **Name**, **Format**, **Owner**, **ARN**, **Catalog Endpoint**, and date **Created**. The **Actions** column includes icons for **Namespaces**, **Tags**, **Bucket Policy**, and **Delete**.

Figure 7-33: S3 Tables Buckets page



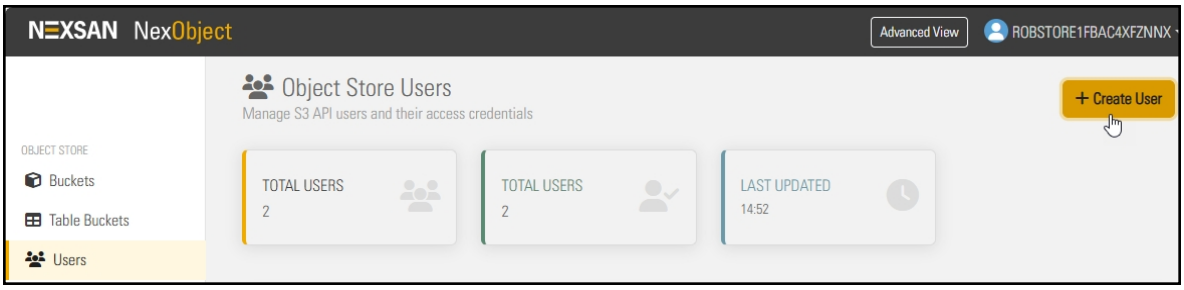
Creating an object store user

Create an S3 API user and with access credentials using NexObject administrative functions.

To create a new user:

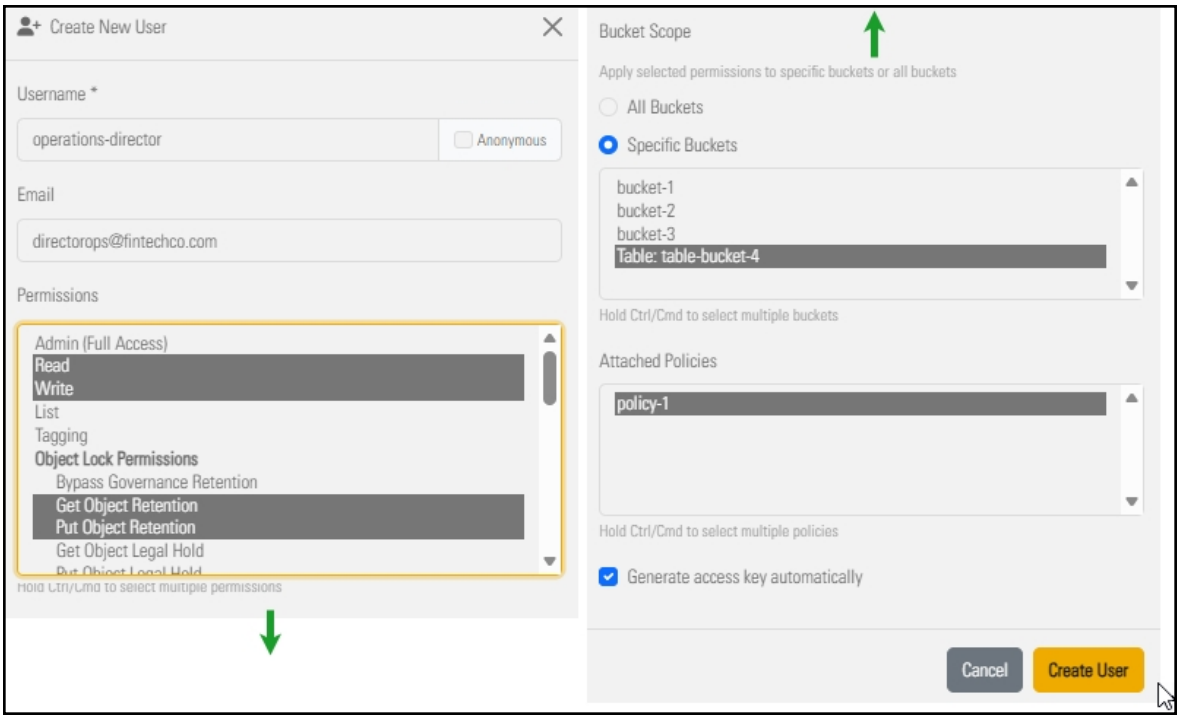
1. From the object store main page, select **Users** on the left side menu.
2. The Object Store Users page appears. Click the **Create User** button on the upper right side.

Figure 7-34: Object Store Users page - Create User



3. The **Create New User** pop-up appears.
   Complete the fields with user details: **Username** (required), **Email**, **Permissions**, **Bucket Scope**, and **Attached Policies**. When done, clidk the **Create User** button.

Figure 7-35: Create New User pop-up



4. The **New Access Key Created** pop-up appears.
   Verify the information. Click the **copy icon** for any of the fields to copy the information to the clipboard.
   Click **Close** to return to the object store main page.

Figure 7-36: New Access Key Created pop-up



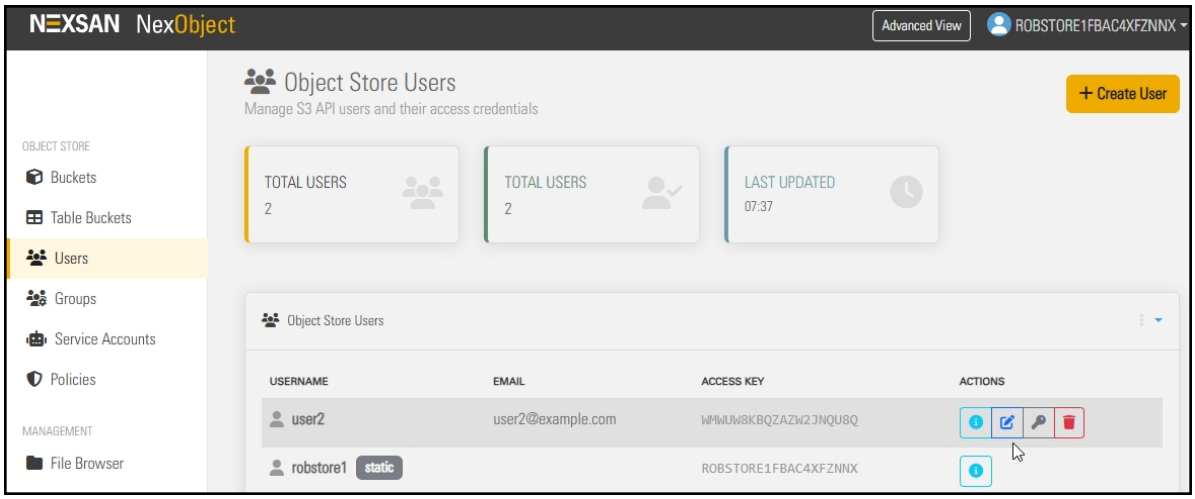
Managing object store users

Manage S3 API users and their access credentials using NexObject administrative functions.

To view existing users:

1. From the object store main page, select **Users** on the left side menu.
2. The Object Store Users page appears. Existing users are listed in a table with the columns **Userrname**, **Email**, **Access Key**, and **Actions**. The following Action icons are available to manage the users: **Information**, **Edit user**, **Manage access keys**, **Delete user**. Each of these is described in the sections that follow.

Figure 7-37: Object Store Users page - Actions



To view users information:

1. In the **Actions** column, click the **Information** icon.
2. The **User Details** pop-up appears, with corresponding read-only information including **Username**, **Email**, **Permissions**, **Policies**, **Groups**, and **Access Keys**. Click **Close** to return to the Object Store Users page.

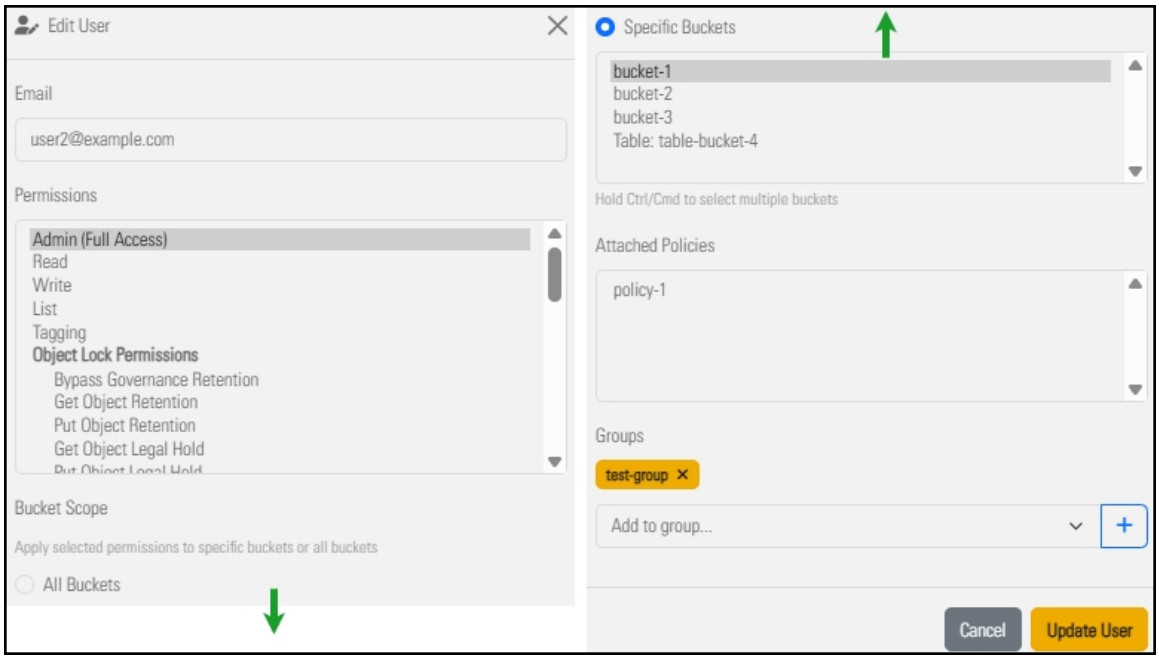
Figure 7-38: User Details pop-up for Object Store Users



To edit user details:

1. In the **Actions** column, click the **Edit user** icon.
2. The **Edit User** pop-up appears. Click within any of the fields to change existing settings for the selected User, including **Email**, **Permissions**, **Bucket Scope**, **Attached Policies**, and **Groups**. When done, click the **Update User** button at the bottom right of the pop-up.

Figure 7-39: Edit User pop-up for Object Store Users



To manage access keys:

1. In the **Actions** column, click the **Manage access keys** icon for a selected User row.
2. The **Manage Access Keys** pop-up appears for the User.
   - In the **Status** column, click the drop-down arrow to set between **Active** or **Inactive**.
   - Under **Actions**, click **View Secret** to reveal the **Access Key Details**
   - Click the **Create New Key** button to create a new access key for the User.
   - Use the **Delete** button to remove the User. A confirmation pop-up appears to complete the action.

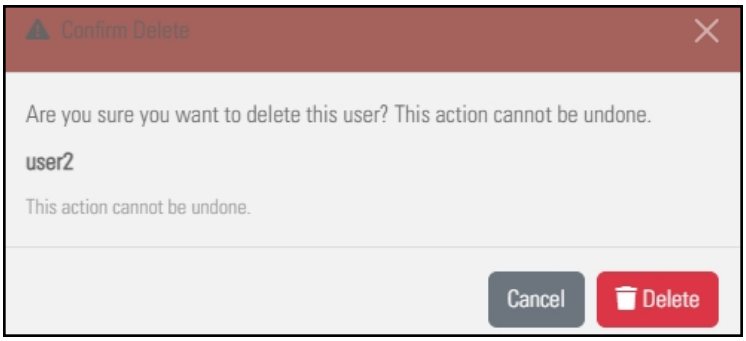
Figure 7-40: Manage Access Keys pop-up for Object Store Users



To delete a user:

1. In the **Actions** column, click the **Delete** icon for a selected User row.
2. The **Confirm Delete** pop-up appears for the User. Click **Delete** to confirm.

Figure 7-41: Confirm Delete pop-up for Object Store Users



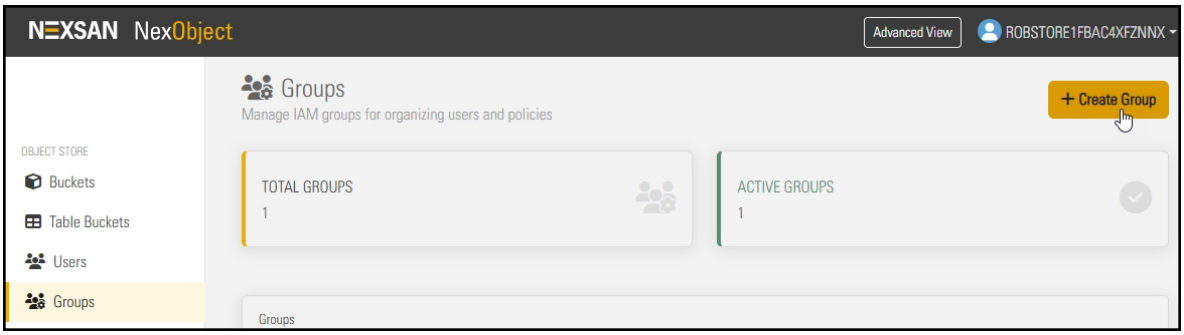
Creating and managing object store groups

Create IAM (Identity and Access Management) groups for organizing object store users and policies.

► To create a new group:

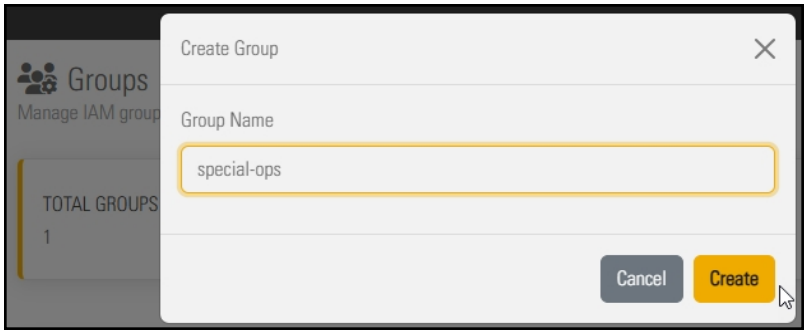
1. From the object store main page, select **Groups** on the left side menu.
2. The Groups page appears. Click the **Create Group** button on the upper right side..

Figure 7-42: Object Store Groups page - Create Group



3. The **Create Group** pop-up appears.
   Enter a **Group Name** in the field, then click **Create**.

Figure 7-43: Create Group pop-up

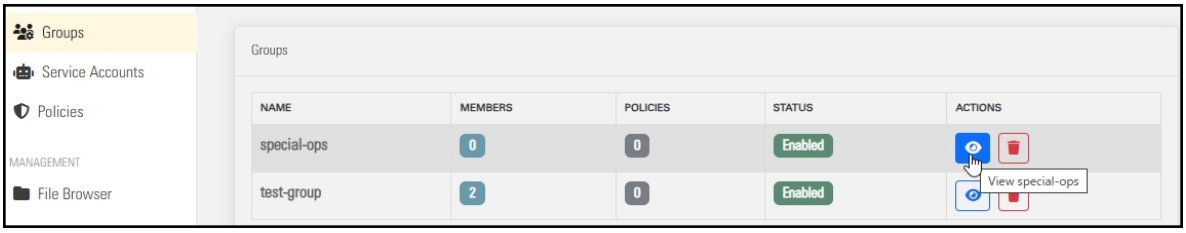


4. The **Group created successfully** pop-up appears.
   Click **Close** to dismiss and return to the Groups page.

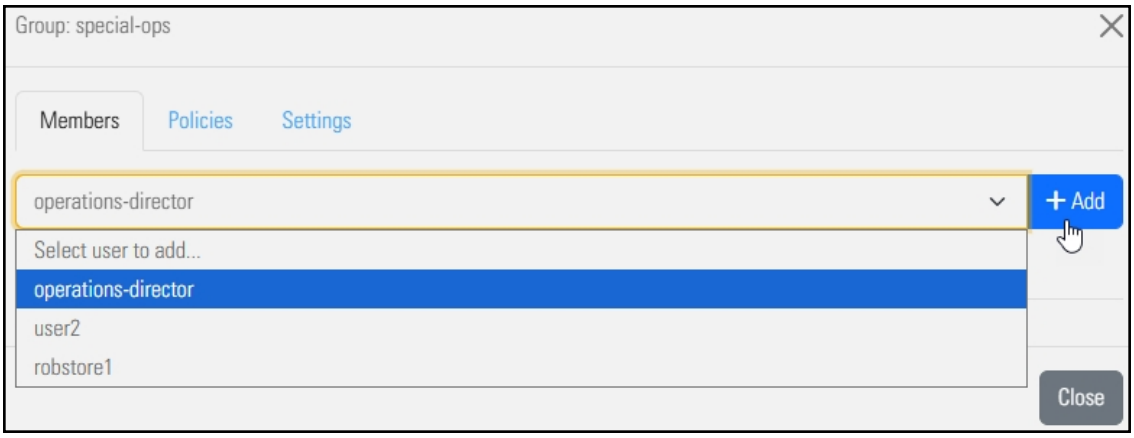
► To view and edit group details:

1. From the **Groups** page, in the list of available Groups, select the **View** icon in the **Actions** column for the target group.

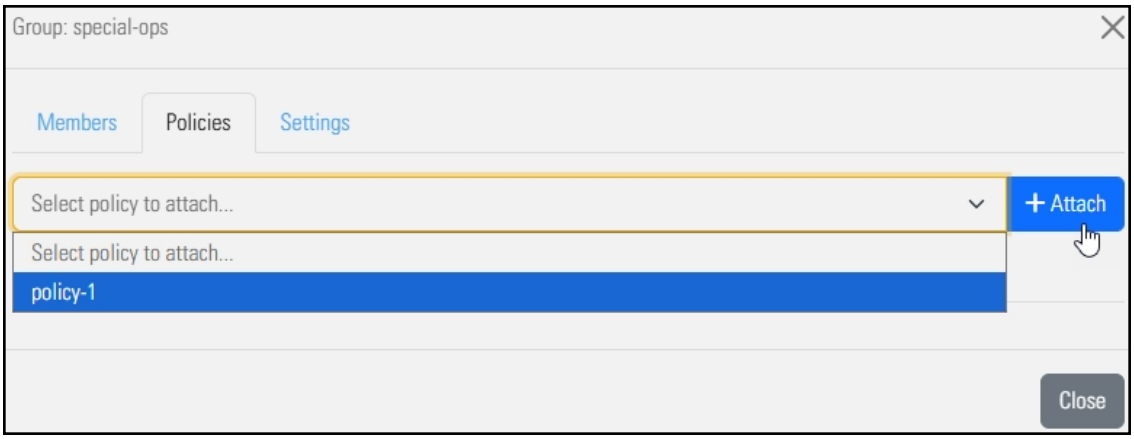
Figure 7-44: Groups page - select view group



2. The **Group name** pop-up appears, with three associated tabs: **Members** (default), **Policies**, and **Settings**.
   - To add **members** to a group, in the Members tab, use the drop-down arrow in the field to select a user, then click the **Add** button. The **Member added** pop-up appears to confirm success. Click **OK** to return to the Members tab. Continue to add members as needed. Added members appear in the list.



   - To attach a **policy** to a group, in the Policies tab, use the drop-down arrow in the field to select a policy, then click the **Attach** button. The **Policy attached** pop-up appears to confirm success. Click **OK** to return to the Policy tab. Continue to add policies if needed. Added policies appear in the list.



- In the Settings tab, the group is **enabled** by default. To **disable** the group, click the button beside **Group Enabled**. A **Group status updated** pop-up appears to confirm the change. Click **OK** to return to the Settings tab.

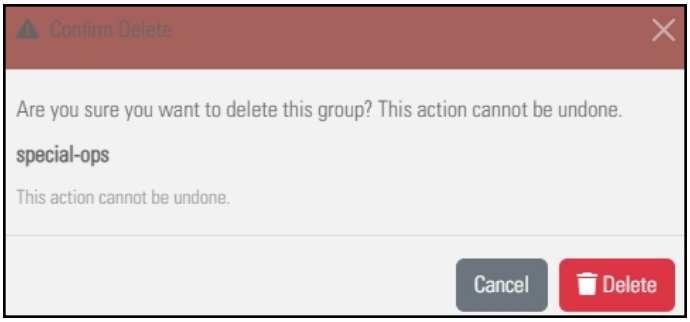


When done with viewing or editing group details, click the **Close** button to return to the Groups page.

To delete a group:

1. From the **Groups** page, in the list of available Groups, select the **Delete** icon in the **Actions** column for the target group. A **Confirm Delete** pop-up appears. Click **Delete** to confirm.

Figure 7-45: Confirm Delete pop-up



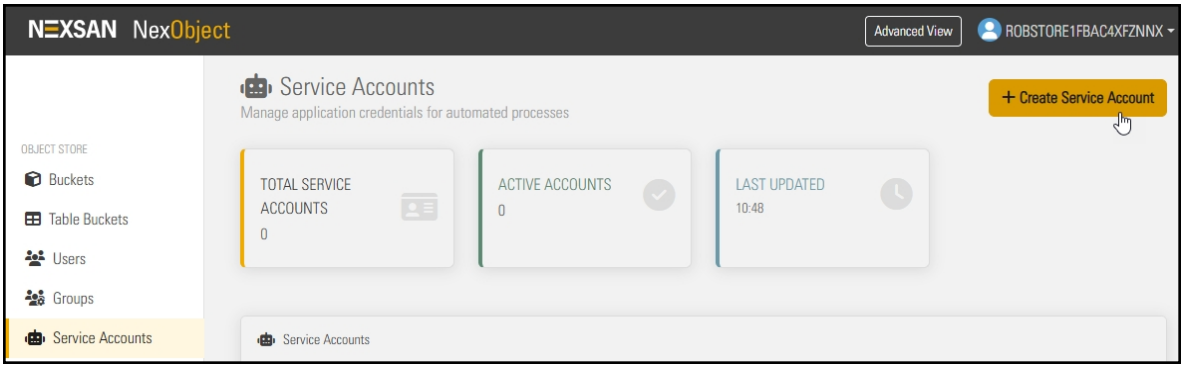
Creating and managing object store service accounts

Manage application credentials for automated processes with service accounts.

To create a service account:

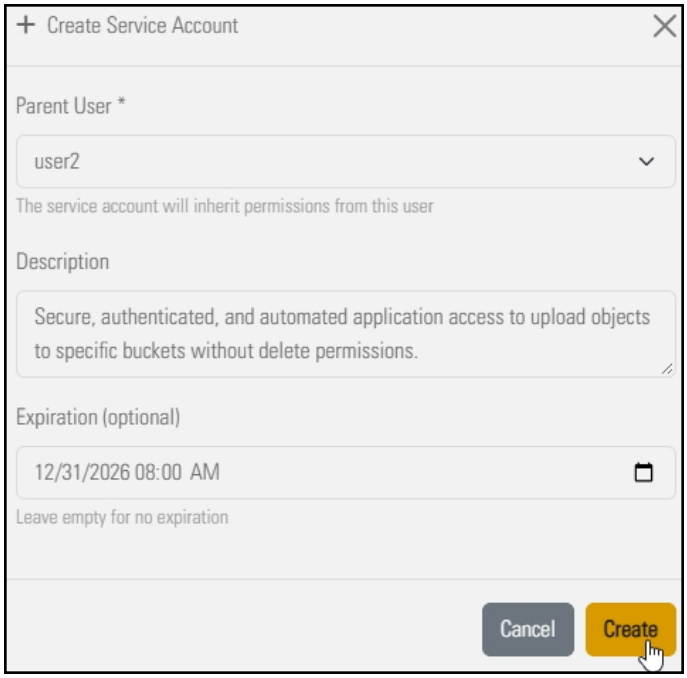
1. From the object store main page, select **Service Accounts** on the left side menu.
2. The Service Accounts page appears. Click the **Create Service Account** button on the upper right side.

Figure 7-46: Object Store Service Accounts page - Create service account



3. The **Create Service Account** pop-up appears.
   - Select the **Parent User** using the drop-down arrow in the field.
   - Enter a **Description** for what the service account will be used for.
   - Set an optional **Expiration** date. If left empty (default), there will be no expiration date.
   - When done, click **Create**.

Figure 7-47: Create Service Account pop-up



4. The **Service Account created successfully** pop-up appears.

   Note This is the only time you will see the secret access key. Please save it securely. Use the credentials to create AWS CLI or SDKs.

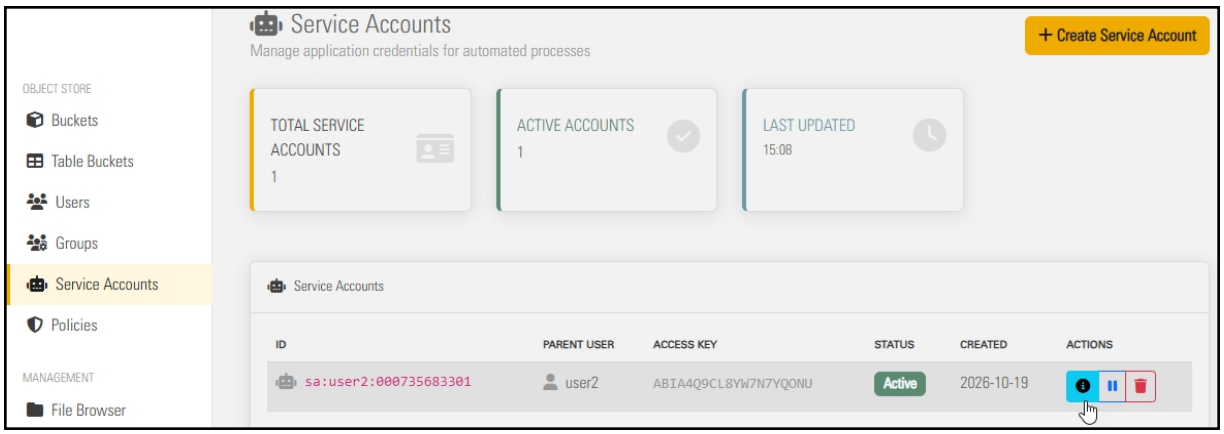
   Click **I have saved the credentials** to return to the Service Accounts page.

5. The Service Accounts page appears, with the newly created service account listed in the table.

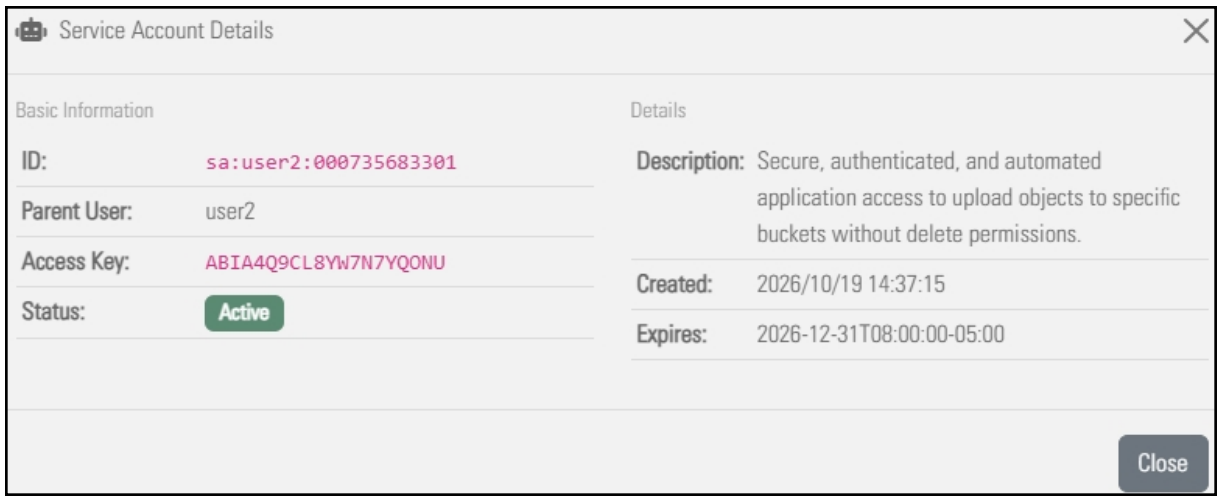
► To view, deactivate or delete service accounts:

The Service Accounts page lists created accounts in a table with the columns **ID**, **Parent User**, **Access Key**, **Status**, **Created**, and **Actions**. The following Action icons are available to manage the service accounts: **View**, **Deactivate**, and **Delete**. Each of these is described below.

Figure 7-48: Service Accounts page - Actions



- **View** the service account details by clicking on the information icon in the Actions column. The pop-up displays Basic information and Details.



- **Activate** (default on) or **Deactivate** the service account by clicking on the play or pause buttton icons in the Actions column. A pop-up appears to briefly confirm the selection.
- **Delete** the service account by clicking on the delete icon in the Actions column. A pop-up appears to confirm the delete.

  Note This action cannot be undone.

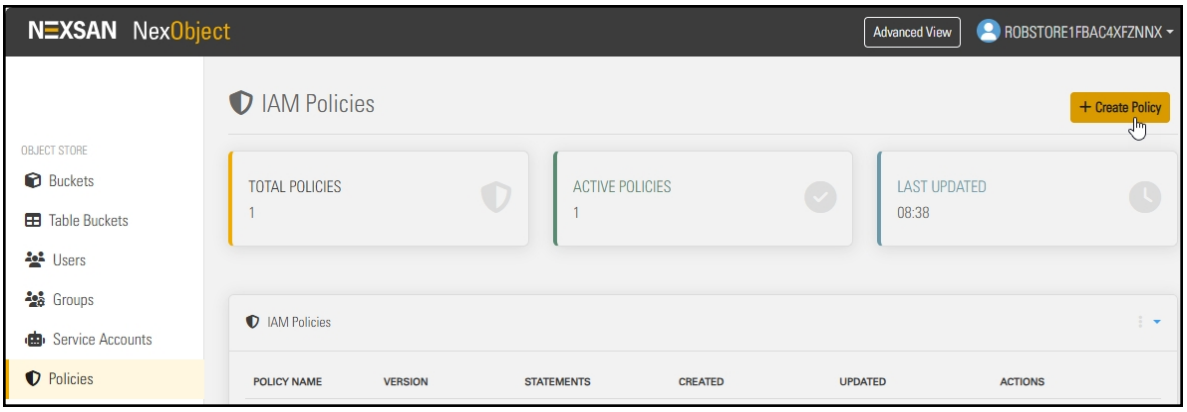
Creating and managing object store policies

Create an Identity Access Management (IAM) policy that can be applied to object store users or groups.

To create a policy:

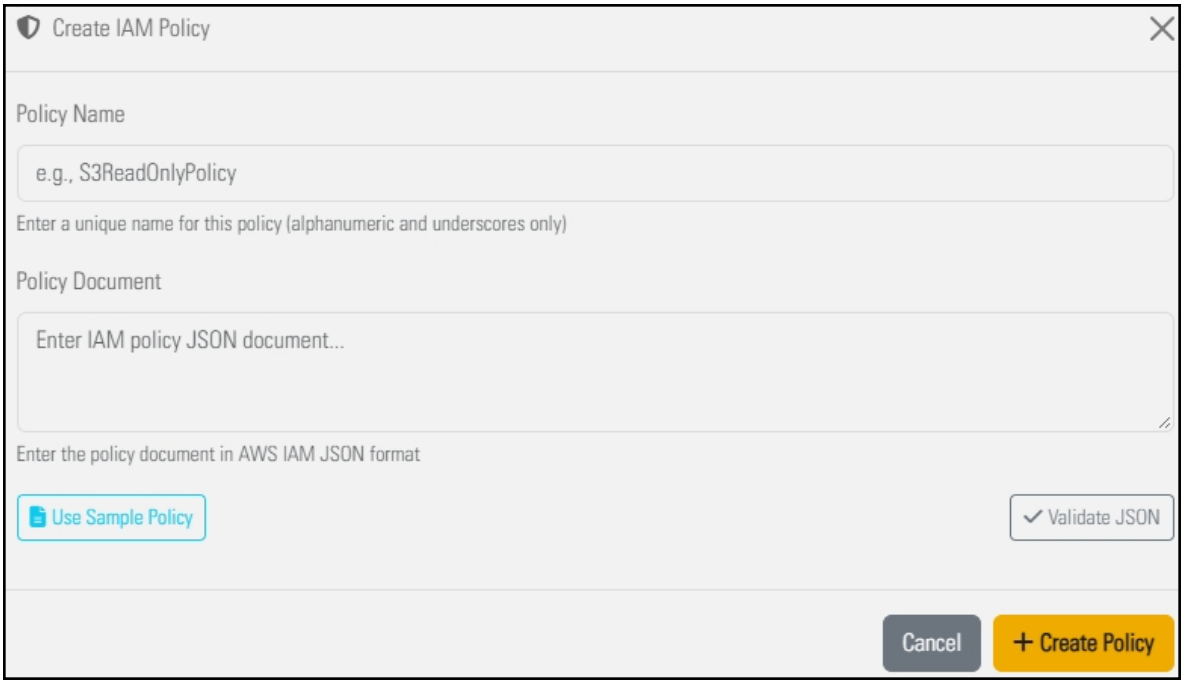
1. From the object store main page, select **Policies** on the left side menu.
2. The IAM Policies page appears. Click the **Create Policy** button on the upper right side.

Figure 7-49: Object Store Policies page - Create policy



3. The **Create IAM Policy** pop-up appears.

Figure 7-50: Create IAM Policy pop-up

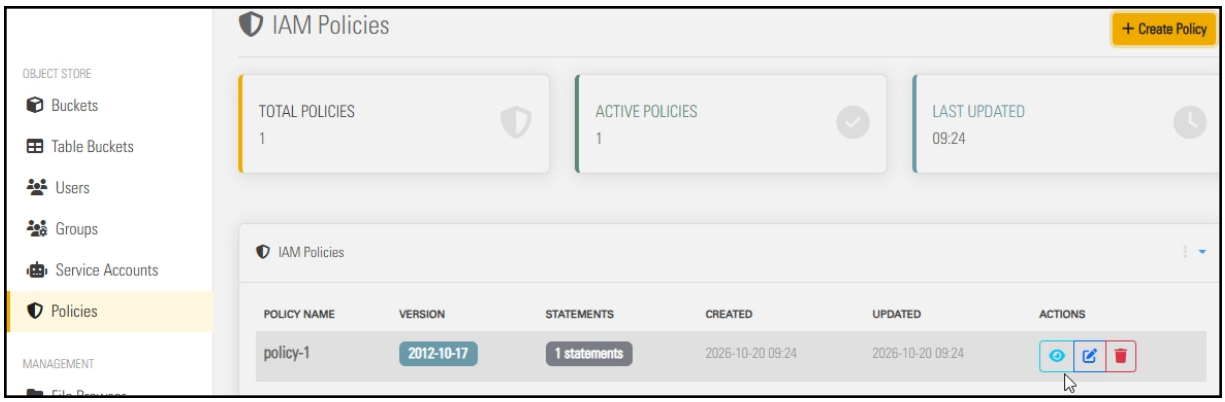


- Enter a unique **Policy Name** using alphanumeric and underscore characters only.
- Enter a **Policy Document** in AWS IAM JSON format. For an example, click the **Use Sample Policy** button. To verify correct format and syntax, click the **Validate JSON** button.
- When done, click **Create Policy**. A pop-up appears to confirm successful creation.

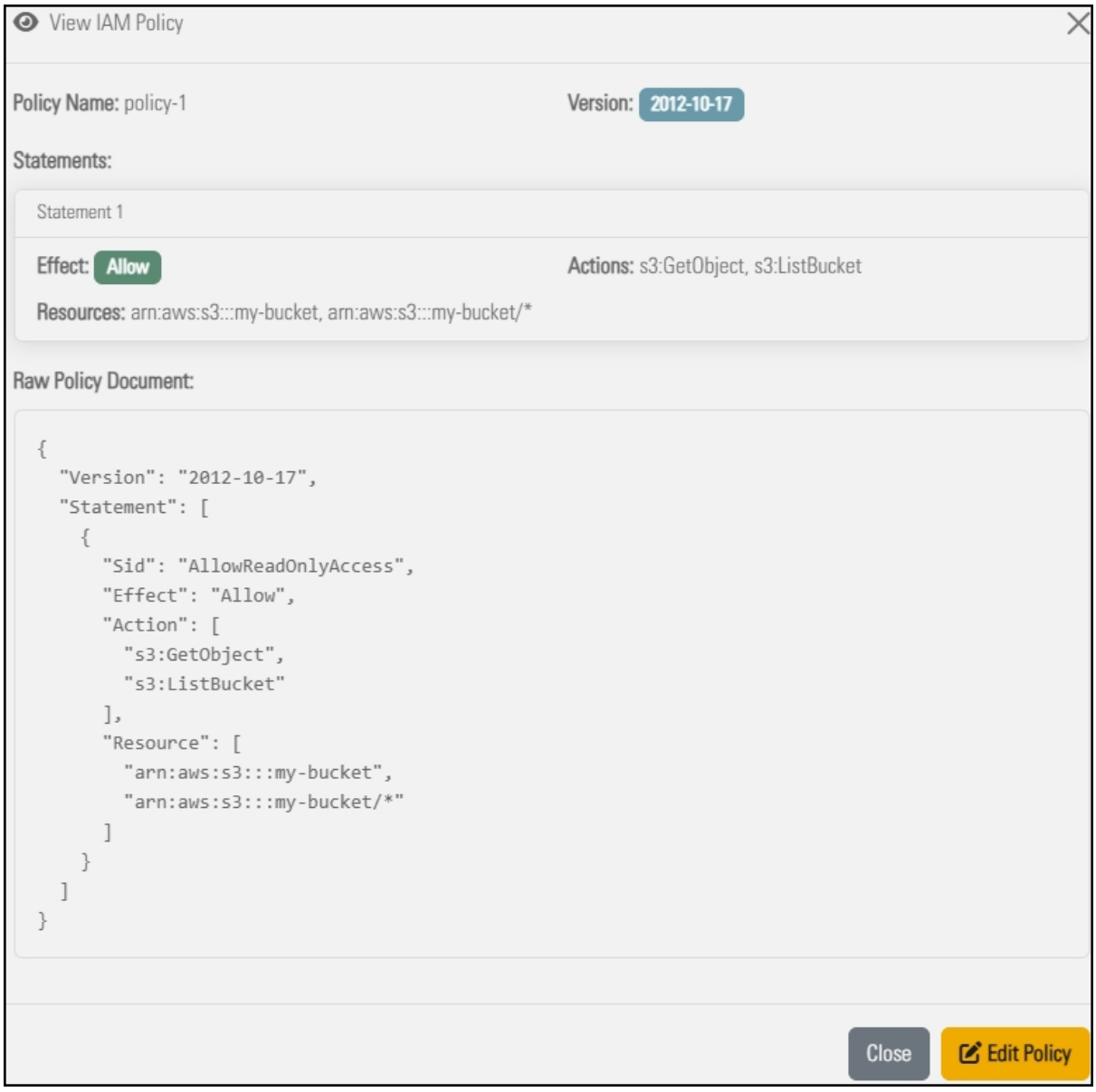
► To view, edit or delete policies:

The IAM Polcies page lists created policies in a table with the columns **Policy Name**, **Version**, **Statements**, **Created**, **Updated**, and **Actions**. The following Action icons are available to manage policies: **View**, **Edit**, and **Delete**. Each of these is described below.

Figure 7-51: IAM Policies page - Actions



- **View** the policy details by clicking on the view icon in the Actions column. The View IAM Policy pop-up displays detailed information. Click **Edit Policy** to make changes, then click **Save Changes** when done.



- Alternately to **Edit** the policy, click the edit icon in the Actions column.
- To **Delete** a policy, click the delete icon in the Actions column. A pop-up appears to confirm the delete.

  Note This action cannot be undone.

7

Chapter 8

Clustering

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 376
Viewing cluster status 386
Moving cluster resources 387
Restarting the cluster or individual controller nodes 389
Shutting down the cluster or individual controller nodes 391
Modifying IP configuration settings 393
Setting or modifying IPMI settings 398
Enabling jumbo frames using Unity 399
Enabling jumbo frames using the nxadmin CLI 400
Enabling LACP using the Unity Web interface 400
Configuring TCP flow control 403

Clustering overview

Unity's Active/Active Clustering configuration provides both high-availability and load balancing for your Nexsan storage infrastructure.

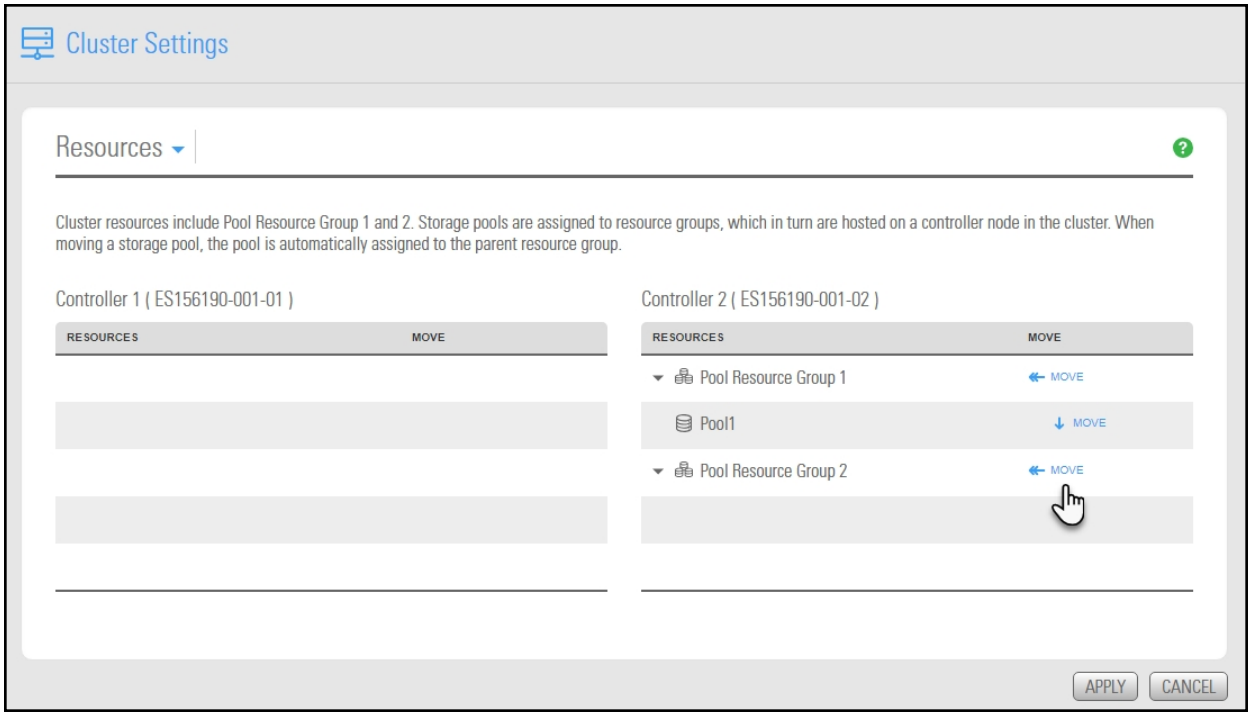
- High-availability ensures minimal down-time by eliminating a single point of failure with a second controller node. If one controller fails, Unity automatically fails over system operations and redirects I/O to the second controller on the system.
- Load balancing enables you to distribute data equally among both controller nodes in the cluster.

To help you achieve load balancing, Unity uses *Pool Resource Groups*: When you create a storage pool on 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 Unity two controllers. 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 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, Unity automatically transitions any Pool Resource Groups on one controller, along with all its underlying storage pools, to the other controller.

8

Figure 8-1: Cluster Settings > Resources: Click move to rebalance



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 enabling 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.

Cluster components and terminology

This table describes Unity cluster components, as well as cluster-related terminology used in Unity.

Table 8-1: Cluster concepts and terminology

Cluster Terminology	Definition
Active/Active Clustering	In Active/Active Clustering 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.
Controller(s), also referred to as controller node, or node	This refers to the physical controller nodes in a Unity cluster. There are two controllers; you assign each controller node a physical IP address during the initial setup of Unity. 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.
Cluster Resources	Cluster resources represent the components of a cluster; these include: • Controller 1 and Controller 2 • Pool Resource Group 1 and Pool Resource Group 2 • System Management
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. **CAUTION:** 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*.

Cluster Terminology	Definition
Pool Resource Group(s)	When you create a storage pool on 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 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 shares 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 386.
Active node, also referred to as active controller, or active controller 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*.
Passive node, also referred to as passive controller, or passive controller node	This refers to the controller node that currently is NOT hosting the System Management component, which includes cluster- and system-related services on 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*.

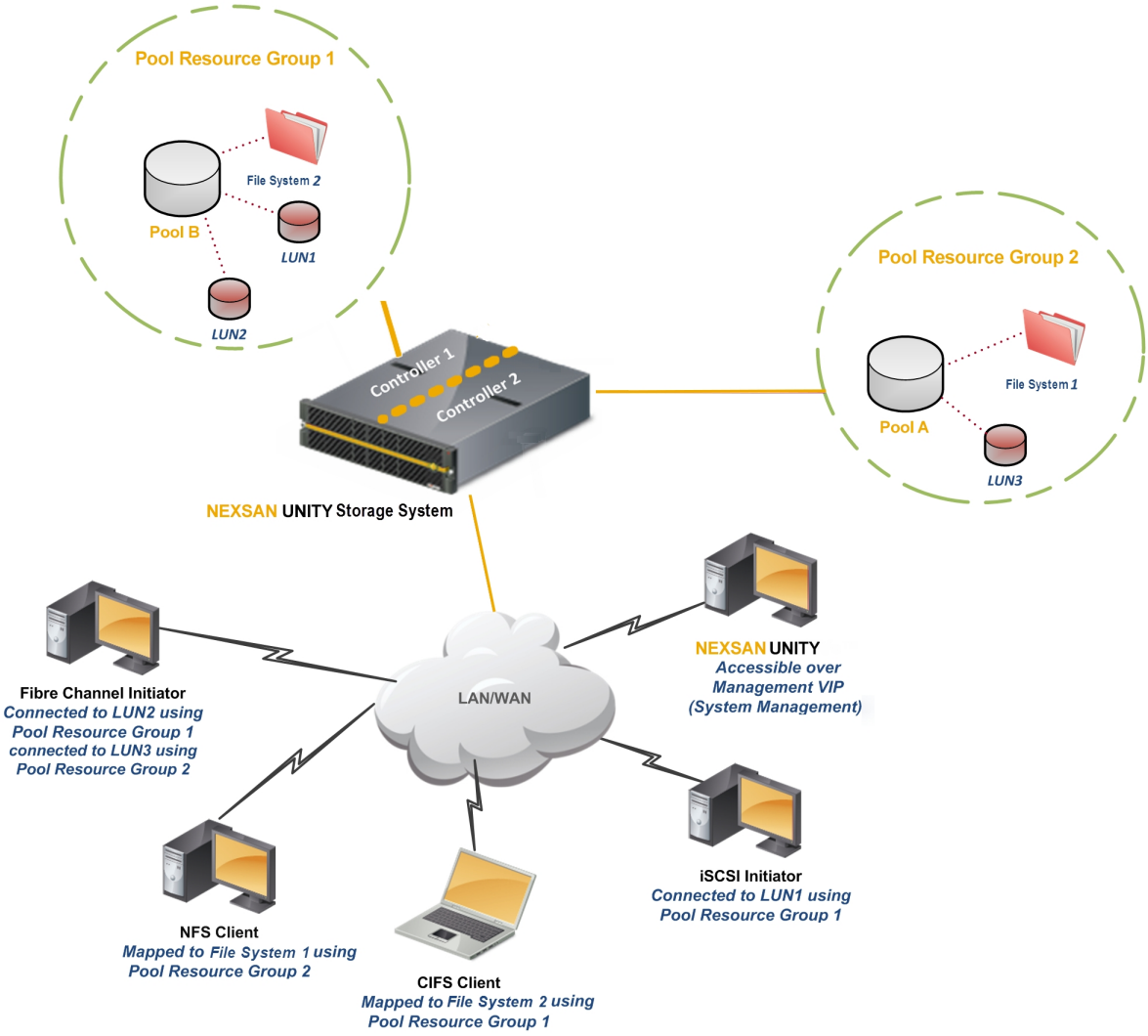
Cluster Terminology	Definition
Failover	This refers to the act of transitioning, or moving, Pool Resource Groups from one controller node to the other. This can be a manual process that you initiate if you want to shut down a controller for maintenance. Or, an automatic process initiated by Unity in the event that a controller node fails.
Move 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. Specifically, when you move a storage pool from one Pool Resource Group to the other, the data sets (shares 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 share 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.

Unity Clustering

This diagram illustrates an Active/Active Clustering configuration; it includes examples demonstrating how client systems access data sets (file systems and/or LUNs) in Pool Resource Groups. The Unity Storage System 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 8-2: Illustration of Active/Active Clustering



Load balancing with Active-Active Clustering

With Nexsan Unity's Active-Active Clustering configuration, you can distribute storage pools between the controller nodes, while still remaining fault tolerant. In the event of a controller failure, the other controller automatically takes over any storage pools that were owned by the failed node.

Important points about load balancing:

- Storage pools are grouped under *Pool Resource Groups*, each of which has its own Virtual IP address.
- Failover occurs at the Pool Resource Group level; specifically, if one of the controller nodes in the cluster fails, or needs to be shut down for maintenance, Unity automatically transitions any Pool Resource Group(s) on the *inactive* controller, along with all its underlying storage pools, to the active controller.
- You use each Pool Resource Group's virtual IP address to access the storage pools assigned to it; this ensures that the virtual end point, through which end users and client systems access their data in the storage pool, does not change during failover.
- Ideally, each controller node on Unity should have a Pool Resource Group assigned to it; with storage pools balanced across the two Pool Resource Groups to ensure both controllers are used effectively.
- More than one storage pool must be available to take advantage of an Active-Active configuration; if there is only 1 storage pool, then only one controller can own it, essentially making it an active-passive configuration.

To create one or more storage pools from Unity, refer to Storage pools on page 89. To create multiple storage pools at the same time, you can use CLI commands as described in the *Nexsan Unity nxadmin Command Line Reference Guide*.

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 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 on the facing page.

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 8-2: Disk heartbeating—Comparison between transient and persistent reservation

State	Transient reservation	Persistent reservation
Normal	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.	1. Controller 1 makes a reservation. 2. Controller 1 sets the failure flag. 3. Controllers 1 and 2 exchange heartbeats periodically.
Controller failure	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.	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.

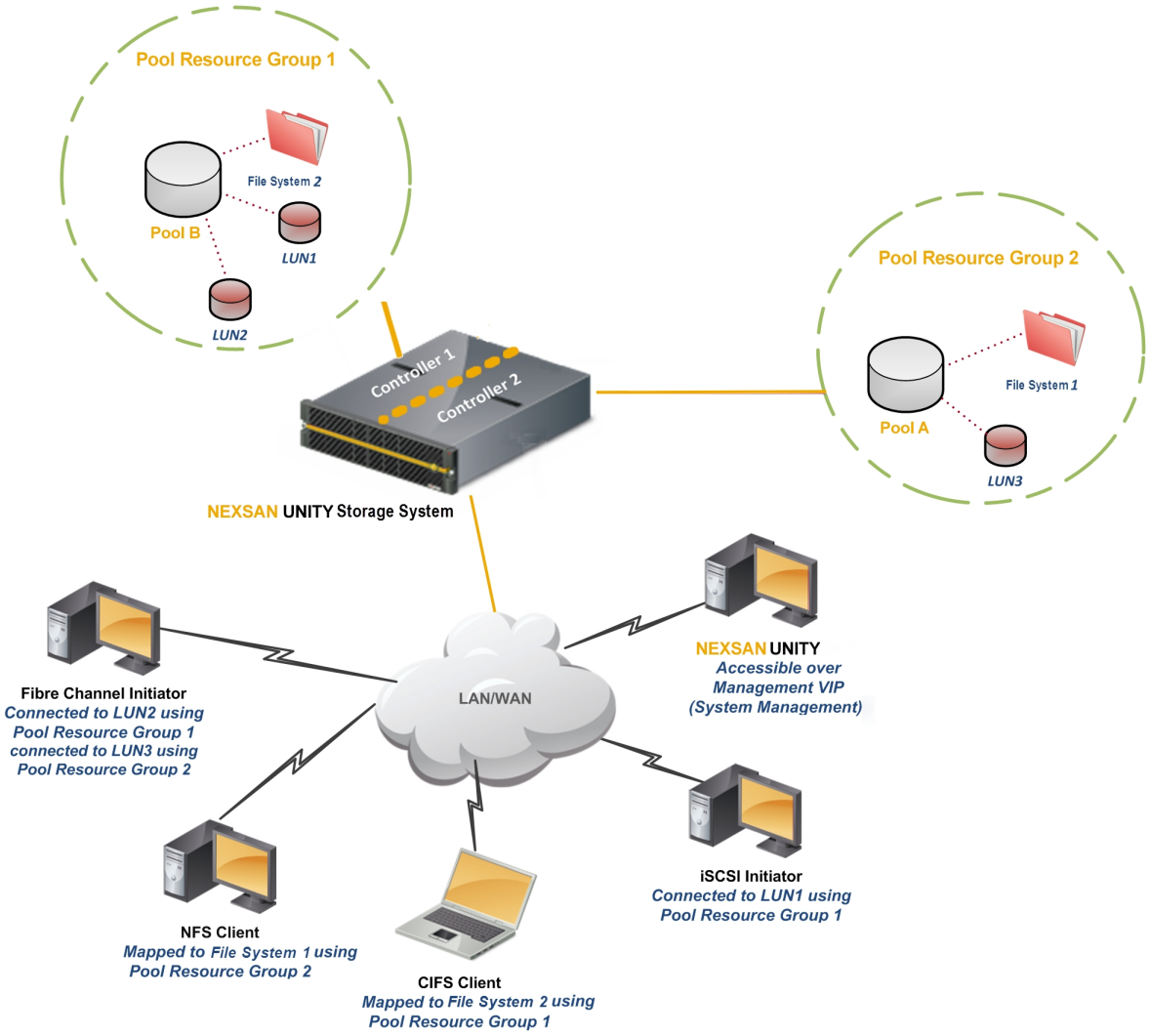
State	Transient reservation	Persistent reservation
Controller freeze	1. Controller 1 freezes and does not send a heartbeat. 2. Controller 2 starts the Pool Resource Group. 3. ***Controller 2 makes a reservation (devices are not reserved at this point).*** 4. Controller 2 sets the failure flag. 5. ***Controller 2 removes its reservation.*** 6. Controller 1 unfreezes. 7. ***Controller 1 does not get a reservation conflict, because the reservation was removed.*** **This results in a split-brain situation.**	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. 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.*** **The split brain situation is avoided.**

Unity NV Series Clustering

This diagram illustrates an Active/Active Clustering configuration for the Unity NV Series; it includes examples demonstrating how client systems access data sets (file systems and/or LUNs) in Pool Resource Groups. The Unity NV Series 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 8-3: Active/Active Clustering for the Unity NV Series



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: 000.01.002.003	Controller 2, Physical IP: 000.01.002.004
Pool Resource Group 1, **Virtual IP: 000.02.002.003**	Pool Resource Group 2, **Virtual IP: 000.02.002.004**
• Storage Pools assigned to Pool Resource Group 1: FinancePool1, containing these data sets: • filesystem1 (CIFS/NFS) • filesystem2 (NFS) • LUN101	• Storage Pools) assigned to Pool Resource Group 2: FinancePool2, containing these data sets: • filesystem3 (CIFS) • LUN201

In order for a client system on the network to access *filesystem3* 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, 000.02.002.004

The CIFS mount point for *filesystem3* is therefore represented as:

```
\\000.02.002.004\filesystem3
```

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 *filesystem3* changes:

```
\\000.02.002.003\filesystem3
```

Viewing cluster status

This section explains how to view Unity cluster status information and access commands, including:

- cluster health
- controller node status (whether each node is up or down)
- controller restart and shutdown

To view cluster status information:

1. Log on to the Unity System that you want to view cluster status information for. The **Dashboard** displays cluster health, controller node status, down or up time for the controllers, and a space overview.
2. Click **Cluster Status** to
   - View cluster status and location per controller
   - **Restart** or **Shut Down** controllers.

See also

- Restarting the cluster or individual controller nodes on page 389
- Shutting down the cluster or individual controller nodes on page 391

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).

Unavailable tasks when a controller 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
- Updating Unity

Moving cluster resources

If one of the controller nodes fails for any reason, 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—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 Group—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.



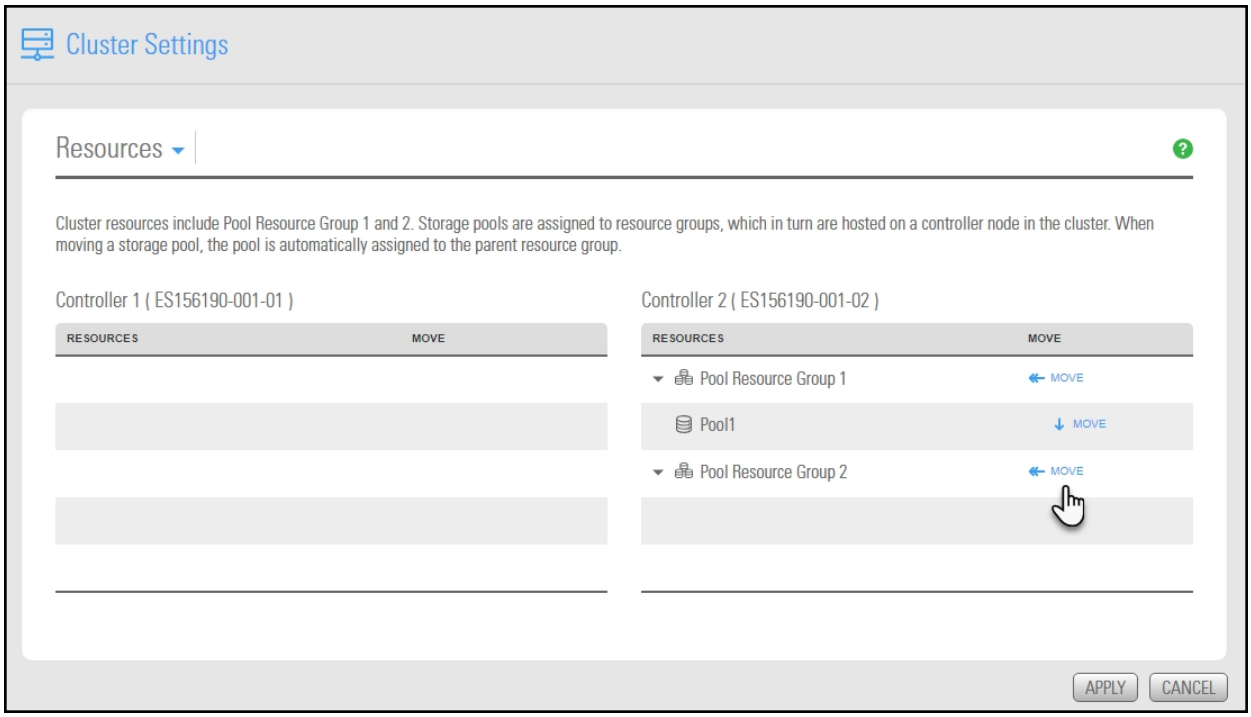
CAUTION: When you move cluster resources from one controller to the other, client systems and applications on the network will temporarily lose connection to data sets (file systems and/or iSCSI LUNs) until the move operation completes and the cluster comes back online; this could result in host delays, or potentially timeouts.

Before moving cluster resources, make sure that client systems with an active connection to any file systems or iSCSI LUNs on Unity are disconnected; also make sure to quiesce any applications with an active connection to Unity.

To move cluster resources from one controller node to the other:

1. From the **Unity dashboard**, select **Cluster Settings**.
2. Select **Status > Resources**. The Cluster Resources panel provides a visual representation of where each resource in the cluster is currently hosted: Controller 1 or Controller 2. In addition, the panel indicates the Pool Resource Group that each storage pool on the systems is currently assigned to.

Figure 8-4: Cluster Settings Resources panel



3. Select the cluster resource that you want to move to by clicking Move in the corresponding Controller box.

   Note You can also move storage pools from one Pool Resource Group to other; see Changing a pool resource group on page 107.

4. If needed, move additional cluster resources.
5. Click the **Apply** button. Unity prompts you to confirm the action. As indicated above, the data will be unavailable until the process completes.
6. Click **Move** when you are ready to continue.

Restarting the cluster or individual controller nodes

Use these instructions if you make changes to the Unity configuration that require a reboot, either of the full Unity Storage System or one of its controllers.

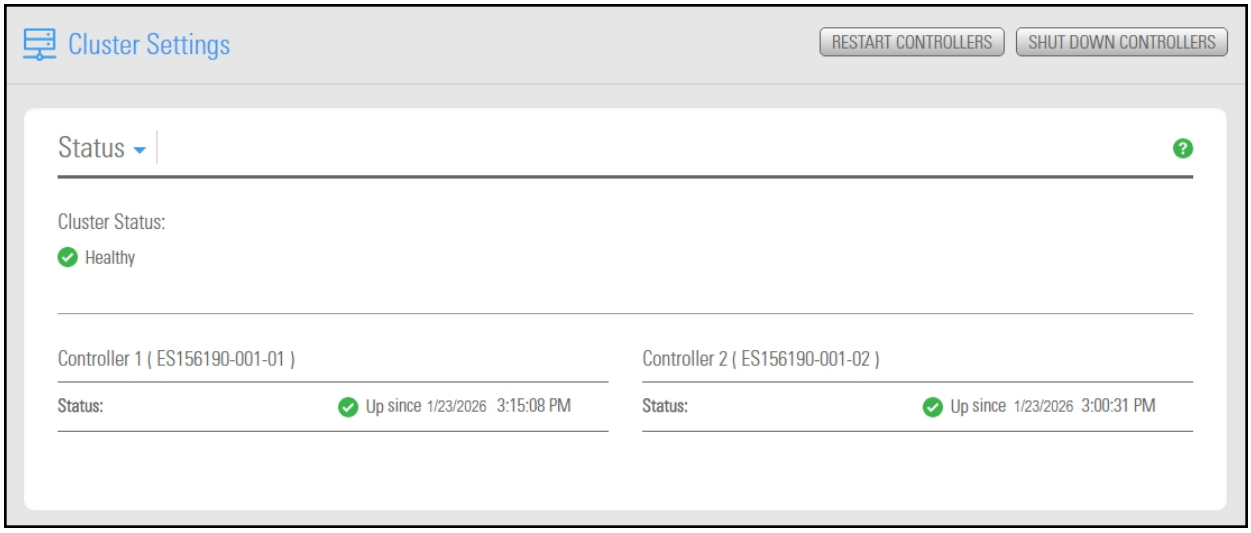
CAUTION: When you restart Unity, or one of its controller nodes, client systems and applications on the network will temporarily lose connection to Unity until the cluster comes back online. This could result in host delays, or potential timeouts.

Before restarting 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 Unity are disconnected; also make sure to quiesce any applications with an active connection to Unity.

To restart Unity or one of its controller nodes:

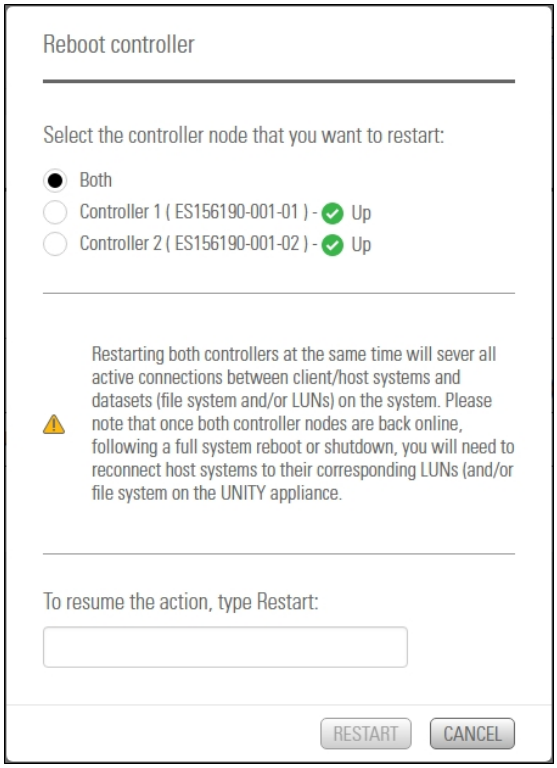
1. From the **Unity dashboard**, select **Cluster Settings**. The Cluster Settings panel opens, displaying controller health and up or down time.

Figure 8-5: Cluster Settings Status panel



2. Click the **Restart Controllers** button. The **Reboot controller** popup window opens.

Figure 8-6: **Reboot controller** popup



3. Select one of the available options:
   - **Both**: If you reboot both controllers, the Unity Storage System will be unavailable until the system restarts.

     Rebooting one controller at a time is recommended to avoid loss of connection, and Unity backs up cluster resources (the peer Pool Resource Group) to the other controller prior to performing the restart.
   - **Controller 1**: In this case, controller 2 remains in service and you can continue accessing and backing up data during the restart.
   - **Controller 2**: In this case, controller 1 remains in service and you can continue accessing and backing up data during the restart.
4. Type **Restart** in the text box.
5. Click **Restart** to continue.

Unity restarts the clustered Unity Storage System or the selected controller. This process may take some time to complete.

Notes:

- If you restart both controllers on Unity, client systems and applications on the network will temporarily lose connection to Unity until the cluster comes back online.

Shutting down the cluster or individual controller nodes

Use this procedure if you need to shut down Unity or one of its controller nodes to perform maintenance on the system, such as, replacing a faulty hardware component, or upgrading a component.

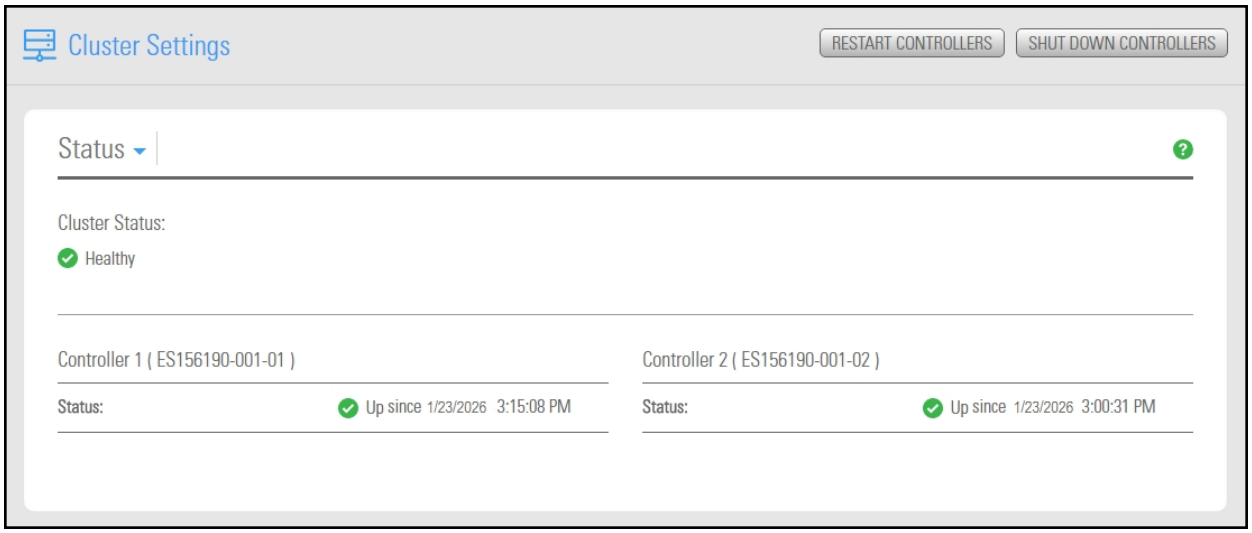
CAUTION: When you shut down Unity or one of its controller nodes, client systems and applications on the network will temporarily lose connection to Unity—until the cluster comes back online; this could result in host delays or potentially timeouts. Before restarting Unity, or one of its controller nodes, make sure that client systems with an active connection to any data set (file systems and/or iSCSI LUNs) on Unity are disconnected; also make sure to quiesce any applications with an active connection to Unity.

The shut down process quiesces system services on Unity; it does not physically shut down the system. When you shut down 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 Unity or one of its controllers:

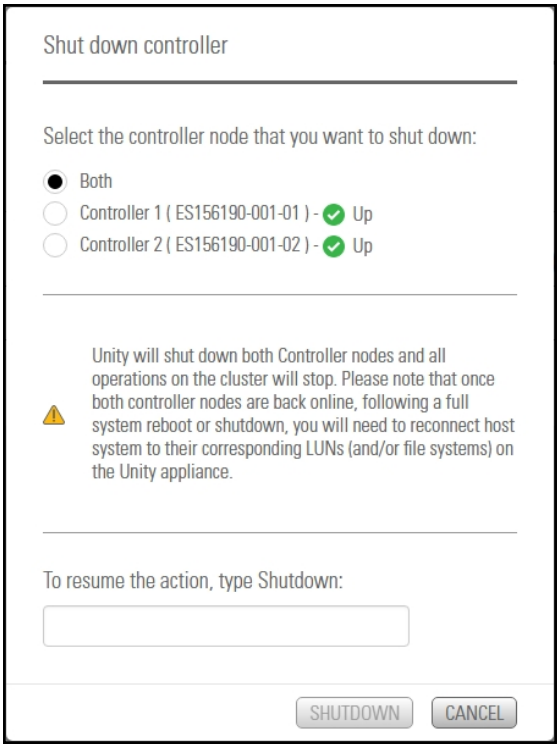
1. From the **Unity dashboard**, select **Cluster Settings**. The **Cluster Settings panel** opens, displaying controller health and up or down time.

Figure 8-7: Cluster Settings Status panel



2. Click the **Shut down controllers** button. The **Shut down controller** popup window opens.

Figure 8-8: **Shut down controller** popup



3. Select one of the available options:
   - **Both**: If you shut down both controllers, the Unity Storage System will be unavailable until the system restarts.
   - **Controller 1**: In this case, controller 2 remains in service and you can continue accessing and backing up data while the peer controller is shut down.
   - **Controller 2**: In this case, controller 1 remains in service and you can continue accessing and backing up data while the peer controller is shut down.
4. Type **Shutdown** in the text box.
5. Click **Shutdown** button to continue.

The shut down process quiesces system services on Unity; it does not physically shut down the system:

- If you shut down Unity (both controllers in the cluster), wait a few minutes, and then press the power button on the front of the Unity enclosure 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 Unity controllers, client systems and applications on the network will lose connection to Unity until you bring the system back online.

- The controller node where the System Management component is currently hosted transitions the System Management component to the peer controller. Unity also transitions any Pool Resource Group on the controller and associated storage pools to the peer controller. Unity also displays a warning condition until the peer 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 Understanding network interfaces on page 395.

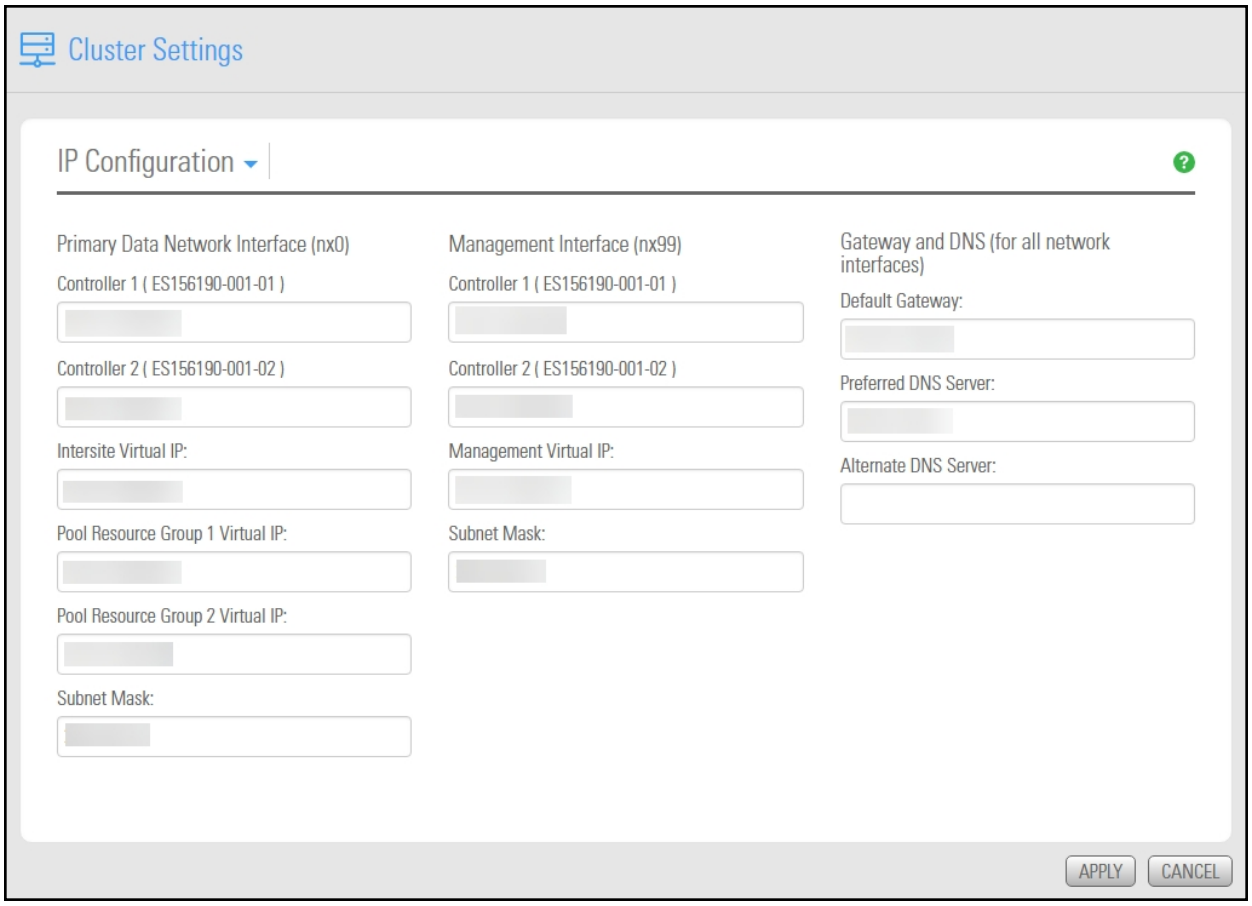
CAUTION: Client systems using these IP addresses will lose connection to Unity. Before modifying IP addresses, disconnect client systems, and quiesce any applications with an active connection to Unity.

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**.

Figure 8-9: Cluster Settings IP Configuration panel



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 an E-Series 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 E-Series 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 8-3: Management interface (nx99) IP addresses

Management Interface (nx99)	Required IP addresses
The management interface requires 3 IP addresses.	
1. Management Virtual IP address	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. Controller 1 (physical) IP address	Physical IP that you must set on the management interface (nx99) for the first controller node in the Cluster.
3. Controller 2 (physical) IP address	Physical IP that you must set on the management interface (nx99) for the second controller node in the Cluster.

Table 8-4: 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. Intersite Virtual IP address	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. Controller 1 (physical) IP address	Physical IP that you set on the primary data network interface (nx0) for the first controller node in the Cluster.
3. Controller 2 (physical) IP address	Physical IP that you set on the primary data network interface (nx0) for the second controller node in the Cluster.
4. Pool Resource Group 1 Virtual IP address 5. Pool Resource Group 2 Virtual IP address	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. 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.

Understanding network interfaces

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.

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 LAN1 port (top-most port) is configured as the primary data network interface.

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.

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.

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.

▶ **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 8-10: 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).

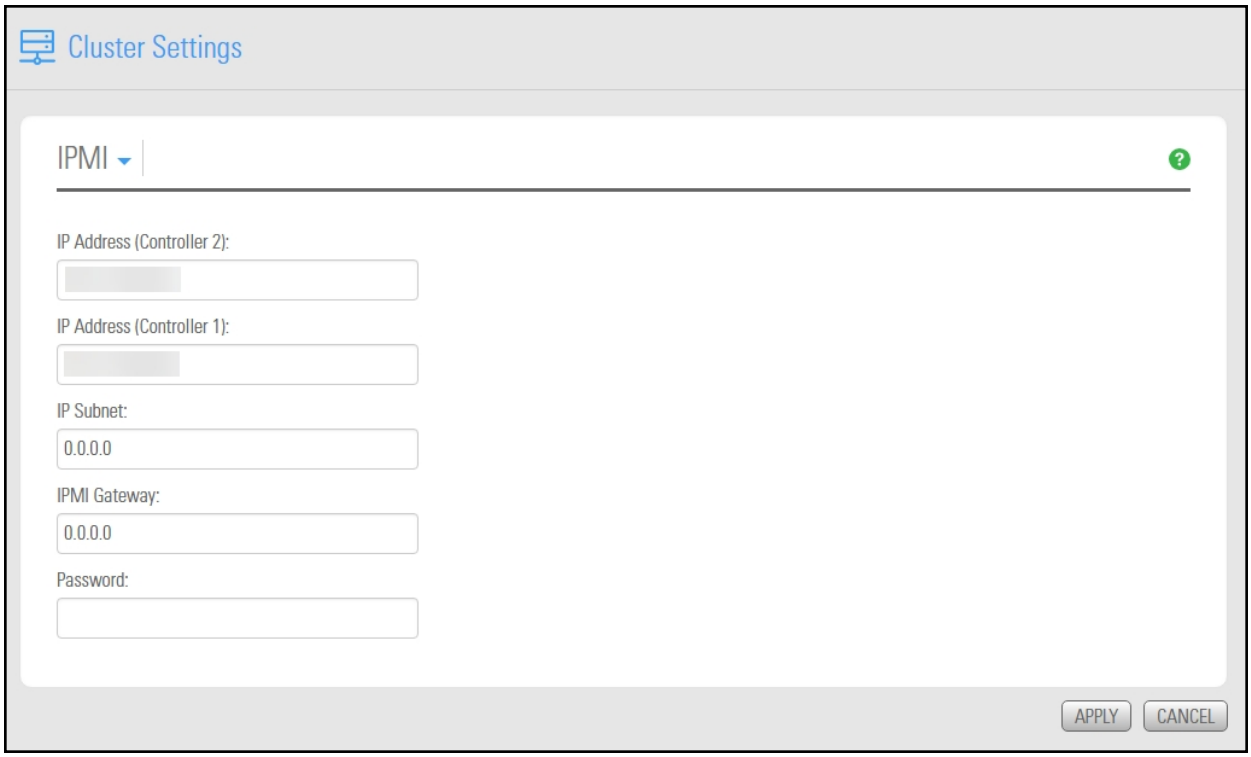
Setting or modifying IPMI settings

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 the Unity Storage System enclosure; this second LAN port is located at the bottom of each controller, closest to the bottom of the controller box.

To set IPMI settings:

1. From the **Unity dashboard**, select **Cluster Settings**. The Cluster Settings panel opens.
2. Select **Status > IPMI**.

Figure 8-11: Cluster Settings IPMI panel



3. 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.
4. 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).
5. 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, enter the IPMI IP address on Unity. The IPMI Web-based interface log on dialog displays.
3. In the **Username** field, type **ADMIN** (all upper case).
4. In the **Password** field, type the IMPI password (the default is **ADMIN**—all upper case). This displays the IPMI Web-based interface main screen.

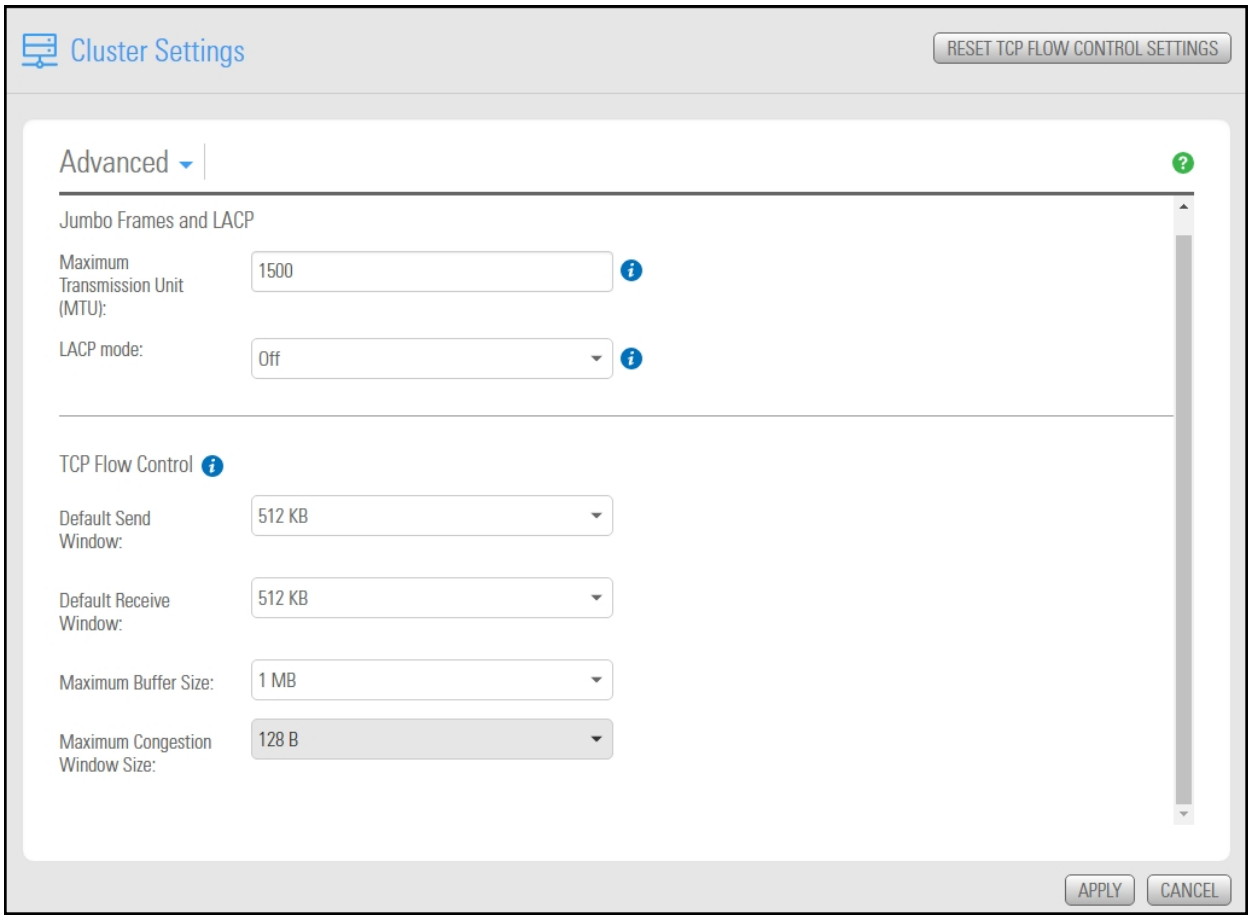
Enabling jumbo frames using Unity

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 nxadmin CLI on the next page.

To enable jumbo frames on Unity:

1. From the **Unity dashboard**, select **Cluster Settings**. The Cluster Settings panel opens.
2. Select **Status > Advanced**.

Figure 8-12: Cluster Settings Advanced panel



3. Enter a number between 1500 and 9000 in the **MTU** field.
4. Click the **Apply** button to save your changes.

Enabling jumbo frames using the nxadmin CLI

Enabling jumbo frames on the Unity Storage System 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 the Unity Storage System is connected to, as well as on all client systems that access it.
- You must make sure that the 10 GigE interface is set as the primary interface (nx0) on the Unity Storage System (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 the Unity Storage System during the reboot and switchover operations. Make sure that client systems with an active connection to any file systems on the Unity Storage System are disconnected; also make sure to quiesce any applications with an active connection to the Unity Storage System.
- We recommend that IPMI settings be configured for the Unity Storage System if you are connected to the Unity Storage System with a system on a separate management network.

To enable jumbo frames on the Unity Storage System:

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 the Unity Storage System (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 the Unity Storage System.
6. Repeat these steps on the second controller node after you transition cluster resources back to the node you finished configuring.

Enabling LACP using the Unity Web interface

Before you begin:

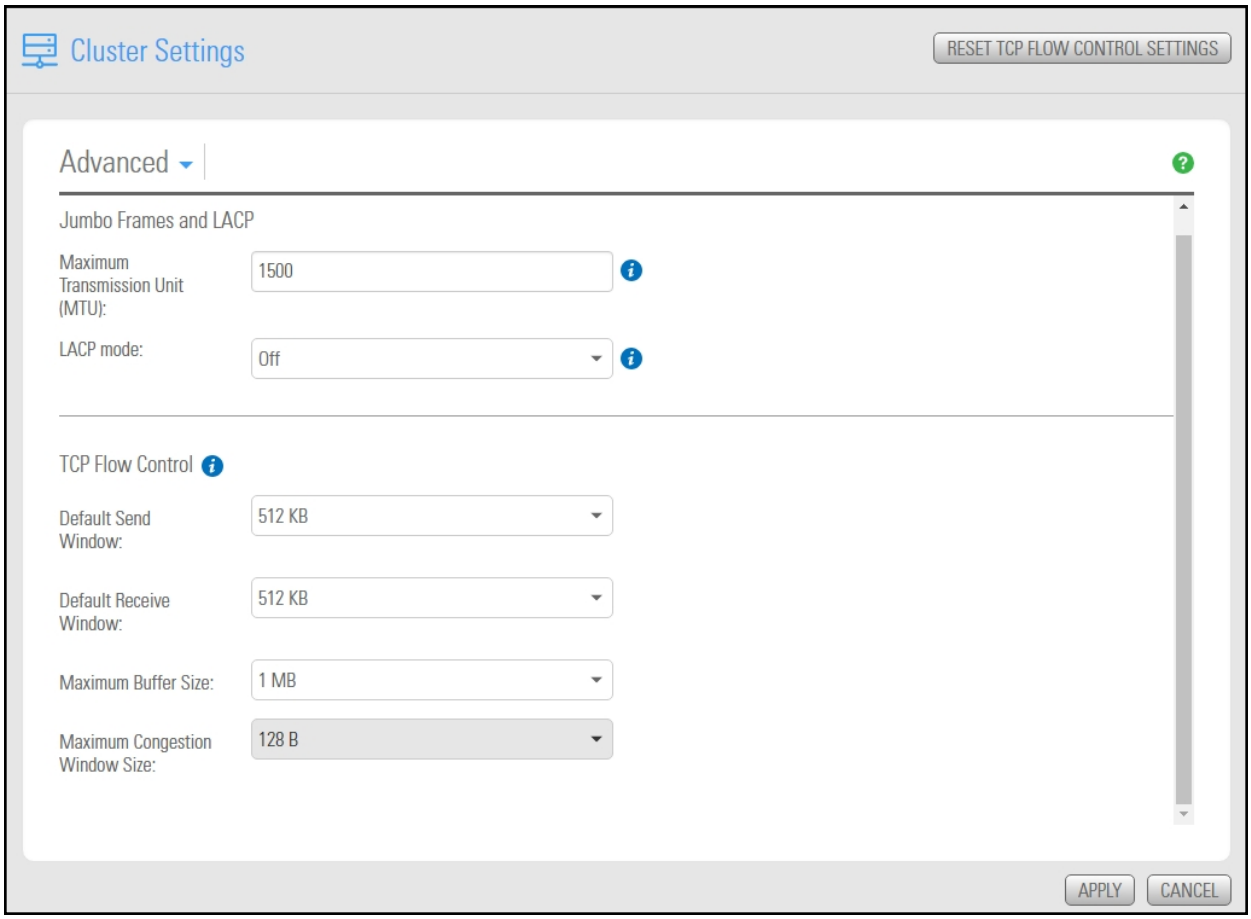
- Read the requirements for LACP; see Requirements and guidelines for implementing LACP on the facing page.
- To learn how link aggregation works, see Understanding link aggregation on page 402.

Note The LACP mode is applied to both nodes on the cluster.

To enable LACP on Unity:

1. From the **Unity dashboard**, select **Cluster Settings**. The Cluster Settings panel opens.
2. Select **Status > Advanced**.

Figure 8-13: Cluster Settings Advanced panel



3. From the **LACP mode** drop-down list, select **Active** or **Passive**.
4. Click the **Apply** button to save your changes.

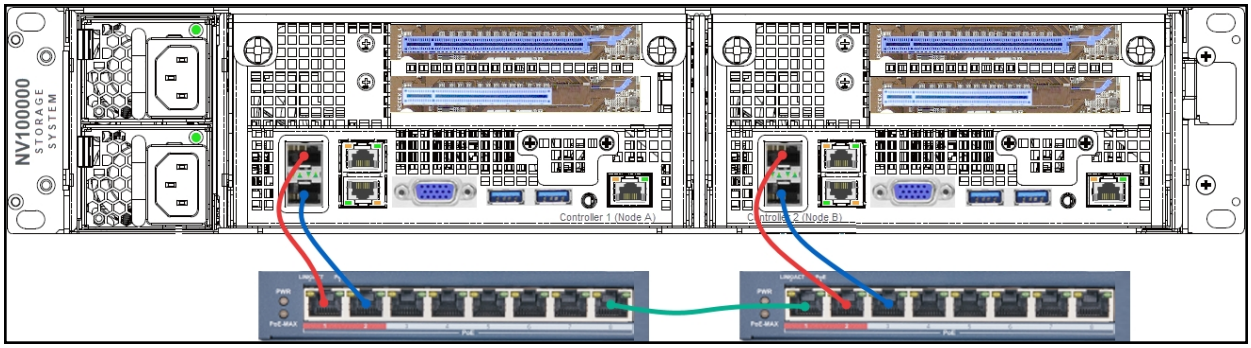
Requirements and guidelines for implementing LACP

This section lists network and infrastructure requirements for implementing LACP, as well as guidelines/best practices for configuring the Ethernet switches for LACP.

- LACP only operates point-to-point between two partner devices connected together: for example, the Unity Storage System and the Ethernet switches.
- 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 switches.
- The link between the Unity Storage System and the Ethernet switch(es) must be Full-Duplex.
- Both the Unity Storage System and the Ethernet switches must be running at the same speed (1Gbps or 10Gbps).
- The Ethernet switches 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 explained in "Understanding network aggregation" in the *Network Configuration Guide*.

Figure 8-14: Connecting controllers to Ethernet switches on the NV10000



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 the nxadmin CLI

The Unity Storage System provides the `nic` command in the Unity Storage System's menu-based nxadmin CLI for enabling and monitoring LACP on the Unity Storage System.

▶ **Before you begin:**

- Enabling LACP over the network will cause disconnection. Perform these steps through KVM console, or through IPMI console.
- 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 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 the Unity Storage System:**

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 the Unity Storage System, in either active or passive mode:
   - Active mode:

     ```
     nic modify-aggr -L active nx0
     ```

     Where `nx0` represents the primary interface on the Unity Storage System. 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 the Unity Storage System. 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. The Unity Storage System disconnects from the network.
5. Configure the Ethernet switch to set the ports that you want to combine into a logical channel. The Unity Storage System comes back online once LACP negotiation is complete.
6. Test and confirm network connectivity to the Unity Storage System.

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.

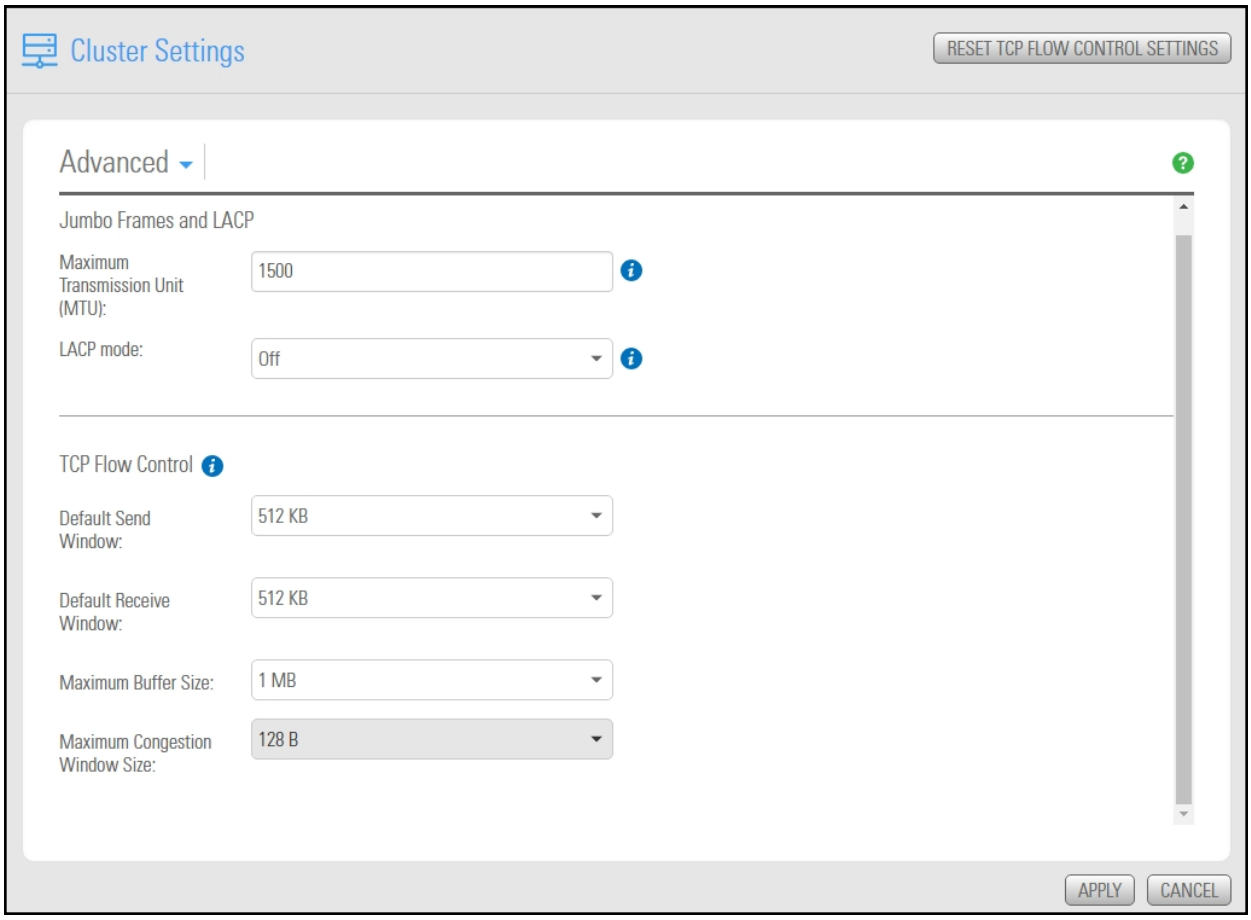
TCP separates receiver congestion from network congestion, and uses flow controls for each (receiver window and congestion window). The congestion window determines the number of bytes that can be outstanding at any time.

Note The TCP flow control settings are applied to both nodes on the cluster.

To configure TCP flow control:

1. From the **Unity dashboard**, select **Cluster Settings**. The Cluster Settings panel opens.
2. Select **Status > Advanced**.

Figure 8-15: Cluster Settings Advanced panel



3. 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.
4. 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.
5. Set the **Maximum buffer size** parameter; specify a value ranging from 8 KB to 1 GB. The default value is 1 MB.
6. Set the **Maximum congestion window size** parameter; specify a value ranging from 128 B to 1 GB. The default value is 1 MB.
7. Click the **Apply** button.

Note If you need to revert to the default settings, click the **Reset TCP Flow Control** button and click the **Apply** button.

Chapter 9

Storage management

Managing storage for Unity involves the following tasks:

Allocating new storage to the Unity System 406
Modifying IP settings for a Nexsan E-Series/BEAST Storage System 412
Renaming a Unity Storage System 413
Adding new drives to a Unity Storage System 414
Resetting the RAID configuration for storage 416
Removing a Unity Storage System 417
Shutting down a Unity Storage System 419
Powering on Unity controllers 421
Shutting down a Nexsan E-Series Storage System 423
Powering on Unity and E-Series Storage Systems 424
Using Self-Encrypting Drives (SEDs) 425
Disabling SED encryption 427

Allocating new storage to the Unity System

When you connect a Unity Storage System, Nexsan Unity Storage Expansion or Nexsan E-Series System to Unity, you must allocate the storage system to Unity and configure its RAID settings. This is also true when you add new disk drives to a system.

Before starting the Add Storage System wizard:

- Make sure the storage system that you want to allocate to the Unity System 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 92.

Notes: All Nexsan Storage Systems are hot-pluggable, so Unity does not need to be powered off when plugging in a new storage system.

To perform this operation, you must have unused storage systems available.

To start the Add Storage System wizard:

1. On the **Unity navigation bar**, select **System > Unity Systems**.
2. Click the link to the Unity Storage System that you want to add storage to.
3. In the **Unity Systems Summary** panel, click the **Storage Systems** link.
4. Click the **Add Storage Systems** button.

This section includes these steps:

Step 1: Discovering new storage and configuring RAID settings 407
Step 2: Verifying settings 410
Step 3: Viewing results 411

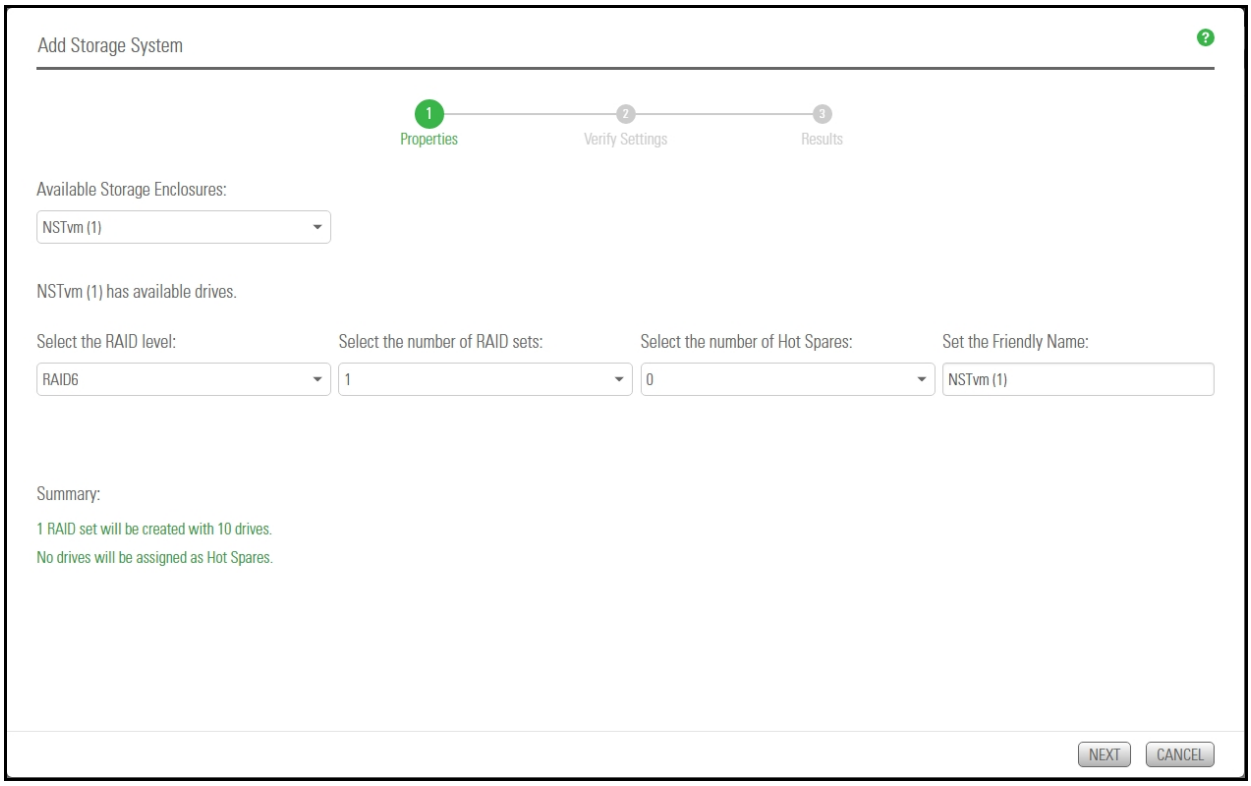
Step 1: Discovering new storage and configuring RAID settings

In *Step 1*, the **Add Storage System** wizard automatically discovers any new storage connected to Unity.

Note If the wizard fails to discover new storage, make sure the Unity system or new drives are 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 a Nexsan E-Series system, you must add the minimum number of disk drives for the new drives to be discoverable, depending on the RAID configuration of the storage enclosure.

Figure 9-1: Add Storage System wizard, Properties settings

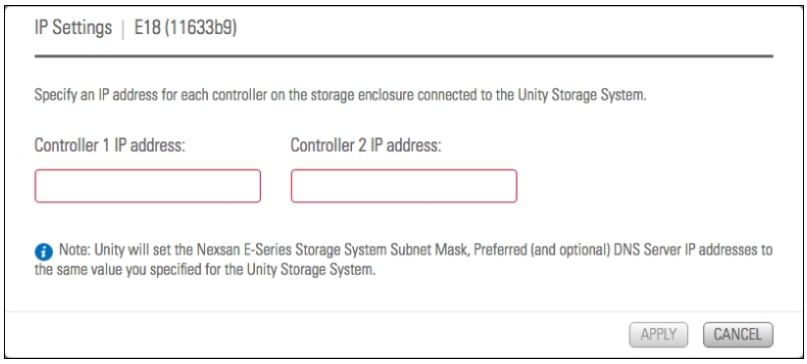


Note If the **Add Storage Systems** wizard discovers a Nexsan E-Series storage enclosure that has DHCP enabled (default configuration), the **Add Storage Systems** wizard prompts you to specify static IP addresses for the controllers on the storage system. You MUST set a static IP addresses for the storage system.

▶ To set static IP addresses for Nexsan E-Series storage:

1. Type a valid IP address in the **Controller 1** field.

Figure 9-2: IP Settings popup



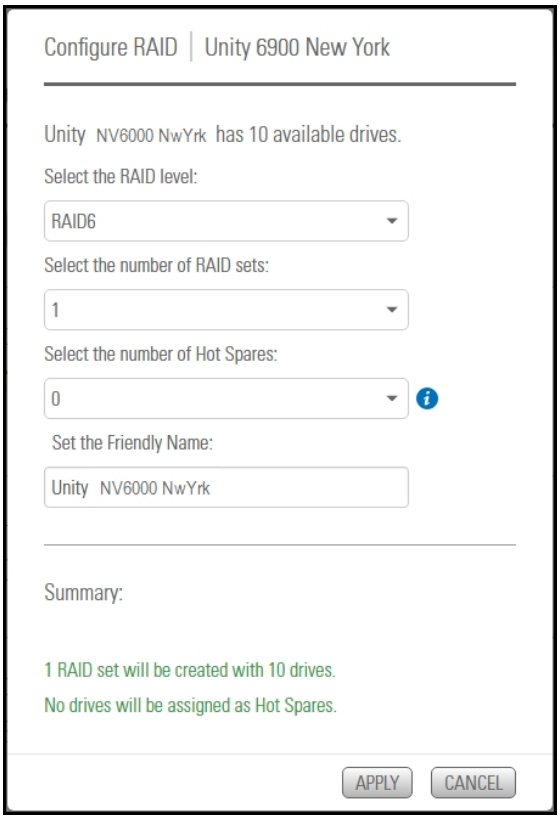
2. If applicable, type a valid IP address in the **Controller 2** field.
3. Click the **Apply** button.

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 addresses on the Unity Storage System, the Storage Configurator opens.

▶ To configure RAID settings for the storage system:

Figure 9-3: Configure RAID set popup



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.
4. (Optionally) Enter a friendly name for the storage enclosure.
5. Click **OK** to save your selections and close the Storage Configurator.
6. When you finish configuring and allocating storage, the Add Storage Systems wizard automatically moves forward to Step 2: Verifying settings on the next page.

Step 2: Verifying settings

Step 2 of the **Add Storage System** wizard summarizes your configuration settings and allocates the storage system to the site when you click **Create**. Review the summary carefully before proceeding.

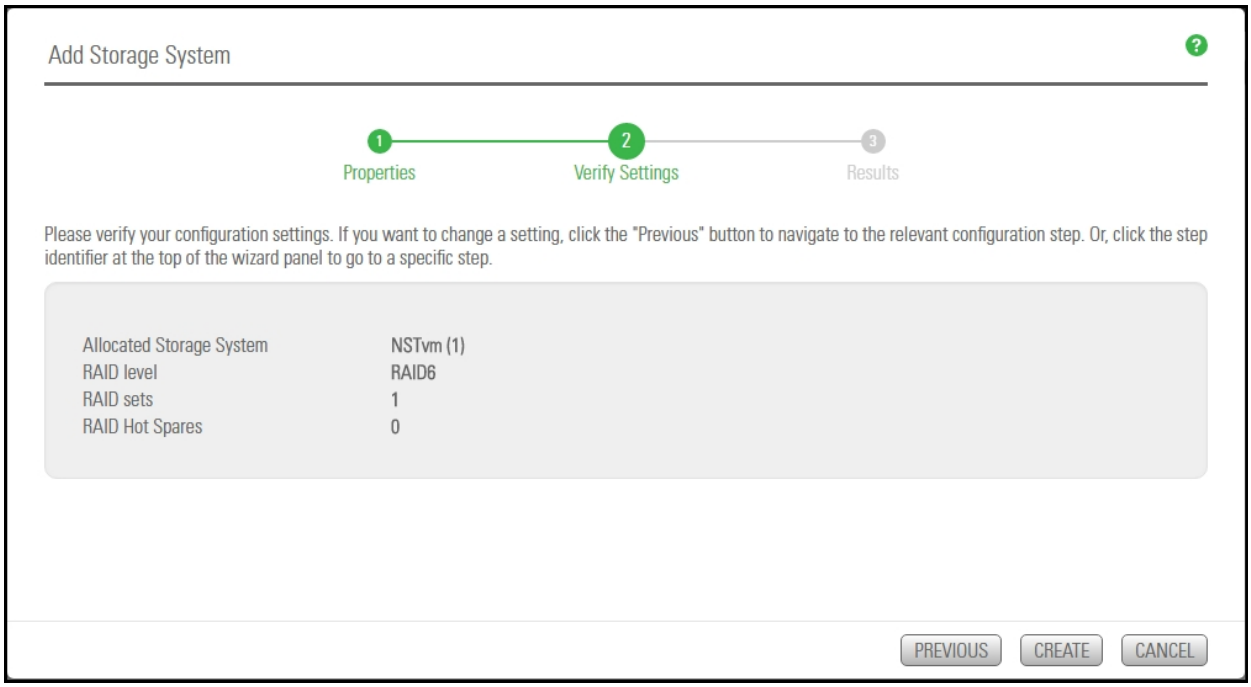
► **To change a configuration setting:**

- Click the **Previous** button to navigate back to the corresponding configuration step.

  Or

- Click the step identifier at the top of the **Add Storage System** 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 9-4: Add Storage System wizard. Verify Settings



If you are satisfied with the configuration settings, click the **Create** button at the bottom of the panel. The **Add Storage Systems** wizard automatically moves forward to Step 3: Viewing results on the facing page.

Step 3: Viewing results

Step 3 of the **Add Storage System** wizard displays progress while it configures the storage system and allocates the storage system to Unity.

The 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 **View Error** link next to the error in the **Results** panel.

Figure 9-5: Add Storage System wizard: Viewing results



Once the wizard finishes configuring the new storage system and allocates it to the Unity System, Unity adds it to the **Storage Systems** panel.

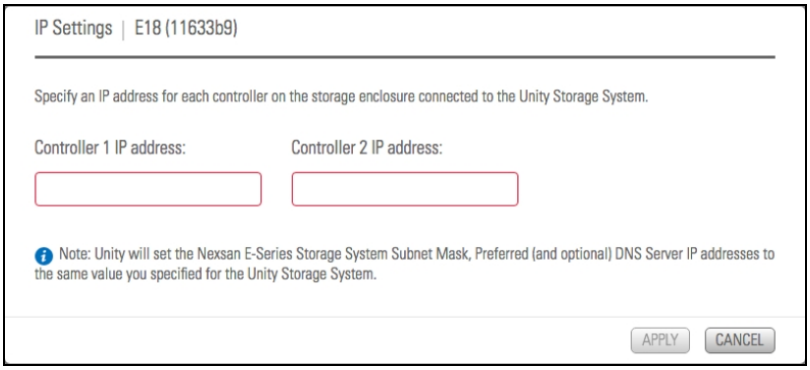
Modifying IP settings for a Nexsan E-Series/BEAST Storage System

Unity sets the Nexsan E-Series Storage System Subnet Mask, Preferred and optional DNS Server IP addresses to the same values you specified for the Unity Storage System. If necessary, you can modify the controller IP addresses as shown here.

To modify a Nexsan E-Series Storage System IP addresses:

1. Log in to a Unity Storage System with E-Series or BEAST storage attached.
2. From the **Unity navigation bar**, select **Storage > Storage Systems**.
3. Click the link to the E-Series/BEAST system.
4. Select **Summary > IP Settings**.

Figure 9-6: IP Settings popup



5. Revise the Nexsan E-Series controller 1 and 2 IP addresses as required.

Renaming a Unity Storage System

You can rename a Unity Storage System at any time. Unity will update the new name for the system for all storage pools using that Unity System.

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

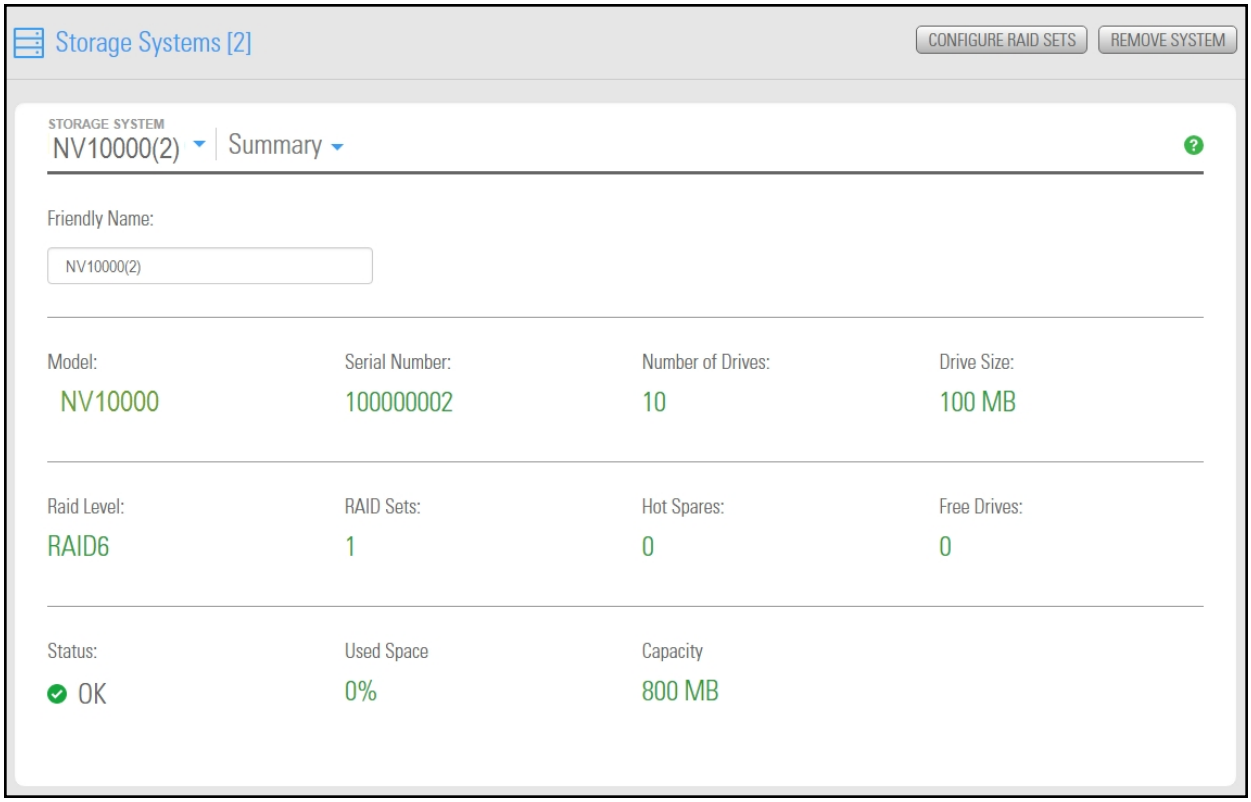
These characters are NOT allowed:

” / \ _ [ ] : ; | = , + * ? < >

To rename a storage system:

1. In the **Unity navigation bar**, select **Storage > Systems**.
2. Click the link to the storage system that you want to rename.
3. Enter a new name in the **Friendly Name** text box.

Figure 9-7: Unity Storage Systems panel



4. Click the **Apply** button.

Adding new drives to a Unity Storage System

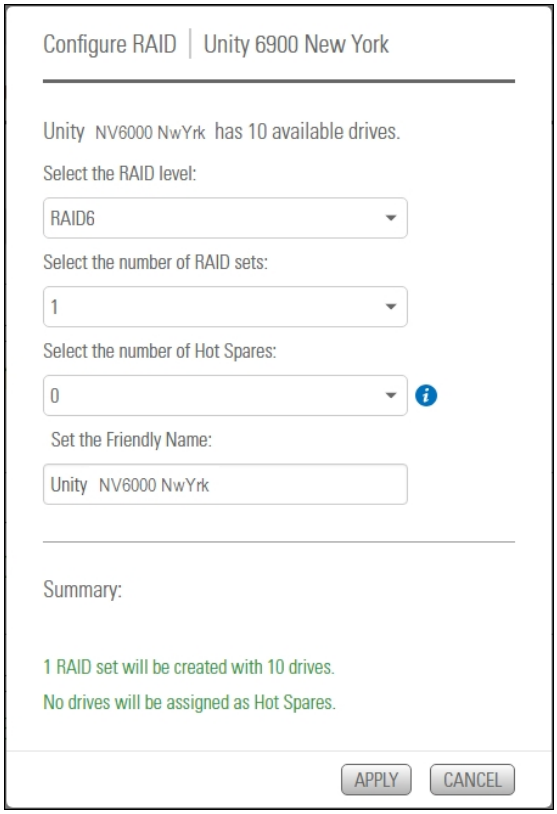
Use this procedure to add new drives to any Unity Storage System.

When new physical drives are added on a Unity Storage System, Unity automatically detects them and displays a new button on the storage properties panel.

To configure the new drives:

1. In the **Unity navigation bar**, select **Storage > Storage Systems**.
2. Click the link to the system you want to add drives to.
3. Click the **Configure RAID sets** button. The **Configure RAID** window opens.

Figure 9-8: Configure RAID window



4. From the **Select RAID level** drop-down list, select the RAID level—5, 6, or 10—that you want Unity to configure on your storage. The window 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.
5. From the **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.

6. 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 Unity 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.

7. Optionally, set a **Friendly Name** for the system.

Resetting the RAID configuration for storage

You can reset the RAID configuration on storage connected to Unity. Perform this operation if you want to specify a new RAID configuration for your storage.

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.

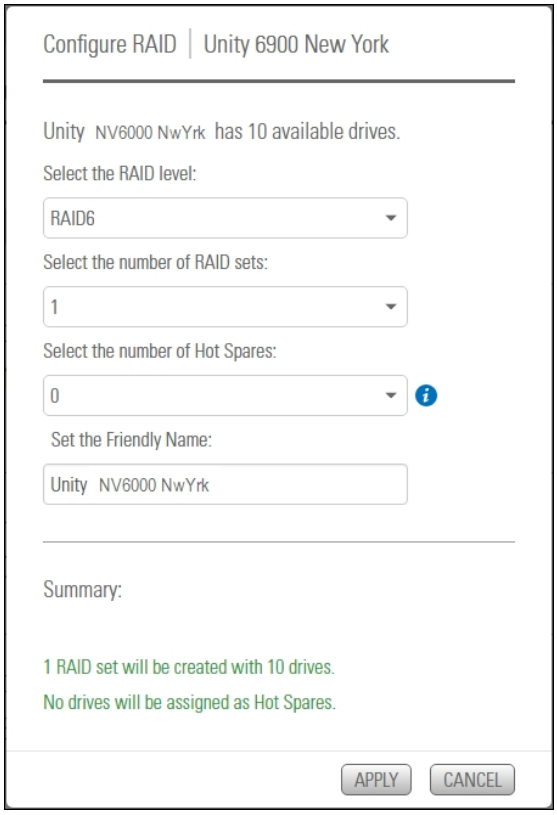
Prerequisites

- This operation can only be performed on a storage system where a volume is not currently allocated to a storage pool.

To reset the RAID configuration on storage connected to Unity:

1. On the **Unity navigation bar**, select **System > Unity Systems**.
2. Click the link to the system that you want to reset RAID settings for.
3. Click the **Configure RAID** button. The **Configure RAID** window opens.

Figure 9-9: Configure RAID window



4. From the **Select RAID level** drop-down list, select the RAID level—5, 6, or 10—that you want Unity to configure on your storage. The window 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.

5. From the **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.
6. 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 Unity 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.
7. Set a **Friendly Name** for the system.
8. Click the **Apply** button to save your selections.

Removing a Unity Storage System

Use this procedure to remove a Unity Storage System.



CAUTION: This action will permanently remove the storage system from the Unity System; if you proceed, the storage system will no longer be allocated to the Unity System.

As part of the removal process, you can specify whether or not you want Unity to delete all existing volumes (RAID sets) on the storage system, or leave them intact.

Note that Unity supports two options for the RAID sets on the system being removed:

- **Delete volumes**: With this option, you remove existing RAID configurations.
- **Leave volumes intact**. With this option, you keep the RAID configurations on the removed system.

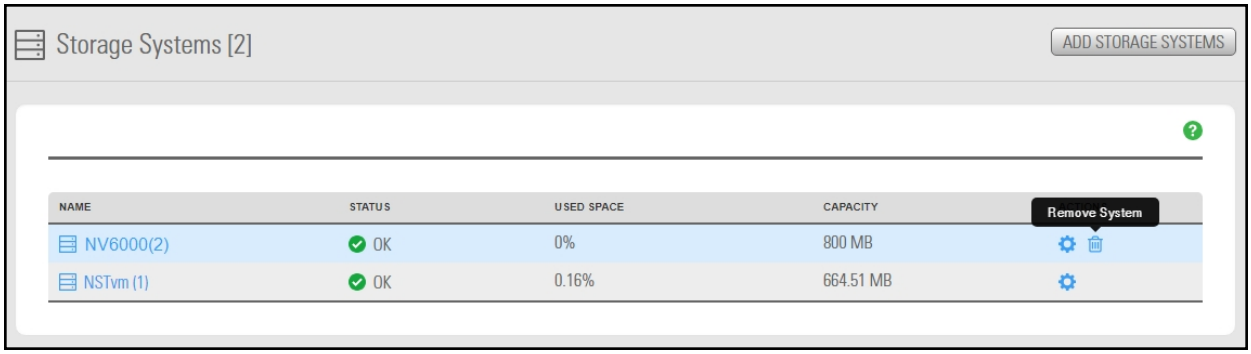
Prerequisites

- Remove storage pools allocated to the system, as described in Deleting a storage pool on page 114.

To remove a Unity Storage System:

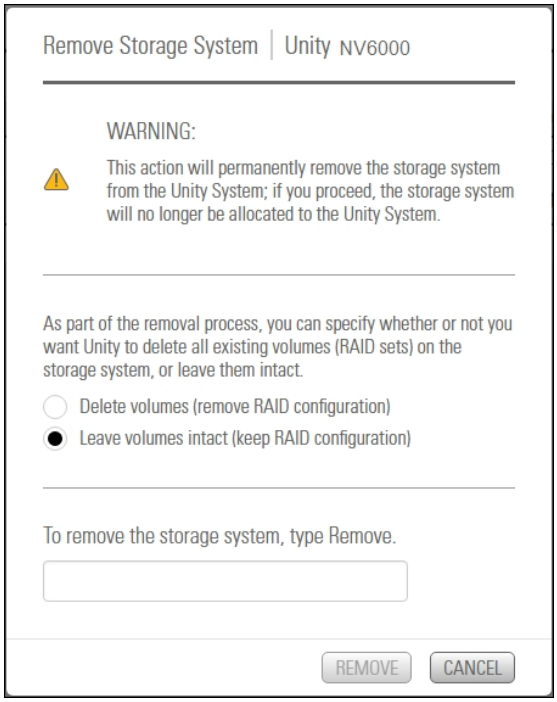
1. From the **Unity navigation bar**, select **Storage > Storage Systems**. The **Storage Systems** panel opens.

Figure 9-10: Storage Systems panel



2. In the row containing the system you that want to remove, click the **Remove System** icon. The **Remove Storage System** window opens.

Figure 9-11: Remove Storage System window



3. Choose one of the following:
   - **Delete volumes**: With this option, you remove existing RAID configurations.
   - **Leave volumes intact**. With this option, you keep the RAID configurations on the removed system.
4. Type **Remove** in the text box.
5. Click the **Remove** button to complete the operation.

What's Next:

You can now remove the storage enclosure physically

Shutting down a Unity Storage System

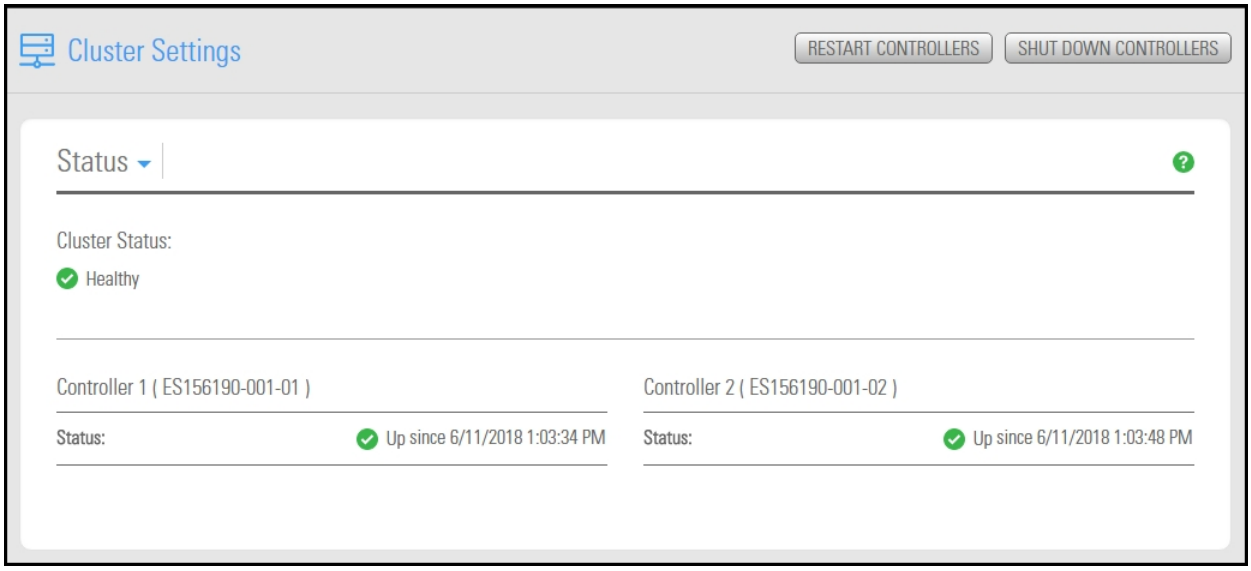
Use this procedure if you need to shut down either or both Unity Storage System controllers for maintenance or replacement. If the storage system hosts volumes associated with one or more storage pools, these storage pools and all underlying datasets will be unavailable if the storage system is shut down.

Note You cannot shut down Nexsan Unity Storage Expansions from Unity. They must be shut down physically by turning off the switches on the power supply units.

To shut down Unity Storage System controllers:

1. In the **Unity Dashboard**, select the **Cluster Status** link. The **Cluster Settings Status** panel opens.

Figure 9-12: Cluster Settings Status panel

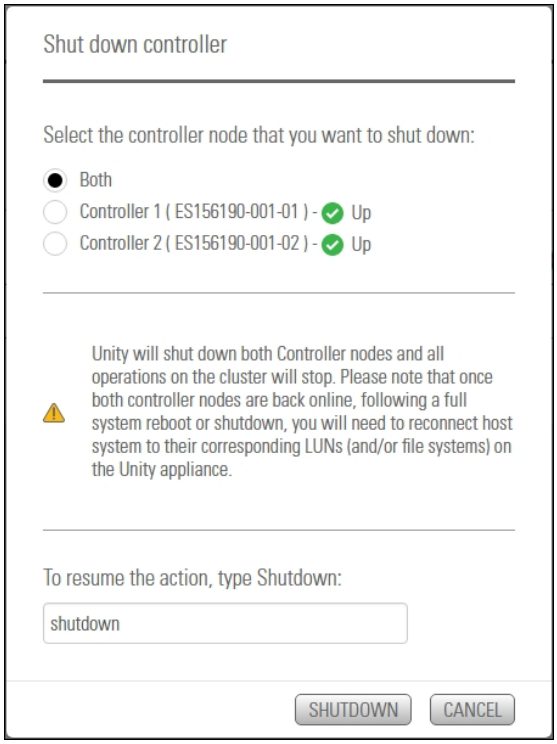


2. Click the **Shut Down Controllers** button.

3. In the **Shut down controller** window, select **Both**, **Controller 1** or **Controller 2**, as required.

   Note If both controllers are shut down, you will need to reconnect file systems and LUNs back to the host system after reboot.

Figure 9-13: Shut down controller window



4. Click the **Shutdown** button to complete the operation.

► **Related topic:**

Powering on Unity and E-Series Storage Systems on page 424

Powering on Unity controllers

This topic describes how to restart Unity controllers after a planned shutdown operation or to recover from a power outage.

If you shut down one or more storage systems as part of a maintenance or replacement operation, you can simply restart the storage systems from Unity.

If you experienced a power outage and all systems are down, you must follow a specific power-on sequence to ensure data integrity.

Power on the systems in this order:

1. If a 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. Power on Unity (see below).

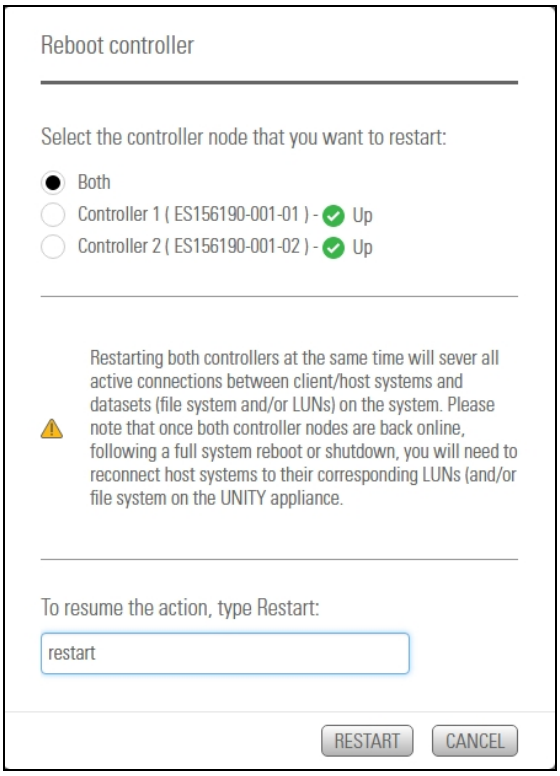
CAUTION: You must not restart Nexsan E-Series storage enclosures using the E-Series graphical user interface. This could result in storage pools being unavailable or data loss.

To power the systems back on:

1. Power on the Unity Storage Expansions using the power button, then verify power and drive LEDs are illuminated.
2. Power on the Unity Storage Systems using the power button, then verify power and drive LEDs are illuminated.

3. Restart the Unity Controllers:
   a. Log in to Unity.
   b. In the **Unity Dashboard**, select the **Cluster Status** link. The **Cluster Settings Status** panel opens.
   c. Click the **Restart Controllers** button.

Figure 9-14: Reboot controllers window



   d. Type **restart** in the text box.
   e. Click the **Restart** button.

Shutting down a Nexsan E-Series Storage System

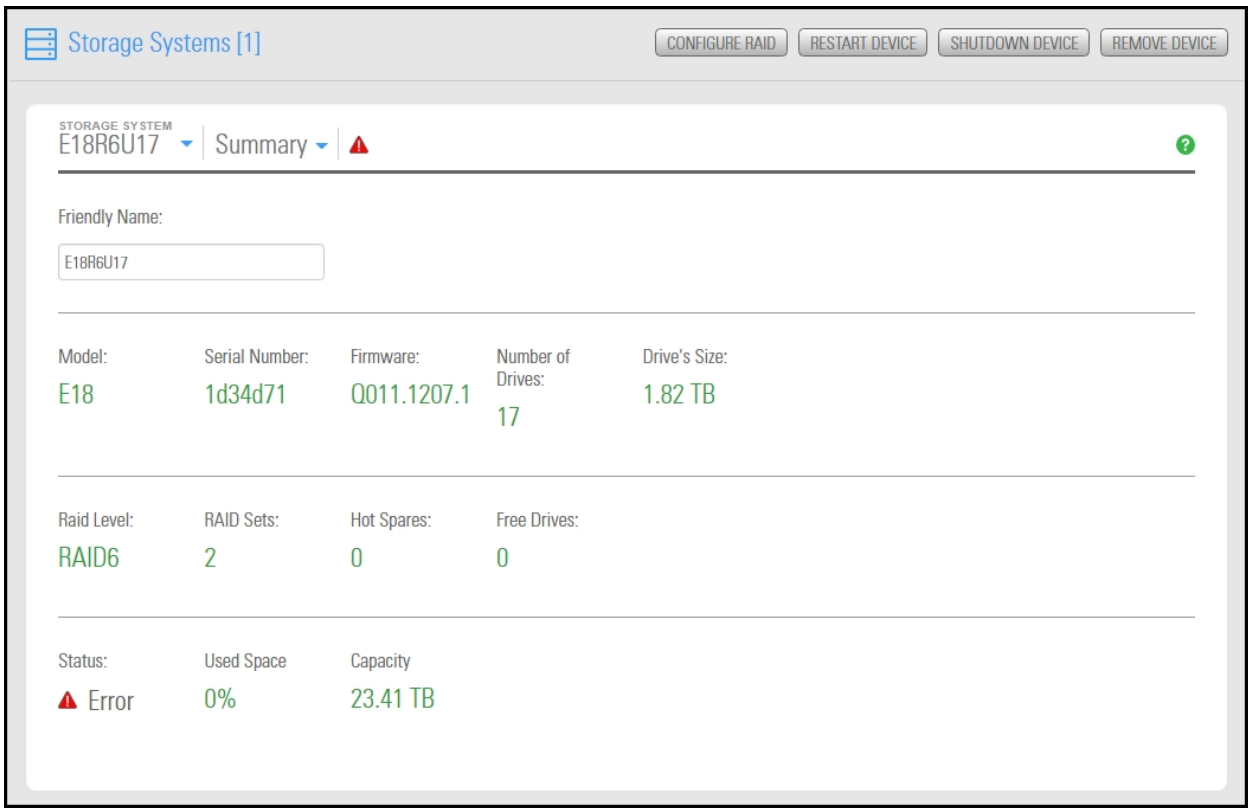
Use this procedure if you need to shut down either or both Unity Storage System controllers for maintenance or replacement. If the storage system hosts volumes associated with one or more storage pools, these storage pools and all underlying datasets will be unavailable if the storage system is shut down.

Note You cannot shut down Nexsan Unity Storage Expansions from Unity. They must be shut down physically by turning off the switches on the power supply units.

▶ **To shut down a Nexsan E-Series Storage System from within Unity:**

1. On the **Unity navigation bar**, select the **Storage > Storage Systems**.
2. Click the link to the system that you want to shut down. The **Storage Systems Summary** panel opens.

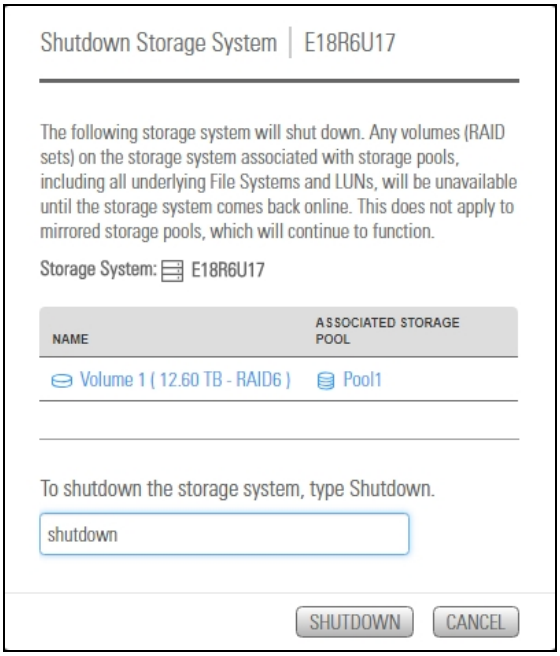
Figure 9-15: Storage Systems panel



3. Click the **Shutdown Device** button.

4. In the **Shutdown Storage System** window, type **shutdown**.

Figure 9-16: Shutdown Storage System window



5. Click the **Shutdown** button to complete the operation.

► **Related topic:**

Powering on Unity and E-Series Storage Systems below

Powering on Unity and E-Series Storage Systems

This topic describes how to restart Unity Storage Systems after a planned shutdown operation or to recover from a power outage.

If you shut down one or more storage systems as part of a maintenance or replacement operation, you can simply restart the storage systems from Unity.

If you experienced a power outage and all systems are down, you must follow a specific power-on sequence to ensure data integrity.

► **Power on the systems in this order:**

1. If a 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.

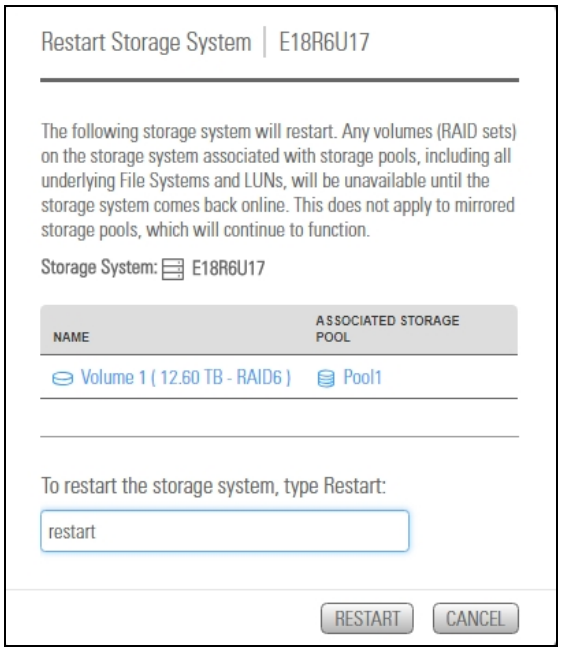
   Note If a drive carrier activity LED does not light up, check to make sure the corresponding drive is properly seated in the chassis.
3. Power on any Unity Storage Expansions.
4. Power on the Unity Storage System (see below).

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 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 Systems and wait 2 minutes.
3. Power on the Unity Storage System using the power button, then verify power and drive LEDs are illuminated..
4. Power on the Unity Storage Expansions as described in the previous step.
5. Reboot the Nexsan E-Series storage enclosures in Unity:
   a. Log in to Unity.
   b. In the **Unity Dashboard**, select the **Cluster Status** link. The **Cluster Settings Status** panel opens.
   c. Click the **Restart Controllers** button.

Figure 9-17: Restarting Storage System window



   d. Type **restart** in the text box.
   e. Click the **Restart** button.

Using Self-Encrypting Drives (SEDs)

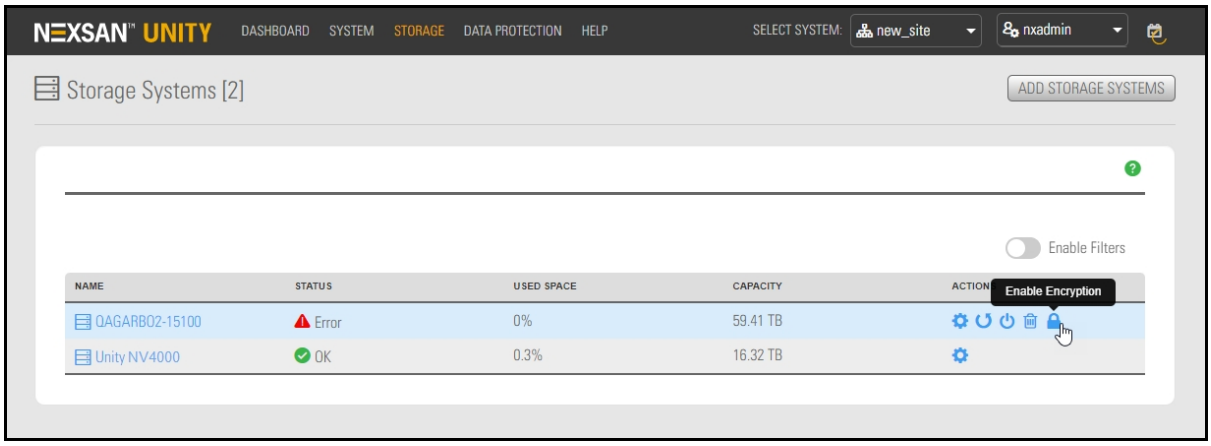
Use this procedure to enable SED encryption on drives with SED capability.

Enabling SED encryption:

1. On the **Unity navigation bar**, click **Storage > Storage Systems**. A list of available systems appears, including those which may be encrypted.

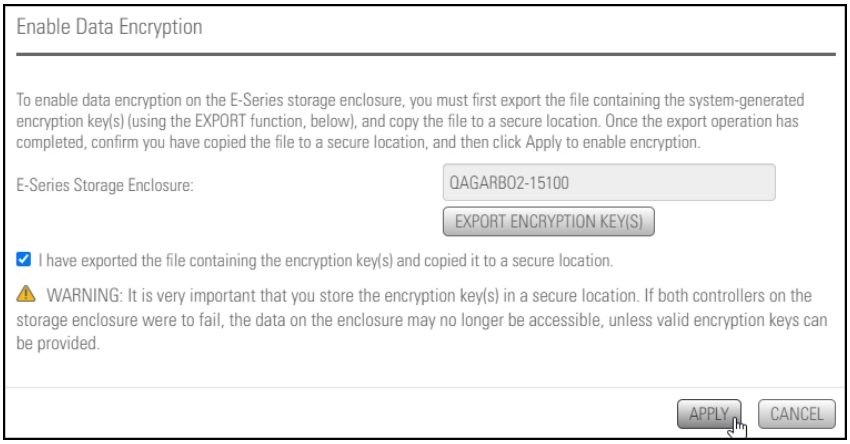
2. For the target system, click the **Enable Encryption** icon in the **Actions** column.
   The **Enable Data Encryption** dialog appears.

Figure 9-18: Storage Systems list showing Enable Encryption icon



3. In the **Enable Data Encryption** dialog, click the **Export Encryption Key(s)** button. In Windows, the keys will be downloaded to the Downloads folder, with the following file name: `Nexsan-<Storage System name>-EKF.dat`.
4. Select the check box indicating that you have backed up the keys.

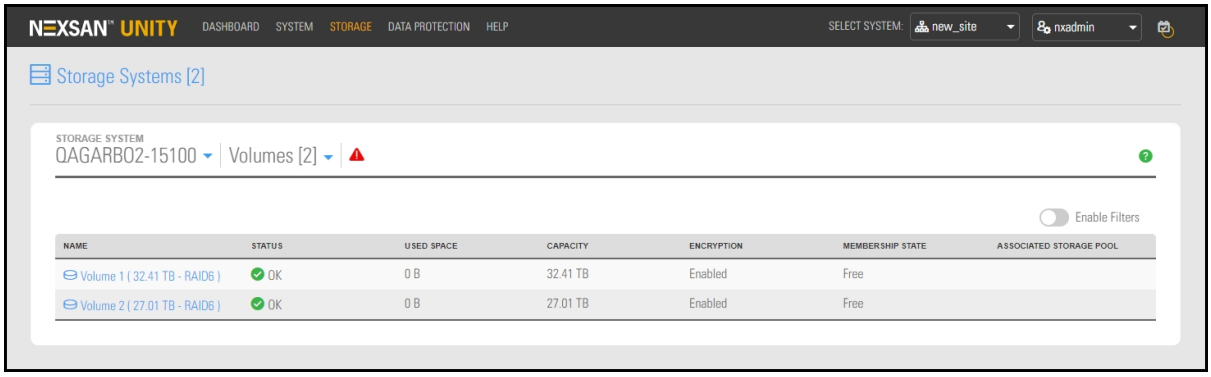
Figure 9-19: Enable Data Encryption dialog



CAUTION: You must back up the keys to a secure location. Loss of keys may result in loss of all data.

5. Click the **Apply** button.
6. In the **Volumes** panel, verify that encryption is enabled for individual volumes in the target system.

Figure 9-20: Volumes panel for selected Storage System



Disabling SED encryption

Use this procedure to disable SED encryption on drives with SED capability.

Disabling SED encryption:

1. On the **Unity navigation bar**, click **Storage > Storage Systems**. A list of available systems appears, including those which may be decrypted.
2. For the target system, click the **Disable Encryption** icon in the **Actions** column.

   The **Disable Data Encryption** dialog appears.
3. To disable encryption on the storage system, type 'Disable', then click the **Disable** button.

Figure 9-21: Disable Data Encryption dialog



4. Verify that encryption is disabled in the **Volumes** panel.

9

Chapter 10

Using Active Archive

When using Unity 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 enables 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

Use this procedure to connect 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.

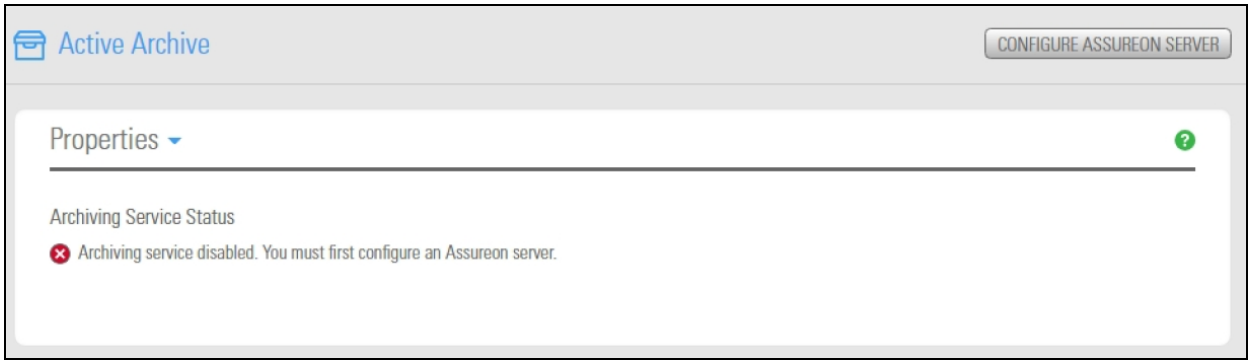
Prerequisites

- The server name, certificate file, and password for the Assureon server.

To configure Active Archive:

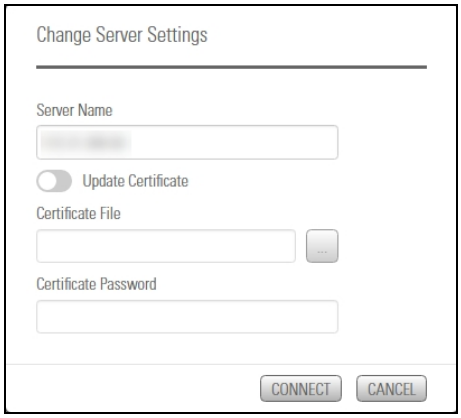
1. On the **Unity navigation bar**, select the **Data Protection > Archive**. The **Active Archive Properties** panel opens.

Figure 10-1: Active Archive Properties panel



2. Click the **Configure Assureon Server** button.
3. Do the following:
   a. Enter the Assureon **ServerName**.
   b. Add a certificate file. Click the browse button to locate the certificate file on your system.
   c. Enter the certificate password.

Figure 10-2: Change Server Settings popup



4. Click the **Connect** button.

See also Managing Active Archive settings for file systems on the facing page

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

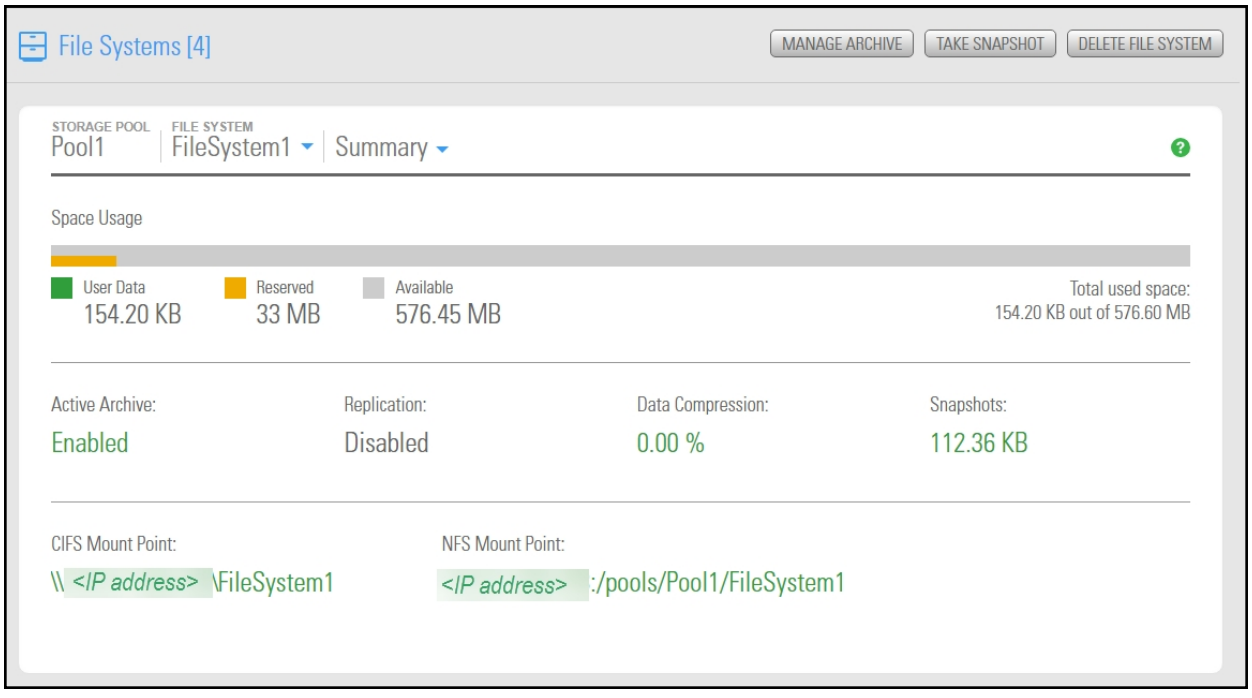
Prerequisites

- 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*, or visit Nexsan.com/support.

To manage Active Archive settings for a file system:

1. On the **Unity navigation bar**, select **Storage > File Systems**.
2. 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.

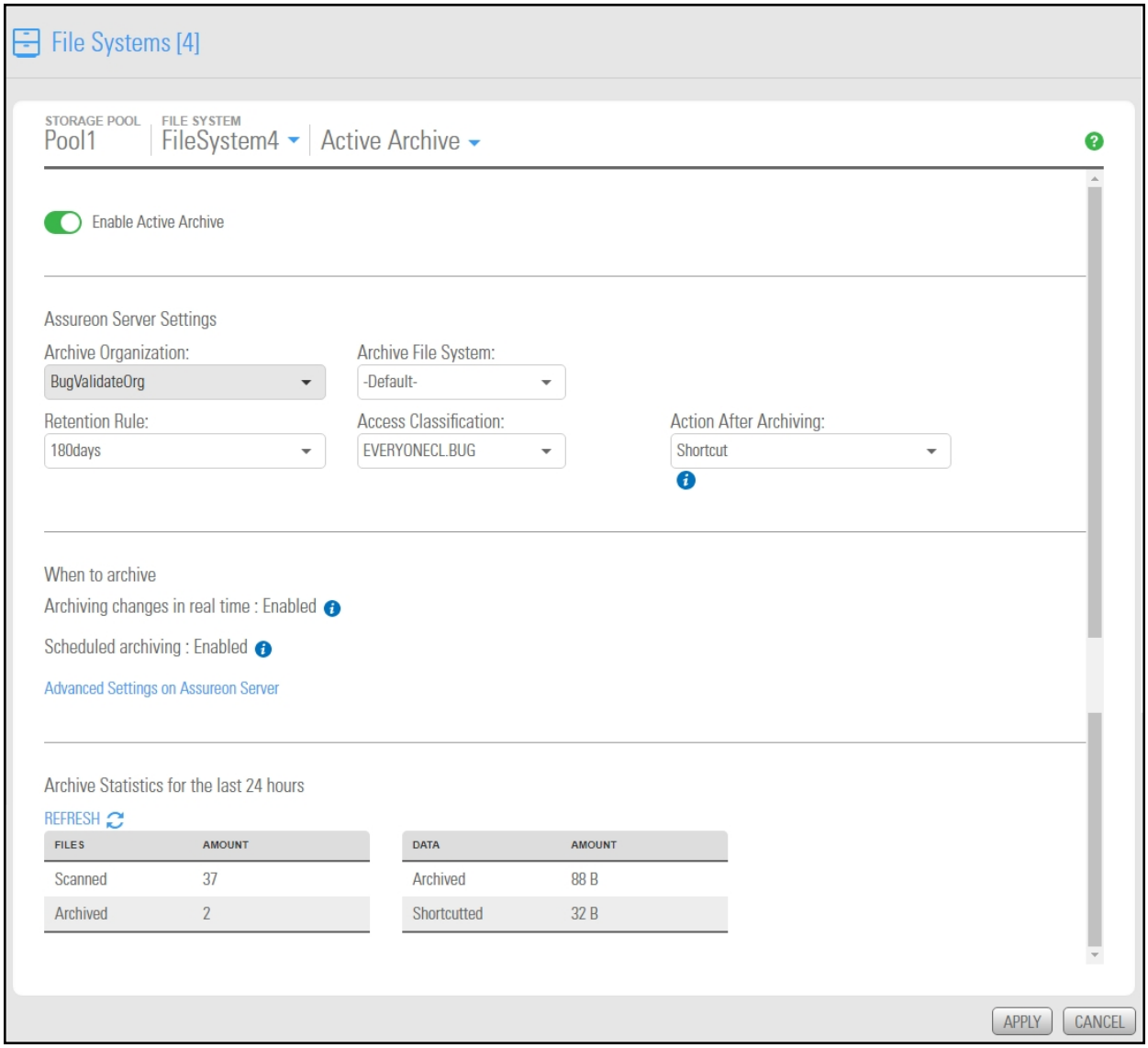
Figure 10-3: File Systems panel



3. Click the **Manage Archive** button. The **Active Archive** panel opens.

4. Select the **Enable Active Archive** button

Figure 10-4: File Systems Active Archive panel



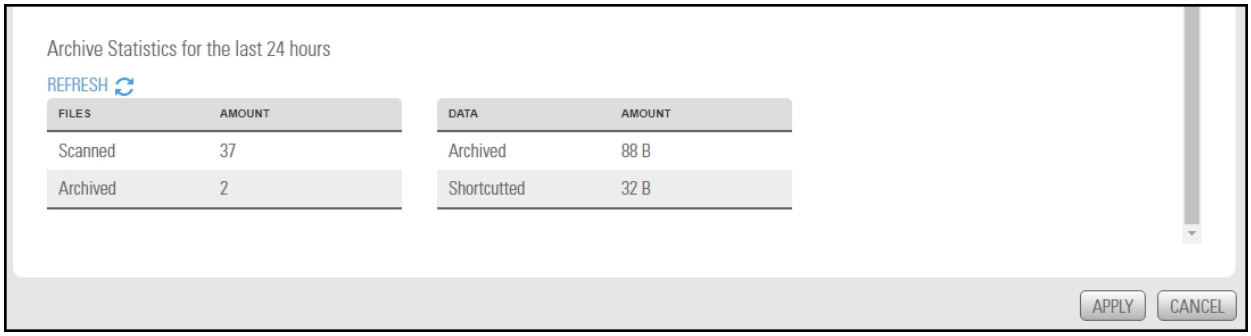
5. The following Active Archive settings are the settings on Assureon Server by which data from your file system will be archived. The options that appear here are defined on the Assureon Server.

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. For example, create a shortcut to the files, leave them as they are, or remove them from the file system. **Note** Files will not be converted to shortcuts, or removed if asynchronous replication is enabled.
Real Time Archiving	Performs a persistent and ongoing archive of files, as changes are detected. Files are checked and archived if necessary every minute. Enabled or disabled on the Assureon Server under **Advanced Settings**, or using the nxcmd command line interface. See "Setting the realtime delay" in the *nxcmd Command Line Interface Reference Guide*, or visit Nexsan.com/support.
Scheduled Archiving	Performs a complete archive of the file system, either manually or on a schedule. This feature does not affect Real Time Archiving. Enabled or disabled on the Assureon Server on the **Advanced Settings > General tab**. Select the **Sync** checkbox.

6. To view archiving statistics for the past 24 hours, click **Refresh**.

Figure 10-5: Archive Statistics



To disable Active Archive:

1. Select the **Enable Active Archive** button .
2. Click the **Apply** button to save your changes.

Viewing archived file systems

Use this procedure for information about viewing archived file systems.

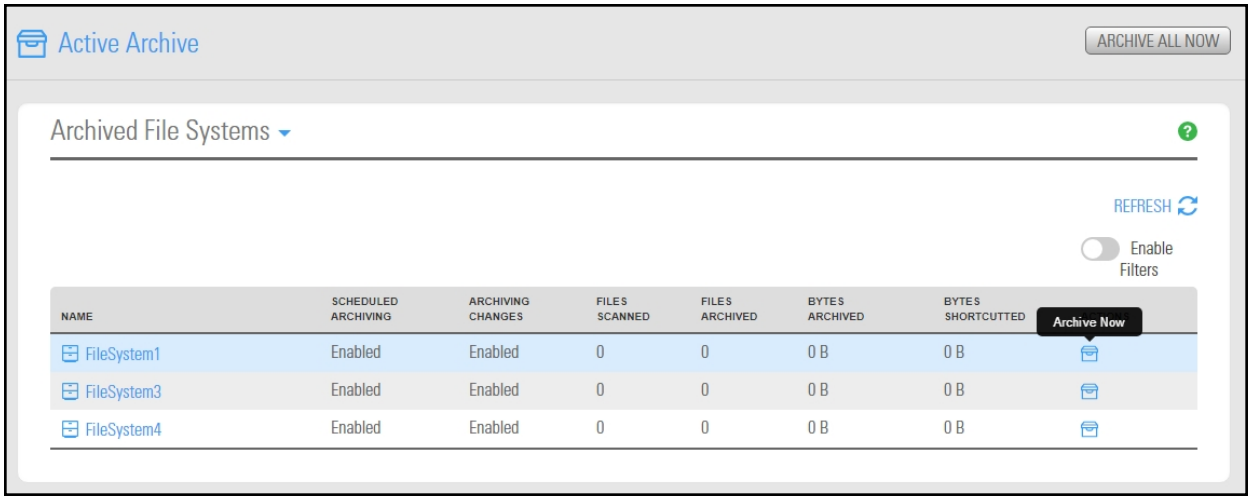
Prerequisites

- You must have the optional Assureon Active Archive service enabled.
- Before the Archived File Systems panel can show a file system as archived, data must be added to the file system.
- 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,* or visit Nexsan.com/support.

To view archived file systems:

1. On the **Unity navigation bar**, select the **Data Protection > Archive**. The **Active Archive Properties** panel opens.
2. Click the **Properties > Archived File Systems**.

Figure 10-6: Archived File Systems



See also Managing Active Archive settings for file systems on page 431

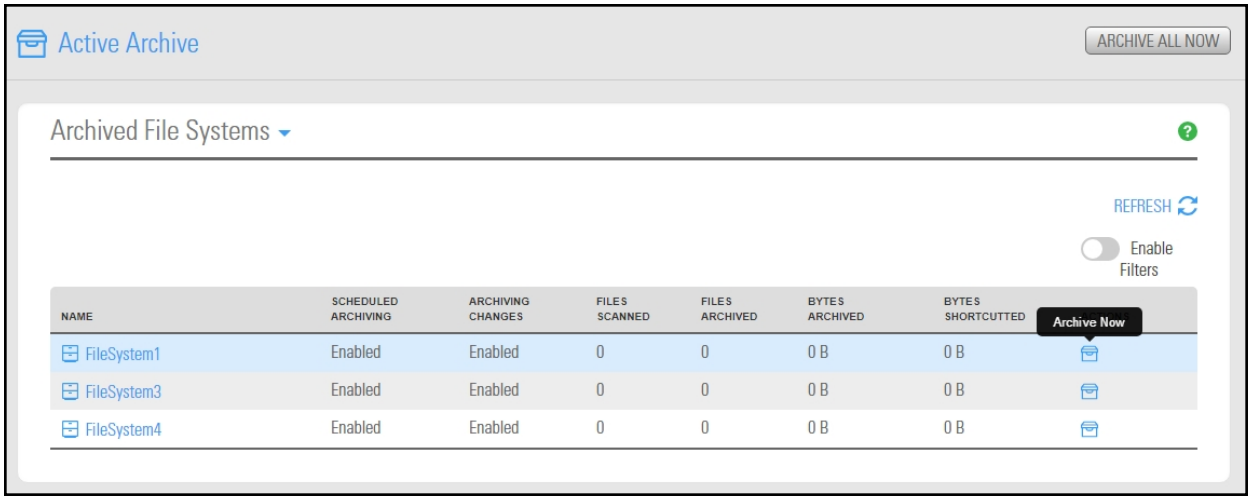
Performing manual archiving to Assureon

The Archived File Systems panel displays information on all the file systems on this Unity System that are currently being archived to the Assureon Server.

To manually archive a file system configured for Active Archive:

1. On the **Unity navigation bar**, select **Data Protection > Archive**.
2. Select **Properties > Archived File Systems**.
3. Select the file system that you want to manually archive.
4. Do one of the following:
   - If the currently selected Unity System has only one file system configured, click the **Archive Now** button.
   - If there are multiple Unity file systems configured, click the **Archive All Now** button or click the **Archive Now** icon in the row of the file system that you want to archive .

Figure 10-7: Archived File Systems panel



10

Chapter 11

Unity System-level tasks

Unity provides several tools and functions for managing 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 Asynchronous data replication on page 501.

This section includes these topics:

Changing the Unity Storage System name 438
Modifying the time server used 438
Setting NDMP configuration options 439
Modifying User Interface preferences 440
Manually refreshing Unity Storage Systems 442
Connecting to a remote Unity System 442
Disconnecting a remote Unity Storage System 443
Disconnecting Unity Systems in a multi-system implementation 444
Updating Unity 446
Modifying authentication settings 452
Troubleshooting Unity System-level warning and error conditions 477
Configuring NFS settings 479
Viewing APAL status 481
Viewing NVDIMM status 481
Enabling FTP support 482
Using the CallHome feature 484
Enabling Internet connectivity 493

Changing the Unity Storage System name

You set the system name for the Unity Storage System during the System Configuration process. You can change the Unity system name at any time.

To change the Unity Storage System name:

1. On the **Unity navigation bar**, select **System > Unity Systems**.
2. Click the link to the Unity System that you want to rename.
3. Enter a new name in the **System Name** box.. Make sure that the new name adheres to these restrictions and conventions:
   - Spaces are allowed
   - The system 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 hyphen (-) and period (.), the name can only contain alphanumeric characters, without spaces.

   These characters are NOT allowed:

   ```
   ” / \ _ [ ] : ; | = , + * ? < >
   ```
4. Click the **Apply** button.

11

Modifying the time server used

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. On the **Unity navigation bar**, select **System > Unity Systems**.
2. Click the link to the Unity System you want to update.
3. Select **Summary > User Authentication**.
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 the **Apply** button 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 enables 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. On the **Unity navigation bar**, select **System > Unity Systems**.
2. Click the link to the Unity System you want to update.
3. Select **Summary > User Authentication**.
4. Select the **Enable NDMP** button to enable NDMP on Unity.
5. Click the **Create NDMP User Account** button.
6. Type the NDMP user name in the **User name** field.
7. Type the password for the NDMP user in the **Password** field.
8. 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.
9. Click the **Apply** button to set the NDMP configuration options for Unity.
10. If needed, set or configure advanced options for NDMP in the nxadmin command line interface (CLI); see the `nstndmp` command in the CLI.

Modifying User Interface preferences

Unity provides the **UI Preferences** panel, available from the Systems menu, for configuring the system auto-refresh interval and date and time formats for the Unity Storage System.

This section includes these topics:

Modifying the auto-refresh interval 440
Modifying date and time formats 441
Changing the Unity System time zone 442

Modifying the auto-refresh interval

You can modify the auto-refresh interval in the **UI Preferences** panel.

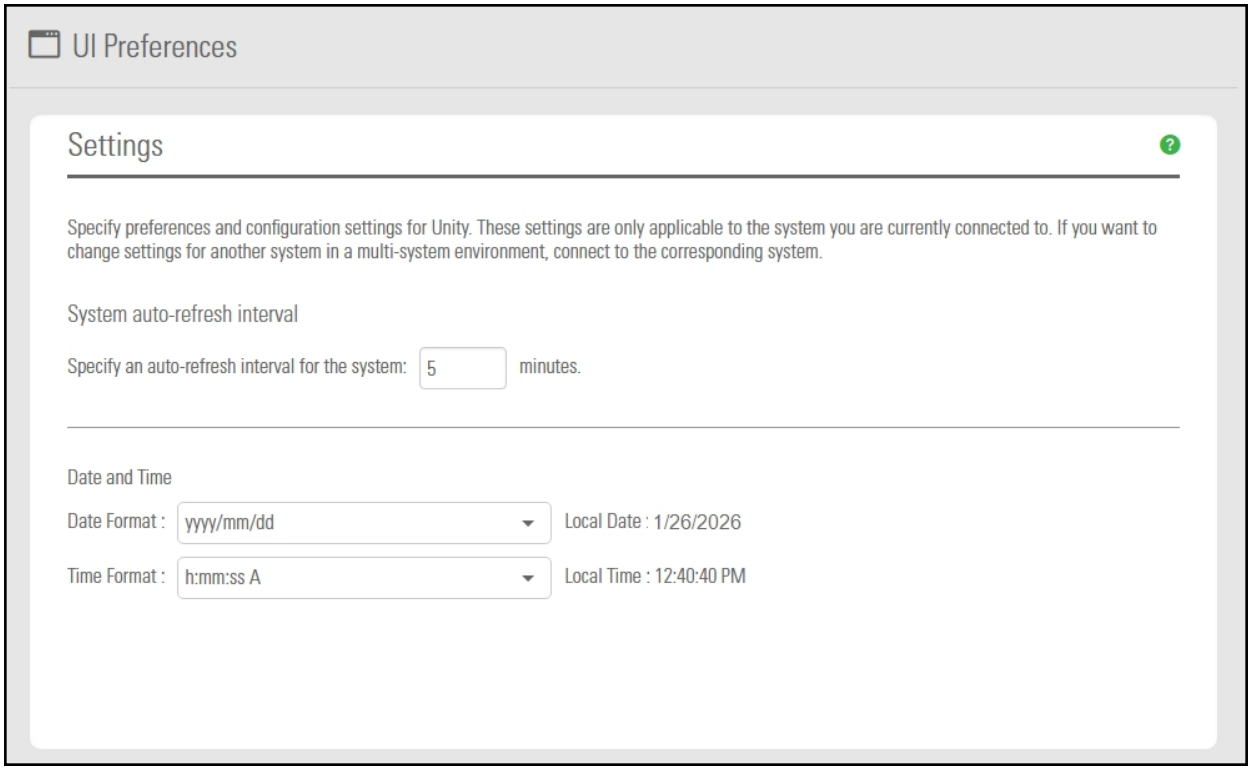
Note Setting too low an interval may cause network congestion and affect the overall performance of the system. If you need to refresh configuration and status information for Unity, you can perform a manual refresh at the Unity System level—or, at the file system-level, to obtain updated information for file systems on the system. See Manually refreshing Unity Storage Systems on page 442.

By default, Unity automatically updates configuration and status information for the Unity Storage System every 5 minutes, and then displays the updated information.

To modify the Unity auto-refresh interval:

1. On the **Unity navigation bar**, click **System > UI Preferences**. The **UI Preferences Settings** panel opens.

Figure 11-1: UI Preferences Settings panel



2. Enter a new auto-refresh interval, in minutes. 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.
3. Click the **Apply** button to save the changes and close the panel.

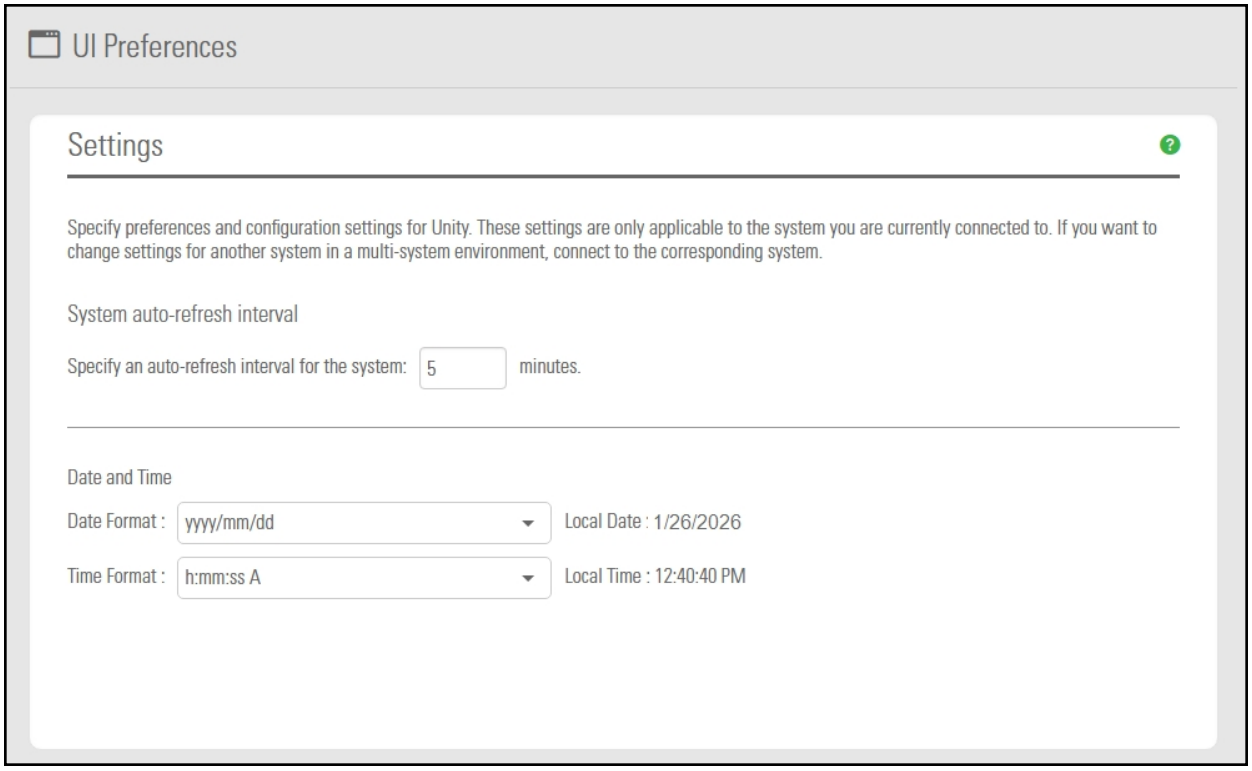
Modifying date and time formats

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.

▶ **To modify the date and time formats displayed in Unity:**

1. On the **Unity navigation bar**, click **System > UI Preferences**. The **UI Preferences Settings** panel opens.

Figure 11-2: UI Preferences Settings panel



2. 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.
3. Click the **Apply** button to save the new date and/or time format, and close the Preferences panel.

Changing the Unity System time zone

Typically, you set the date, time, and time zone for Unity during the Unity System configuration process. If you need to change the system time after initial setup, please see "Setting the Unity system time" *in the nxcmd Command Line Interface Reference Guide.*

Manually refreshing Unity Storage Systems

You can manually refresh Unity Storage System information. This does not impact the auto-refresh schedule.

To manually refresh system-level information:

1. On the **Unity navigation bar**, select **System > Unity Systems**.
2. Click the **Refresh System Cache** button.

Connecting to a remote Unity System

Unity provides central management for multiple Unity Storage Systems on the network. This enables you to manage multiple Unity Systems from a single browser session. From a single Unity that you designate as the central management hub for all Unity Systems installed on your LAN or WAN.

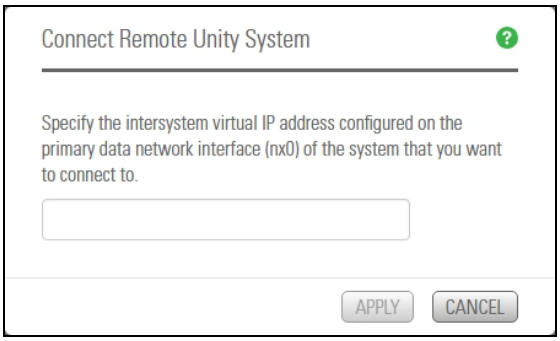
For example, if you have three systems installed in three different geographic locations: Hong Kong, Montreal, and San Diego, you can designate the system in Montreal as the management hub for your Nexsan storage infrastructure. Then, to enable multi-site management, you add the systems in Hong Kong and San Diego to Unity in Montreal using the Unity software. You can now administer all three Unity Systems from a Unity session running on the system in Montreal by navigating between systems.

Note This task can also be performed using the **Asynchronous Replication** wizard. See Setting up asynchronous data replication on page 506.

To add a remote Unity Storage System:

1. On the **Unity navigation bar**, select **System > Unity Systems**.
2. Click **Connect Remote Unity System**.

Figure 11-3: Connect to a Remote Unity System popup



3. In the text box, type the Intersite virtual IP address configured on the primary data network interface (nx0) of the remote site.
4. Click the **Apply** button to establish a connection to the remote Unity Storage System.

   Unity connects to the remote system and checks to ensure that it is configured properly: the remote system must be properly set up using the System Configuration wizard. Depending on the speed of your network connection, this process can take some time to complete.

5. 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 Administrator role on the remote site, Unity prompts you for user credentials to connect to the remote system.

   You must provide the Unity Administrator (**nxadmin**) credentials for the remote Unity:

To...	Do this
log on as the Unity Administrator (**nxadmin**)	a. In the **User name** field, type the user name of a Administrator on the remote Unity. b. In the **Password** field, type the password for the Administrator on the remote Unity. c. In the **Password** field, type the password for the Unity Administrator (**nxadmin**) on the remote Unity. d. 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.

Disconnecting a remote Unity Storage System

Use this procedure to disconnect a remote Unity Storage System from the primary Unity Storage System.

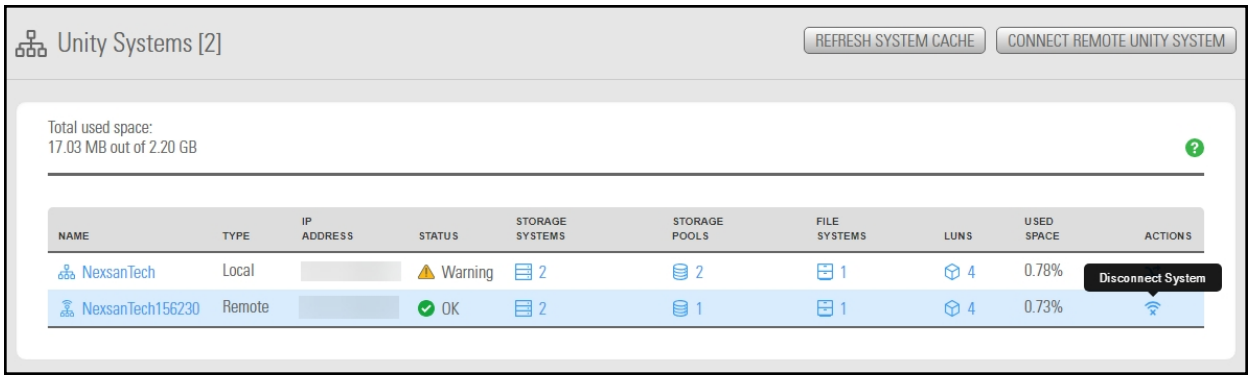
11

Prerequisites

- If the Unity System has replication set up, you must remove the replication for all storage pools on that system first, as described in Removing asynchronous data replication for a storage pool on page 532.

▶ **To disconnect a remote Unity Storage System:**

1. On the **Unity navigation bar**, select **System > Unity Systems**.



2. Select the **Disconnect System** icon in the row listing the remote system.
3. In the **Disconnect System** popup window, click the **Disconnect** button complete the action.

Note If Unity displays an error message because the system is inaccessible, proceed only if you expect the system to be permanently inaccessible.

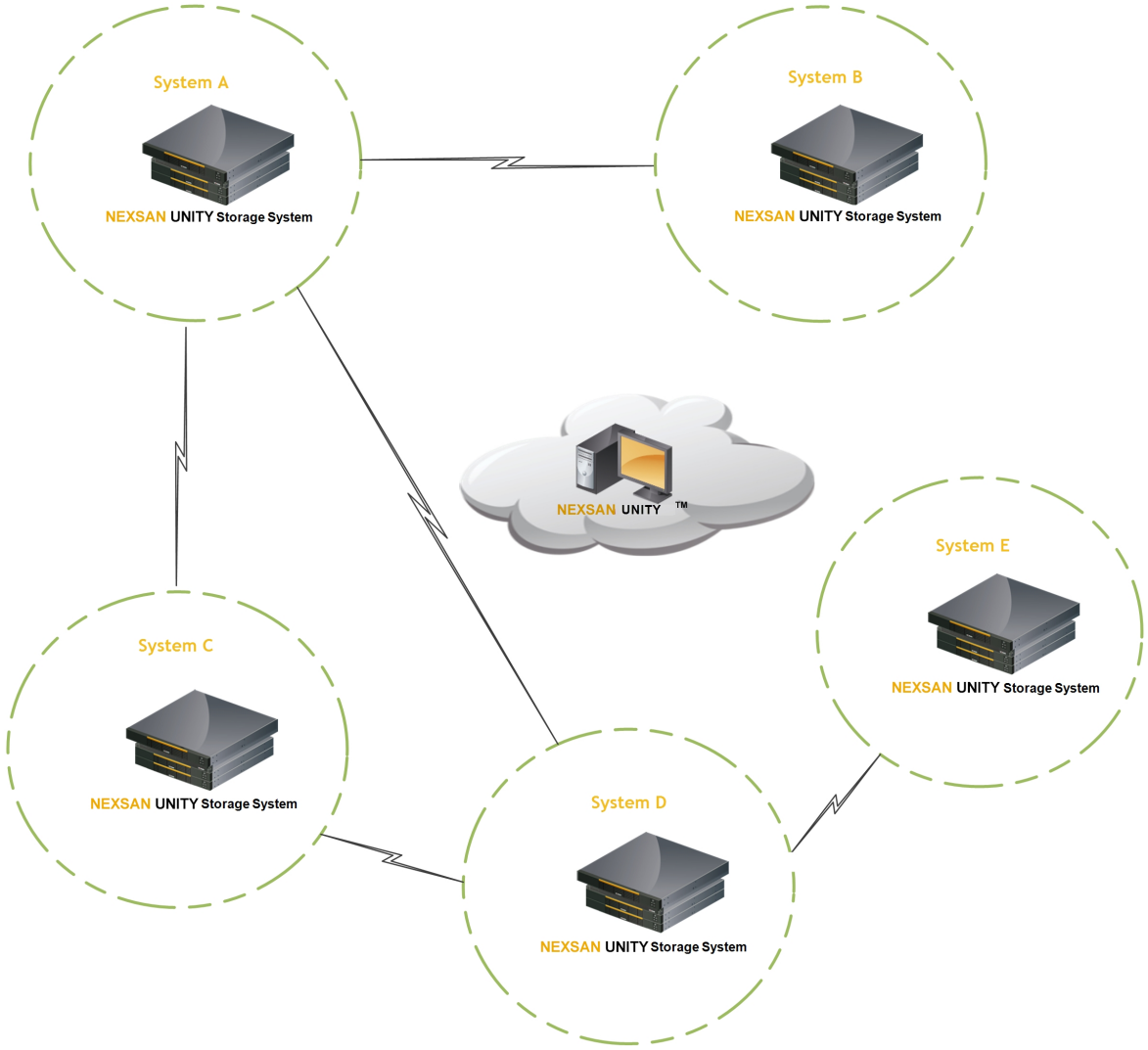
The selected Unity Storage Systems are no longer connected to the primary Unity Storage System.

Disconnecting Unity Systems in a multi-system implementation

In a multi-Unity Storage System implementation, one system can be connected to two or more others. You can choose to remove a connection between two Unity Systems while keeping the connection between others. When you disconnect a Unity System from one remote system, connections to other remain intact. To completely remove a Unity System from your multi-system implementation, you must disconnect it from all systems to which it is connected. If a selected system is connected to only one system, it is removed from Unity immediately.

You must select the primary system from which a remote system was connected in order to disconnect the remote system.

Figure 11-4: An example mufti-system implementation

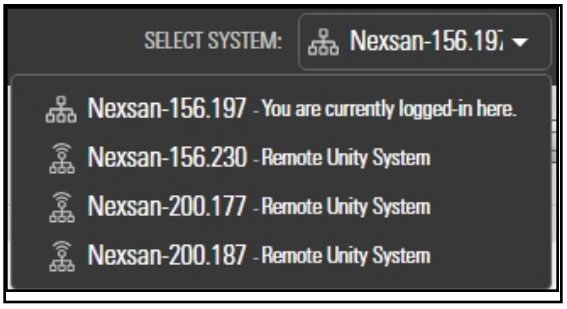


Prerequisites

- If the Unity System has replication set up, you must remove the replication for all storage pools on that system first, as described in the *Nexsan Unity Snapshots and Replication Guide*.

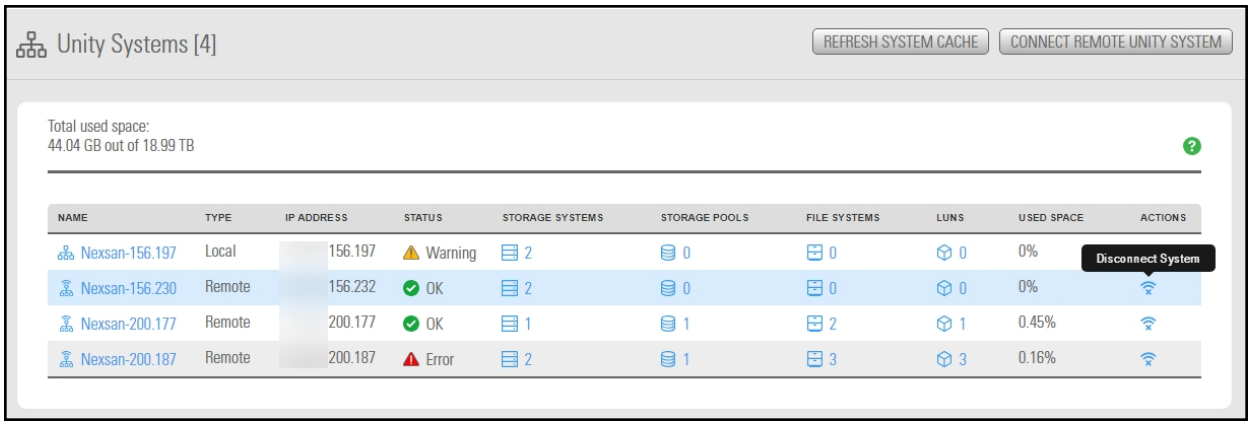
To disconnect sites in a multi-site implementation:

1. In the **Unity navigation bar**, select the primary system that you want to disconnect other systems from.



2. In the **Unity navigation bar**, select **System > Unity Systems**. Unity displays the list of Unity Storage Systems connected to the selected system.

Figure 11-5: A multi-system Unity configuration



3. Select the **Disconnect System** icon beside the Unity Storage System that you want to disconnect.
4. Unity displays the **Disconnect System** popup window.
5. Click the **Disconnect** button.

   Note If Unity displays an error message because the system is inaccessible, proceed only if you expect the system to be permanently inaccessible.

The selected Unity Storage Systems are no longer connected to the primary Unity Storage System.

Updating Unity

The Nexsan firmware updater provides options you can use to:

- update firmware components on Unity. This also updates the firmware updater itself.
- add new features to Unity
- update the cluster license to a permanent license

Topics in this section:

Upgrading to the latest firmware 447
Adding new features 449
Upgrading the cluster license 451

11

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 upgrade you are entitled to perform on Unity depends on whether 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: 6.x.x to 7.x.x.
- Without a maintenance plan, you can only update firmware components to a minor release; for example: 7.2.x to .7.3.x.

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 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 updating, we recommend the following:

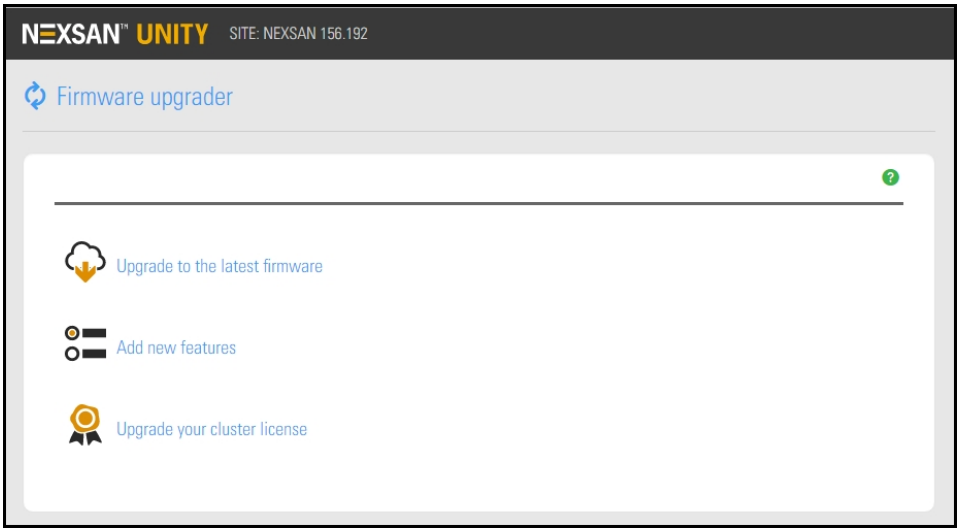
- Disconnect any client system with an active connection to datasets (file systems and/or iSCSI LUNs) on Unity.
- Quiesce any applications with an active connection to Unity.

Note If there is an attached E-Series that also needs a firmware upgrade, your Unity will need to be taken offline.

To perform a firmware upgrade:

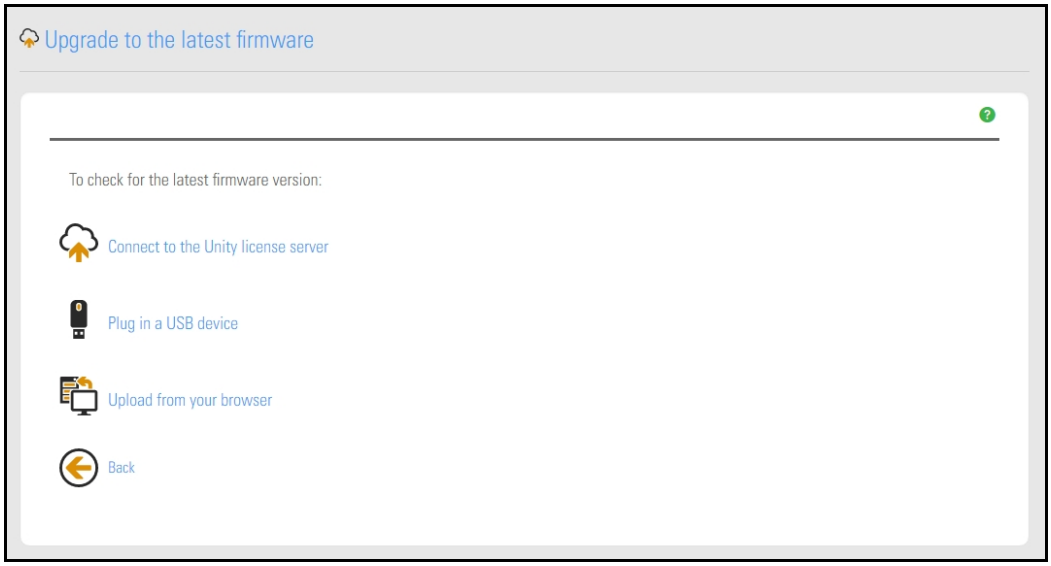
1. On the **Unity navigation bar**, select **System > Check for Updates**. Unity checks system health and opens the firmware upgrader.

Figure 11-6: Nexsan Unity firmware upgrader



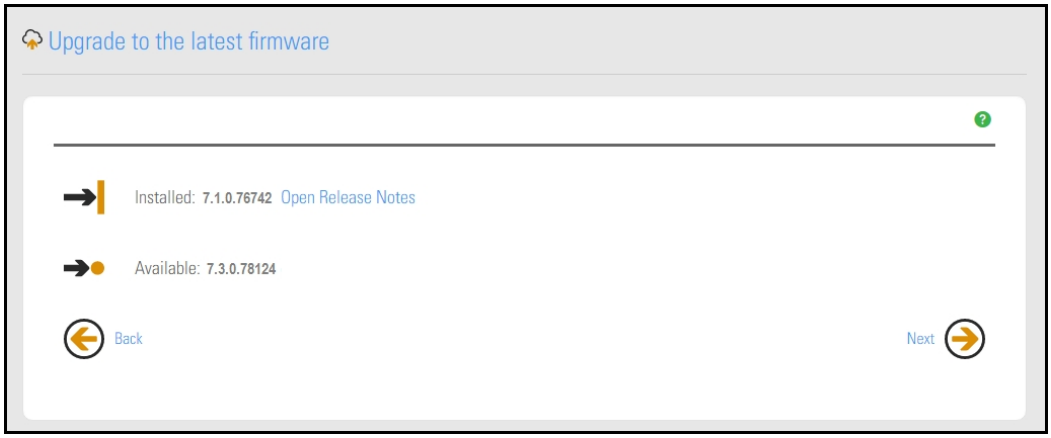
2. Select **Upgrade to the latest firmware**.
3. Select one of the following:
   - **Connect to the Unity license server** to check for updates on the Nexsan Unity license server using the Internet.
   - **Plug in a USB drive** to upgrade firmware components from a USB key loaded with the update files 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 the Unity chassis.
   - **Upload from your browser** to browse for the upgrade package file (`.tgz`) and select it from a directory on your network.

Figure 11-7: Downloading the latest firmware



The firmware upgrader displays the installed Unity firmware version and the latest available version.

Figure 11-8: The upgrader compares current and latest versions



4. Click **Next** to begin the upgrade process. Unity validates and prepares the package for installation.

5. Click **Proceed**, review the upgrade steps, and click **Start** when you are ready.

   The firmware upgrader displays the steps as it performs the upgrade. It will automatically fail over the resource groups on one controller and upgrades the other controller.

6. After successfully upgrading the first controller, the upgrader pauses. Before proceeding with the upgrade of the peer controller, verify that your data (VMs, shares, LUNs) are accessible on controller 2. Click **Proceed** when you are ready to continue.
7. The upgrader proceeds with the upgrade of controller 1. When the upgrade process completes successfully, click **Restart Unity**.

   Unity prompts you to login when the restart completes

Related Topics:

Adding new features below

Upgrading the cluster license on page 451

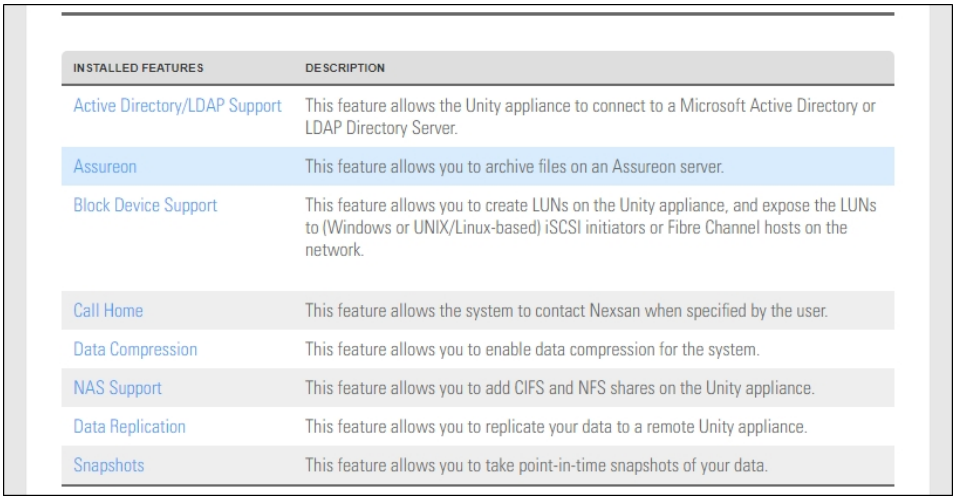
Adding new features

The Unity firmware upgrader enables you to add new features to Unity.

To add features:

1. Launch the Unity firmware upgrader, as described in Upgrading to the latest firmware on page 447.
2. Select **Add new features**.
3. Unity displays the features currently installed in your Unity System. Click the right arrow to continue.

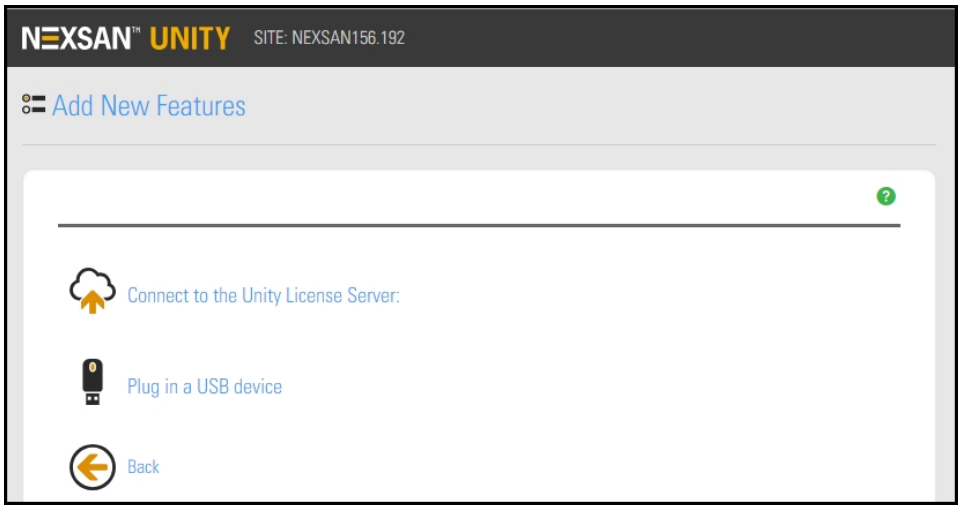
Figure 11-9: Viewing installed features



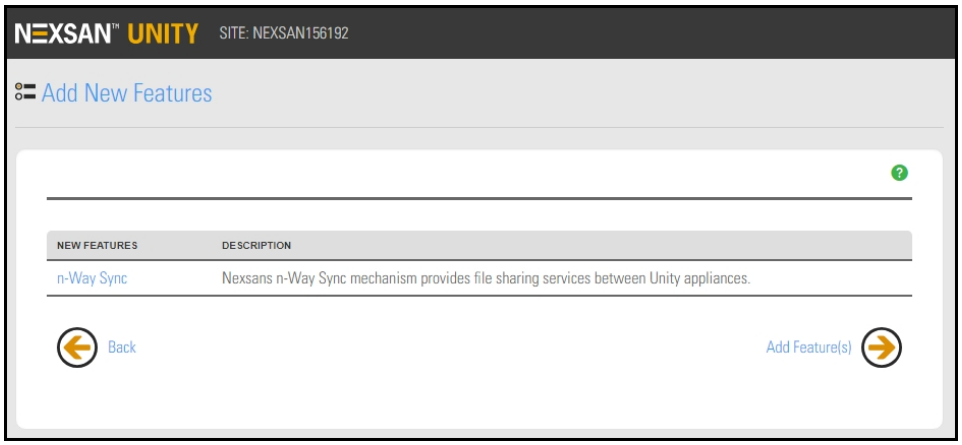
INSTALLED FEATURES	DESCRIPTION
Active Directory/LDAP Support	This feature allows the Unity appliance to connect to a Microsoft Active Directory or LDAP Directory Server.
Assureon	This feature allows you to archive files on an Assureon server.
Block Device Support	This feature allows you to create LUNs on the Unity appliance, and expose the LUNs to (Windows or UNIX/Linux-based) iSCSI initiators or Fibre Channel hosts on the network.
Call Home	This feature allows the system to contact Nexsan when specified by the user.
Data Compression	This feature allows you to enable data compression for the system.
NAS Support	This feature allows you to add CIFS and NFS shares on the Unity appliance.
Data Replication	This feature allows you to replicate your data to a remote Unity appliance.
Snapshots	This feature allows you to take point-in-time snapshots of your data.

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 11-10: Checking for new features



5. The Unity 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 the right arrow to start the update process.



   - If no new features are found, click the left arrow to go back to the main screen and close the Updater.
6. When the upgrade is complete, perform one of these actions:
   - If the new features were installed successfully, click the right arrow to start Unity.
   - If an error occurred while trying to add features, hover your mouse on the error text to view the error tool tip and try to resolve the issue accordingly.

Upgrading the cluster license

The Unity firmware upgrader enables 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 Unity firmware upgrader as described in Updating Unity on page 446.
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 Updater.
4. The Unity 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 system 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.

About Joining an Active Directory Domain

This section includes these topics:

Microsoft Active Directory domain requirements below

Creating computer objects on the Active Directory server on the facing page

Joining a Microsoft Active Directory domain on page 458

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	Supported Windows Server versions:
	• Windows Server 2025
	• Windows Server 2022
	• Windows Server 2019
	• Legacy Support:
	  • Windows Server 2016
	  • Windows Server 2012 R2

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.

Requirement	Description
Time server	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. 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.
Domain administrator privileges	You will need to provide domain credentials for a domain administrator, or of a user who has full domain administrative privileges. 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.
DNS alias for non-standard domain names	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 (-). You must also add a resource record for the alias in the reverse DNS lookup zone. Later, when you configure the Unity Storage System 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. As an example, if the domain controller uses this name: **1MYDC_001.mydomain.lan**, 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. 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**
LM Manager authentication level	By default, Unity uses NTML 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.
Creation of machine accounts	The Microsoft Active Directory implementation must support the creation of machine accounts in the default Organizational Unit (OU).

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:

- 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.



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 System Configuration wizard—that is, an uninitialized Unity—you must type the default password for the nxadmin (Nexsan Unity Administrator) account: PASSWORD (all upper-case).

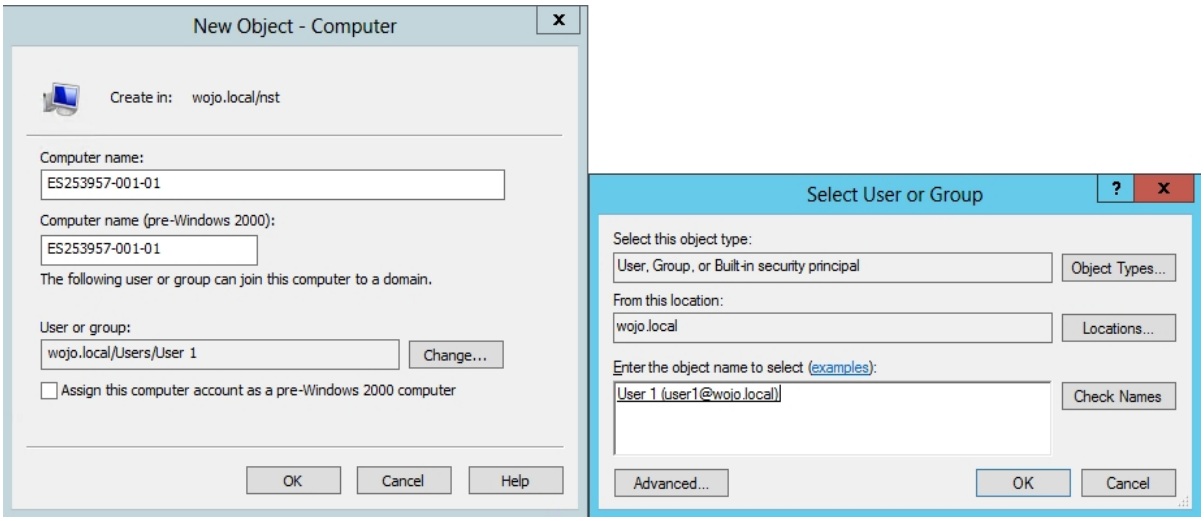
e. On each controller node, run the `hostname` command.

f. Take note of 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>.<domain name>`
	For example:
	`ES777666-001-01.qadomain.net`

msDS-SupportedEncryptionTypes	31
servicePrincipalName	• `cifs/<NESTHOSTNAME>.<domain name>` For example: `cifs/ES777666-001-01.qadomain.net` • `host/<NESTHOSTNAME>.<domain name>` For example: `host/ES777666-001-01.qadomain.net` • `HTTP/<NESTHOSTNAME>.<domain name>` For example: `HTTP/ES777666-001-01.qadomain.net` • `nfs/<NESTHOSTNAME>.<domain name>` For example: `nfs/ES777666-001-01.qadomain.net` • `root/<NESTHOSTNAME>.<domain name>` For example: `root/ES777666-001-01.qadomain.net` • `host/<NESTHOSTNAME>` For example: `host/ES777666-001-01`

userPrincipalName	`host/<NESTHOSTNAME>.<domain name>@<DOMAINNAME>`
	For example:
	`host/ES777666-001-01.qadomain.net@QADOMAIN.NET`

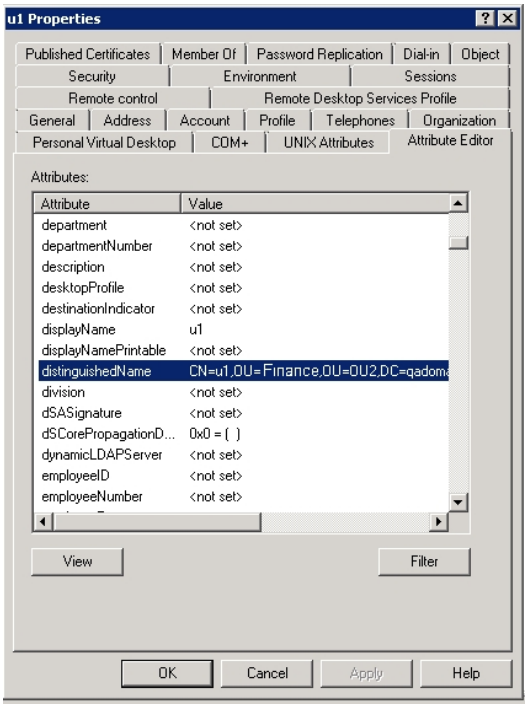
userAccountControl	4130

Note If the domain you are joining is `department.company.com`, make sure to use that whole name in *Step 7*.

4. 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*.



5. Repeat **step 3** above for the computer object that you added for the 2nd controller node.
6. Configure Unity using the Nexsan Unity System Configuration wizard (if not already configured).
7. Join Unity to the Microsoft Active Directory Domain in Nexsan Unity. See also Joining a Microsoft Active Directory domain on the next page

   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.

   Make sure to use the same (whole) domain name as in *Step 3*.

   a. At the Configure User Authentication Mode step, click the **Advanced** button.

   b. Enter the Organizational Unit (OU) names obtained in *Step 4*.

   c. Select the **Use pre-defined computer objects** option.

   d. Click the **Apply** button.

8. 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.

Joining a Microsoft Active Directory domain

The Unity Authentication service is preconfigured by default during initial system setup. Use this procedure if you want to instead join a Microsoft Active Directory domain.

CAUTION: If Unity is currently connected to a domain, and you subsequently join Unity to a new domain, 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 Administrators, as well as all file system-level access permissions on the system.

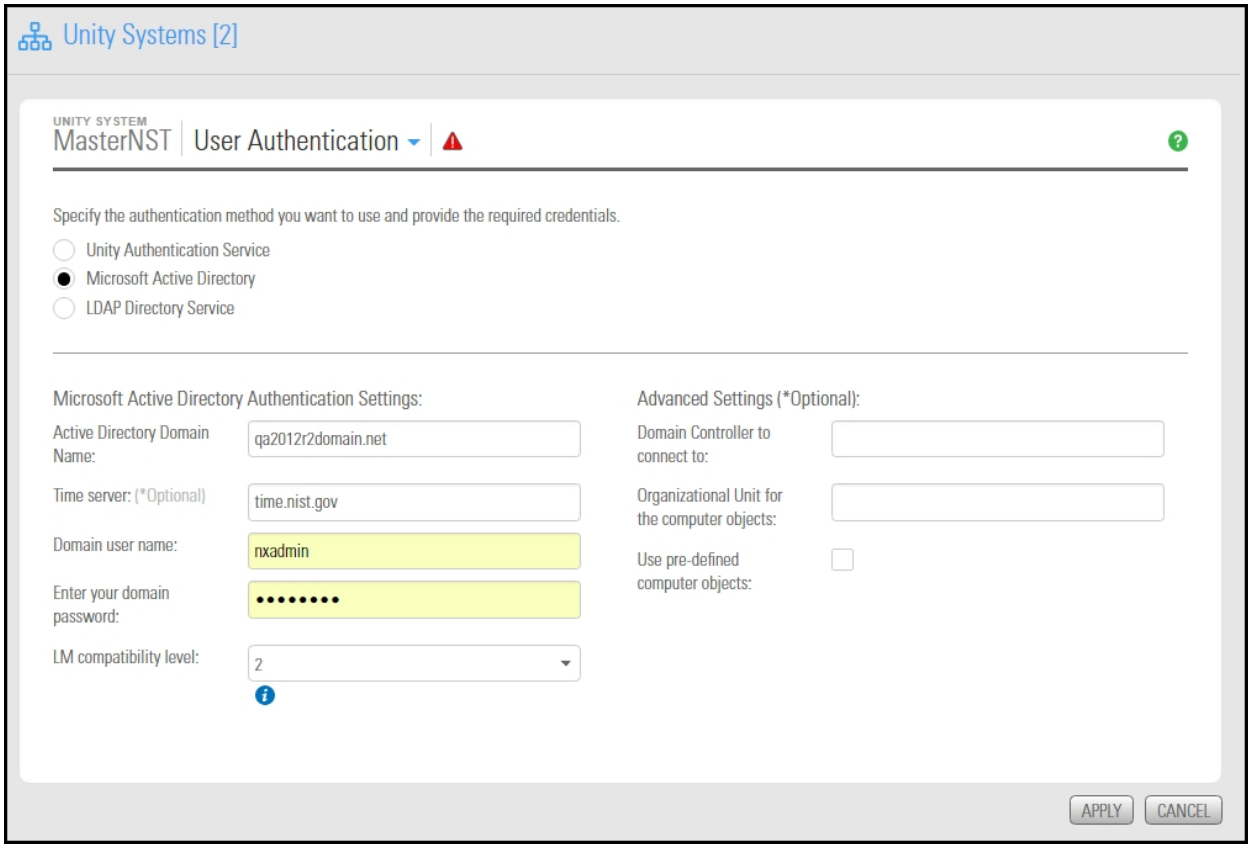
CAUTION: Joining a new domain or rejoining a former domain

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 a CIFS file system on page 463.

Before you begin:

Read the Microsoft Active Directory domain requirements on page 452.

Figure 11-11: Joining a Microsoft Active Directory domain



To join a Microsoft Windows Active Directory domain:

1. From the **System** menu, select **Unity Systems**.
2. Click **Summary** > **User Authentication**.
3. Select **Microsoft Active Directory**. The connection settings for Microsoft Active Directory display.

4. In the **Active Directory Domain Name** field, type the fully qualified domain name (FQDN) of the Microsoft Active Directory domain server that you want Unity to connect to.

   Note If you are integrating Unity in a multiple domain environment (Microsoft Active Directory forest implementation), and you want Nexsan Unity to display all users and groups from all domains, make sure to specify the domain name of the root, or top-level domain server of your network's Microsoft Active Directory implementation.

5. Optionally, 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 default time server is already defined.

   Note Unity supports multiple time servers: if you specify a time server in the **Time server** field, we highly recommend that you specify at least two time servers; this ensures that date and time synchronization on Unity continues 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`.

6. In the **Domain user name** and **Domain password** fields, type the user name and password of the domain administrator, or of a user that has administrative access to the Microsoft Active Directory server.

   For **LM compatibility level**, we recommend that you use the recommended level (2). The security level allows NTLMv1 client authentication, or NTLMv2 session security if the NFS server supports it. The Domain Controller accepts LM, NTLM, and NTLMv2 authentication.

7. Optionally, under **Advanced Settings**:

   - **Domain Controller to connect to**: If you are working in a multi-domain environment (that is, a Microsoft Active Directory forest implementation), enter the IP address of the domain controller in the 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.
   - **Organizational Unit (OU) for the computer objects**: Computer objects are stored under `Computers` by default. To change the default location where Unity adds its computer objects on your Active Directory server, enter Organizational Unit (OU) names in the format: `OU=NAME1,OU=NAME2`

     If the names do not exist, Unity 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.
   - **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. The Organizational Unit path you provide creates 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.

8. Click the **Apply** button.

9. When the **Confirm DNS Settings** prompt appears, do one of the following:
   a. If the new domain server is in a different network domain, specify the IP addresses of the corresponding DNS servers, and click the **Apply** button, or
   b. If the new domain server is in the same network domain as the previous domain server, click the **Apply** button to keep the current DNS settings.
10. When the **Domain controllers** window appears, select the primary and secondary controllers to be used for AD, and click the **Apply** button.
11. The wizard applies your settings and if all are successful, prompts you to click the **OK** button.

Note If you need to change your User Authentication method later,

- On the **Unity navigation bar**, select **System.**
- Click the link to the **Unity System** that you want to update.
- Select **Summary > User Authentication**.
- Make changes as required.

Delegating control to a 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.

11

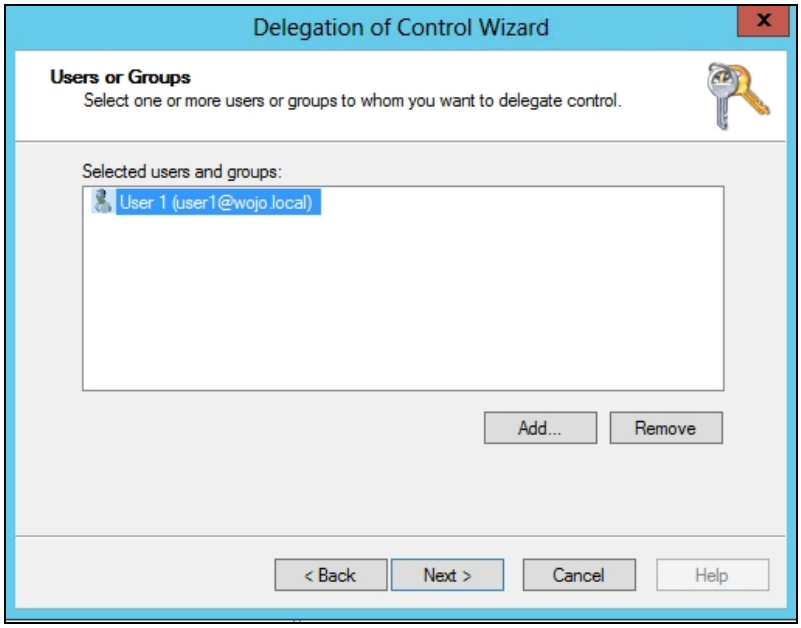
▶ **To delegate control:**

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.

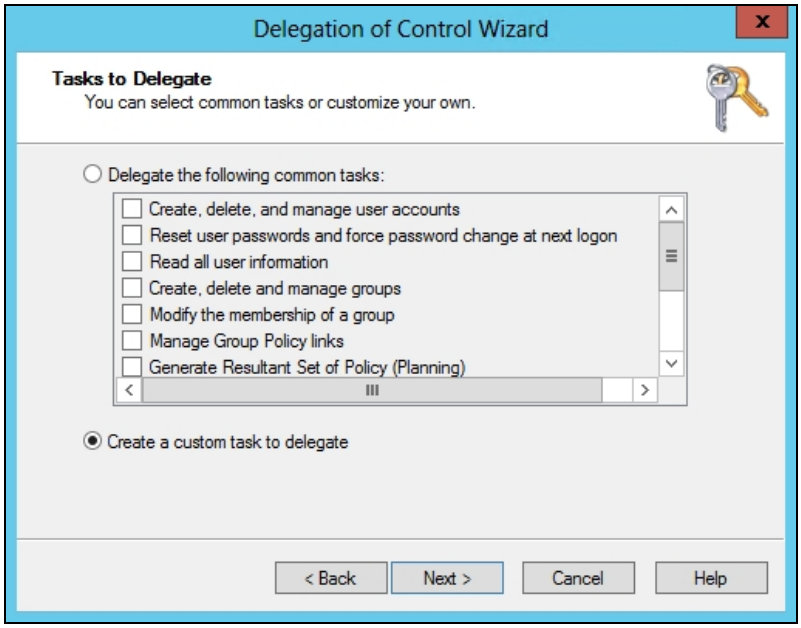
4. Click **Add** and select the non-Administrator user account used in the previous section. Click the **Next** button.

Figure 11-12: Active Directory - Delegation of Control wizard: select a user



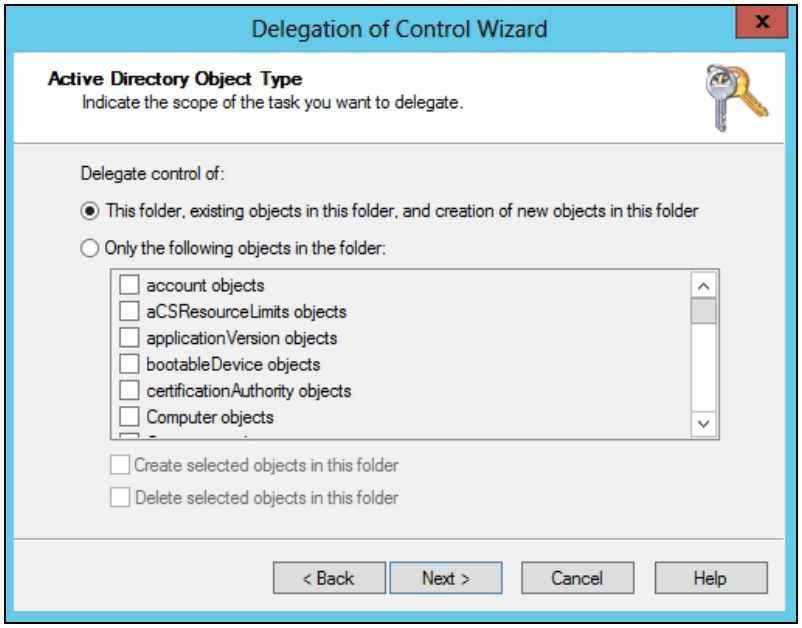
5. Select **Create a custom task to delegate** and click the **Next** button.

Figure 11-13: Active Directory - Delegation of Control wizard: select tasks to delegate



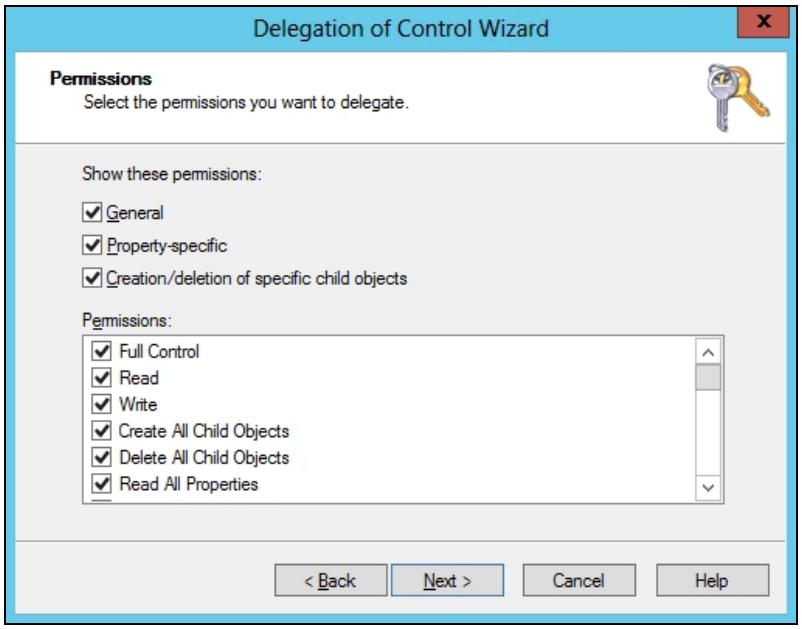
6. Select **This folder...** and click the **Next** button.

Figure 11-14: 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 11-15: Active Directory - Delegation of Control wizard: select permissions



8. Click **Finish**.

Enabling Kerberos for accessing a CIFS file system

To enable Kerberos support on Unity, you must perform these configuration tasks:

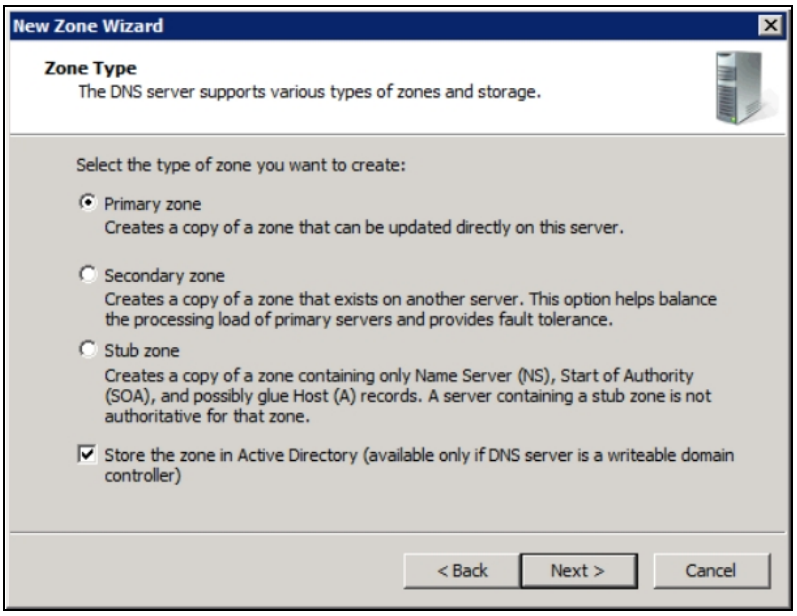
1. Add a reverse lookup zone for the subnet of your Resource Groups in DNS Manager on your Active Directory domain.
2. Add a host in DNS Manager for each Resource Controller.
3. Configure the host in Active Directory Users and Computers.

Note Your Unity must have CIFS server version 2.1 to be able to use Kerberos.

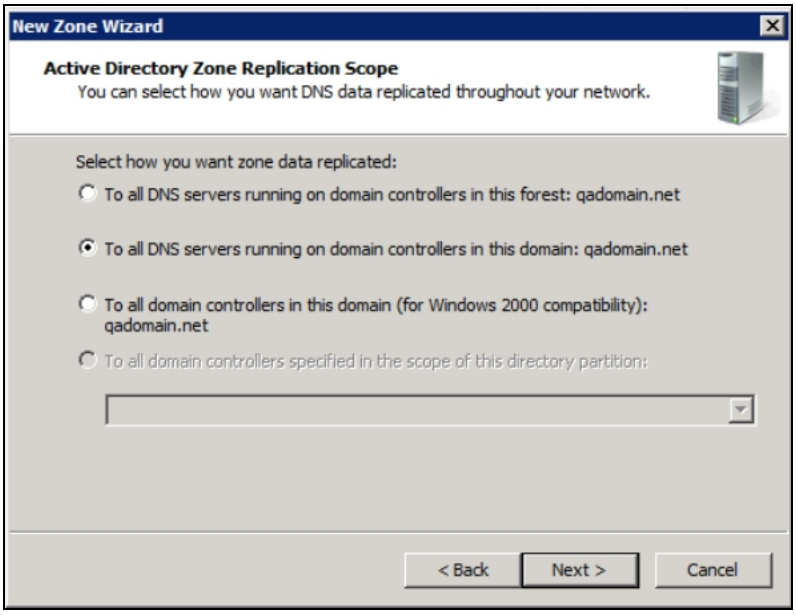
Adding a Reverse Lookup Zone in DNS Manager

To add a Reverse Lookup zone:

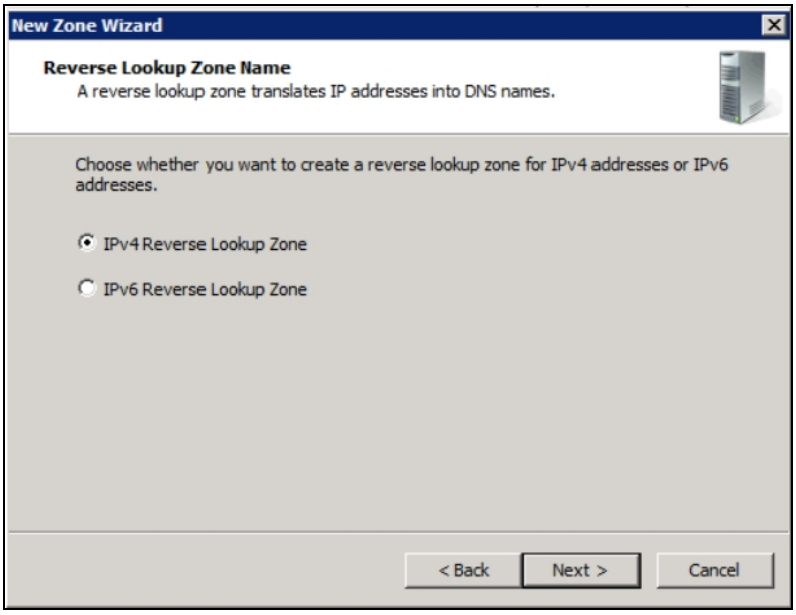
1. In DNS Manager, right-click **Reverse Lookup Zones** and select **Add Reverse Lookup Zone**.
2. The New Zone wizard opens. Select the **Primary Zone** and click **Next**.



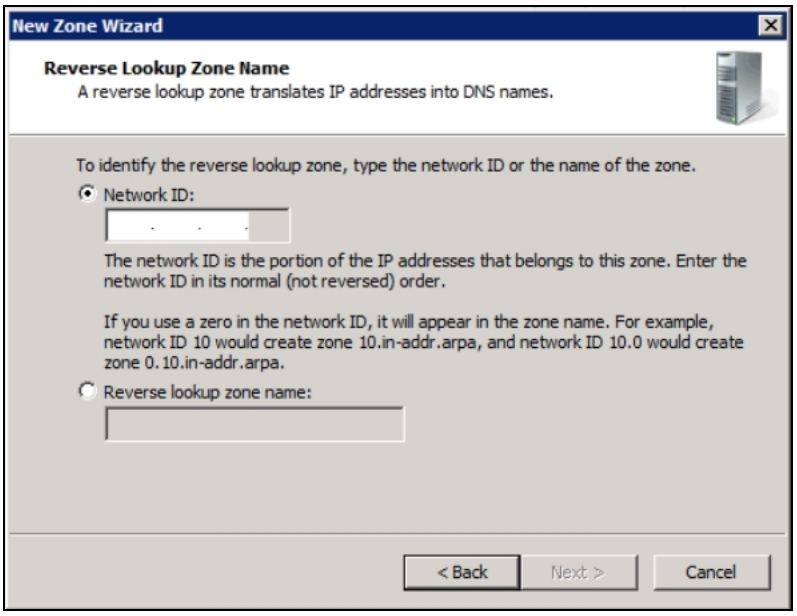
3. Select the zone replication scope, as applicable in your Active Directory domain, and click **Next**.



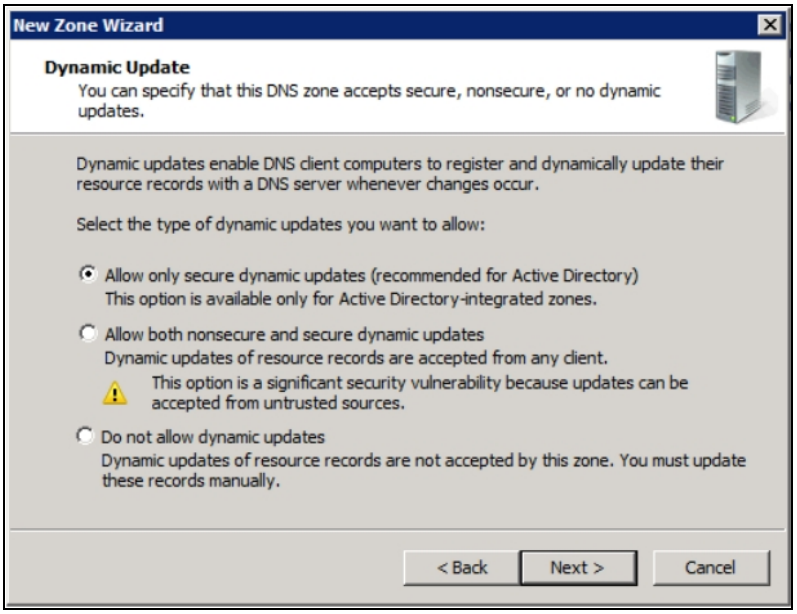
4. Select the version of IP addressing and click **Next**.



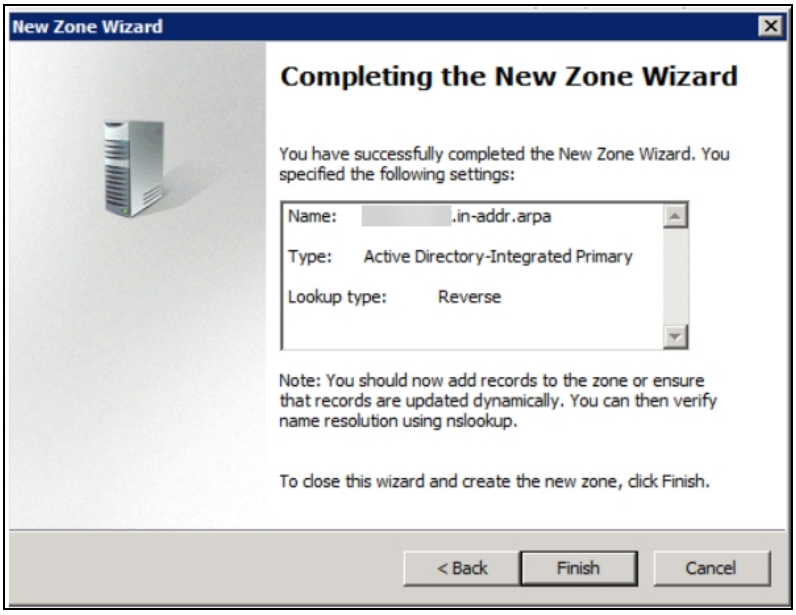
5. Enter the portion of IP address that belongs to this zone and click **Next**.



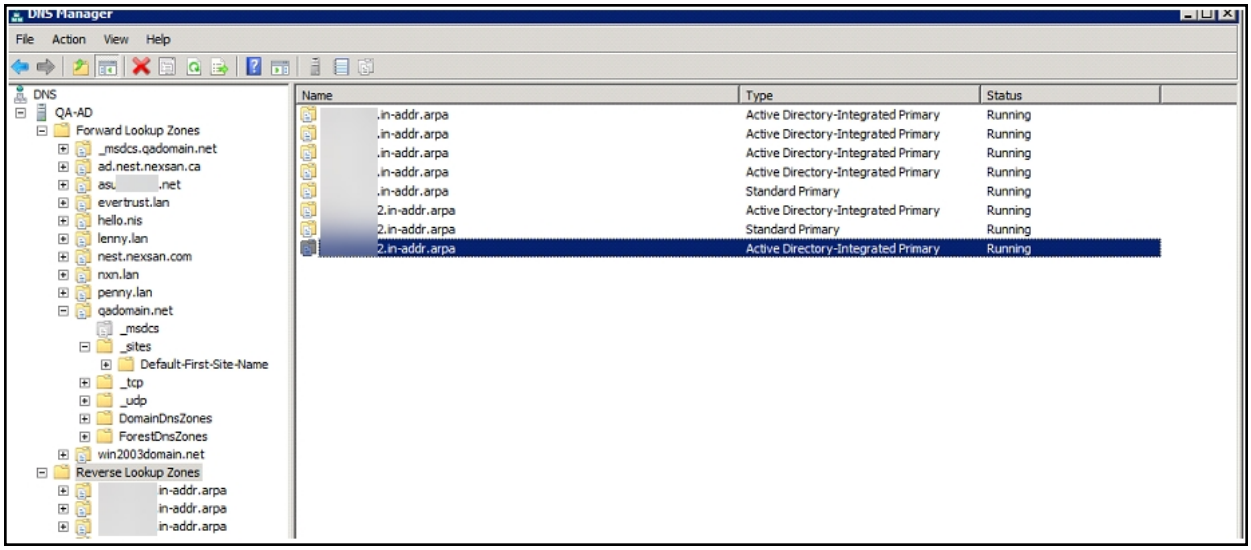
6. Select secure dynamic updates and click **Next**.



7. Click **Finish**.



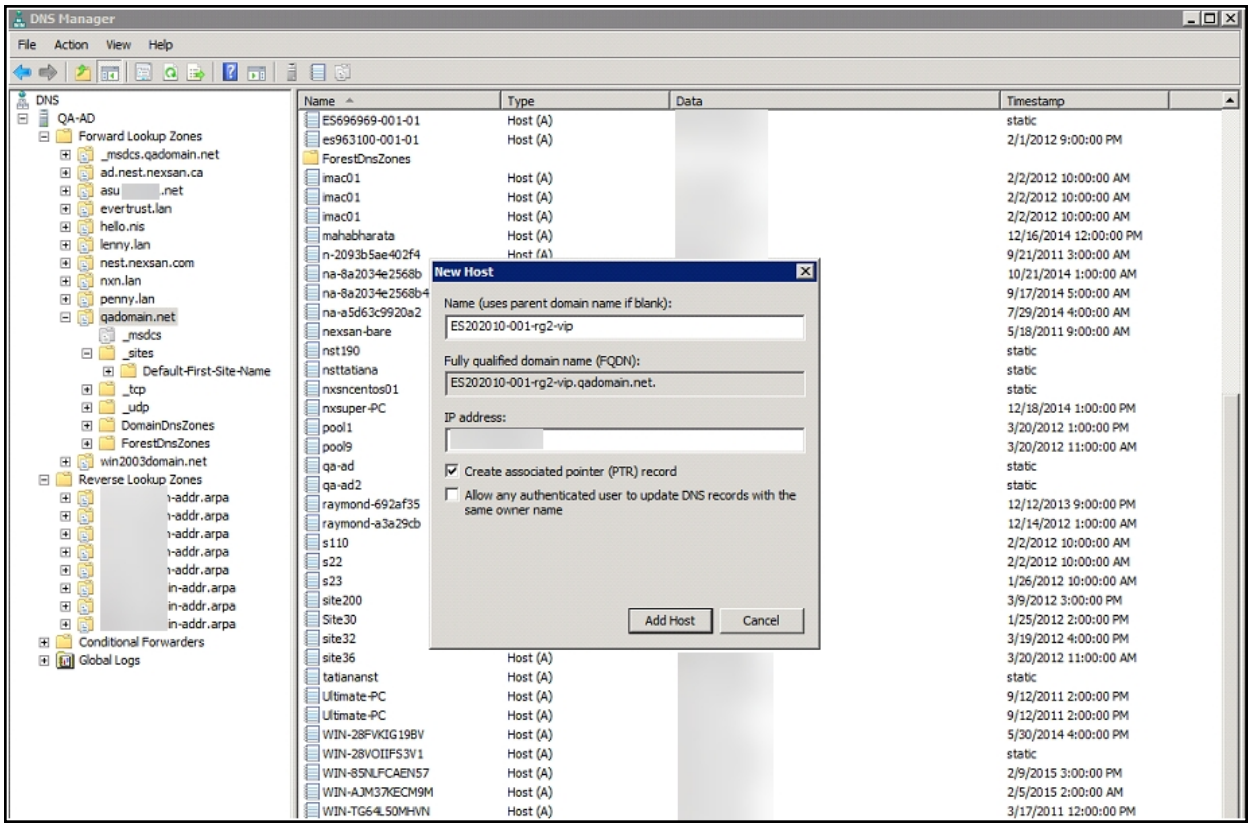
The new DNS lookup zone is listed in DNS Manager.



Adding a host for each Resource Controller in DNS Manager

To add a host:

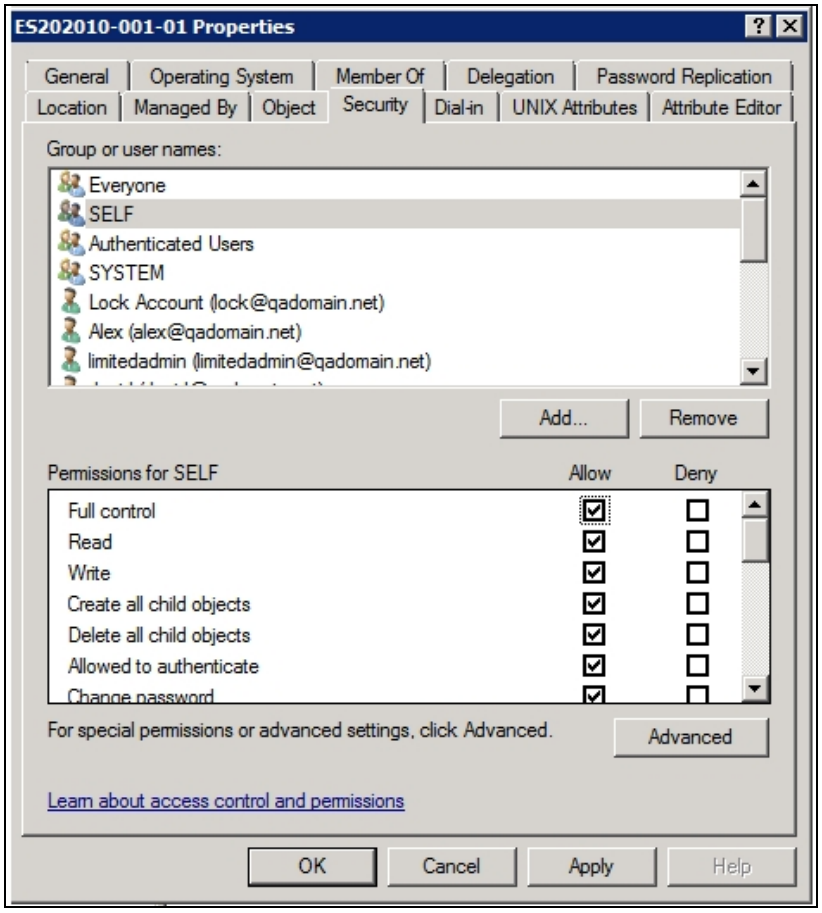
1. Right-click your domain name and select **New Host**.
2. Enter the host name of your Resource Group 1.
3. Enter the IP address of your Resource Group 1.
4. Click **Add Host**.
5. Repeat these steps for Resource Group 2.



Configuring the host in Active Directory

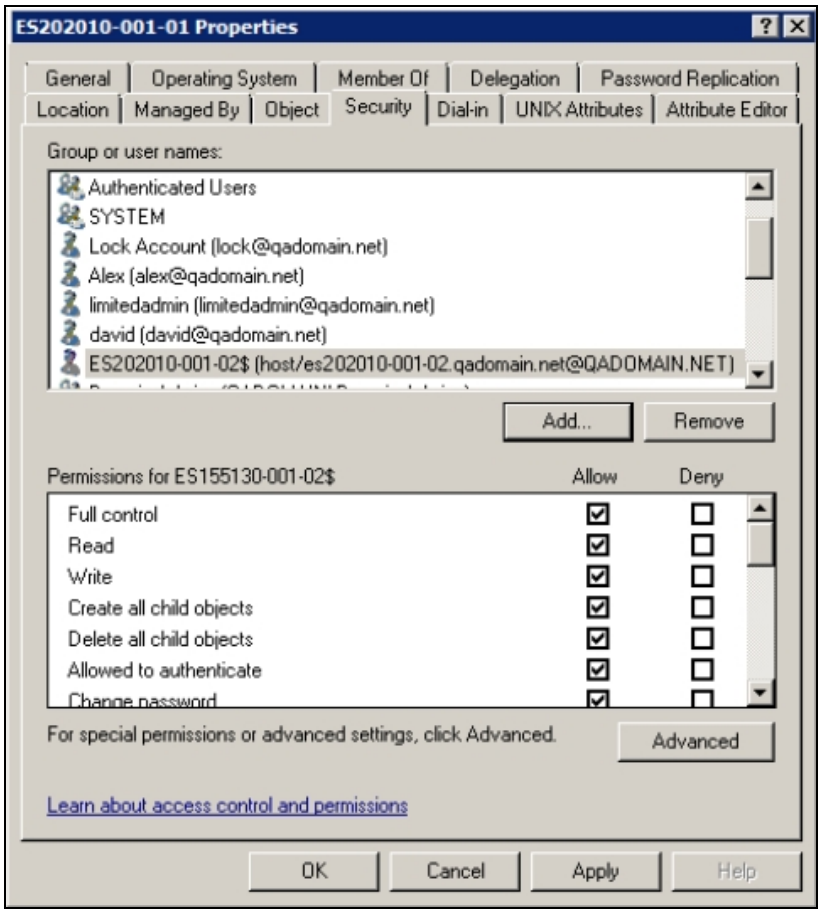
To configure the host:

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 (ES202020-001-01 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**.

8. The peer node is added to the list in the Properties dialog box. Select the **Full Control** option and click **OK**.



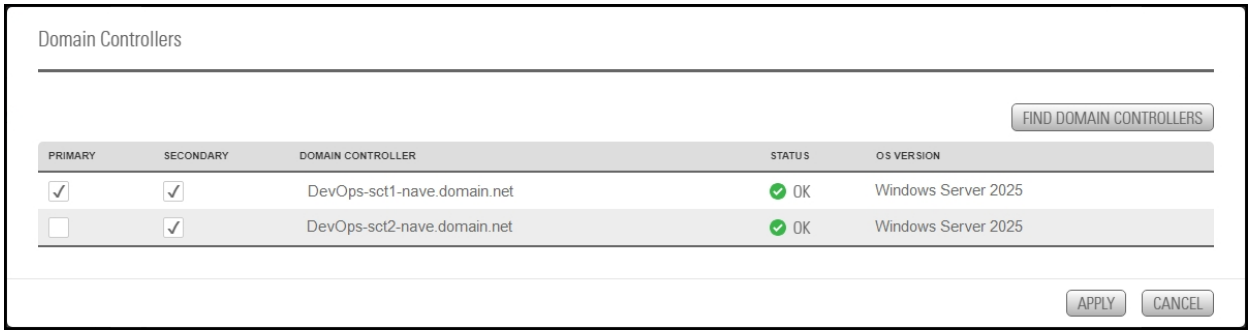
9. Repeat steps **2** to **8** to modify the permissions for Controller 2.

You can now use Kerberos if you connect to the share using the Resource Group's host name.

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 **Domain Controllers** popup window after the Domain Controllers are discovered.

Figure 11-16: Domain Controllers popup



The **Domain Controllers** window contains a grid that displays all discovered controllers in the domain. If the system has previously been configured, the grid identifies the primary domain controller that Unity is currently connected to. Also, if applicable, the grid displays the secondary domain controller currently selected for the system.

For each discovered domain controller, the grid indicates whether the domain controller is supported by Unity: a green 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 452.

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 or secondary domain controllers on the facing page

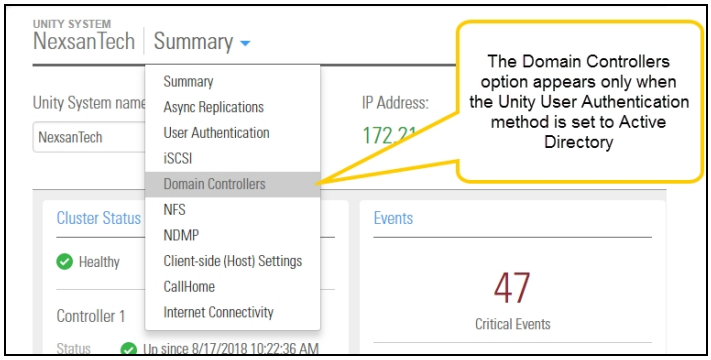
Discovering new domain controllers

This section explains how to discover new domain controllers in the Unity domain.

Prerequisites

- To view the Domain Controllers panel, Unity User Authentication must be set to Active Directory. See Joining a Microsoft Active Directory domain on page 458

Figure 11-17: Domain Controllers command



To discover domain controllers:

1. On the **Unity navigation bar**, select **System > Unity Systems**.
2. Click the link to the system that you want to find new domain controllers for.

3. Click **Summary > Domain Controllers**. If Unity User Authentication is set to use Active Directory, Unity displays the currently discovered controllers.

Figure 11-18: Unity Systems Domain Controllers panel



4. 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 or secondary domain controllers

This section explains how to select alternate primary and/or secondary domain controllers for the Unity Storage System.

11

Prerequisites

- To view the Domain controllers panel, Unity User Authentication must be set to Active Directory. See Joining a Microsoft Active Directory domain on page 458

To select alternate primary and/or secondary domain controllers:

1. On the **Unity navigation bar**, select **System > Unity Systems**.
2. Click the link to the system that you want to find new domain controllers for.
3. Click **Summary > Domain Controllers**. Unity displays the currently discovered controllers.

Figure 11-19: Unity Systems Domain Controllers panel



4. Select a new primary domain controller by clicking its corresponding check box in the **Primary** column of the grid.

5. (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.
6. Click the **Apply** button.

   Unity updates controller connectivity settings for Unity. This process may take some time to complete.
7. Once Unity updates controller connectivity settings, it may prompt you to restart Unity. Click the **Restart Unity** button.

Unjoining Unity from an Active Directory domain

To unjoin the Active Directory domain, you will typically join the Unity Authentication Service, as documented in this procedure.

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 As a result If you enable Unity authentication, when Unity restarts, you can only log on to the system as the Unity Administrator (**nxadmin**. 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 Siteadministrators, as needed. For more information about adding local users and/or group accounts to the system, see Users and access rights on page 69.



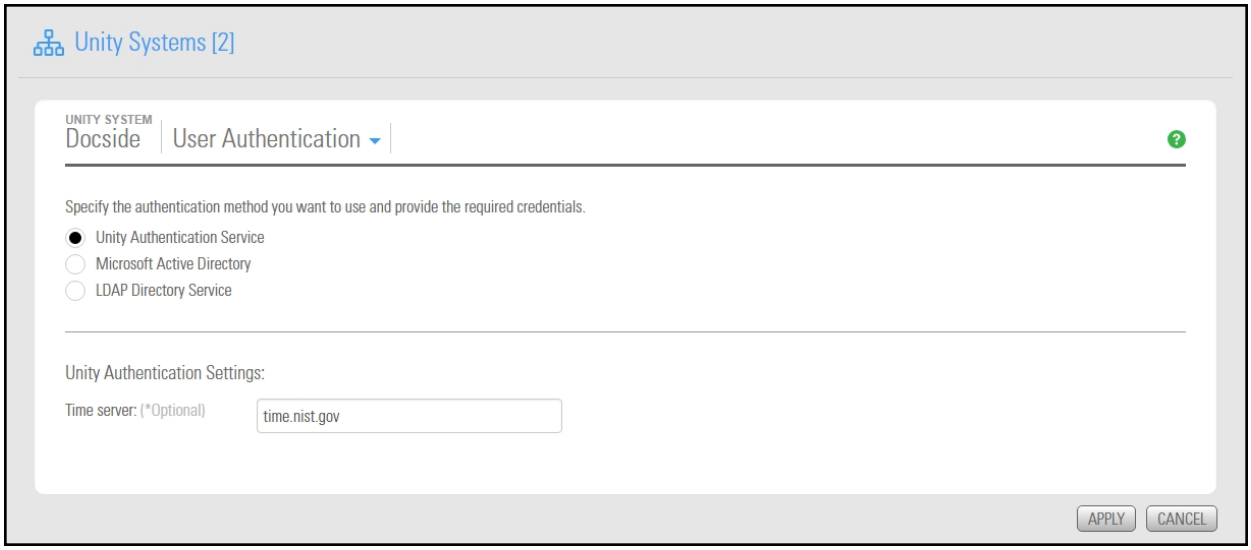
CAUTION: All file system-level access permissions are also removed, although file- and folder-level ACLs (CIFS) and permissions (NFS) remain unchanged. However, when you rejoin the same domain that you unjoined Unity from, or join a new domain with the same set of user and group accounts as the previous domain, Unity restores all file system-level access permissions on the system.

► **To unjoin Unity from an Active Directory domain:**

1. On the **Unity navigation bar**, select **System > Unity Systems**.
2. Select the Unity system that you want to update.
3. Click **Summary** > **User Authentication**.

4. Select **Unity Authentication Service**.

Figure 11-20: Unity Authentication panel



5. Optionally, 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 default time server is already defined.

   Note Unity supports multiple time servers: if you specify a time server in the **Time Server** field, we highly recommend that you specify at least two time servers; this ensures that date and time synchronization on Unity continues 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`.

6. Click the **Apply** button. Unity applies your settings.
7. When the **Confirm DNS Settings** prompt appears, do one of the following:
   a. If the new domain server is in a different network domain, specify the IP addresses of the corresponding DNS servers, and click the **Apply** button, or
   b. If the new domain server is in the same network domain as the previous domain server, click the **Apply** button to apply the current DNS settings.
8. When the **Domain controllers** window appears, select the primary and secondary controllers to be used for AD, and click the **Apply** button.
9. The wizard applies your settings and if all are successful, prompts you to click the **OK** button.

Connecting to an LDAP Directory Service

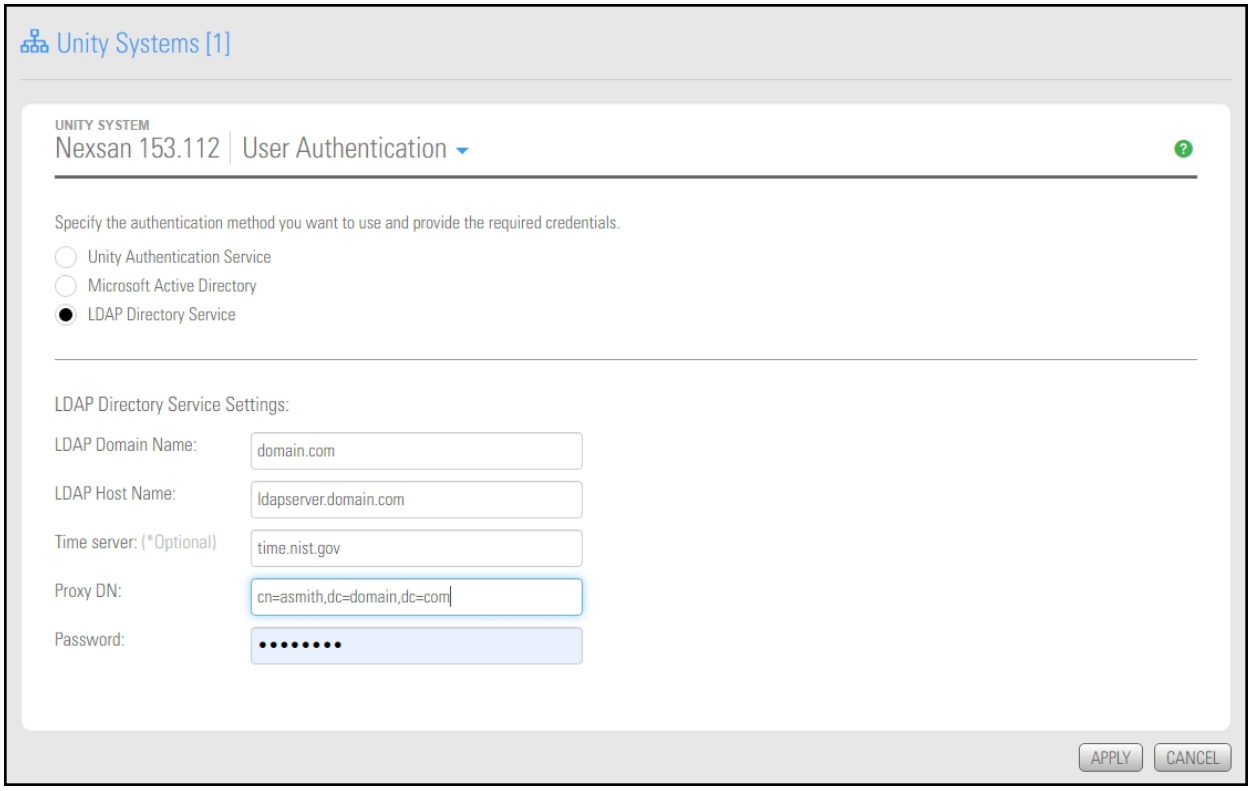
The Unity Authentication service is preconfigured by default during initial system setup. Use this procedure if you want to instead connect to an LDAP Directory Service.

▶ **To connect to an LDAP Directory Service:**

1. From the **System** menu, select **Unity Systems**.
2. Click the link to the Unity System you want to connect to LDAP.

3. Click **Summary** > **User Authentication**.

Figure 11-21: Connecting to an LDAP Directory Service



4. Select **LDAP Directory Service**. The settings display for connecting to an LDAP Directory service on the network.
5. 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`.
6. (Optionally) In the **LDAP Host Name** field, type the host name of the LDAP Directory server that you want Unity to connect to. For example, `ldapserver.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.

7. Optionally, 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 the 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 continues in the event that one of the time servers you specify is no longer available.

   Note To specify multiple time servers, use a comma to separate each entry, for example: `tick.utoronto.ca,time.nrc.ca`.

8. 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.

9. Type the Proxy identity's password in the **Password** field.
10. Click the **Apply** button.
11. When the **Confirm DNS Settings** prompt appears, do one of the following:
    a. If the new domain server is in a different network domain, specify the IP addresses of the corresponding DNS servers, and click the **Apply** button, or
    b. If the new domain server is in the same network domain as the previous domain server, click the **Apply** button to keep the current DNS settings.
12. The wizard applies your settings and if all are successful, prompts you to click **OK**.

Reverting to Unity Authentication

Use this procedure if you have the Microsoft Active Directory Service or LDAP Directory Service, and want to revert to the default Unity Authentication for your Unity Storage System. Unity is not connected to a user directory or authentication service on the network.

With Unity authentication, you create Unity user and group accounts for user authentication for operations with file systems and CIFS shares.



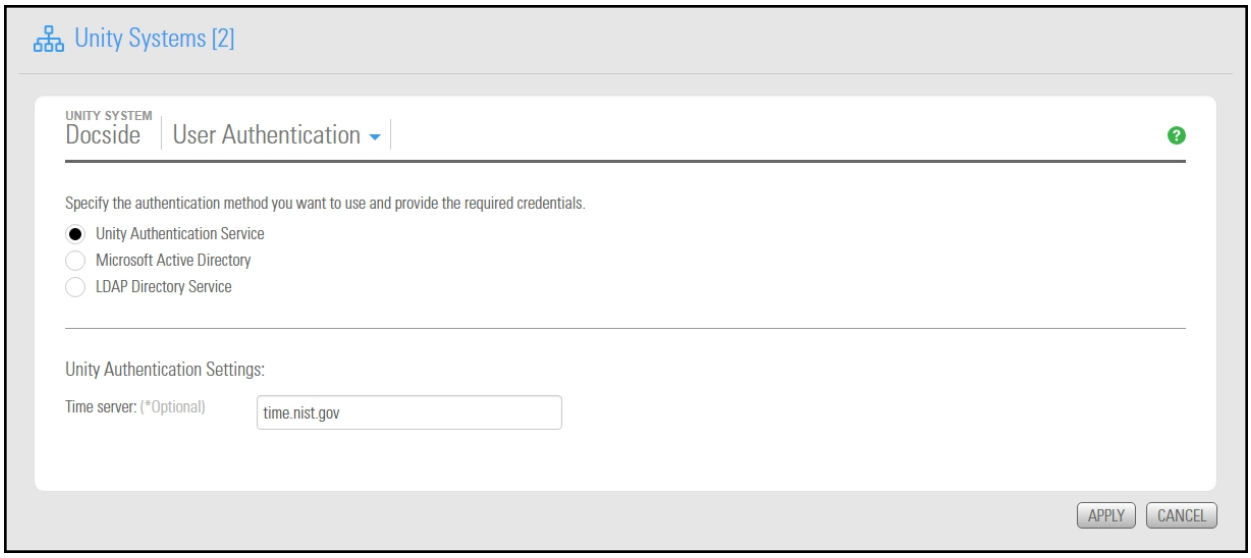
CAUTION: If Unity is currently connected to a domain, and you subsequently configure Unity authentication for the system, all file system-level access permissions are removed, although file- and folder-level ACLs (CIFS) and permissions (NFS) remain unchanged.

When you rejoin the previous domain that Unity was connected to, Unity restores all file system-level access permissions on the system.

To revert to Unity Authentication:

1. On the **Unity navigation bar**, select **System > Unity Systems**.
2. Select the Unity System you want to change the authentication method for.
3. Select **Summary > User Authentication**.
4. Select **Unity Authentication Service**.

Figure 11-22: Unity Systems panel—User Authentication view



5. Optionally, specify a time server in the **Time Server** field.
6. Click the **Apply** button.
7. When prompted confirm your DNS settings.
   - If the new domain server is in a different network domain, specify the IP addresses of the corresponding DNS servers, and then click the **Apply** button, or
   - If the new domain server is in the same network domain as the previous domain server, click the **Apply** button to keep the current DNS settings.
8. Click **OK** to confirm.

Troubleshooting Unity System-level warning and error conditions

Unity provides enhanced reporting of hardware-specific events—including disk and component failures and sensor readings—for both Unity Storage Systems or other 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

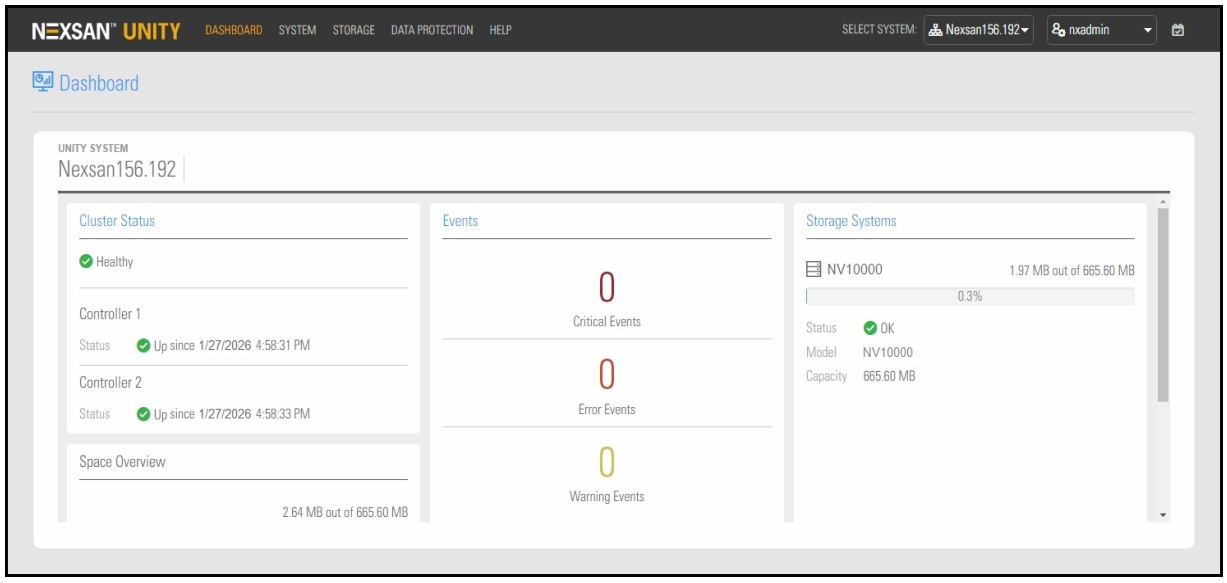
When a hardware event occurs, Unity displays error or warning indicators on the corresponding **Unity System Dashboard** or **Unity System** panel. Events are also recorded in the system event logs, which you can then access from Unity's Event Viewer and receive as alerts via email.

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.

▶ **To view high-level details about error or warning conditions:**

1. On the **Unity navigation bar**, click **Dashboard**. The Dashboard displays events display under:
   - **Cluster Status:** Displays an event indicator ( ) next to the Unity System name.
   - **Health:** Displays the aggregate number of events of each level.

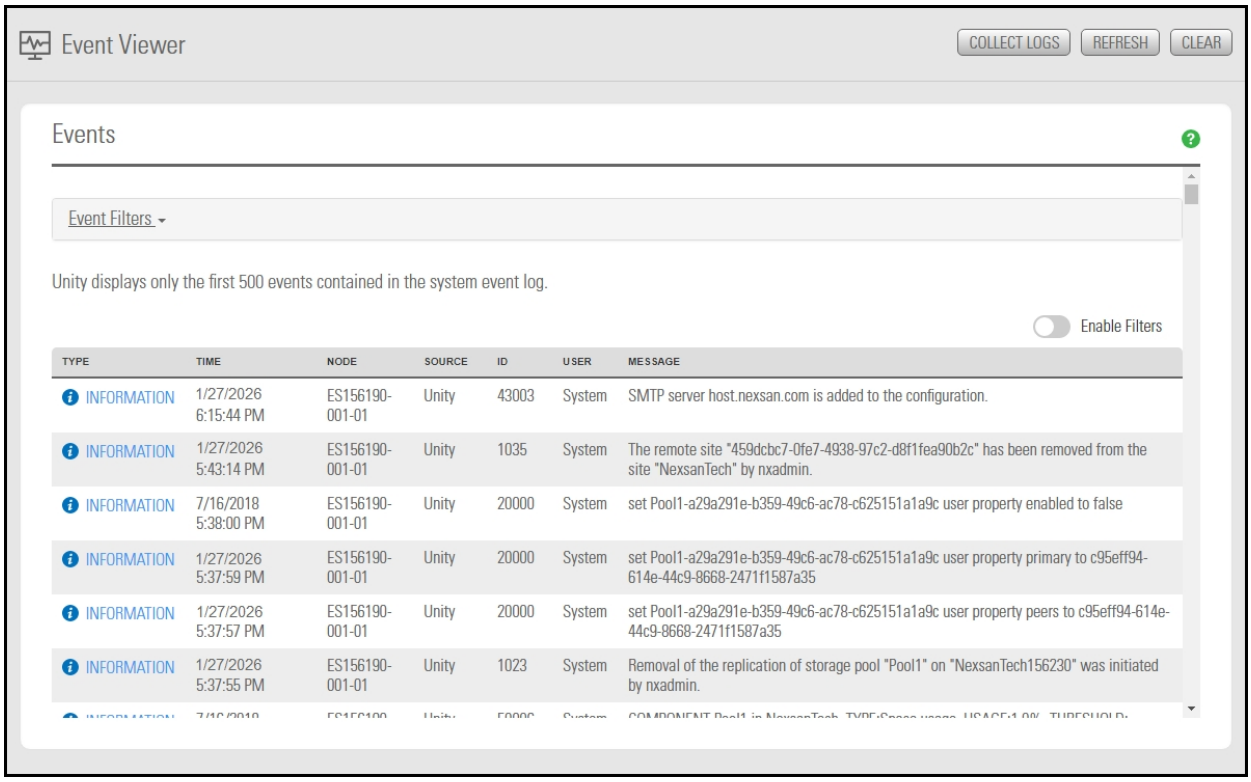
Figure 11-23: Unity System dashboard panel



To view all events:

- On the **Unity navigation bar**, select **System > Event Viewer**.

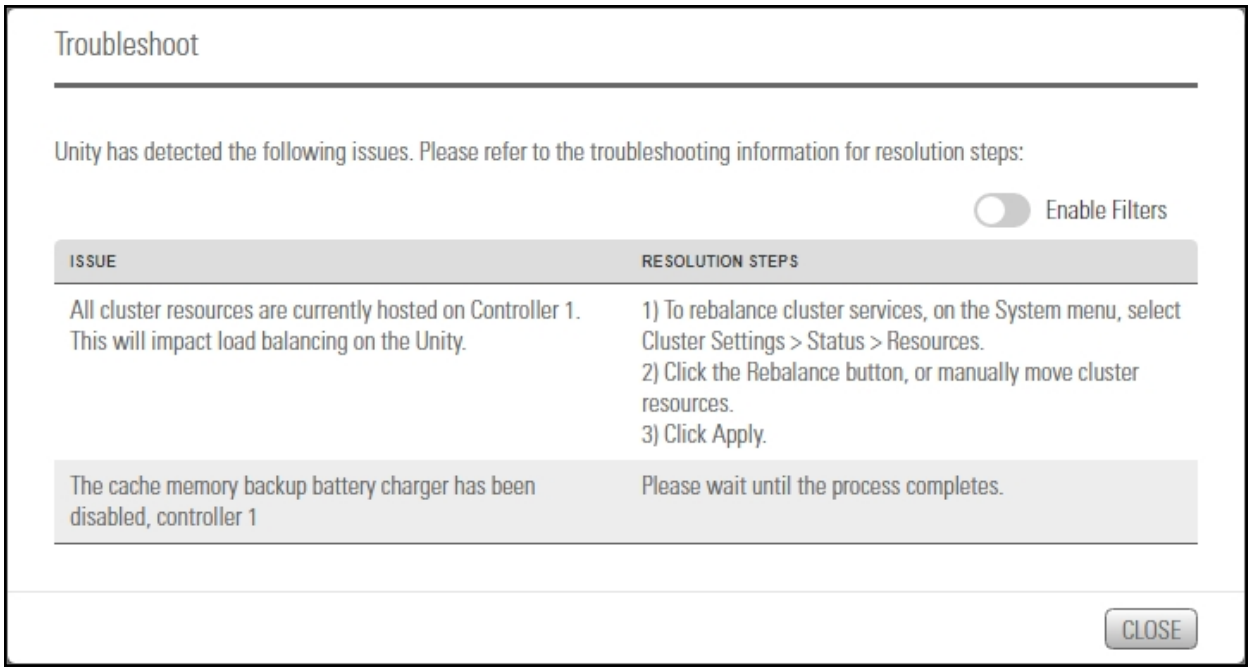
Figure 11-24: Event Viewer panel



To find troubleshooting information:

1. On the **Unity navigation bar**, select **System > Troubleshoot**. If there are issues to troubleshoot, the **Troubleshoot** pop-up opens, providing
   - Details about the source of the error or warning condition affecting the Unity System or components.
   - Resolution steps for rectifying the condition, if applicable.

Figure 11-25: Troubleshoot popup



Configuring NFS settings

This section describes how to enable an Network File System version 4 domain and how to modify NFS general settings.

For further details on NFS support for file systems, see:

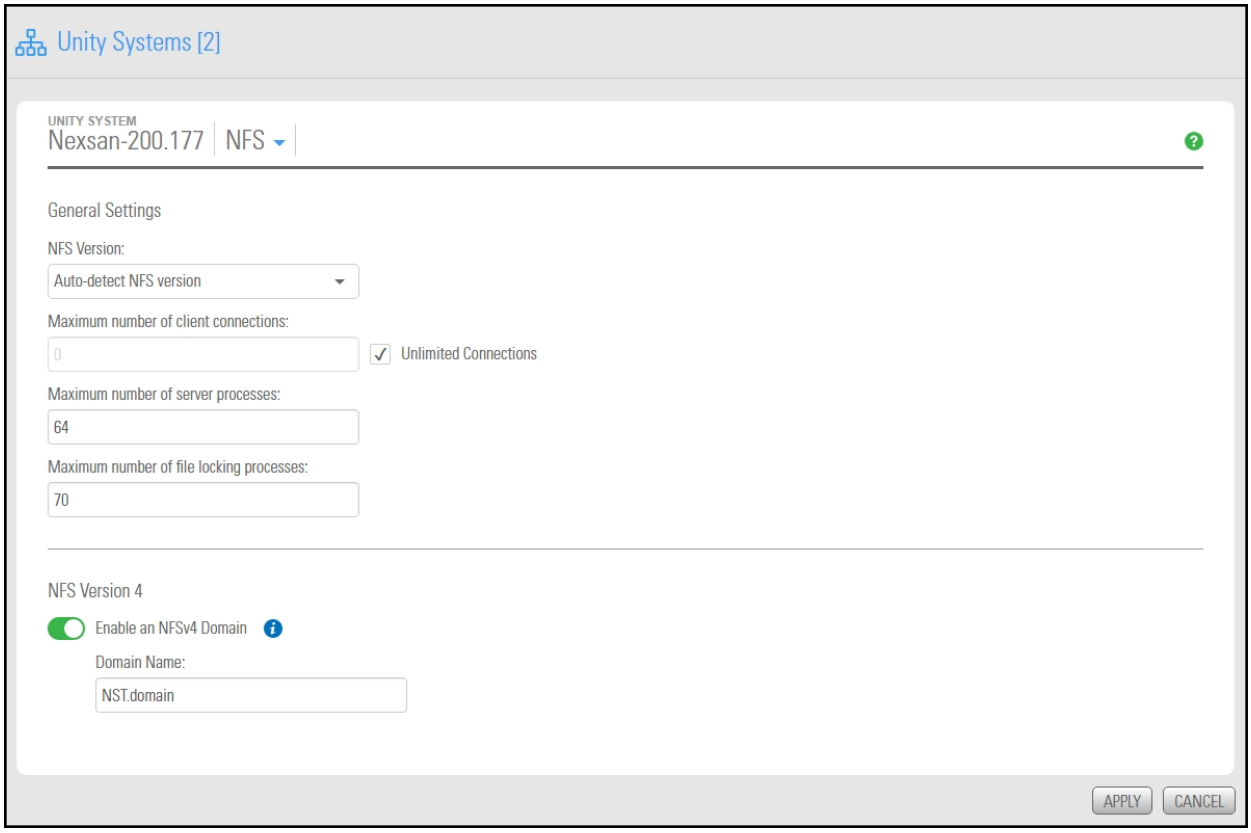
- Using an NFS version 3 (NFSv3) client to access an NFS share with Microsoft Active Directory on page 185
- Using an NFS version 4 (NFSv4) client to access an NFS share on page 186

To configure NFS settings:

1. On the **Unity navigation bar**, select **System > Unity Systems**.
2. Click the link to the Unity System that you want to update.

3. Click **Summary > NFS**.

Figure 11-26: Unity Systems NFS panel



4. 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.
5. Enter the maximum number of **client connections** in the corresponding field. Enter a value between **0** and **512** or select the **unlimited** option.
6. Enter the maximum number of **server processes** in the corresponding field. This setting enables 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 *processors*)

   where *processors* is the number of additional processors on the NFS server. Enter a value between 0 and 512.
7. 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.

8. Specify a domain name to enable user mapping between Unity and your NFSv4 clients:
   a. Click the selection button 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 (.).
9. Click the **Apply** button 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. On the **Unity navigation bar**, select **System > Unity Systems**.
2. Click the link to the Unity System that you want to view.
3. Click **Summary > APAL**. Status can be **Enabled** or **Disabled**.

Figure 11-27: Unity Systems APAL panel



For each controller, you can view the status of the connection and the channel used.

Note The chassis inter-connect card status and location can be viewed on the **Cluster Settings > Status** panel; see Viewing cluster status on page 386.

Viewing NVDIMM status

Non-Volatile Dual In-line Memory Modules (NVDIMMs) provides the memory used for Nexsan FASTier write cache drives. In the event of a power failure, the NVDIMM Power Management Unit (PMU) supplies sufficient power for the in-memory data to flush to the NVDIMM non-volatile internal flash prior to powering off.

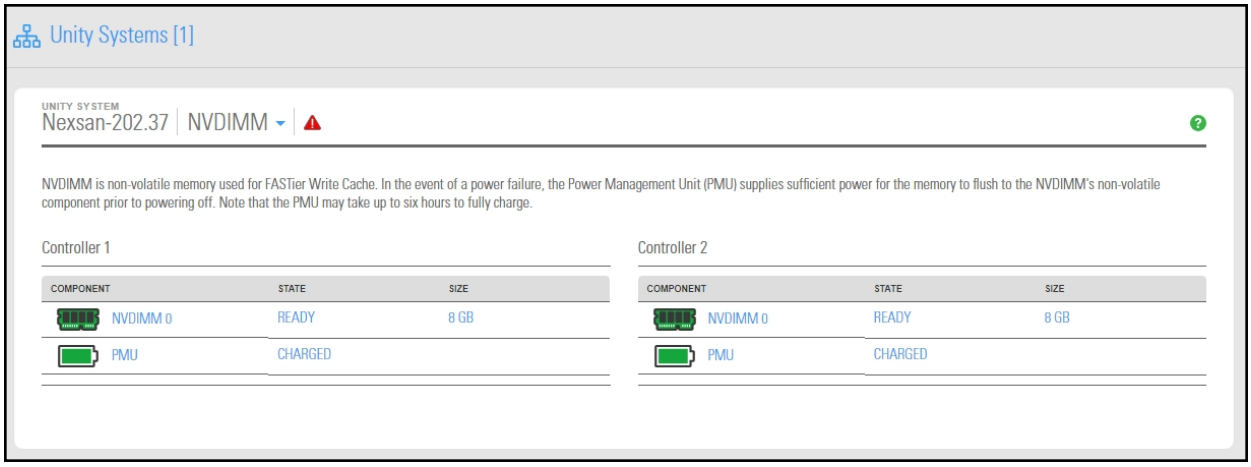
Prerequisites

- A Unity System equipped with a FASTier write cache disk and NVDIMM.

To view the NVDIMM status:

1. On the **Unity navigation bar**, select **System > Unity Systems**.
2. Click the link to the Unity System that you want to view.
3. Click **Summary > NVDIMM**.

Figure 11-28: Unity Systems NVDIMM panel



For each NVDIMM, the panel 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

Unity enables you to use FTP sharing to expose file systems for access by UNIX-, Linux-, and Windows-based systems.

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. For proper FTP behavior, do not modify these folders.

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.
- 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.

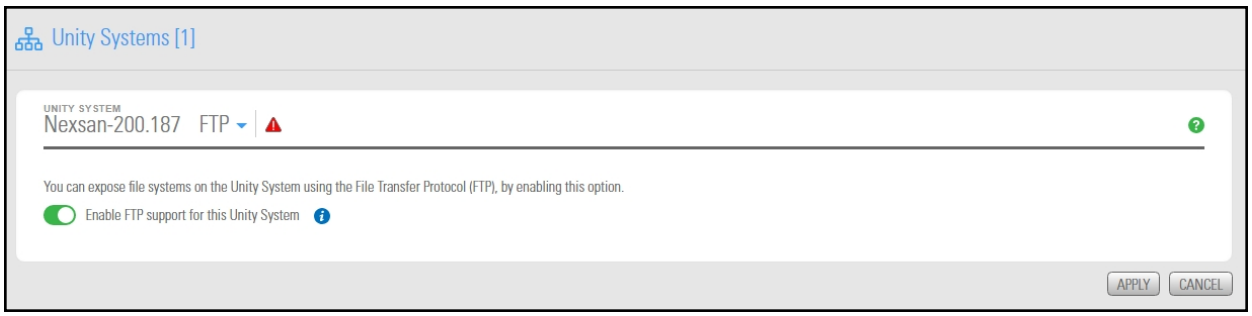
Prerequisites

- FTP support must be enabled at the Unity System level before you can expose file systems over FTP. Enabling FTP support opens port 21 by default.

To enable FTP support for the Unity System:

1. On the **Unity navigation bar**, select **System > Unity Systems**.
2. Click the link to the Unity System that you want to enable FTP support for.
3. Click **Summary > FTP**.

Figure 11-29: Unity Systems FTP panel



1. Select the **Enable FTP support for this Unity System** option.
2. Click the **Apply** button to save your changes.

Related topics:

Step 3: Configuring the access protocol on page 122

Using 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 system setup, or you can enable them later in Unity using the **CallHome** panel for the Unity System. See Enabling CallHome log collection settings on page 491.

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 Storage System 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 remote connectivity for CallHome on page 492. You can disable CallHome 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 on the facing page.

- 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 488.

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 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.

Event ID	Severity Level	Description	Resolution
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.
042003	**Critical**	A storage pool cannot be imported after a storage enclosure was powered up. Unity is unable to locate all volumes required to access the storage pool.	If a member of our technical support team has not contacted you, please reach out to us as soon as possible.
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.

Event ID	Severity Level	Description	Resolution
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.
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.
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 one of the NVDIMMs is failing.	If a member of our technical support 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.

Event ID	Severity Level	Description	Resolution
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 device 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.	Perform these steps: • Verify the cluster configuration using the `clustering` command. • Verify the cabling to the storage enclosure. If the problem persists, please contact Nexsan Technical Support.
140002	**Critical**	Fault management has fault with the following classes: • fault.io.pciex.device-interr-corr • fault.io.pciex.bus-linkerr-corr • defect.sunos.smf.svc.maintenance • defect.sunos.kernel.panic • ereport.sensor.failure • fault.io.disk.predictive-failure	If a member of our technical support team has not contacted you, please reach out to us as soon as possible.

Rule ID	Severity level	Description	Resolution
140003	**Critical**	System logs: ● 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.	If a member of our technical support team has not contacted you, please reach out to us as soon as possible.
140004	**Critical**	Unity sends logs for services that are in these modes: ● *Panicking* ● *Panicked* ● *Broken(unsafe)* ● *Broken(safe)* ● *Aborting*	If a member of our technical support team has not contacted you, please reach out to us as soon as possible.
140005	**Critical**	Any service that is in one of these states: ● Any cluster service that is in *Manual* mode for at least an hour ● Any service that is in *Maintenance* 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.

Rule ID	Severity level	Description	Resolution
140008	**Critical**	Storage pools errors, including: ● Any storage pool that is not *Online*. ● Any storage pool device that has more than 5 write, read, or checksum errors.	Perform these steps: ● Verify the storage pool status by running the `nstpool status` command. ● Clear the pool errors by running the `nstpool clear` command or using Unity. If the problem persists, please contact Nexsan Technical Support.
140009	Warning	Unity sends warning logs about the following: ● 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 *Manual* 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

Use this procedure to enable CallHome log collection.

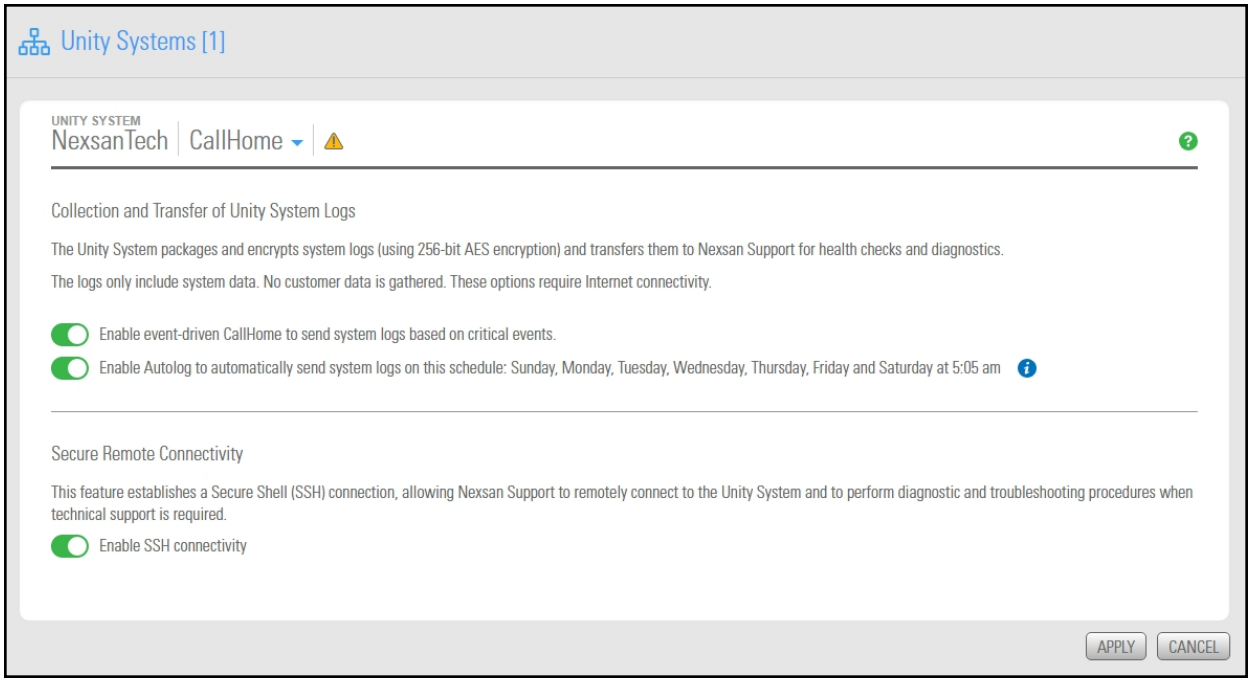
Prerequisites

- Unity must have Internet access; see Enabling Internet connectivity on page 493.
- 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. On the **Unity navigation bar**, select **System > Unity Systems**.
2. Click the link to the Unity System that you want to connect from.
3. Select **Summary > CallHome**.

Figure 11-30: Unity Systems CallHome panel



4. Select one or both of these options:
   - **Enable event-driven CallHome to send system logs based on critical events**
   - **Enable Autolog to automatically send system logs on this schedule**

Note If necessary, you can use the **Enable SSH Connectivity** option to establish a Secure Shell (SSH) connection, allowing Nexsan Support to remotely connect to the Unity System and to perform diagnostic and troubleshooting procedures when technical support is required. See Enabling SSH remote connectivity for CallHome on the next page

5. Click the **Apply** button to save your changes.

▶ **Related topics:**

Using the CallHome feature on page 484

How CallHome is triggered on page 484
Enabling SSH remote connectivity for CallHome below

Enabling SSH remote 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 all ten attempts fail, the CallHome feature will send a signal to the Event Viewer.

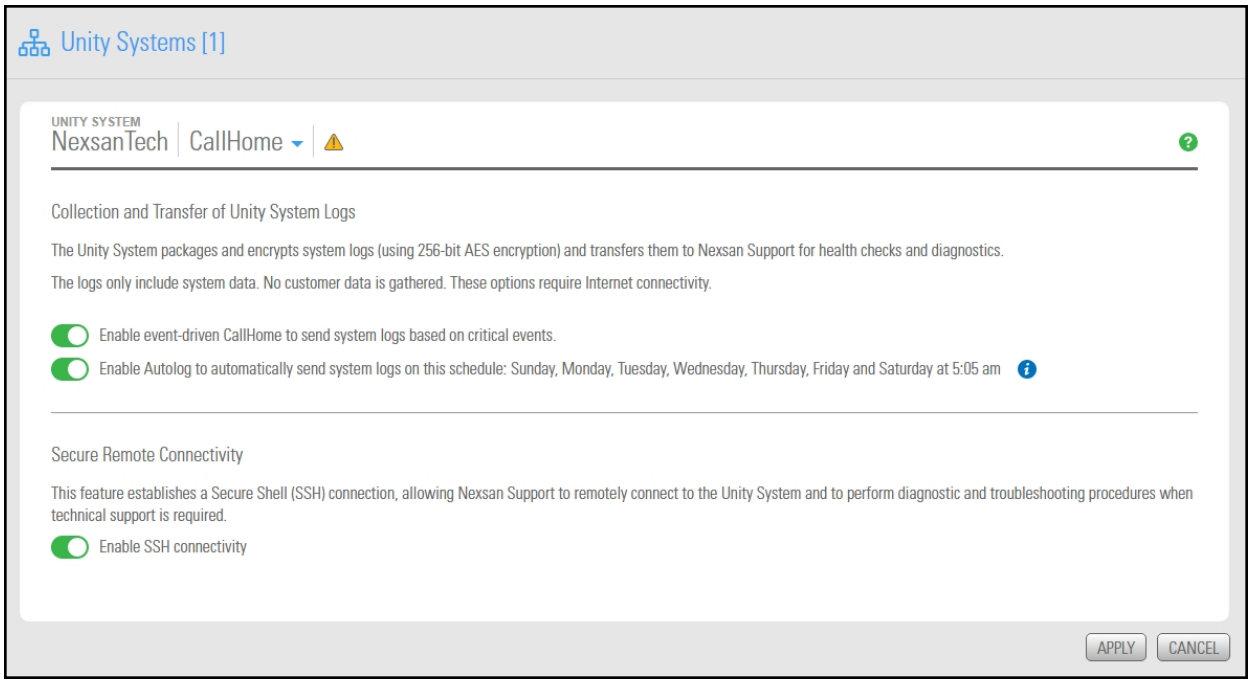
Prerequisites

- Unity must have Internet access; see Enabling Internet connectivity on the facing page.
- At least one of these ports must be open and allowed between Unity and the network firewall:
  - 20022
  - 80

To enable SSH connectivity:

1. On the **Unity navigation bar**, select **System > Unity Systems**.
2. Click the link to the Unity System that you want to connect from.
3. Select **Summary > CallHome**.

Figure 11-31: Unity Systems CallHome panel



4. Select the **Enable SSH connectivity** option.
5. Click the **Apply** button to save your changes.

You can disable SSH connectivity at any time by clearing the option.

Related topics:

Using the CallHome feature on page 484

How CallHome is triggered on page 484

Enabling CallHome log collection settings on page 491

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 Using the CallHome feature on page 484. 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 next page
- Connecting to the Internet using HTTP on page 495
- Connecting to the Internet using a workstation on page 496

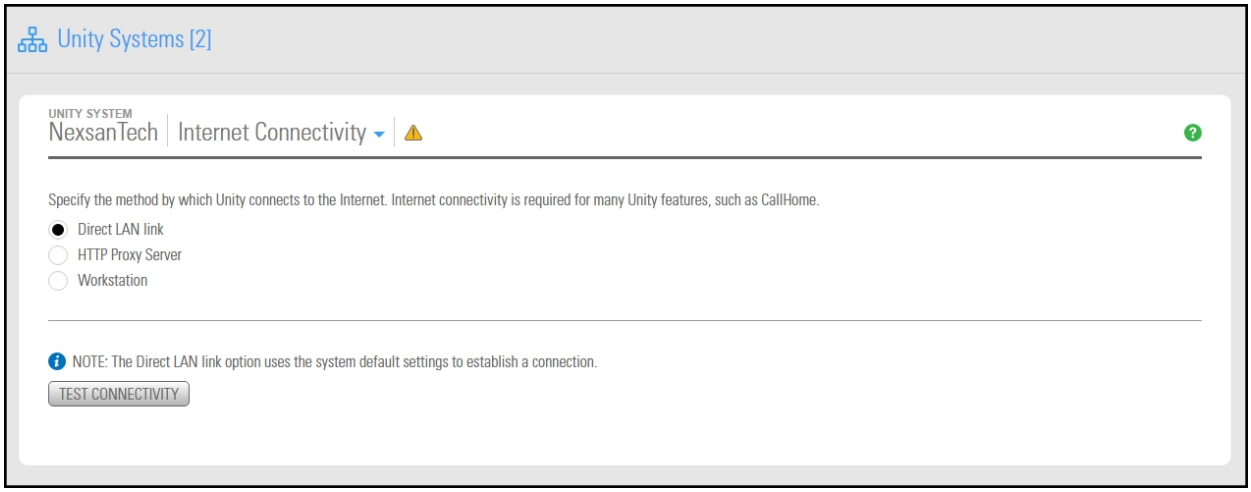
Connecting to the Internet using a Direct LAN link

This method uses the system default settings to establish a connection to the Internet.

To configure the direct LAN connection:

1. On the **Unity navigation bar**, select **System > Unity Systems**.
2. Click the link the Unity Storage System that you want to set up a **Direct LAN link** for.
3. Select **Summary > Internet Connectivity**.
4. Select **Direct LAN link**.

Figure 11-32: Internet Connectivity panel



5. Click the **Test Connectivity** button.
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 the **Apply** button to finalize the configuration.

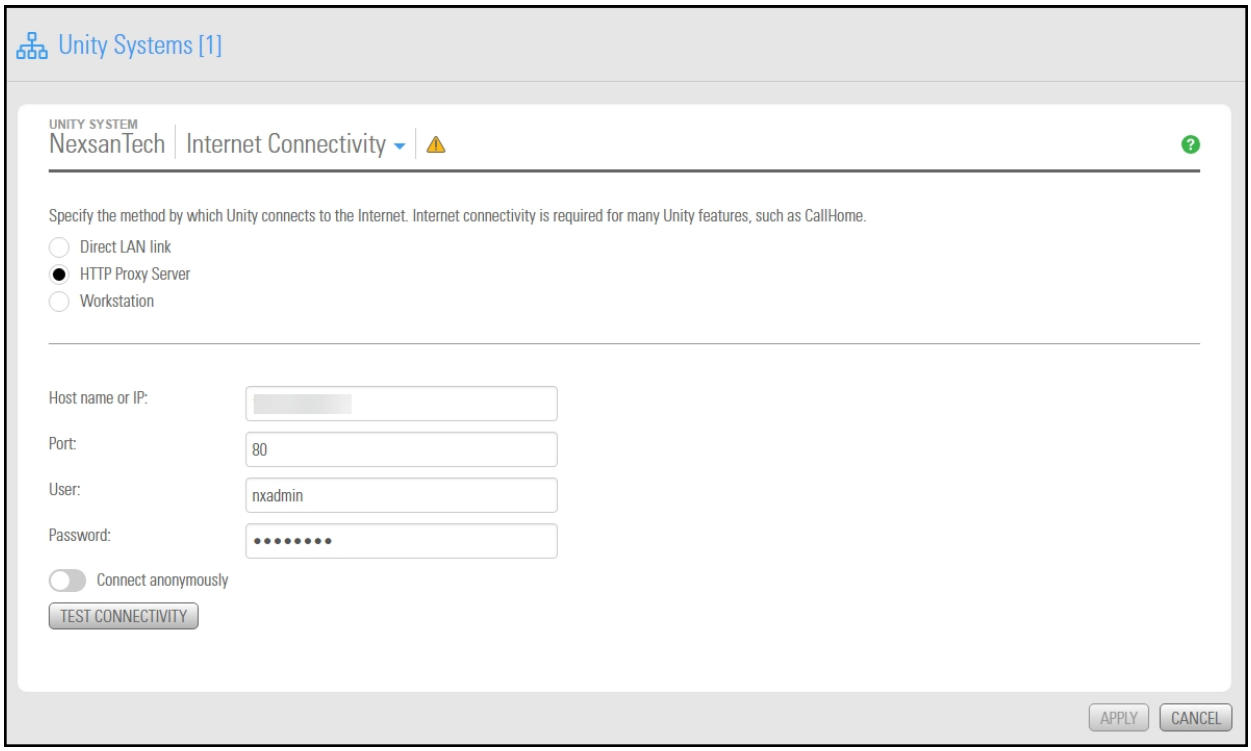
Connecting to the Internet using HTTP

This method connects to the Internet through an HTTP proxy server configured on your network.

To configure the connection to an HTTP proxy server:

1. On the **Unity navigation bar**, select **System > Unity Systems**.
2. Click the link to the Unity System that you want to connect from.
3. Select **Summary > Internet Connectivity**.
4. Click the **HTTP Proxy server** radio button.

Figure 11-33: Internet Connectivity panel: 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 the **Apply** button 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.

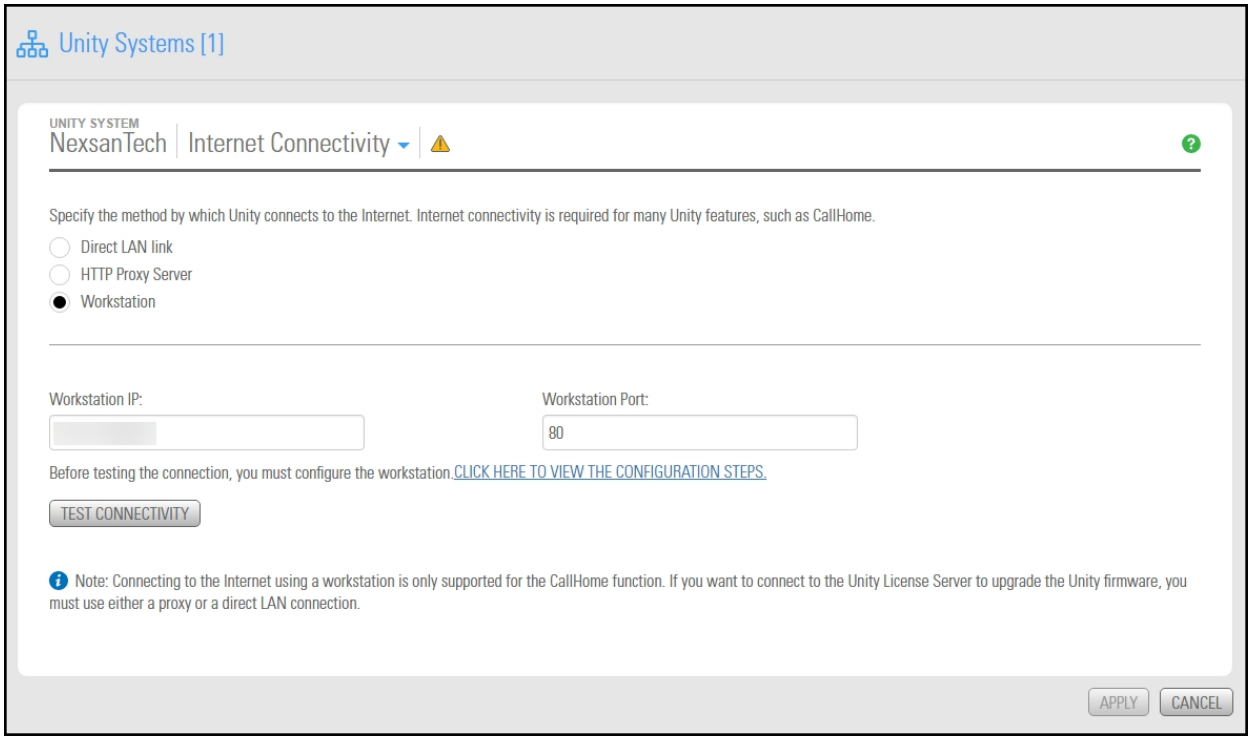
This method is only supported for the Call Home feature. For details on Call Home, see Using the CallHome feature on page 484. For all other features, you must use a direct LAN or proxy connection; see Connecting to the Internet using a Direct LAN link on page 494 or Connecting to the Internet using HTTP 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. On the **Unity navigation bar**, select **System > Unity Systems**.
2. Click the link to the Unity System that you want to connect from.
3. Select **Summary > Internet Connectivity**.
4. Click the **Workstation** radio button.

Figure 11-34: Internet Connectivity Workstation panel



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=000.01.002.003 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 the **Apply** button to finalize the configuration.

11

Chapter 12

Data replication

Unity provides comprehensive data protection for your Unity deployment, including off-site disaster recovery and remote redundancy, through its replication functions.

Use the asynchronous data replication feature to designate a secondary Unity as the replication system for a storage pool. Once you set up data replication, Unity automatically creates a replica of the storage pool on the remote Unity System. Later, when you add file systems to the storage pool on the primary Unity System, you can enable or disable replication for each dataset (file systems and/or iSCSI LUNs) to the remote Unity System, as needed.

This section provides an overview of Unity's data replication functions, and describes how to set up and manage data replications for your Unity storage infrastructure.

Note Configuration of the synchronous data replication feature is currently supported:

- in the Unity HTML5 user interface.
- using the NestOS `nxcmd SyncReplication` commands. Please refer to the *nxcmd Command Line Interface Reference Guide* on the Nexsan.com/support webpage.

This section includes these topics:

Data replication concepts and terminology 500
Asynchronous data replication 501
Usage implementations 501
Asynchronous data replication features 504
Setting up asynchronous data replication 506
Performing a manual replication 516
Configuring asynchronous replication for a dataset 518
Modifying asynchronous replication properties and configuration settings 520
Failing over to a remote Unity Storage System for disaster recovery 523
Configuring asynchronous replication settings 528
Removing asynchronous data replication for a storage pool 532
Enabling browsing of a replicated file system snapshot 534
Configuring the network type for data replication 536
Synchronous data replication 538
Cloud Connector 539

Data replication concepts and terminology

This table describes Unity replication concepts and terminology used.

Table 12-1: Replication concepts and terminology

Replication terminology	Description
primary, primary system, or primary Unity Storage System	A primary system refers to a Unity Storage System that contains the data to be replicated (to a secondary Unity Storage System). A Unity Storage System can be the primary system in a replicated environment and also perform double-duty as the secondary data replication system for another Unity System.
secondary system, replication system, or remote Unity Storage System	A secondary system represents the system to which data from the primary Unity is replicated. In a deployment where asynchronous replication is not implemented, a secondary Unity represents a system that is being managed remotely from another Unity Storage System.
source, source storage system source storage pool	Source storage pool refers to the storage pool that contains the data to be replicated to a *target*.
target, target storage system target storage pool	Target storage pool refers to the replica of the source storage pool on the target system.
peer, peer Unity system, peer system, or replication peer	A peer Unity Storage System represents a Unity System that you set up data replication to or from.
replica, pool's replica or storage pool replica	A replica, or a storage pool's replica, refers to the target storage pool that is created on the secondary Unity System. The replica is an exact copy of its source storage pool on the primary Unity System.
full replication	Full replication refers to a replication operation that sends all the data on the primary to the secondary Unity Storage System. Only the initial replication, when you first set up asynchronous data replication is a full replication.replication between two systems, is a full replication. All successive replications are incremental.
incremental replication, or incremental update	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).

Replication terminology	Description
scheduled or automatic 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.
offline or manual 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 Storage System, or to a USB storage device attached to the primary Unity Storage System.
scrubbing	Unity provides a disk scrubbing mechanism that checks the physical hard disks, which comprise the volumes in a storage pool on a Unity Storage System, 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 Storage System. By default, the scrub schedule is enabled on the replica. See .

Asynchronous data replication

Asynchronous data replication enables you to replicate data between two Unity Systems—a primary and a remote Unity—over a LAN or WAN connection.

This section covers these topics:

Asynchronous data replication features on page 504

Usage implementations below

Usage implementations

You can use the asynchronous data replication for:

- Disaster recovery: You can set up data replication between two Unity systems—a primary and a secondary system—for disaster recovery. In the event of a disaster that impacts user access to the primary Unity System, 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 Unity System, you can then *demote* the disaster recovery Unity System back to secondary status. During the demotion process, the asynchronous data replication function automatically preserves any data that changed while the secondary Unity System was in service, and creates a *difference* file on the secondary Unity System listing the changes. This process is explained in detail in Failing over to a remote Unity Storage System for disaster recovery on page 523.
- 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 Unity Systems 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	These ports must remain open across the WAN (and/or LAN) links: • TCP ports **22** and **873** • UDP port **873** All switches, routers, and firewalls between each source Unity System and the remote/DR Unity System must be configured accordingly to allow the source and destination Unity Storage Systems to communicate. The network should also be secured using firewalls, VPN, encryption, or other means. 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. Also, since Unity uses port aggregates, you cannot connect systems directly. You must use a switch between systems.
Remote Unity System	• Make sure the system is properly configured using Unity. • The remote system must have the Data Replication feature installed. • Make sure the secondary Unity System is connected to the network and powered on. It should be accessible from the primary Unity System. • If the remote Unity System has any Nexsan storage enclosures connected to it, and you intend to allocate volumes on the storage systems to the replicated data, make sure the system is cabled properly and connected to the secondary Unity System, and that it is powered on and online. The Unity Storage System(s) must also be configured properly with Unity and added to the secondary system as a Unity System.
Disaster recovery	• 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.

Element	What to do before creating a replication process
Storage capacity	The Unity Storage System that you intend to use as your remote system should have adequate storage capacity to match the capacity on the primary system—although this is not a requirement for setting up asynchronous data replication for your system. For example, if the total disk space of the volumes allocated to the storage pool on the primary system is 100 TB, the remote system should also have a minimum of 100 TB of disk (volume) space available for the storage pool's replica. If the remote system 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. For additional details on storage capacity, see Understanding disk space consumption on page 233.
Authentication	Make sure that you have the **nxadmin** password, or if applicable, the user name and password for a System Administrator on the remote system. When setting up data replication, if the user account you are currently logged on with on the primary system does not exist on the remote system, you will need the **nxadmin** password for the remote system, or optionally, the user name and password of a System Administrator configured on the remote system.
USB storage device	If you replicate the datasets to a USB storage device attached to the primary system, you will need to connect the USB device to one of the USB ports on the *active* node. To determine which node is *active* prior to starting the procedure, see Viewing cluster status on page 386.
Thick LUNs	If you intend to replicate thick LUNs, follow the recommendations mentioned in Understanding disk space consumption on page 233.

Element	What to do before creating a replication process
Data compression on file systems	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 system. If you set a space quota on the file system and that quota is almost full, the file system on the remote system 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 systems.
Data compression on LUNs	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 system. 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 system does not have enough space. In this instance, it is recommended to enable data compression on both systems before replication. For procedural steps, see .

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 systems. You can automate replication updates based on a user-defined schedule, or perform manual replications of your data to either the secondary Unity System 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 system 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 file system- 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 (file systems and/or iSCSI LUNs).
- Remote access to replicated data: You can access read-only copies of replicated data on the secondary Unity System for off-site backup or data distribution.

- Security: The asynchronous data replication feature uses a secure file transfer protocol to transmit data streams between systems. This ensures that all your data, including file system- and file-level access permissions, are transferred securely to the secondary Unity System. In addition, a Unity System can only replicate to/from another Unity System that you manually add to its list of peer systems.

  Note The streams take additional space on Unity before they are replicated. That amount of space does not apply to the secondary system.

- Flexible configuration: You have the flexibility to replicate all the datasets (file systems 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 enables you to replicate one or more storage pools on the primary Unity System to a single secondary Unity System. Alternately, you can replicate each storage pool on Unity to a different secondary Unity system.

Setting up asynchronous data replication

This section describes the process for setting up data replication for a storage pool on the primary Unity Storage System.

See Before you begin on page 502

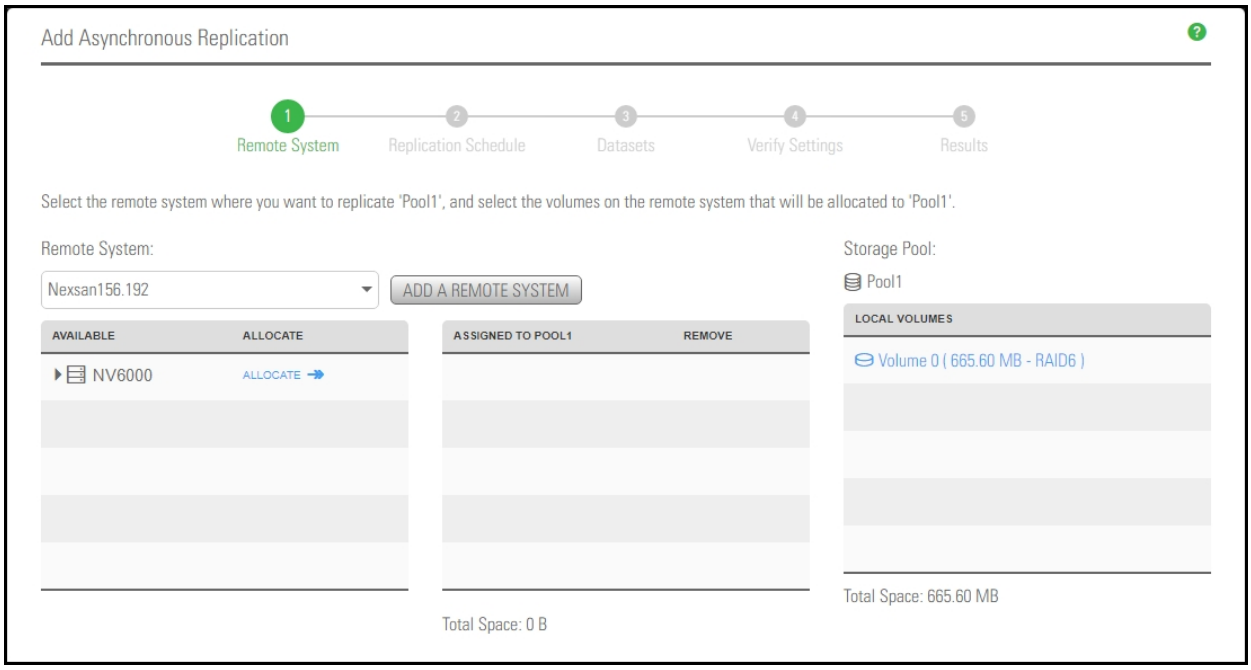
Prerequisites

- Define at least one storage pool on the primary Unity System. Replication of compressed pools is also supported.

To start the Asynchronous Data Replication wizard:

1. On the **Unity navigation bar**, select **Data Protection > Replications**.
2. In the **Replications** panel, click the **Add Asynchronous Replication** button.

Figure 12-1: Add Asynchronous Replication wizard, Step 1



Note The **Add Asynchronous Replication** wizard is available only when storage pools, file systems, and/or LUNs are defined in the storage pool.

This section includes these steps:

Adding a remote Unity System and assigning space 506
Configuring a replication schedule 509
Allocating FASTier cache devices to replication 513
Verifying settings 514
Viewing results 515

Adding a remote Unity System and assigning space

In *step 1* of the **Add Asynchronous Replication** wizard, you

- add a remote Unity Storage System where you want to replicate the storage pool, and
- select one or more volumes from a pool on the remote system to maintain the replica.

To add a remote site as the data replication site:

1. In the Asynchronous Replication wizard, click the **Add a Remote System** button.

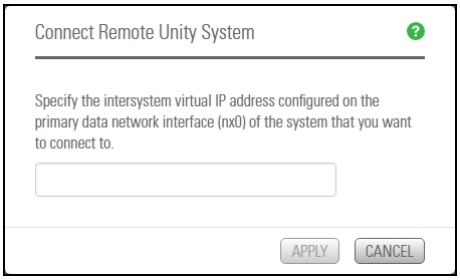
   Note If a remote site has already been added, select it from the Remote system box and skip to step 5, below.

   Unity automatically displays the storage systems connected to the remote site, along with their available volumes. If no volumes display, this means the remote system does not have any free volumes; they are all in use by one or more storage pools.

2. In the **Connect Remote Unity System** window, enter the **inter- system virtual IP address** for the **Primary Data Network (nx0) interface** of the remote Unity that you want to use.

   This IP address, configured when you set up your Unity System, enables connectivity between two or more sites for data replication and inter-site communication. See the *Unity Quick Start Guide* shipped with your system, and posted on the nexsan.com/support webpage.

Figure 12-2: Connecting to a remote site



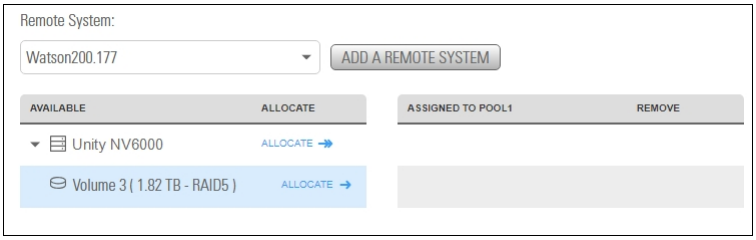
3. Click the **Apply** button to establish a connection to the remote Unity.

   Depending on the speed of your network connection, this process can take some time to complete.

   You must provide the Unity Administrator (**nxadmin**) credentials for the secondary Unity.

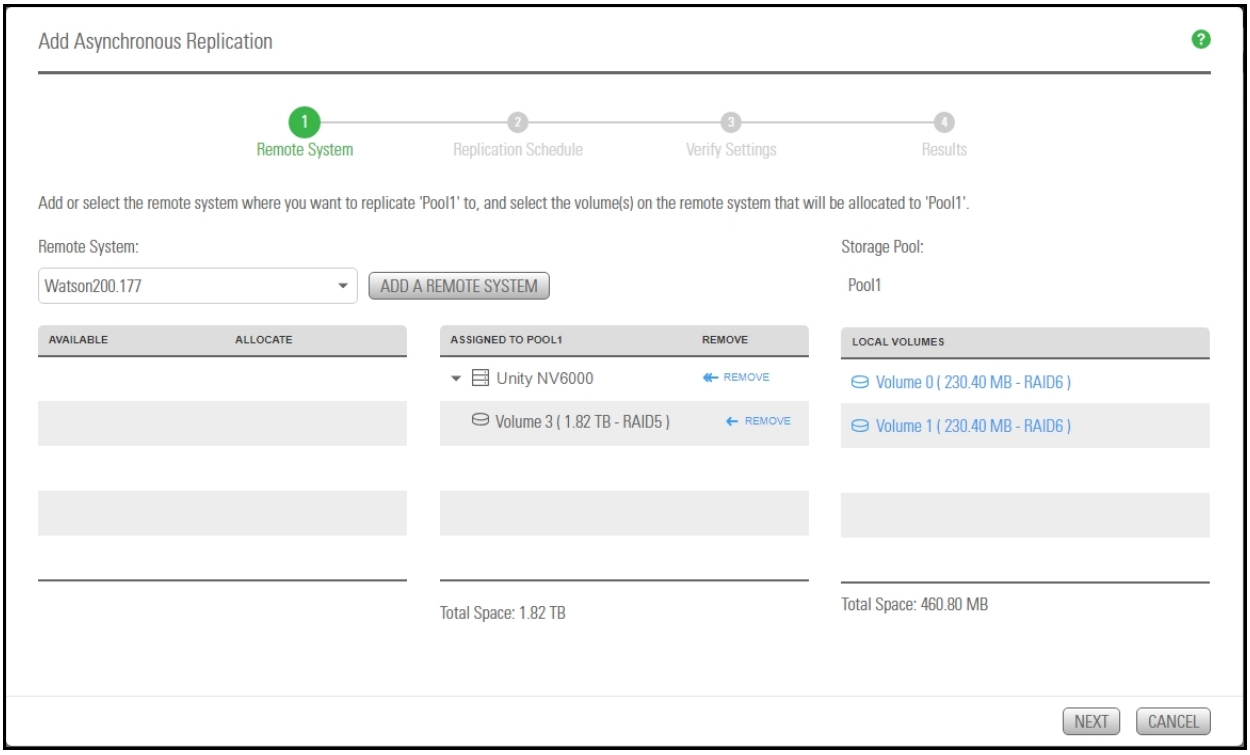
4. When the connection is established, click the **OK** button.
5. Expand the Unity Storage System displayed in the **Available** column.

Figure 12-3: Available systems



6. Click **Allocate** to assign a volume to an available pool on the remote system.

Figure 12-4: Assigning a volume to a remote system



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.

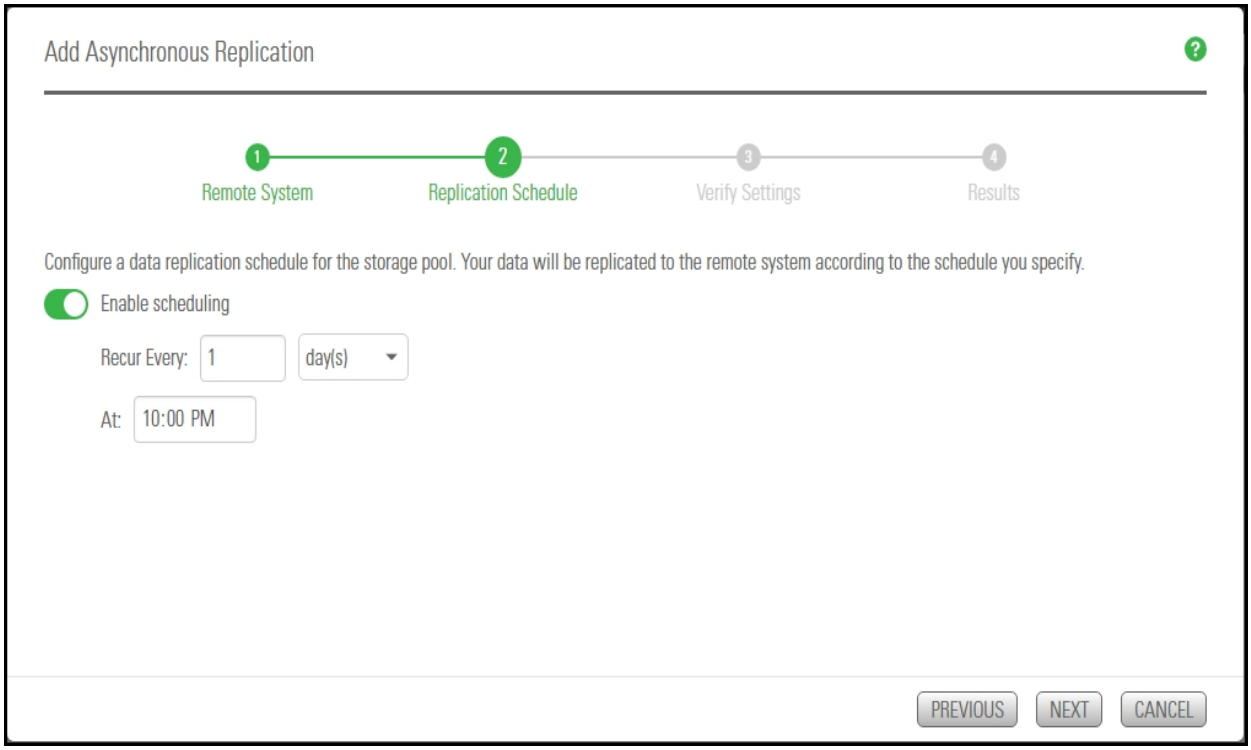
7. Click the **Next** button on the panel to continue to Configuring a replication schedule on the facing page.

Configuring a replication schedule

In *step 2* of the Add Asynchronous Replication 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 12-5: Add Asynchronous Replication wizard, step 2: Replication schedule



To configure the replication schedule for the storage pool:

1. Optionally, revise any of the following defaults.
   - Disable scheduled replication. The default is enabled.
   - Specify a recurrence schedule by typing a value in the **Recur every** field. The default recurrence is once a day.
   - Change the recurrence period from the drop-down list. The default is 1 day. You can set the recurrence in **minutes**, **days**, **hours**, **weeks,** or **months**.
   - Specify the time of day when you want Unity to perform data replications. The default time is 10 PM.
2. When you finish configuring the data replication schedule for the storage pool, click the **Next** button on the panel.

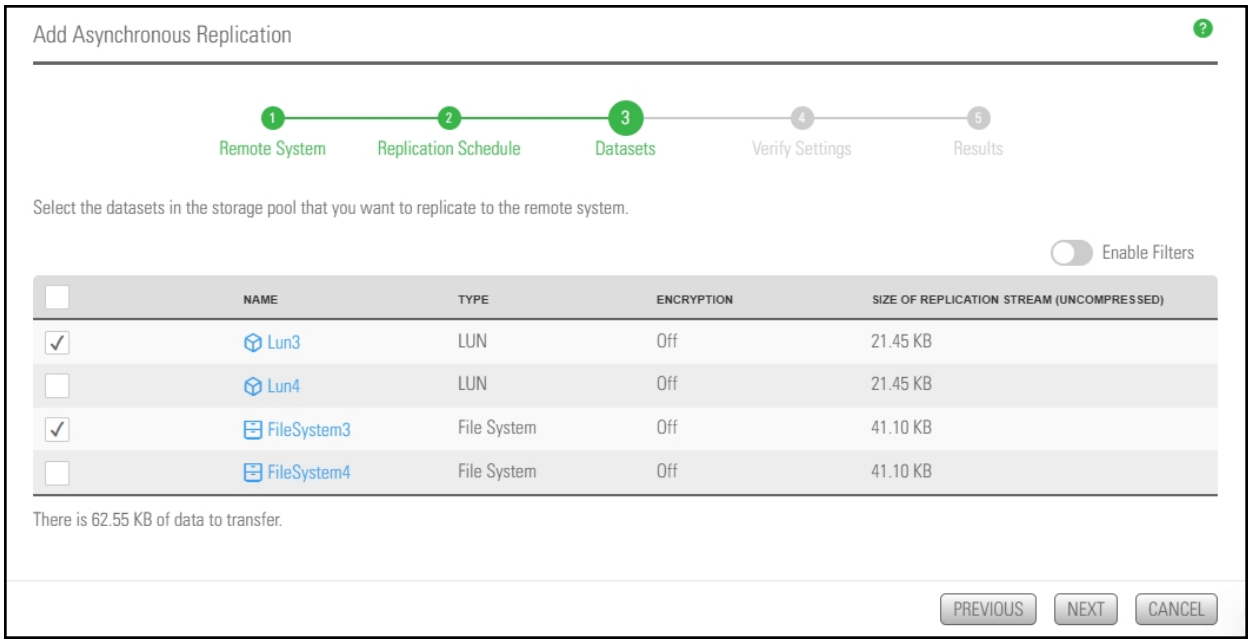
Selecting datasets to replicate

This step is only displayed if you have datasets defined in the storage pool to be replicated. The term "datasets" refers to file systems and/or iSCSI LUNs.

Note Some datasets contain no user data, and do not need to be replicated for off-site disaster recovery. In such cases, you can deselect the dataset to exclude it from replication.

You can enable data replication for your datasets later; see Configuring asynchronous replication for a dataset on page 518.

Figure 12-6: Add Asynchronous Replication wizard: Datasets



▶ To select the datasets for replication to the remote site:

1. Ensure that the check box corresponding to the datasets that you want to replicate to the secondary Unity is enabled.

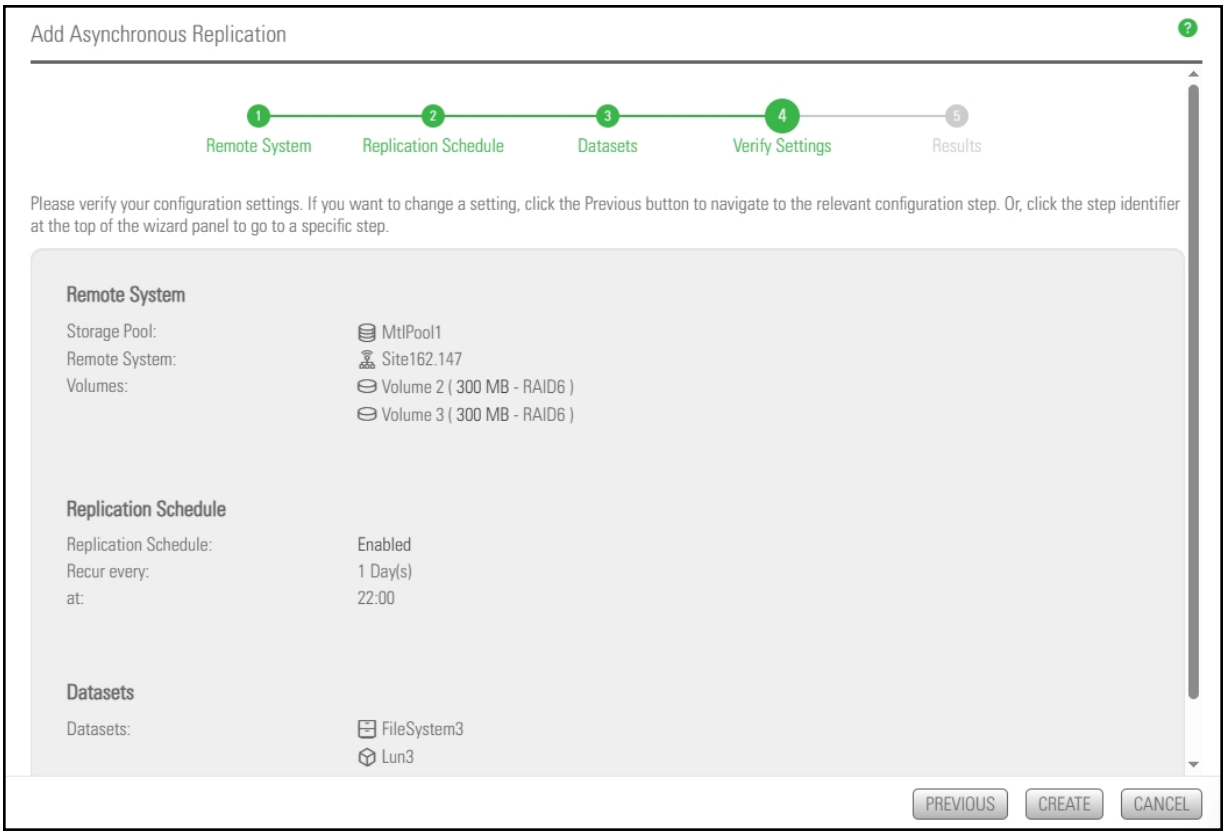
   You can search for a specific dataset by clicking the Enable Filters button and entering its name in the text box above the **Name** column heading. The grid automatically filters the list as you type.

   If you want to replicate all the datasets in the storage pool, click the **All** check box at the top of the first column.

   Click the **Next** button.

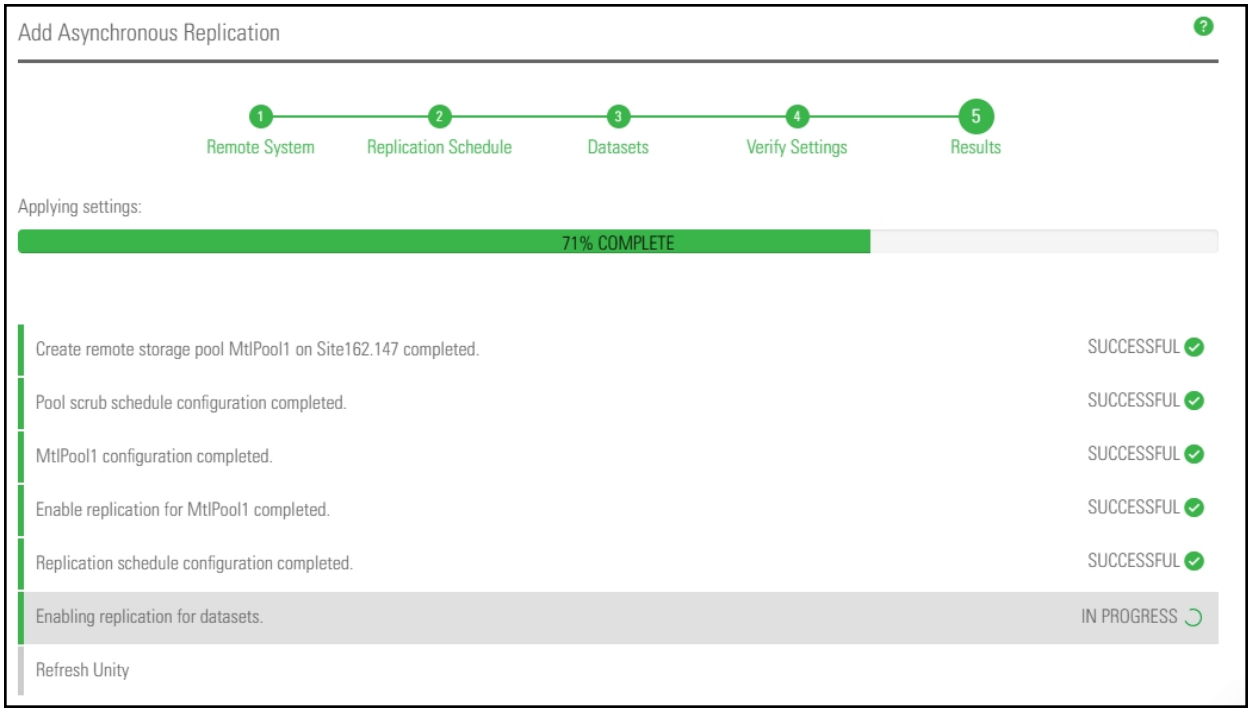
2. In Step 4 **Verify Settings**, review the details to ensure the configuration is correct. To make changes, click the **Previous** button, or click the step identifier at the top of the wizard panel to go to a specific step. When ready to proceed, click the **Create** button to add the asynchronous replication.

Figure 12-7: Add Asynchronous Replication wizard: Verify Settings



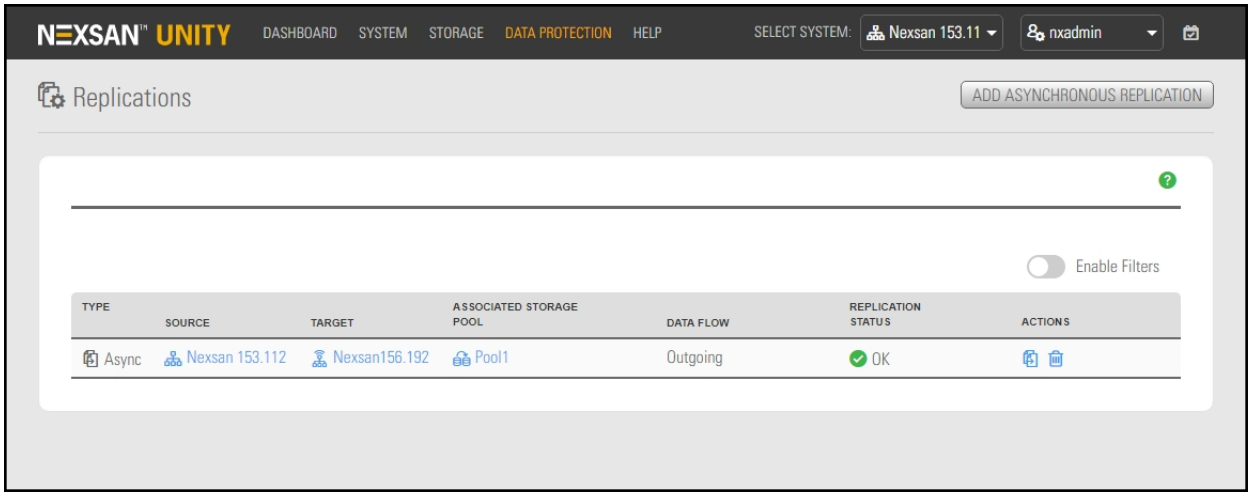
3. Unity creates the replication, and displays the results in Step 5 of the wizard. A system dialog confirms that asynchronous replication is successful. Click the **Close** button to dismiss.

Figure 12-8: Add Asynchronous Replication wizard: Results



4. The replications panel appears,showing details of the replication.

Figure 12-9: Replications panel



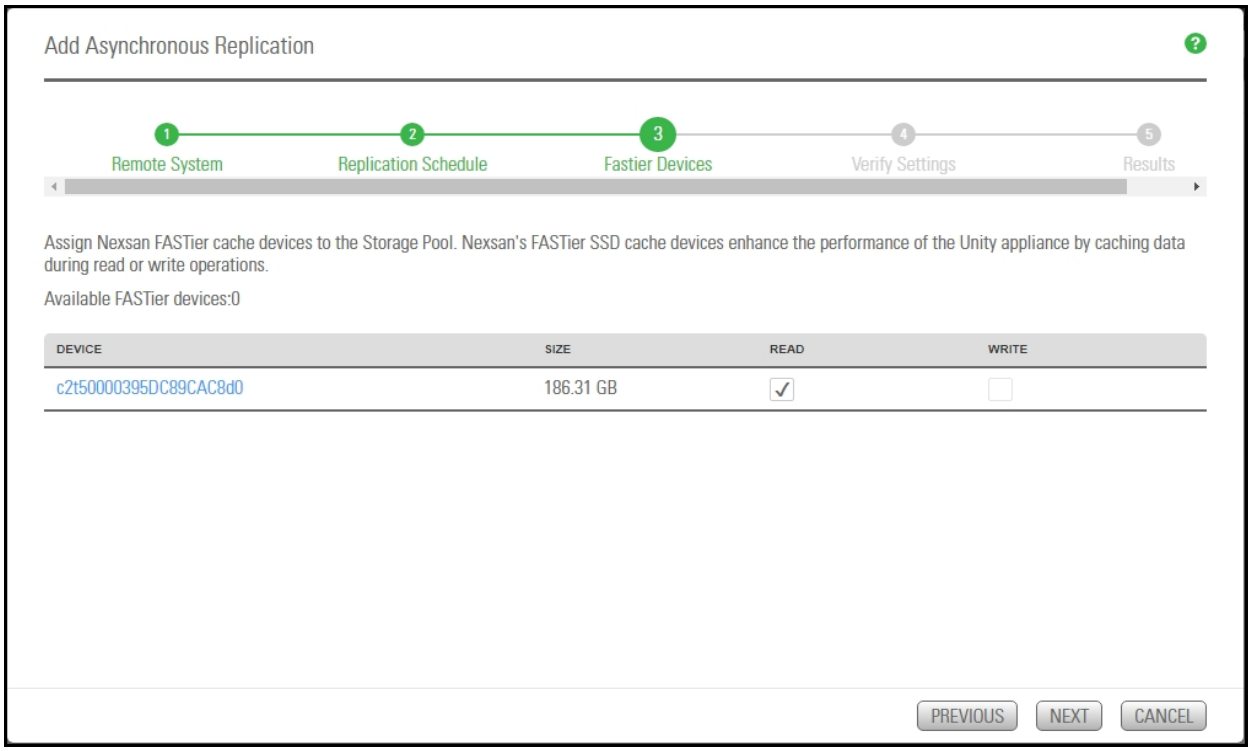
Allocating FASTier cache devices to replication

This step displays only if the remote Unity System has 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, not both.
- 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.

Figure 12-10: Add Asynchronous Replication wizard: FASTier devices



To allocate FASTier cache devices to the storage pool's replica:

1. Select which of the listed FASTier cache devices on the remote system should be used for **READ** only or **WRITE** access.

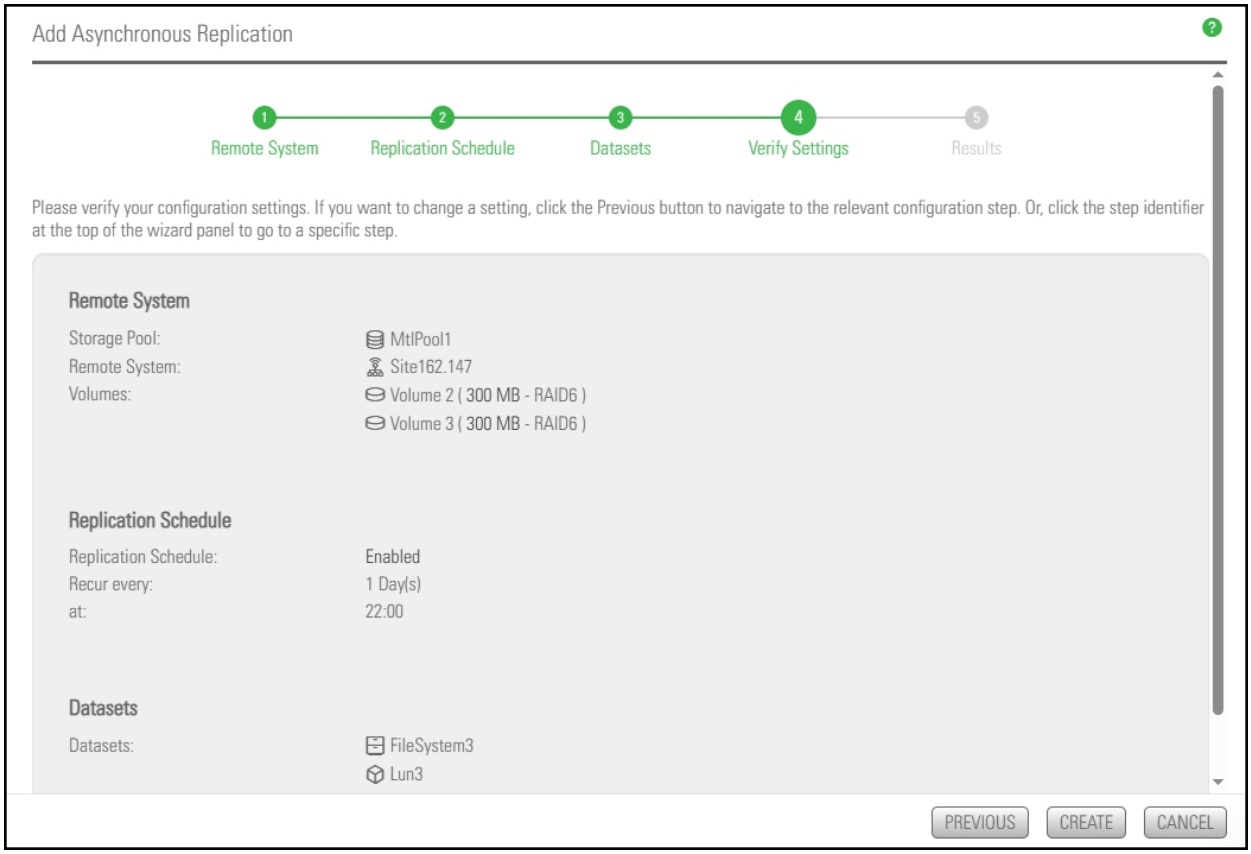
   As you select the number of read and write cache devices to allocate to the storage pool's replica, the **Available FASTier devices** section on the wizard panel automatically updates to display how your selections impact cache assignment on the remote site.

2. When you finish allocating FASTier cache devices to the storage pool's replica, click **Next** on the wizard panel to continue to Verifying settings on the next page.

Verifying settings

This step of the Asynchronous Data Replication Setup wizard summarizes the settings you selected for data replication and applies the settings when you click **Create**. Review the summary carefully before applying the data replication settings.

Figure 12-11: Add Asynchronous Replication wizard: Verifying settings



To change a configuration setting:

- Click the back arrow to navigate back to the corresponding configuration step.

  Or

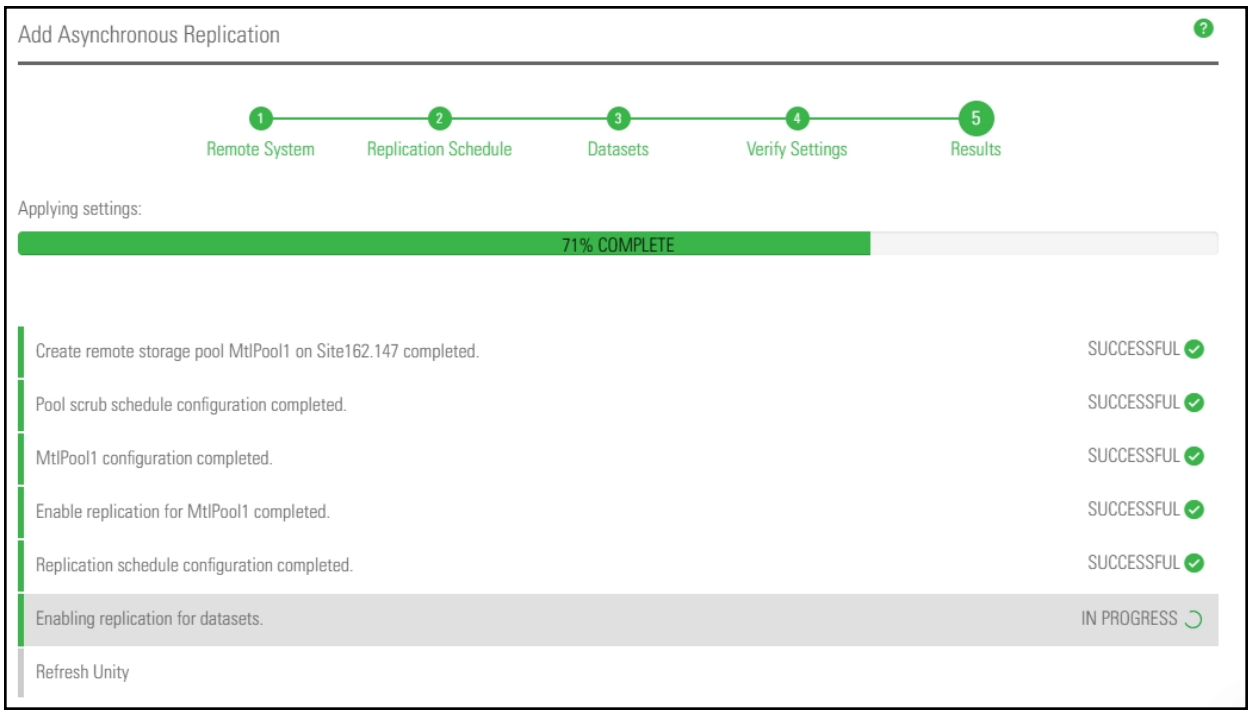
- Click the corresponding step identifier at the top of the wizard panel. For example, if you want to modify the replication schedule, click 2.

If you are satisfied with the configuration settings, click the **Create** button at the bottom of the panel. The wizard automatically proceeds to Viewing results on the facing page.

Viewing results

This step of the Add synchronous Replication wizard displays progress as Unity applies your replication configuration to the primary and secondary systems.

Figure 12-12: Add Asynchronous Replication wizard: Viewing results



The Asynchronous Data Replication Setup wizard displays the progress as the replication is configured. It also shows error events, if applicable, that the system encounters during the configuration process. You can view more details about an error event by expanding the corresponding entry.

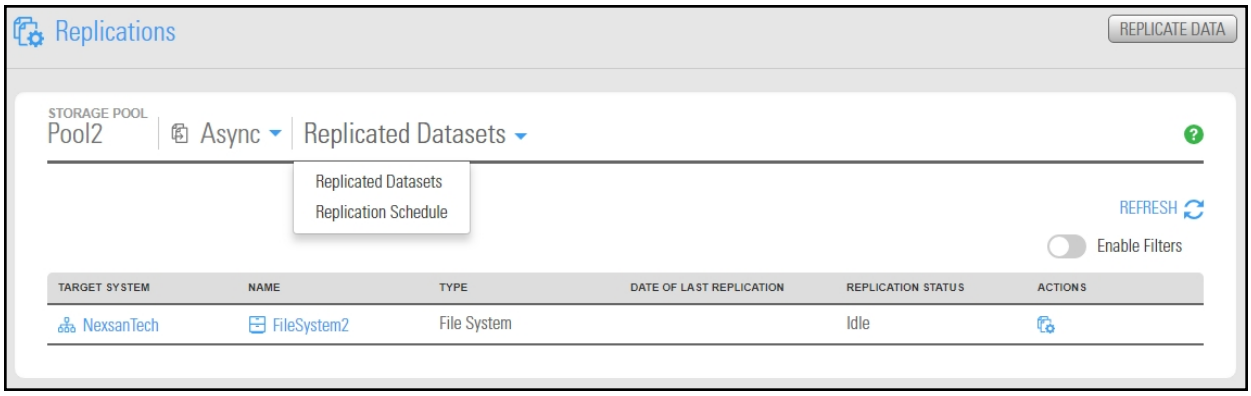
To view more details for an error event:

- Click the **View Error** link next to the error in the **Results** panel.

Click the **Close** button to close the wizard.

The replications panel will now show the replication details and available actions. For example:

Figure 12-13: Replications panel



Icon	Name and description
	Replicate Data: Runs data replication immediately
	Remove Replication: Removes the configured replication schedule

The replication will start at the new replication schedule. To change the schedule, see Modifying a storage pool's replication schedule on page 520.

Performing a manual replication

This section explains how to perform a manual replication of the data in a storage pool to a remote Unity System configured as a replication target for a storage pool.

When replicating to a remote system, 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.

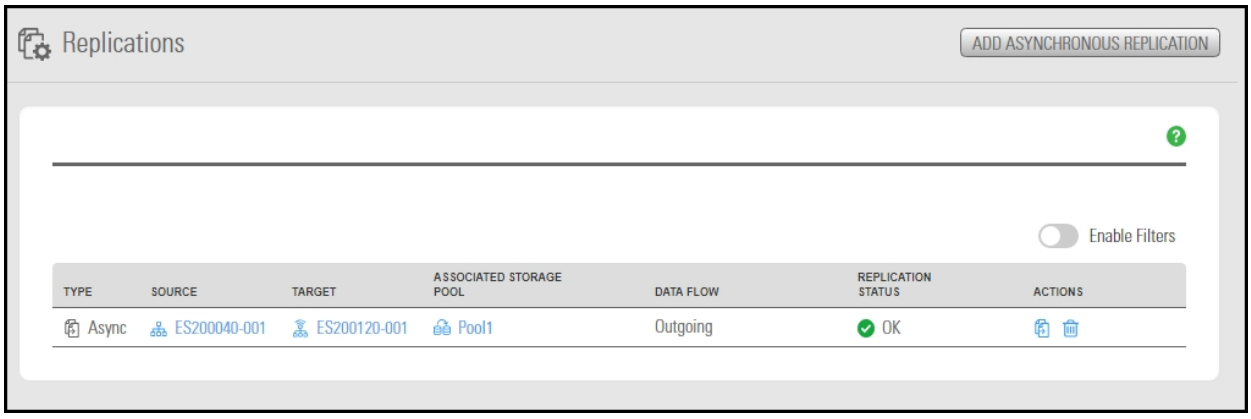
Prerequisites

- To perform this operation, you must have configured data replication for the storage pool and added at least a file system or a LUN to the storage pool.

To perform a manual data replication:

1. On the **Unity navigation bar**, select **Data Protection > Replications**.

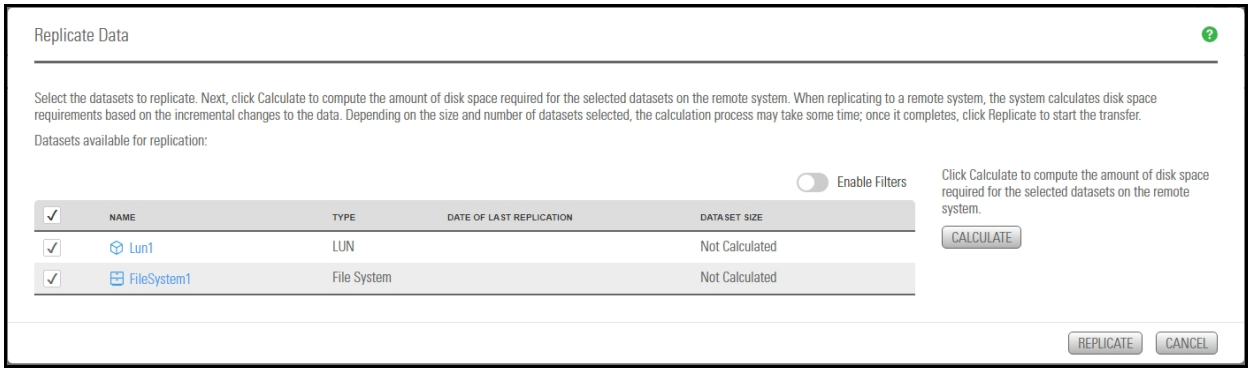
Figure 12-14: Replications panel



2. Do either of the following:
   - Click the **Replicate Data** icon
   - Click the link to the **Source** or **Target** Unity System where you want to perform the replication.

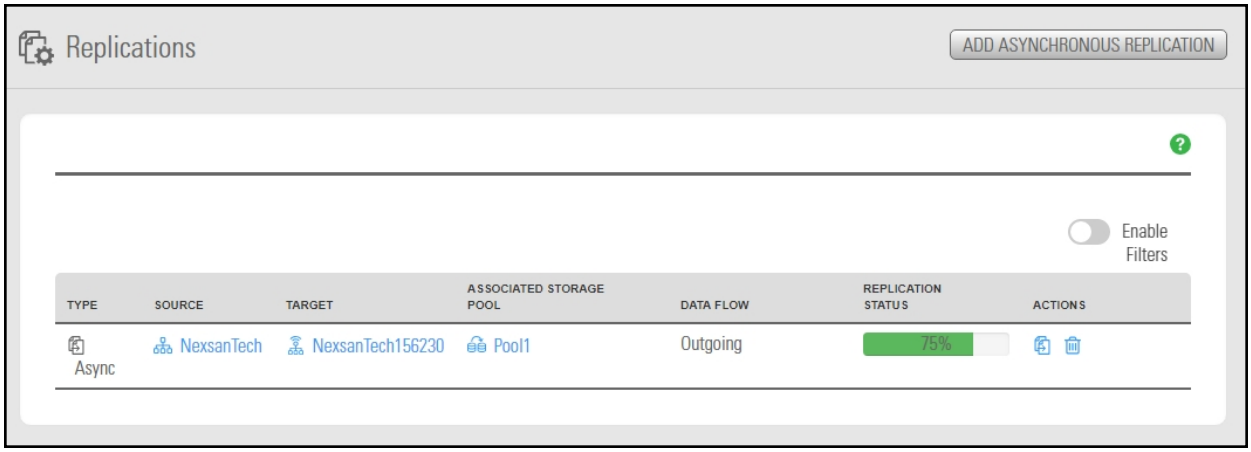
   The **Replicate Data** popup opens.

Figure 12-15: Replicate Data popup



3. Select the datasets to replicate.
4. Click **Calculate** to compute the amount of disk space required for the selected datasets on the remote system.
5. Once the calculation completes, click **Replicate** to start the incremental replication.
   Unity starts the replication and displays the replication progress in the **Replications** panel.

Figure 12-16: Replications panel: Replication in progress



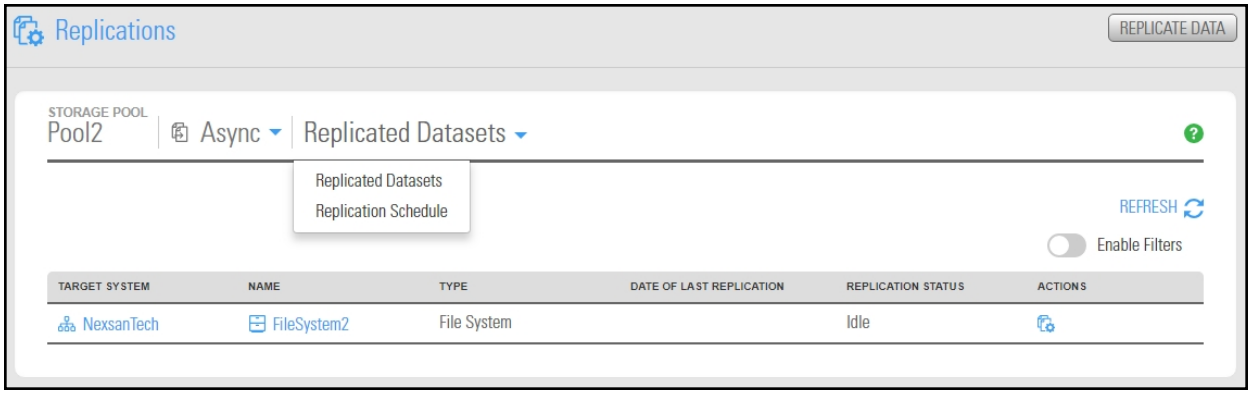
Configuring asynchronous replication for a dataset

Unity enables you to enable or disable asynchronous data replication for individual datasets (file systems 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 asynchronous data replication for a dataset:

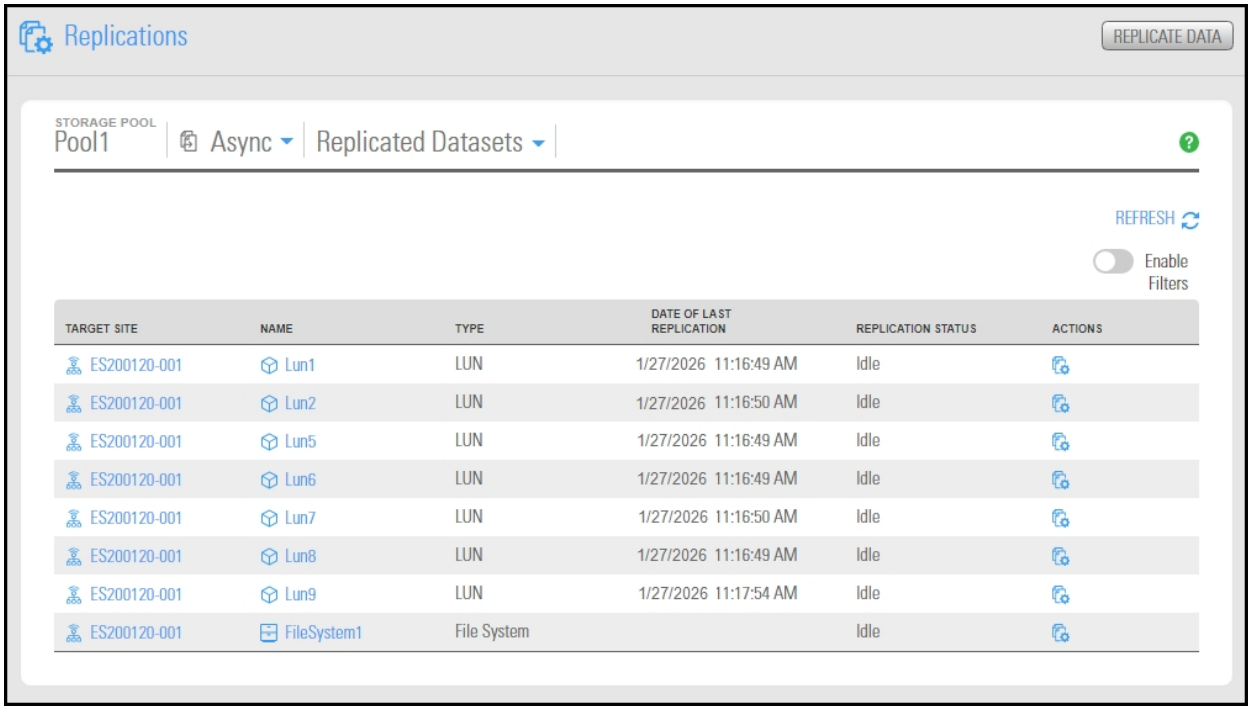
1. On the **Unity navigation bar**, click **Data Protection > Replications**.

Figure 12-17: Replications panel



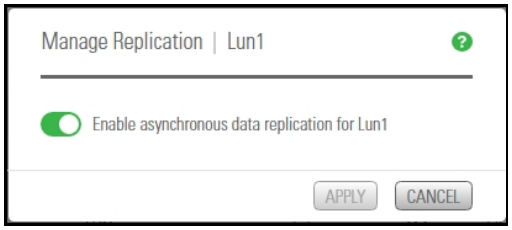
2. Click the entry in the table to open the **Replicated Datasets** panel.

Figure 12-18: Replicated Datasets panel



3. To search for a specific dataset, **Enable Filters** and enter relevant search information in one of the text boxes. The grid automatically filters the list as you type.
4. Click the **Manage Replication** icon. The **Manage Replication** popup opens.

Figure 12-19: Manage Replication popup window



5. Click the **Enable asynchronous data replication** button for the dataset, as required.

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:

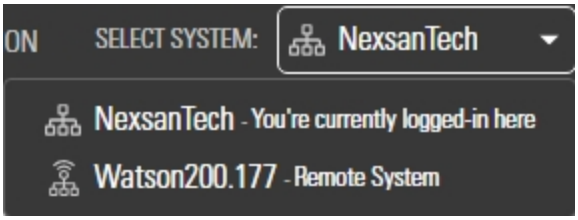
Modifying a storage pool's replication schedule 520
Disabling a storage pool replication schedule 521
Configuring asynchronous replication for a dataset 518

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.

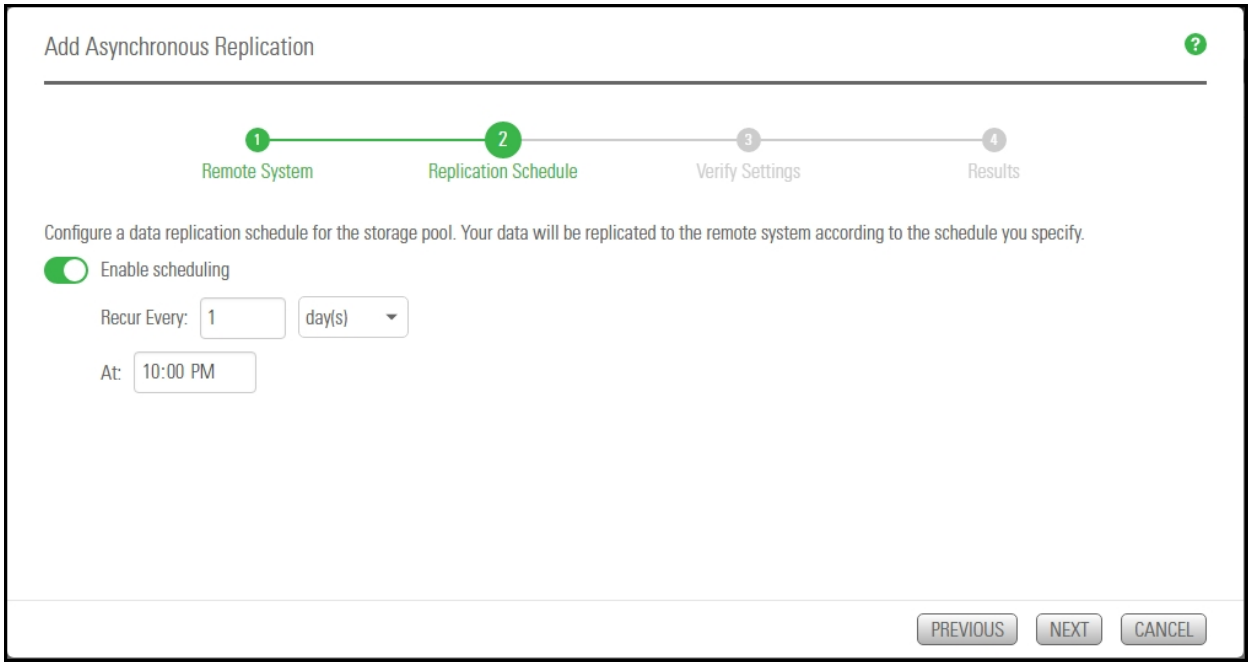
► **To modify a storage pool's replication schedule:**

1. On the **Unity navigation bar**, select the primary Unity System.



2. Select **Data Protection > Replications**.

Figure 12-20: Replication schedule



3. Specify whether you want automatic replication. The default is enabled.
4. Specify a recurrence schedule by typing a value in the **Recur every** field.
5. Select the recurrence type from the drop-down list: the default is 1 day. You can set the recurrence in **minutes**, **days**, **hours**, **weeks,** or **months**.
6. Specify the time when you want Unity to perform data replications. The default time is 10 PM.
7. When you finish modifying the data replication schedule for the storage pool, click the **Apply** button to save the new schedule.

Disabling a storage pool 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.

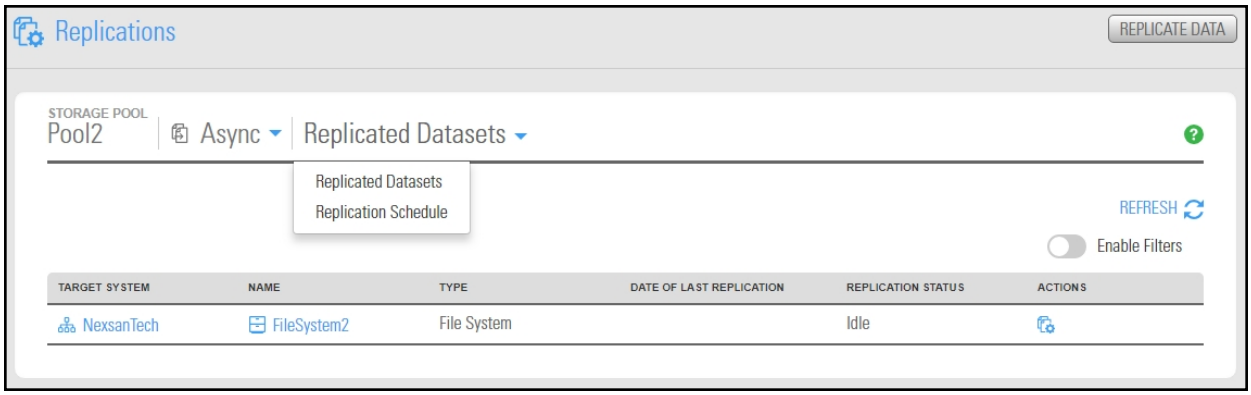
Prerequisites

- Replication must already be set up to a remote system.

To disable a storage pool replication schedule:

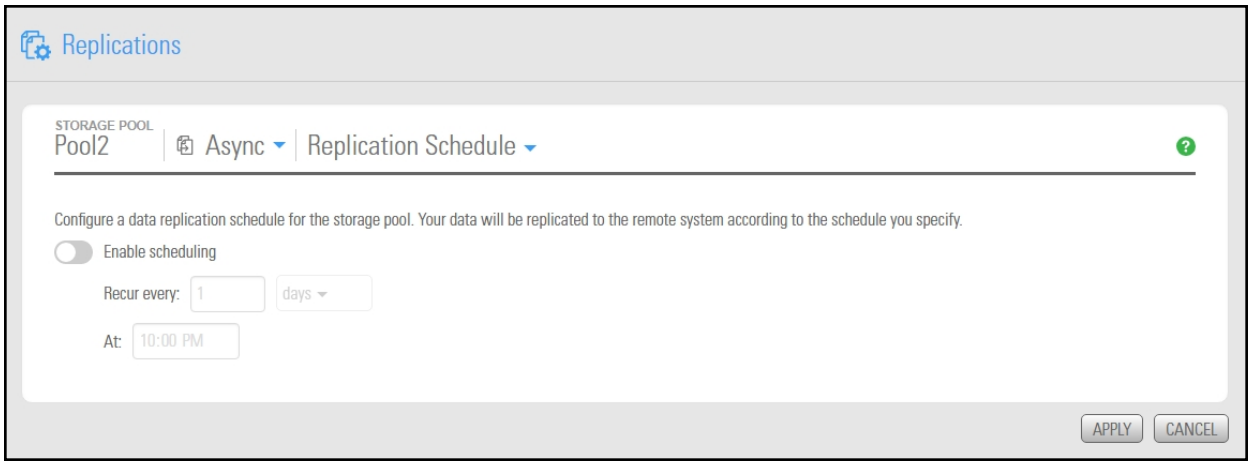
1. On the **Unity navigation bar**, click **Data Protection > Replications**. The **Replications** panel opens.

Figure 12-21: Replications panel



2. Click **Replicated Datasets > Replication Schedule**.
3. Click the **Enable scheduling** button  to disable scheduled replication.

Figure 12-22: Replications panel



4. Click the **Apply** button to complete the operation.

Failing over to a remote Unity Storage System for disaster recovery

The Unity data replication function provides a failover mechanism for your Unity deployment that enables you to automatically switch over all data and system operations on the primary Unity Storage System to a standby remote Unity Storage System.

This section includes these topics:

Failover vs. promote 523
Performing a failover of the entire Unity Storage System 525

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	• System maintenance on the primary system, including hardware component upgrade or replacement • Imminent system failure • Data migration • Load balancing	When you start the failover function, it first performs an incremental replication to update the data on the remote system. It then promotes the remote system to primary status in your deployment, and demotes the primary system to secondary status. If you only fail over a storage pool, or a subset of pools on the primary system, the failover function promotes the storage pool's replica on the remote system to primary status, and demotes the storage pool on the primary system to secondary status. After the failover completes, all storage pools that you failed over and their datasets are now accessible on the remote system. If the primary system has only one storage pool, failing over the storage pool has the same result as failing over the entire system. **Note** Only datasets that have replication enabled are failed over to the remote system. Datasets that do not have replication enabled remain on the primary system.
Promote	• Complete system failure on the primary system (primary system is non-responsive)	When you promote the remote system, the promote function changes the status of the secondary system to primary. The promote function does not replicate data from the primary system to the remote system. If you only promote a storage pool, or a subset of pools on the remote system, the promote function changes the status of the secondary storage pool to primary. After the promote completes, all storage pools that you promoted and their datasets are now accessible on the remote system. If the remote system has only one storage pool, promoting the storage pool to primary status has the same result as promoting the entire system. **Note** Only datasets that are replicated to the remote system are available after a promotion. When you restore the primary system, your deployment will have 2 primary systems or storage pools; you must then *demote* one of the systems or pools to secondary status.

Unity System failover vs. pool failover

The failover functionality enables you to fail over a single storage pool, or only a subset of the storage pools, to the corresponding remote Unity Systems. Alternately, you can fail over an entire Unity System to remote systems. Pool or System failover of a pool that has a compressed dataset is supported.

For example, on a primary Unity—System A—with two storage pools, Pool 1 and Pool 2:

- Pool 1 is replicated to secondary system B
- Pool 2 is replicated to secondary system C

You can:

- Fail over each pool separately to its corresponding remote system;
- Fail over the entire system. Each storage pool is failed over to the remote system where the pool is replicated.

Similarly, if both Pool 1 and Pool 2 on System A are replicated to the same remote system, System B, you can:

- Fail over each pool separately to System B;
- Fail over the entire system. Both storage pools are failed over to System B.

On a system with only one storage pool, failing over the storage pool has the same result as failing over the entire Unity System.

Performing a failover of the entire Unity Storage System

This section describes the process for performing a failover of a primary Unity Storage System to the remote system where the storage pools from the primary system 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 transitioned to the replicated system. During this time, all LUNs to be transitioned will be inaccessible and file systems will be accessible in read-only mode. In addition, you will be unable to perform any other operation in Nexsan Unity.

CAUTION: Both the primary and remote systems are unavailable during the failover process. To prevent data loss, close any applications that access data on the primary system and also terminate any active connections to the system.

12

Prerequisites

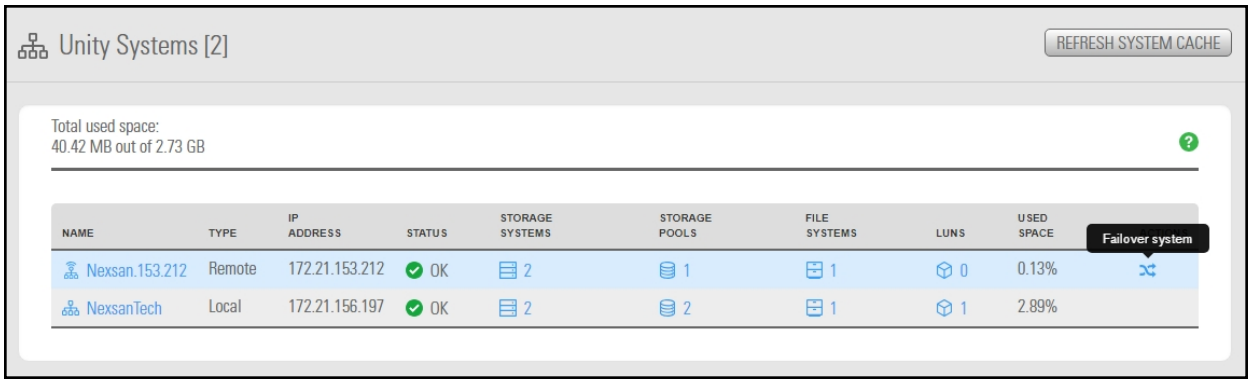
- The primary site must be connected to a remote site.
- At least one replication to a secondary system must have already been performed.

Note Datasets that do not have replication enabled remain on the primary system, and are only accessible from that system.

To failover the primary system to the remote system:

1. On the **Unity navigation bar**, select **System**.

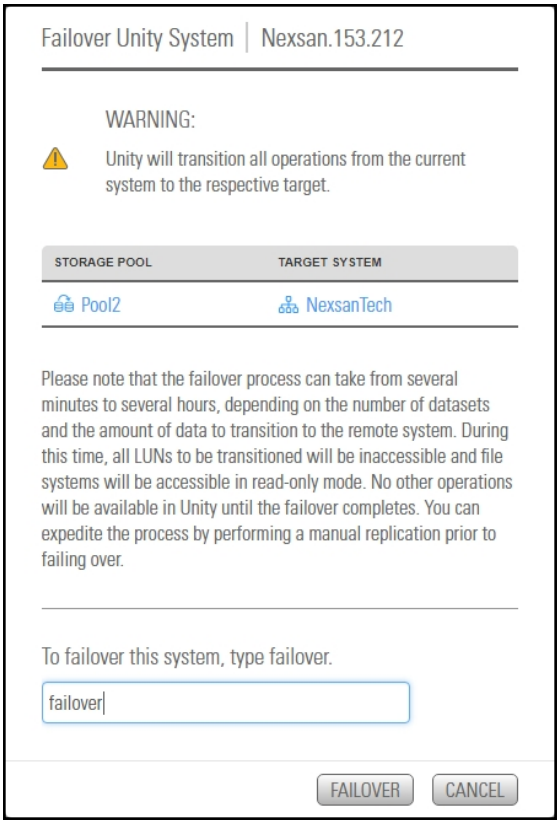
Figure 12-23: Unity Systems panel: Failover System



2. Click the **Failover System** icon in the table showing the primary and remote Unity Systems.

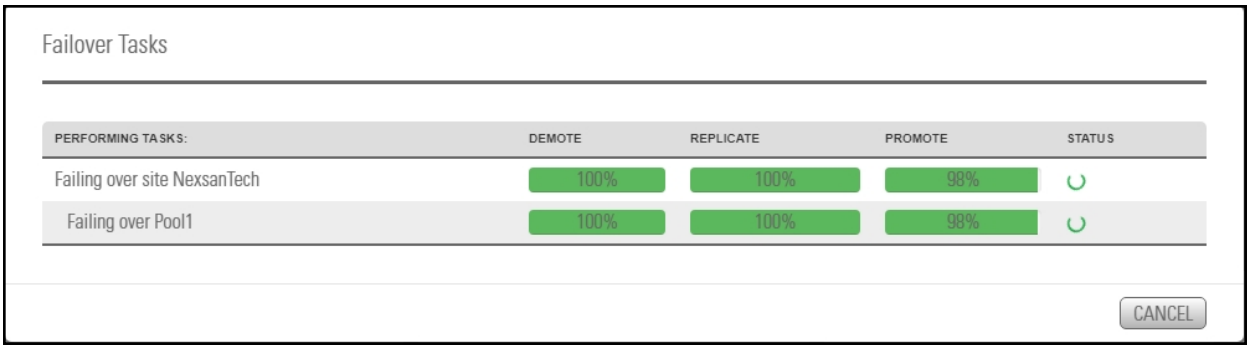
3. Unity displays the storage pool to be failed over and target system name, prompting you to confirm the action. Type **Failover** in the text box to continue.

Figure 12-24: Failover Unity System popup



Unity starts the failover process, starting with demoting the primary site, then replicating it and promoting it to the remote site.

Figure 12-25: Failover Tasks window



If the primary system has multiple storage pools replicated to different remote systems, the failover function fails over each pool to its corresponding remote system.

On the remote system, Unity moves all replicated storage pools from the **Incoming Replications** node to the **Storage Pools** node. On the primary system, Unity moves the replicated pools from 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 system.

If the failover of the primary system 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 system individually, or
- promote the remote system, or
- promote the storage pools on the remote system 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.

Configuring asynchronous replication settings

You can configure the general settings for Asynchronous Replication at the Unity System level before or after configuring replication. The new settings are applied at the next replication if replication is already configured.

The **Replications** panel, you can 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 530

Configuring encryption settings for asynchronous replication on page 530

Configuring network settings for asynchronous replication

You configure network settings for Asynchronous Replication at the Unity System level. All replication processes that will be created for each Unity System will inherit the same settings. You can specify the type of network connection between the primary and remote systems, 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 enables 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 system) and on the inbound data stream (at the remote or DR system).

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:

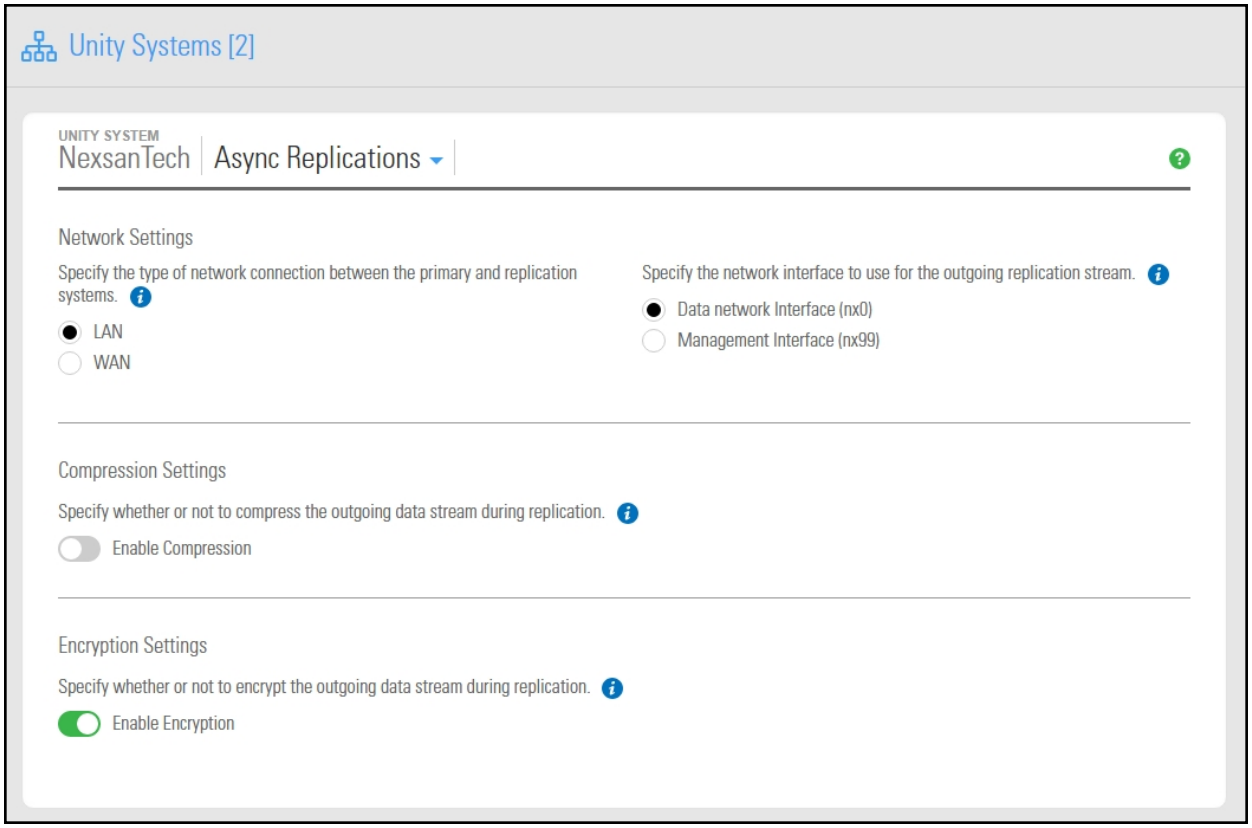
- The network interface that you set on the primary system (for the outgoing replication stream) must be the same as the one on the remote system (for the incoming replication stream).
- If you select nx99 for replication, nx0 still needs to be configured and reachable on your network. Using nx99 offers 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 on page 393.

To configure network settings:

1. On the **Unity navigation bar**, select **System > Unity Systems**.
2. Select the system that you want to configure asynchronous replication for.
3. Select **Summary > Async Replications**. The **Unity Systems Async Replication panel** opens.

Figure 12-26: Async Replication panel



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 systems	Select **LAN** or **WAN**.
network interface for the replication stream	Select the desired network interface.

5. Click the **Apply** button.

What's next:

If you changed the network interface, you must make the same change on the remote system.

Configuring compression settings for asynchronous replication

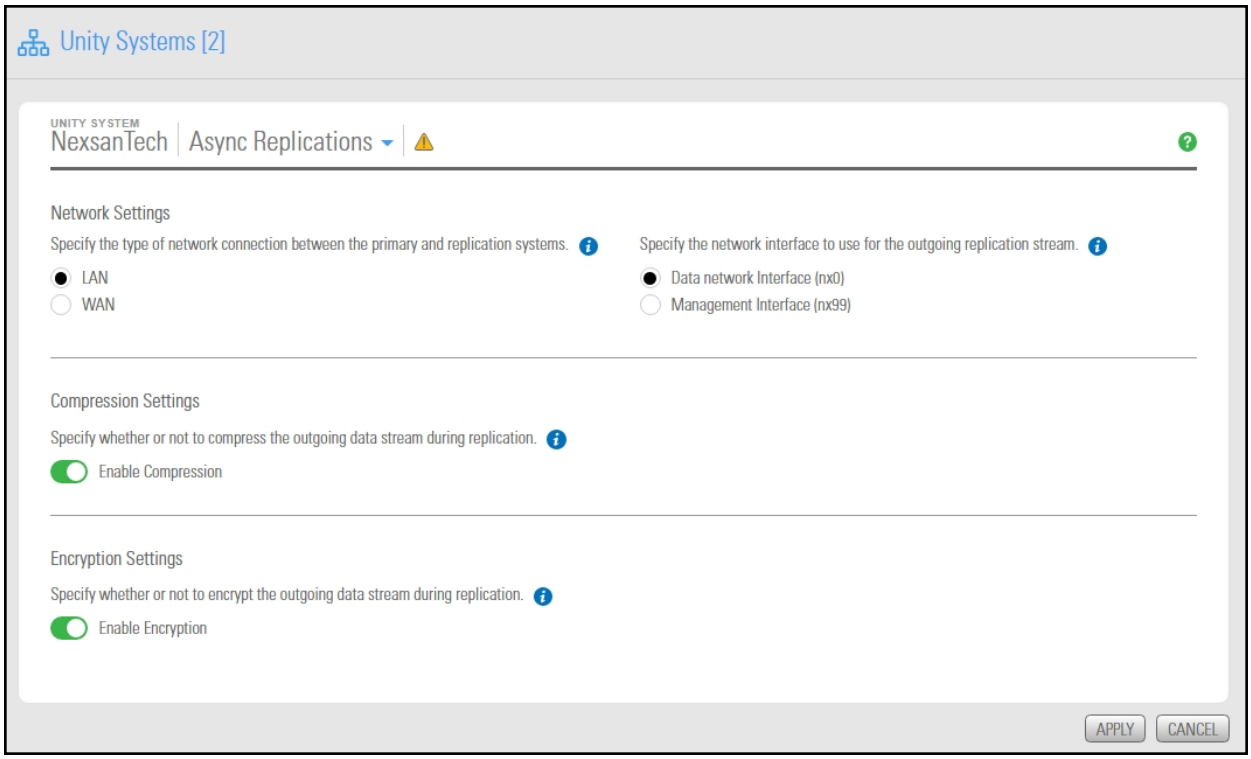
You configure compression settings for Asynchronous Replication at the system level. All replication processes that will be created for that system will inherit the same settings.

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. On the **Unity navigation bar**, select **System > Unity Systems**.
2. Select the system that you want to configure asynchronous replication for.
3. Select **Summary > Async Replications**. The **Unity Systems Async Replication panel** opens.

Figure 12-27: Async Replication panel



4. Under **Compression Settings**, click the **Enable Compression** button
5. Click the **Apply** button.

Configuring encryption settings for asynchronous replication

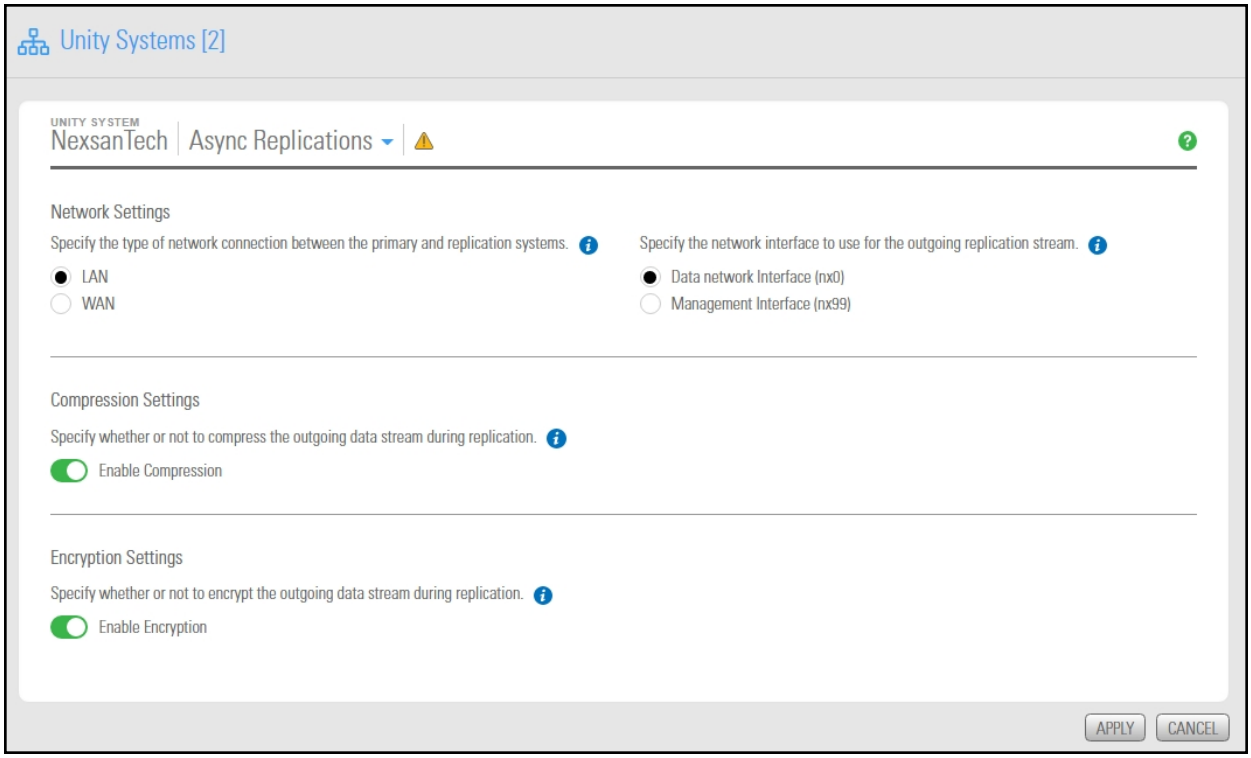
You configure encryption settings for Asynchronous Replication at the Unity System level. All replication processes that will be created for that Unity System will inherit the same settings. By default, data encryption is enabled. This allows the outgoing data stream to be encrypted during replication to provide an extra layer of data security. This process can be CPU intensive.

Note If one Unity System has encryption enabled, the data will be encrypted. If both Unity Systems have encryption disabled, the data will not be encrypted.

To configure encryption settings:

1. On the **Unity navigation bar**, select **System > Unity Systems**.
2. Select the system that you want to configure asynchronous replication for.
3. Select **Summary > Async Replications**. The **Unity Systems Async Replication panel** opens.

Figure 12-28: Async Replications panel



4. Under **Encryption Settings**, make sure the **Enable Encryption** button is enabled (the default).
5. Click the **Apply** button.

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 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 a manual replication on page 516.

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 file systems on the replica that were NOT previously replicated to the remote site will be deleted, resulting in data loss.

12

Prerequisites

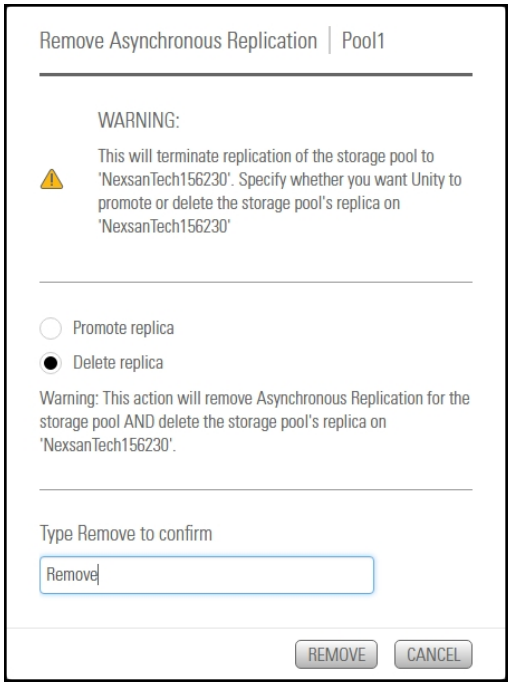
- To perform this operation, at least one replication must be in place.

To remove asynchronous data replication for a storage pool:

1. On the **Unity navigation bar**, select **Data Protection > Replications**.
2. In the **Replications** panel, click **Remove Replication**

   Unity displays a pop-up asking you whether you want to promote or delete the replica.

Figure 12-29: Removing asynchronous replication



3. Do one of the following:

- If you want to promote the replica, leave the default **Promote replica** option selected to promote the replica to be a primary pool, or
- Select **Delete replica** to remove the replicated pool from the remote Unity.

4. Type **Remove** where indicated to confirm the action, then click the **Remove** button.
5. 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**.

Enabling browsing of a replicated file system snapshot

Use this procedure for instructions about how to browse replicated file systems.

When you replicate a file system, Unity automatically enables sharing for the replicated dataset (file system or LUN) on the remote Unity System.

Unity makes the snapshot available to host systems of the LUN as a read/write clone. The host system can then both read from and write data to the clone, however Unity will NOT preserve direct changes to the clone.

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 settings to allow host connectivity to the replicated LUN.
- You cannot browse a replicated file system using FTP sharing.

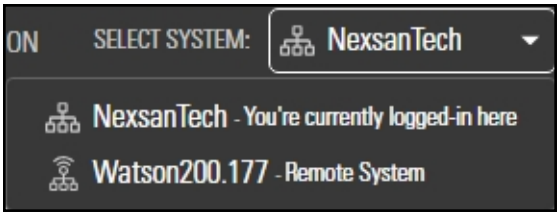
Prerequisites

- A primary Unity System and remote Unity System with replication set up.
- At least one file system snapshot must be available.

To enable browsing of a replicated file system snapshot:

1. On the **Unity navigation bar**, click the **Select System** box.

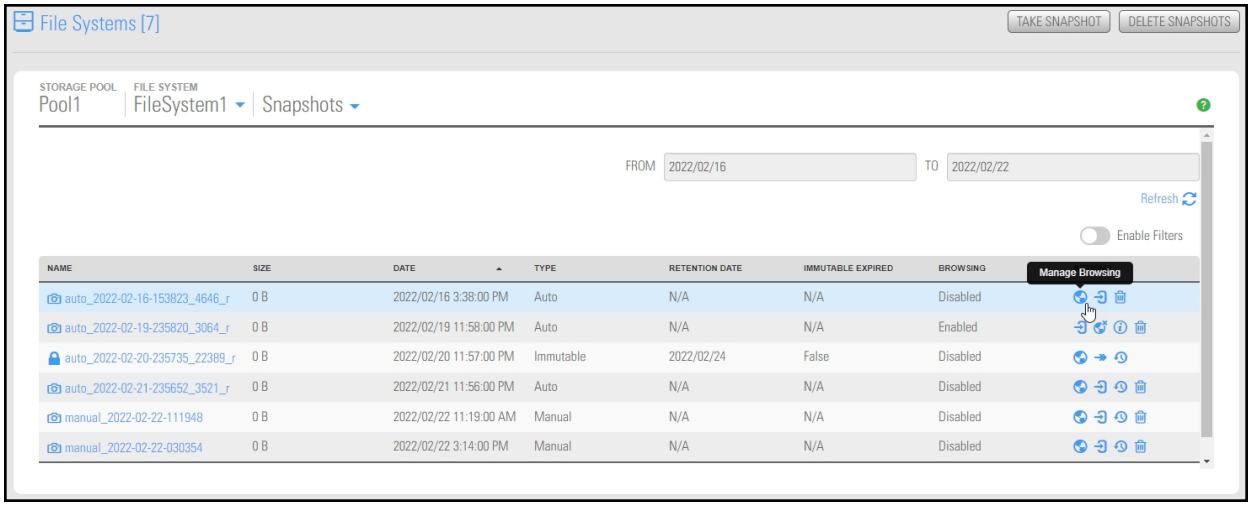
Figure 12-30: Select System



2. Select the system that has replications that you need to browse.

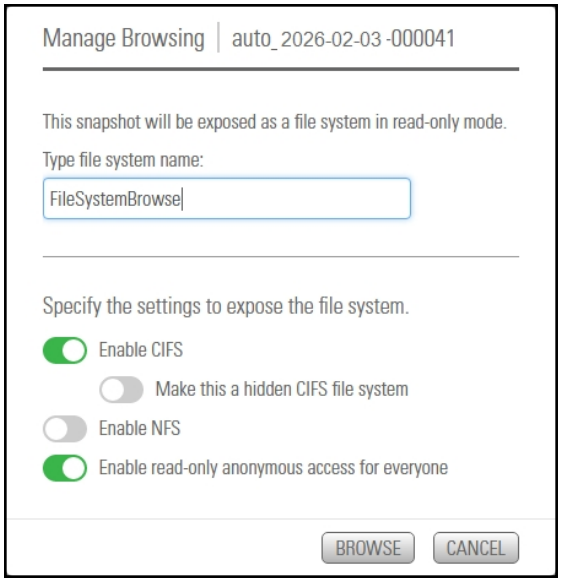
3. On the **Unity navigation bar**, select **Data Protection > Snapshots**.

Figure 12-31: Snapshots panel: Manage Browsing



4. Click the **Manage Browsing** icon next to the snapshot of the file system that you want to browse. The **Manage Browsing** popup opens.

Figure 12-32: Manage Browsing popup

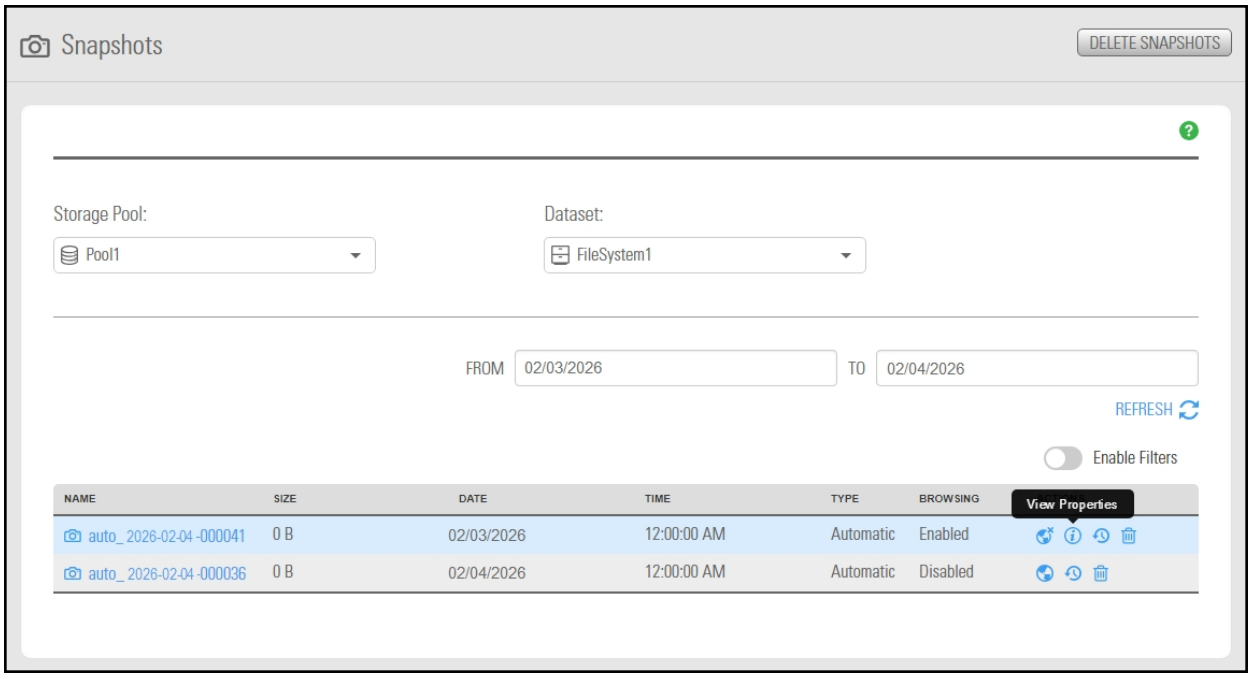


5. Apply the following settings as needed for File System Snapshot browsing.
   - Enable CIFS.
     - Make this a hidden CIFS file system
   - Enable NFS
   - Enable read-only anonymous access for everyone.
6. Click the **Browse** button to enable browsing.

To browse the contents of a replicated dataset:

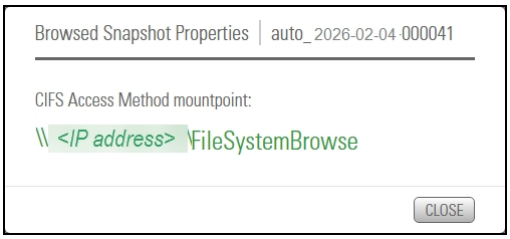
- In the **Snapshots panel**, click the **View Properties** icon .

Figure 12-33: Snapshots panel: View Properties



The **Browsed Snapshot Properties popup** opens.

Figure 12-34: Browsed Snapshot Properties popup



You browse a replicated dataset in the same way that you browse the source dataset on the primary Unity System, 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 .

Configuring the network type for data replication

The Unity Storage System may terminate a replication session if the network response time falls below the acceptable threshold. This threshold may not be high enough for slow WAN links. The Unity Storage System provides a configuration setting that enables you to specify the network connection, or link type between a source system and the Disaster Recovery (DR) system: either a LAN or WAN connection.

Using the CLI, 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 system), and on the inbound data stream (at the remote or DR system).

Note The network type can also be set from Unity, as described in Configuring network settings for asynchronous replication on page 528 .

To set the network type to WAN:

1. Access the nxadmin CLI:
   a. Connect to a controller node on the Unity Storage System via SSH (Putty), using the Management Virtual IP address.
   b. Log on using the nxadmin user and password.
2. When the nxadmin CLI prompt displays, type **menu**.
3. In the NestOS Admin Menu, type **1** (**Network Menu**) and then press Enter. This displays the **NestOS Network Menu**.
4. Type **3** (**Replication Settings**) and press Enter. This displays the **NestOS Replication Bandwidth Menu**.
5. Type **7** (**Show Replication Network Type Setting**), and press Enter.

   ```
   The Current Network Type for replication is set to: lan
   ```
6. Type **8** (**Change Replication Network Type Setting**), and press Enter.
7. At the prompt, type **2** to select the `wan` network type and press Enter.
8. Press any key at the confirmation message.
9. Verify that the new setting was applied. Type **7** (**Show Replication Network Type Setting**), and press Enter.

   The command should return:

   ```
   The Current Network Type for replication is set to: wan
   ```
10. Repeat these steps the DR system, as well as on all source sites connected to the DR system over a WAN connection.

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:

- from the `nxcmd` command-line interface.
- for systems configured with the appropriate hardware.

To configure Synchronous data replication:

- Using the nxcmd command-line interface, for command information enter

```
nxcmd syncreplication
```

For detailed instructions, see

- "Synchronous Replication" in the *Unity Software User Guide*.
- "SyncReplication" in the *nxcmd Command-Line Interface Reference Guide*.

This section includes these topics:

Synchronous data replication features below

Usage implementations on the facing page

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 enables 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.

Cloud Connector

The Unity Cloud Connector module links local servers, file systems, and on-premises network-attached storage (NAS) directly to remote cloud storage providers, including Amazon S3 compliant, Microsoft Azure Files, and Microsoft Azure Blob Storage. With native protocol integration such as NFS and SMB on the local side and REST based APIs on the cloud side, the need for custom scripting or manual file uploads is eliminated. Data can be moved automatically with support for scheduled background synchronization and rule-based archiving, and is encrypted in transit and at rest for security. The use cases include expanding on-premises server capacity to hybrid public and private cloud object storage, disaster recovery and backup, as well as multi-site collaboration.

This section covers these topics:

Adding cloud storage configurations below

Editing cloud storage configuration on page 542

Deleting cloud storage configuration on page 543

Transferring data manually to cloud storage on page 544

Scheduling automatic data transfer to cloud storage on page 546

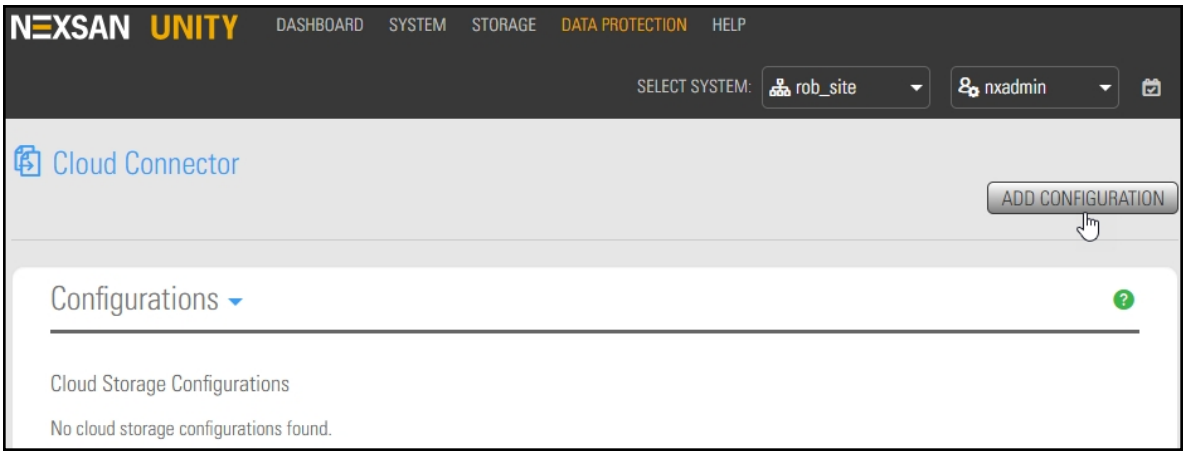
Adding cloud storage configurations

Use the Unity Cloud Connector to add a cloud storage configuration specific to a storage type and a storage provider.

To add a storage configuration:

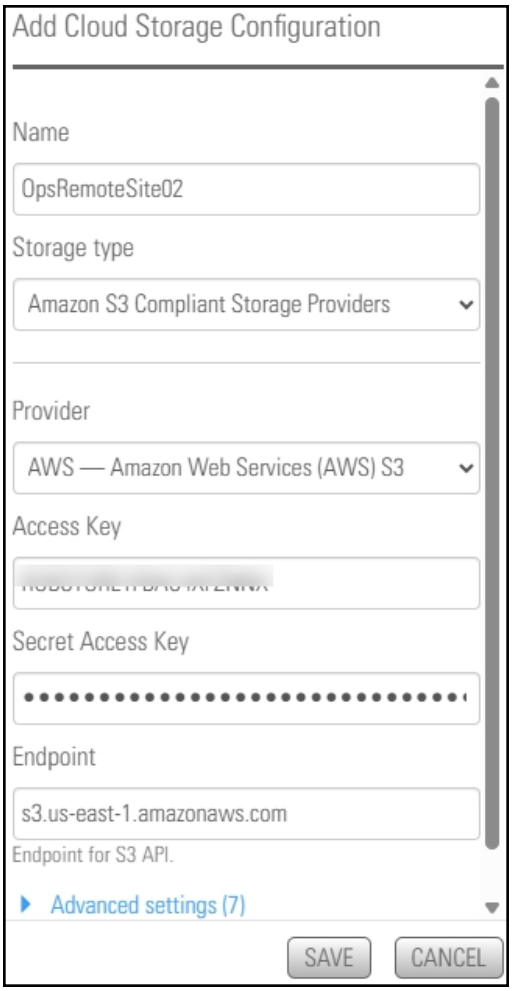
1. On the **Unity navigation bar**, select **Data Protection** > **Cloud Connector**.
2. The **Cloud Connector** page appears. Click the **Add Configuration** button.

Figure 12-35: Cloud Connector page - Add Configuration



3. The **Add Cloud Storage Configuration** pop-up appears. Add a **Name** in the corresponding field. The name must start with an (upper-case or lower-case) alphabetic or numeric character; and, with the exception of hyphen (-) and period (.), the name can only contain alphanumeric characters, without spaces. These characters are NOT allowed: ” / \ _ [ ] : ; | = , + * ? < >

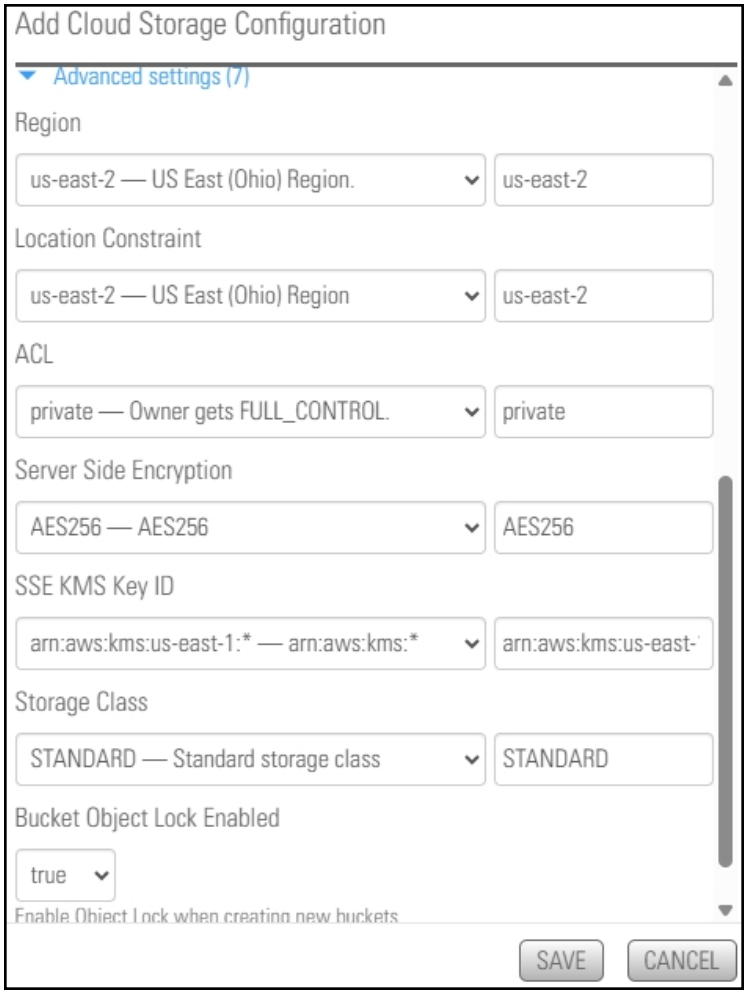
Figure 12-36: Add Cloud Storage Configuration pop-up



4. Complete the remaining required fields:
   - **Storage Type**, select among: Amazon S3 Compliant Storage Providers (default), Microsoft Azure files, Microsoft Azure Blob Storage.
   - **Provider**, select among: AWS - Amazon Web Services (AWS) S3 (default), Ceph - Ceph Object Storage, GCS - Google Cloud Storage, SeaweedFS - SeaweedFS S3, Unity - Unity Object Store, Wasabi - Wasabi Object Storage.
   - **Access Key**
   - **Secret Access Key**
   - **Endpoint** (optional): enter an Endpoint for S3 API.

5. Use **Advanced settings** (optional). Click the drop-down arrow to expose available fields: Region, Location Constraint, ACL, Server Side Encryption, SSE KMS Key ID, Storage Class, Bucket Object Lock Enabled. Use the drop-down arrow for each field to select an option, or type a value in the adjoining field.

Figure 12-37: Add Cloud Storage Configuration pop-up - Advanced settings



6. When done, click the **Save** button.

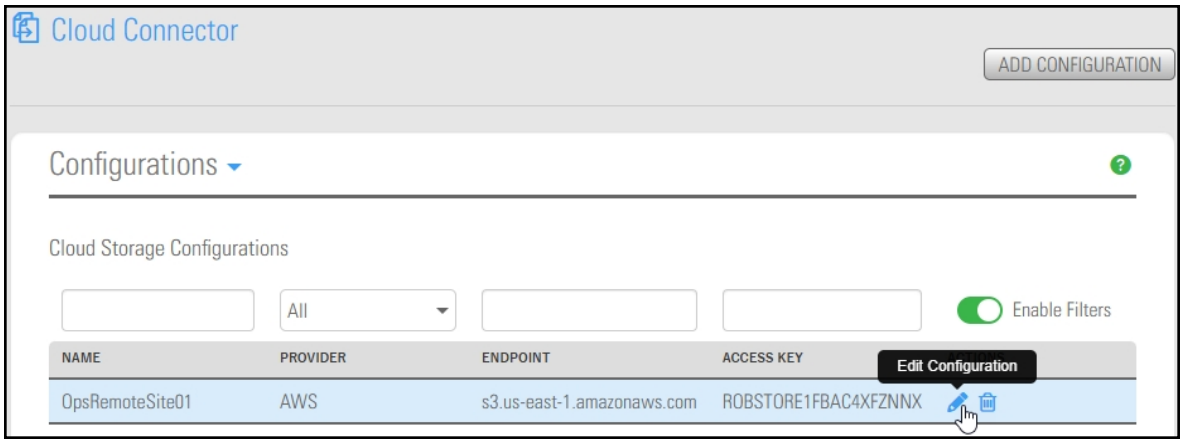
Editing cloud storage configuration

Edit an existing cloud storage configuration with Unity Cloud Connector.

To edit a storage configuration:

1. On the **Unity navigation bar**, select **Data Protection** > **Cloud Connector**.
2. The **Cloud Connector** default page appears with a list of Configurations. If there are several configurations, use the **Enable Filters** button to sort the table results. Click the **Edit Configuration icon** in the **Actions** column for the target configuration.

Figure 12-38: Cloud Connector page - Edit Configuration



3. The **Edit Cloud Storage Configuration** pop-up appears. The **Name** and **Storage type** fields cannot be modified. Proceed to edit available fields including **Provider**, **Access Key**, **Secret Access Key** (leave blank to keep the current value), and **Endpoint** (optional).
4. Click the drop-down arrow to expose **Advanced settings** (optional). Complete any or all of the available fields using the drop-down arrow to make a selection, or type a value in the adjoining field.
5. When done, click the **Save** button.

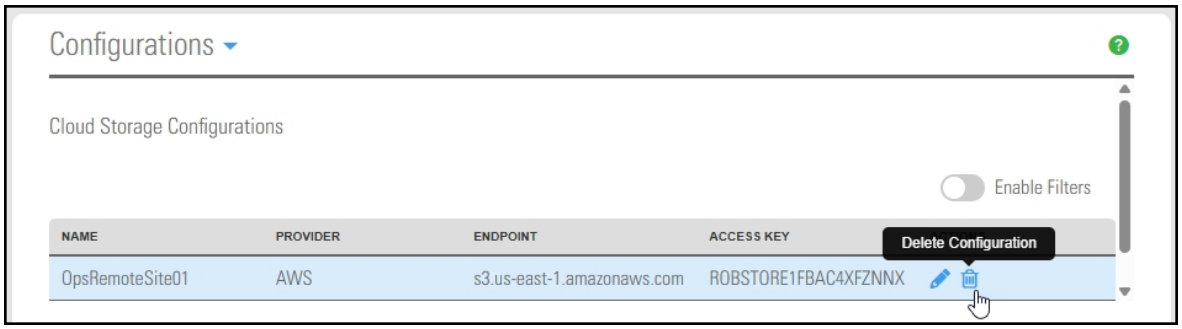
Deleting cloud storage configuration

Delete an existing cloud storage configuration using the Unity Cloud Connector.

To delete a storage configuration:

1. On the **Unity navigation bar**, select **Data Protection** > **Cloud Connector**.
2. The **Cloud Connector** default page appears with a list of Configurations. If there are several configurations, use the **Enable Filters** button to sort the table results. Click the **Delete Configuration icon** in the **Actions** column for the target configuration.

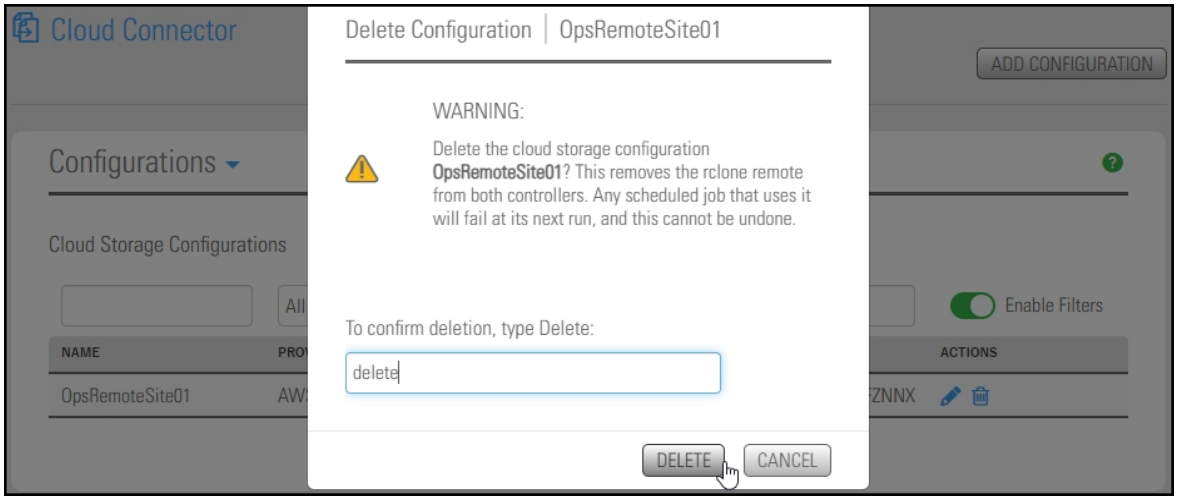
Figure 12-39: Cloud Connector page - Delete Configuration



3. A **Delete Configuration** pop-up appears indicating the name of the selected configuration. To confirm deletion, type 'delete' in the field, then click the **Delete** button.

   Note This operation cannot be undone.

Figure 12-40: Delete Configuration pop-up confirmation



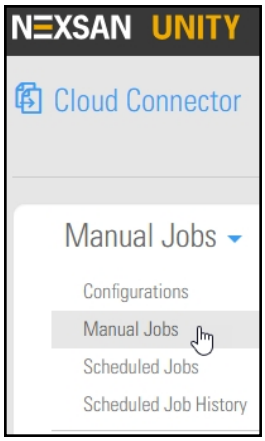
Transferring data manually to cloud storage

Create or run a data transfer to cloud storage manually with Unity Cloud Connector.

To create a new transfer:

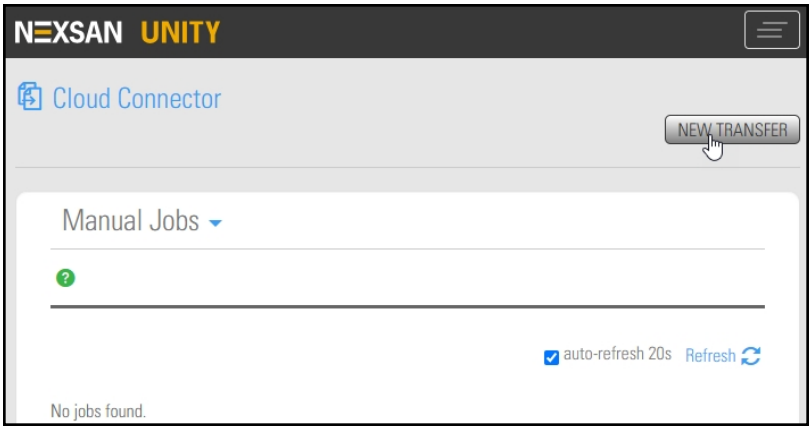
1. On the **Unity navigation bar**, select **Data Protection** > **Cloud Connector**.
2. The **Cloud Connector** default page appears with a list of Configurations. Use the **drop-down arrow** beside **Configurations** and select the next item in the list, **Manual Jobs**.

Figure 12-41: Cloud Connecter menu, Manual Jobs



3. The **Manual Jobs** page appears. Click the **New Transfer** button.

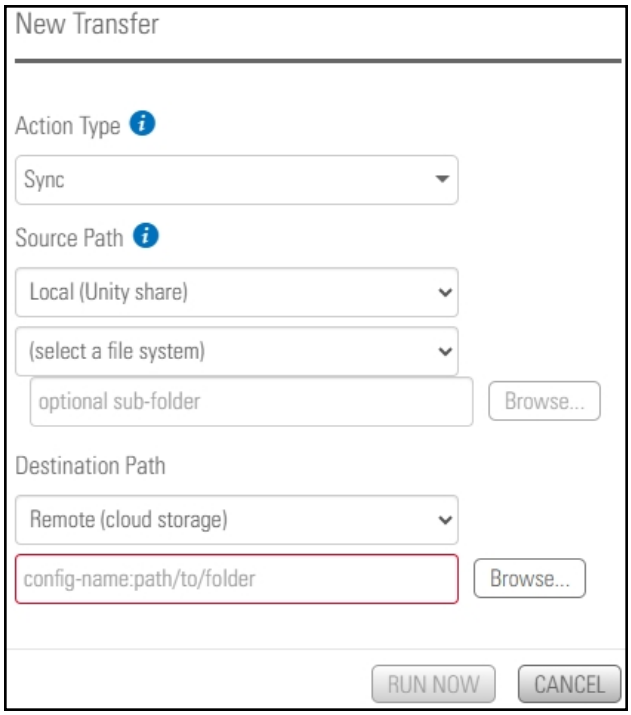
Figure 12-42: Manual Jobs page, New Transfer



4. The **New Transfer** pop-up appears. Complete the fields:
   - **Action Type**: **Sync** (default, makes the destination identical to the source, deleting anything the source does not have), **Copy** (copies new and changed files to the destination, nothing is deleted), or **Move** (copies the files, then removes them from the source).
   - **Source Path**: **Local** (Unity Share), or **Remote** (cloud storage). Select a file system from the list. Use the Browse button to add an optional sub-folder.
   - **Destination Path**: **Remote** (cloud storage), or **Local** (Unity Share). Use the Browse button to add the path.

     Note Source Path and Destination Path cannot both be Unity local shares, cloud connector transfers data to and from cloud storage.

Figure 12-43: New Transfer pop-up



5. When done, click the **Run Now** button.

Scheduling automatic data transfer to cloud storage

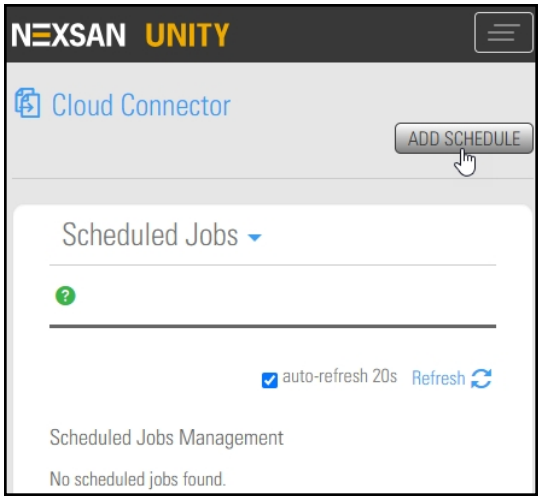
Add or run a schedule for automatic data transfers to cloud storage with Unity Cloud Connector.

To add a schedule:

1. On the **Unity navigation bar**, select **Data Protection** > **Cloud Connector**.
2. The **Cloud Connector** default page appears with a list of Configurations. Use the **drop-down arrow** beside **Configurations** and select the menu item **Scheduled Jobs**.

3. The **Scheduled Jobs** page appears. Click the **Add Schedule** button.

Figure 12-44: Scheduled Jobs page, Add Schedule

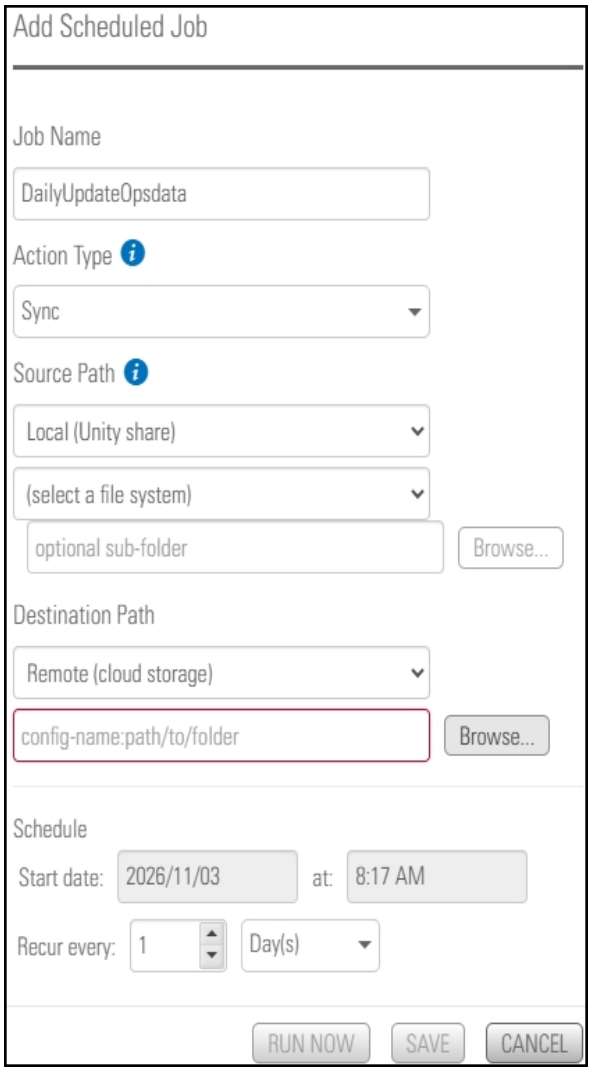


4. The **Add Scheduled Job** pop-up appears. Add a **Job Name** in the corresponding field.
   The name must start with an (upper-case or lower-case) alphabetic or numeric character; and, with the exception of hyphen (-) and period (.), the name can only contain alphanumeric characters, without spaces. These characters are NOT allowed: ” / \ _ [ ] : ; | = , + * ? < >

5. Complete the remaining fields:
   - **Action Type**: **Sync** (default, makes the destination identical to the source, deleting anything the source does not have), **Copy** (copies new and changed files to the destination, nothing is deleted), or **Move** (copies the files, then removes them from the source).
   - **Source Path**: **Local** (Unity Share), or **Remote** (cloud storage). Select a file system from the list. Use the Browse button to add an optional sub-folder.
   - **Destination Path**: **Remote** (cloud storage), or **Local** (Unity Share). Use the Browse button to add the path.

     Note Source Path and Destination Path cannot both be Unity local shares, cloud connector transfers data to and from cloud storage.
   - **Schedule**: use the fields to add a **Start date**, **at** time, and **Recur every** (numeral), of measure (**Minute(s)**, **Hour(s)**, **Day(s)**, **Week(s)**, **Month(s)**).

Figure 12-45: Add Scheduled Job pop-up



6. When done, click the **Run Now** button.

Chapter 13

System monitoring

You can use the following methods 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 live performance information in graphical format in the 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 Unity System, in addition to space usage, system health, and reports for file systems, LUNs, pools, and storage devices on Unity.

The Nexsan Unity Reports feature enables you to generate dashboard-type, graphical reports detailing storage capacity across Unity storage infrastructure.

This chapter includes these sections:

Viewing and recording performance metrics 550
Viewing historical performance data 554
Changing the duration to keep sampling data 556

Viewing and recording performance metrics

Unity displays live and historical performance information in graphical format in the Performance Monitor. The Performance Monitor provides a visual display of built-in performance counters, featuring graphical and tabular views of the data.

Metric selection

You can view performance measurements for the following Unity components:

Site

- CPU usage: Performance counter values for CPU usage for each controller over the specified time interval. The table includes current, minimum, maximum, and average CPU usage values in percent.
- Memory usage: Performance counter values for memory usage for each controller over the specified time interval. The table includes current, minimum, maximum, and average memory usage values in percent.
- Network usage: Performance counter values for the site network I/O in KB/s over the specified time interval. This includes read and write I/O statistics for each controller. The table includes current, minimum, maximum, and average network usage values in KB/s.

Pool

- Latency: Performance counter values for the average delay of response time for disks in the storage pool. Latency is displayed in microseconds (µs) over the specified time interval. The table includes current, minimum, maximum, and average network usage values.

Storage device

- I/O statistics: Performance counter values for device I/O at the specified time interval in KB/s. This includes read and write I/O statistics for all disks and storage systems connected to Unity.

  You can filter the display to show only I/O statistics for the disks/devices currently allocated to a specific storage pool on the system, including the devices reserved for the Unity Storage System's operating system pool, and the system pool (on Clustered systems).

  Each slot of a Unity storage device and each storage device volume is represented in a different color. The table includes current, minimum, maximum, and average storage device usage values in KB/s.

File system

- I/O and IOPS statistics: Performance counter values for file system I/O at the specified time interval. This includes read and write I/O statistics. You can filter the display to show only statistics for a specific file system. The table for file system I/O values includes current, minimum, maximum, and average in KB/s.

  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.

  The table includes current, minimum, maximum, and average network usage values.

  Note Monitoring of NFS performance metrics is disabled by default. You can enable NFS measurement 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

- LUN I/O and IOPS statistics: Performance counter values for LUN I/O over the specified time interval. This includes read and write I/O statistics. You can filter the display to show only I/O statistics for a specific LUN. LUN I/O values include current, minimum, maximum, and average for read and write operations, measured in KB/s.

  The counter values for LUN input/output operations per second (IOPS) are displayed over the specified time interval. This includes read and write operations. The table for LUN I/O and IOPS values includes current, minimum, maximum, and average.

  LUN IOPS values include current, minimum, maximum, and average for read and write operations, measured in IOPS.

FASTier

- I/O, IOPS, and access statistics: Performance counter values for FASTier cache devices installed on Unity. FASTier I/O and Access values include current, minimum, maximum, and average, measured in KB/s.

  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 pools or devices (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 pools or devices (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.

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:

- From the Unity navigation bar, select **System > Performance Monitor**.

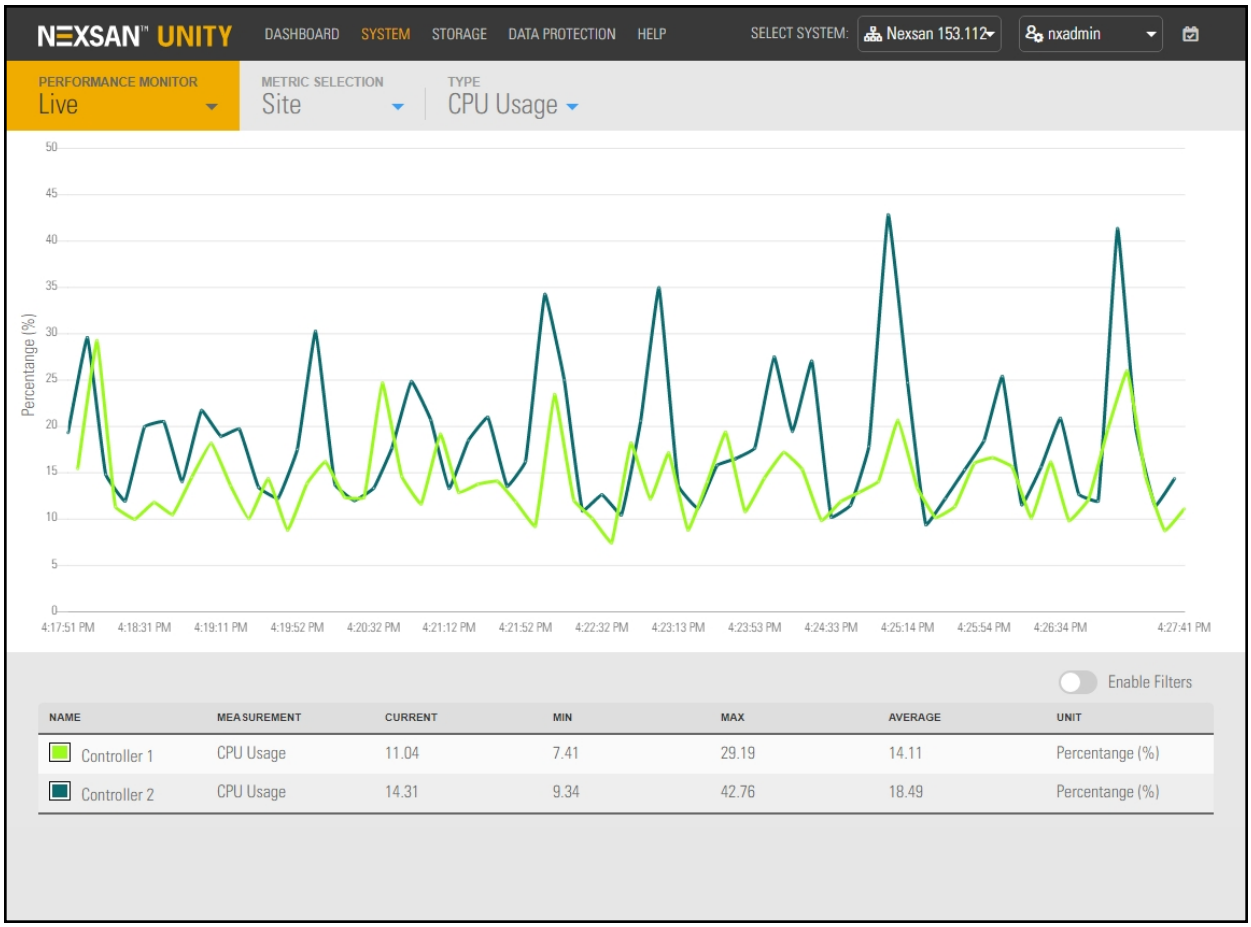
The Performance Monitor opens, displaying live statistics for the Site and CPU usage for controllers 1 and 2.

The Performance Monitor includes a graphical chart and a table for each of the following Unity components:

Table 13-1: Performance metrics and types

Metric	Type
LUN	I/O IOPS
File System	I/O IOPS
Pool	Latency
Unity System	CPU Usage Memory Usage Network
Devices	I/O
FASTier	I/O (read and write cache) IOPS (read and write cache) Access (read cache)

Figure 13-1: Performance Monitor—Live view



When the Performance Monitor opens, only the graphical chart and table for CPU performance is shown. You can open the graphical chart and table for another performance metric by selecting it from the title bar.

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 timeline at the bottom of each graphical chart indicates the current sampling interval. You can modify the sampling period in the Performance Monitor **Options**; see Changing the duration to keep sampling data on page 556.

Filtering live performance metrics

The Performance Monitor enables 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).

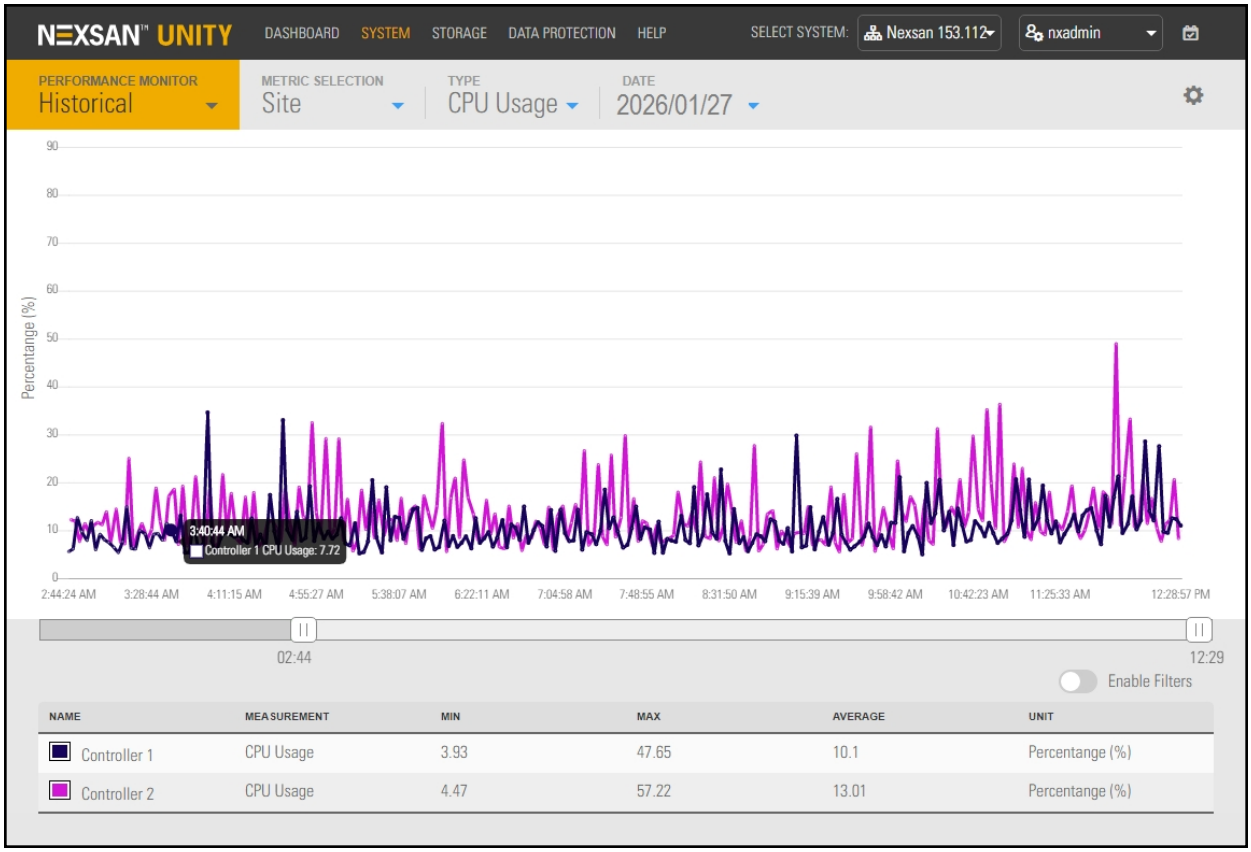
This procedure provides an example of how to filter CPU usage performance metrics for controller 1 on a Unity System, or site.

To filter performance information:

1. Start the Performance Monitor; see Starting the performance monitor on page 551.
2. Select the down arrow on the **Performance Monitor** tab (**Live** opens by default).
3. Select **Historical**, and then choose your **Metric selection**, **Type**, and **Date**.
4. Select **Enable Filters** at the bottom right of the graphical chart.

5. In the table at the bottom of the panel, select the component that you want to filter performance information for. For example, select controller 1 in the table.

Figure 13-2: Filtering performance metrics



6. Use the sliders under the graph to narrow the time span for the data during the current day.

   Tip You can hover the mouse pointer over the graph to display a popup with data for a specific time of day.

   The graphical chart automatically adjusts to display performance statistics for the selected component.

Viewing historical performance data

The Performance Monitor enables 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 page 556.

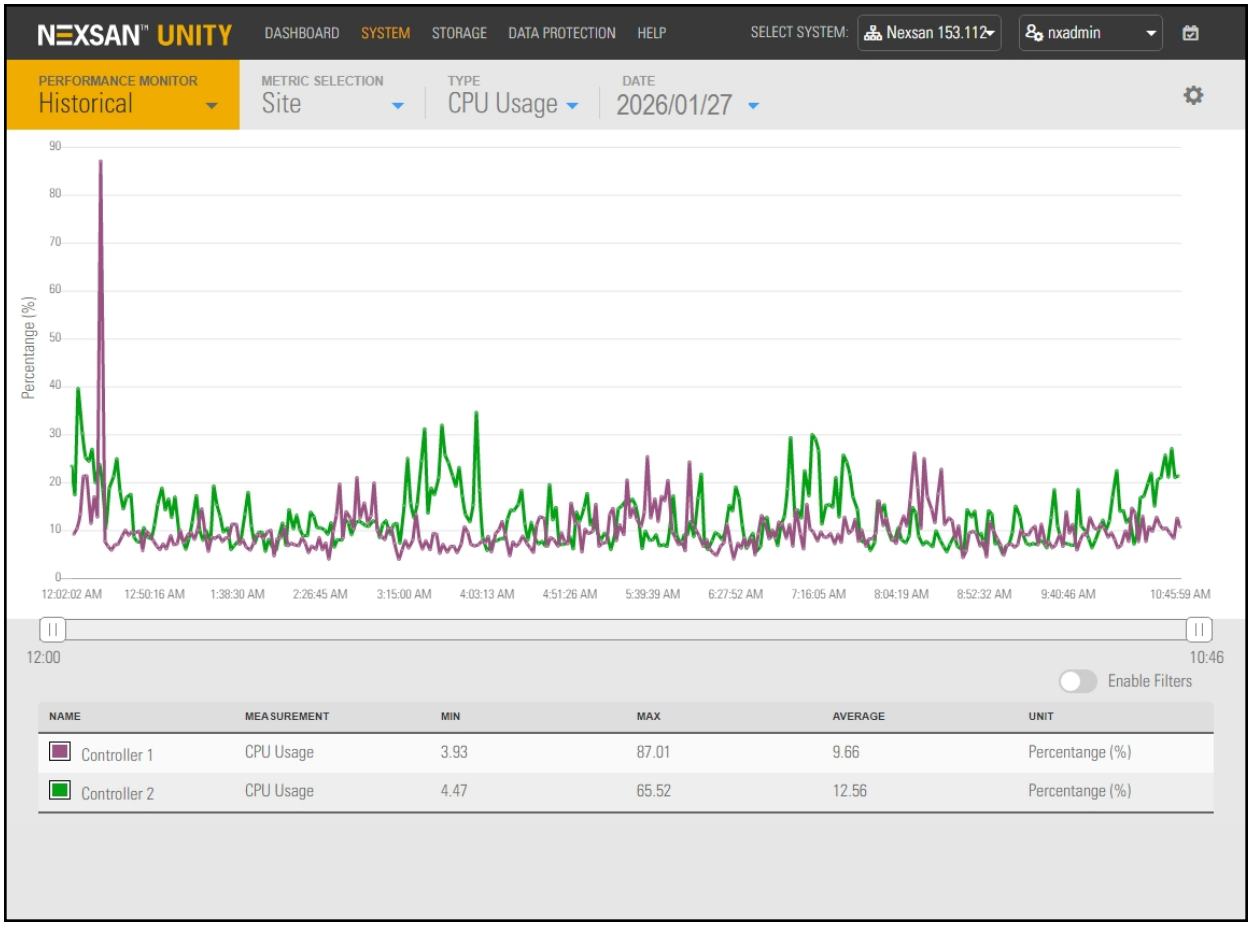
Similarly to the Live and Recordings views, you can filter performance metrics and sort all columns.

To view historical performance data:

1. Start the Performance Monitor; see Starting the performance monitor on page 551.
2. Select the down arrow on the **Performance Monitor** tab (the **Live** view of the data opens by default).

3. Select **Historical**, and then choose your **Metric selection**, **Type**, and **Date**.

Figure 13-3: Performance Monitor—Historical view



Tip To highlight a component in the graph, select it in the table.

Changing the duration to keep sampling data

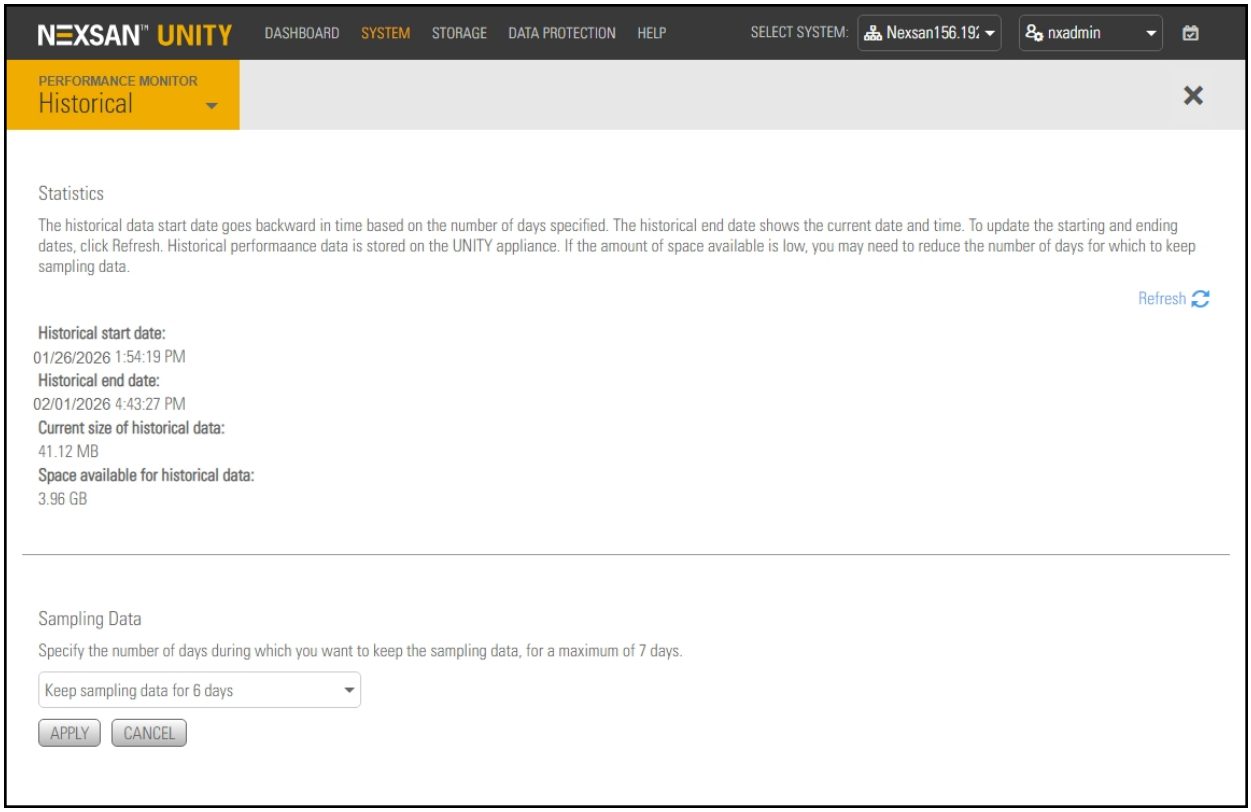
The Performance Monitor Historical Sampling Data Options panel enables you to change the number of days for which Unity keeps performance sampling data. This data is saved on Unity, not in storage pools.

By default, the Performance Monitor keeps sampling data for 7 days, from the current time and dating back the number of days specified in the **Sampling Data** setting.

To change the number of days:

1. Start the Performance Monitor; see Starting the performance monitor on page 551.
2. Select the down arrow on the **Performance Monitor** tab (**Live** opens by default).
3. Select **Historical**, and then click the Options icon
4. In the **Sampling Data** box, select an option to increase the number of days for Unity to keep sampling data. The maximum is 7 days.

Figure 13-4: Performance Monitor—Options view



5. Click the **Apply** button.

Note Once deleted, sampling data cannot be recovered.

Chapter 14

Event logging and notification

All event messages generated by Unity (including any events issued by an external Nexsan storage 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 558
Configuring event viewer logging options 559
Collecting and emailing event logs 560
Clearing event logs 562
Setting up email notification for events 563

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.

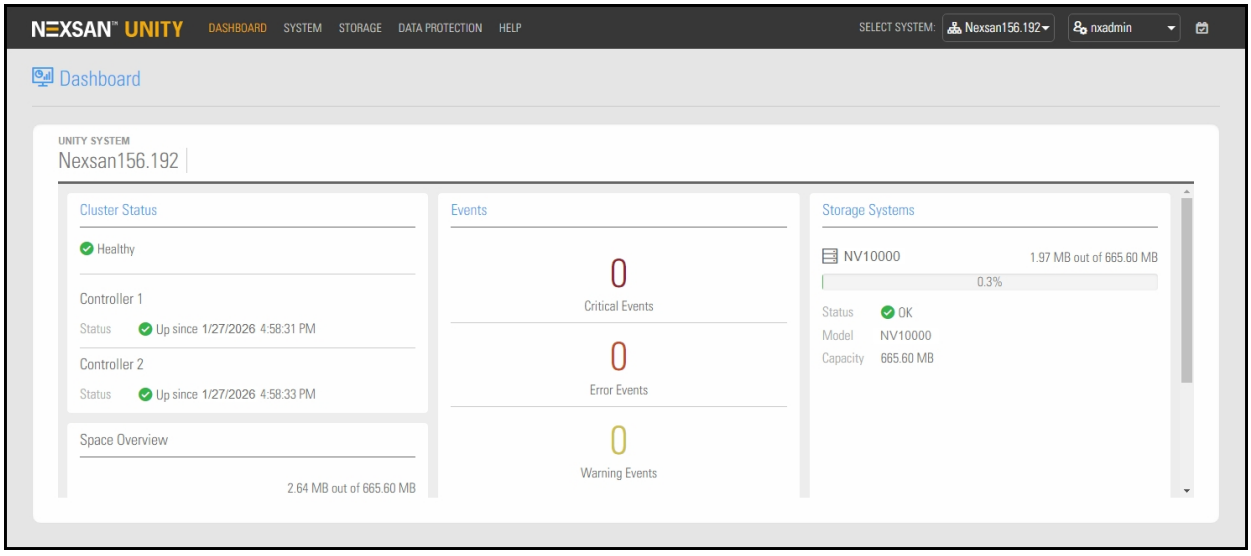
By default, Unity keeps events in the event logs for up to one year, after which the system automatically clears the event logs; you can change this default setting if needed. For more information, see Configuring event viewer logging options on the facing page.

You view and filter events contained in the event logs in the Unity Event Viewer. The Event Viewer also enables 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 view an event summary:

- On the **Unity navigation bar**, click **Dashboard**. The Dashboard panel **Health** section lists any critical, error any warning events.

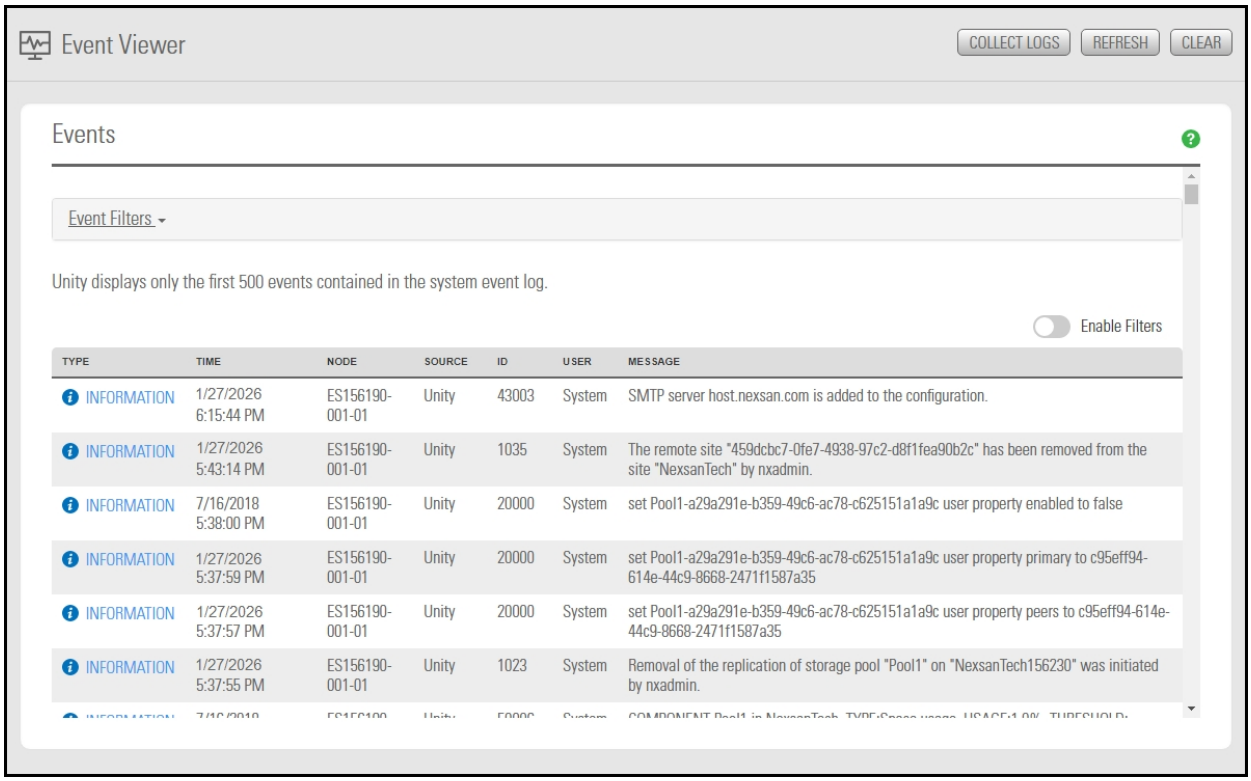
Figure 14-1: Unity Dashboard panel



To access the Unity Event Viewer:

- On the **Unity navigation bar**, select **System > Event Viewer**.

Figure 14-2: Unity Event viewer



Configuring event viewer logging options

Unity provides **Event Filters** to configure logging options to let you customize logging options.

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:

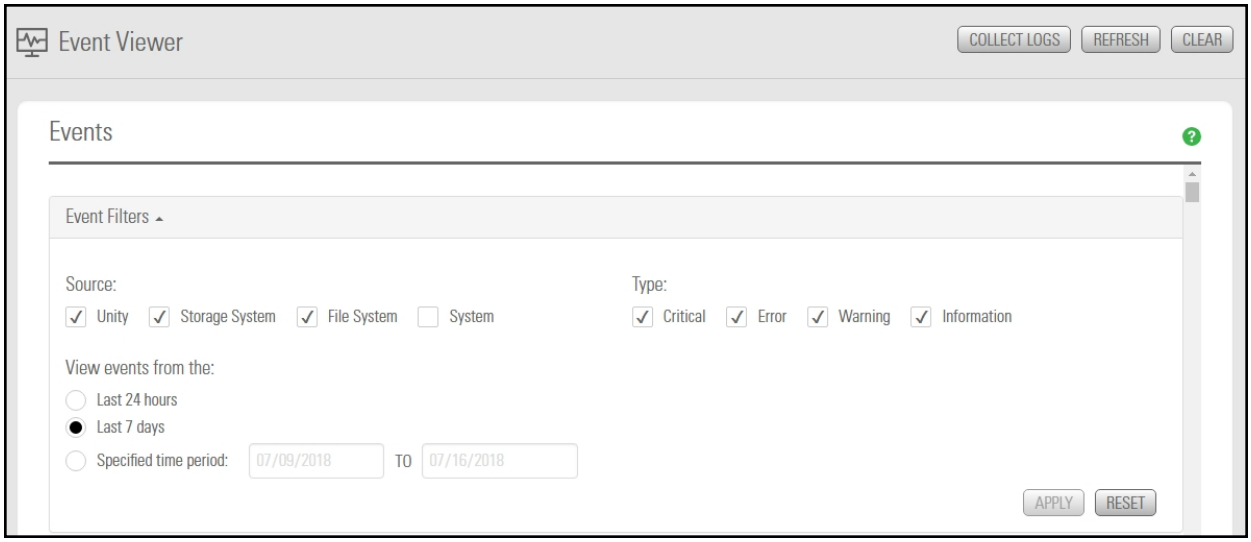
- the duration that you set for keeping logs on the system has elapsed; or,
- the disk space reserved for the log files is at over 80% used capacity.

To configure Event Filters:

1. On the **Unity navigation bar**, select **System > Event Viewer**.
2. Select **Event Filters**.

3. Select the **Source** for events (any or all): **Unity, Storage System, File System, or System**.

Figure 14-3: Event Filters



4. Select the **Type** of events to be collected: **Critical, Error, Warning, or Information**.
5. Specify a time period for event collection:
   a. **Last 24 hours**
   b. **Last 7 days**
   c. **Specified time period**

14

Collecting and emailing event logs

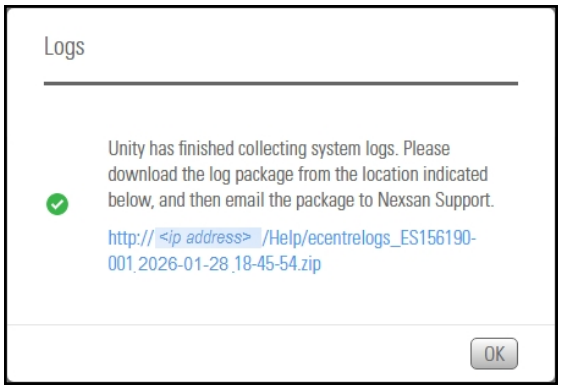
This function collects all system log files on Unity and creates an encrypted package that you download from Unity. This function is similar to the `createlogpackage` command in the nxadmin command-line interface (CLI). After downloading the encrypted package, you can send it to Nexsan Technical Support for analysis.

To collect logs:

1. On the **Unity navigation bar**, select **System > Event Viewer**.
2. Click Event Filters and specify the types of logs you want to collect. See Configuring event viewer logging options on the previous page
3. Click the **Collect Logs** button. Unity begins the log collection process and generates a log package.

4. Once this log package is created, the **Logs** popup window 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 14-4: Event Viewer, Logs popup



5. Click the URL in the dialog box to download the log package locally.
6. Send the log package to Nexsan.com/support.

Clearing event logs

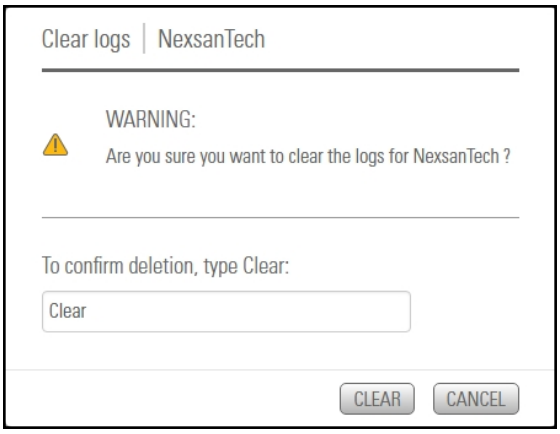
If needed, you can clear the event logs on Unity. This permanently deletes all log entries in the event logs.

Note Before clearing the logs, we recommend that you save the logs to disk using the **Collect Logs** function. See Collecting and emailing event logs on page 560

To clear the event logs:

1. On the **Unity navigation bar**, select **System > Event Viewer**.
2. Click the **Clear** button. Unity prompts you to confirm the clear operation.

Figure 14-5: Event Viewer, Clear logs popup



3. Type **Clear** in the text box to clear the event logs.
4. Click the **Clear** button to complete the operation.

Setting up email notification for events

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 enables 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) of events generated by Unity.

You set up event notification in the **Email and SNMP Notifications Settings** panel.

Note Before you set up email notification for system events and space usage threshold violations on storage pools and file systems, you must configure SMTP server settings for the Unity Storage System.

► **To access the Email and SNMP Notification Settings:**

- On the **Unity navigation bar**, select **System > Notifications**.

This section includes these topics:

Setting up email notification for system events 563
Setting up system notifications 565
Configuring SMTP server settings for the Unity System 566
Setting up SNMP notification 567

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 enables you to send separate email notifications for each event type or severity level — Critical, Error, Warning, and Information; and Unity also enables you to configure the notification frequency for each event type. For more information about event types, see Viewing events on page 558.

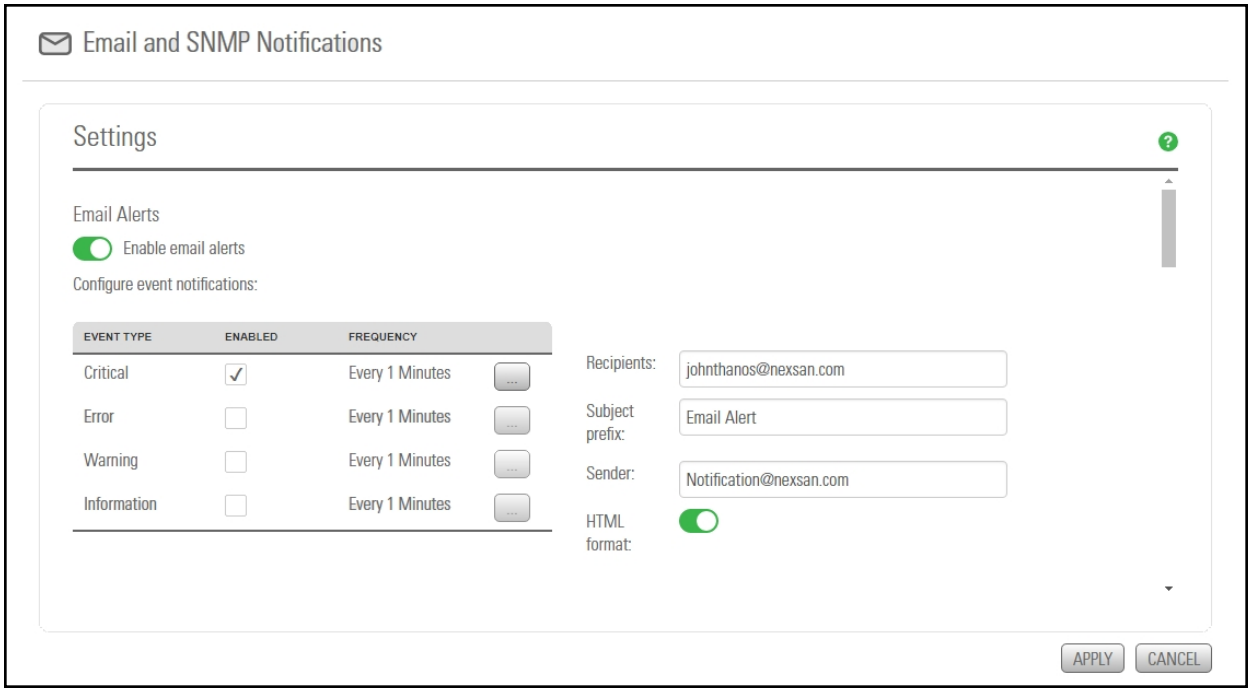
Prerequisites

- valid email addresses for notification recipients
- a sender email address

To set up the SMTP server settings for the Unity System:

1. On the **Unity navigation bar**, select **System > Notifications**. The **Email and SNMP Notifications Settings** panel opens.

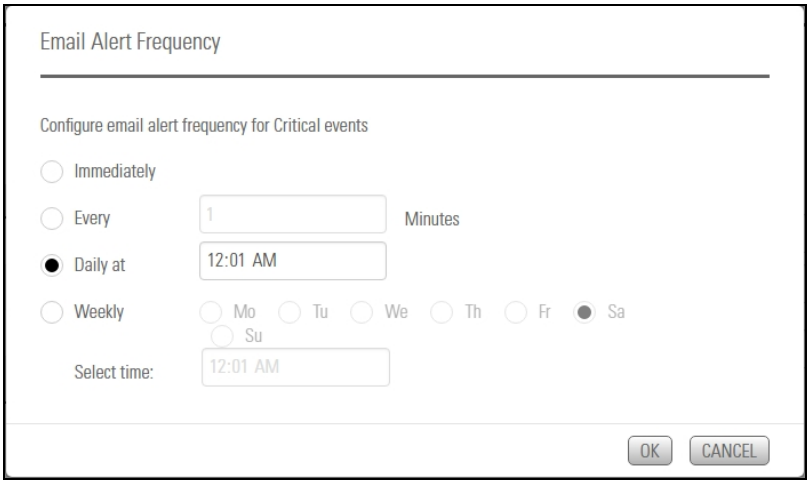
Figure 14-6: Email alerts



2. Under **Email Alerts**, click the **Enable Email Alerts** button

3. Click the configuration frequency button ... if you want to specify a notification schedule:

Figure 14-7: Email Alert Frequency



Unity can send you notifications immediately, every n minutes, or daily or weekly at a specific time of day, as shown.

4. In the **Recipients** box, type valid email addresses where you want to send the notifications.

5. In the **Sender** box, type a valid email address that you want to send the alerts from.

6. If you prefer have the email messages sent in text format, deselect the **HTML format** button
7. Click the **Apply** button to save **Email Alerts** settings.

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 file systems on Unity.

Unity enables 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.

To enable Unity to send system notifications for space usage threshold violations, you must first enable and configure space usage thresholds for storage pools and/or file systems.

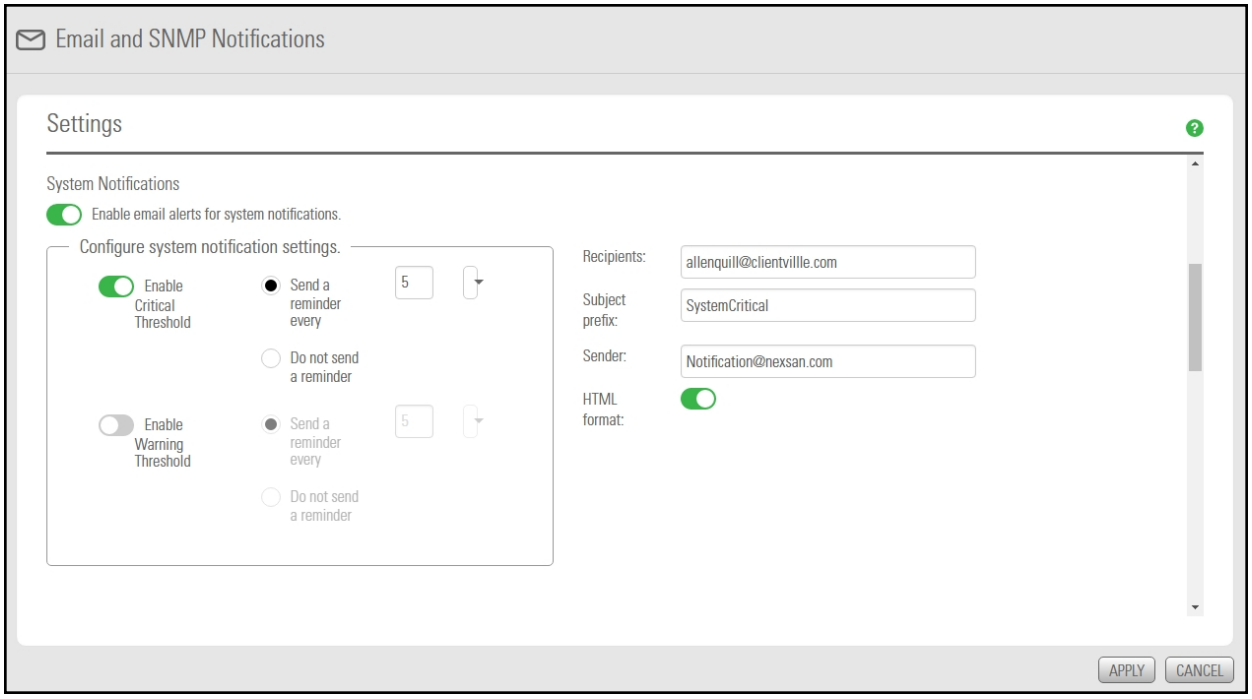
Prerequisites

- valid email addresses for notification recipients
- a sender email address

To set up system notifications:

1. On the **Unity navigation bar**, select **System > Notifications**. The **Email and SNMP Notifications Settings** panel opens.

Figure 14-8: System Notifications



2. Under **System Notifications**, click the **Enable email alerts for system notifications** button
3. Select the **Event Types** you want to be sent notifications for.

4. Under **Configure system notification settings**, do any of the following:
   - Click the **Enable Critical Threshold** button to receive critical system notifications.
   - Click the **Enable Warning Threshold** button to receive critical system notifications.
   - Optionally, select whether you want to receive reminders and how often. You can specify frequency in minutes, hours, or days.
5. In the **Recipients** box, type valid email addresses that you want to receive the notifications.
6. In the **Sender** box, type a valid email address that you want to send the alerts from.
7. If you prefer have the email messages sent in text format, deselect the **HTML format** button 
8. Click the **Apply** button to save **System Notifications** settings.

Configuring SMTP server settings for the Unity System

Before you set up email notification for system events and space usage threshold violations on storage pools and file systems, you must configure SMTP server settings for the Unity System. Nexsan Unity sends email notifications to the SMTP server, which then routes the email notifications to the recipients that you specify.

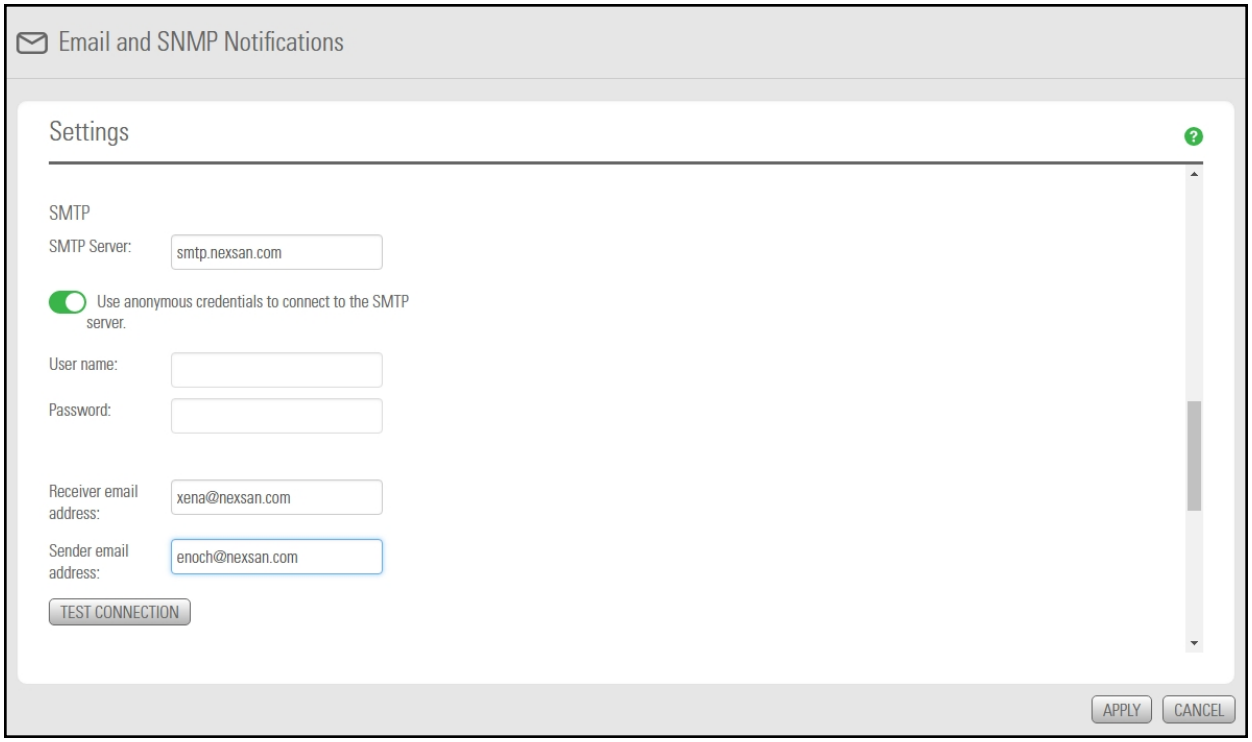
Prerequisites

- 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.

To set up the SMTP server settings for the Unity System:

1. On the **Unity navigation bar**, select **System > Notifications**. The **Email and SNMP Notifications Settings** panel opens.

Figure 14-9: SMTP settings



2. In the **SMTP** section, enter the SMTP server address. For example, `smtp.nexsan.com`
3. If user name and password authentication is required to access the server,
   a. Enable **Use anonymous credentials to connect to the SMTP server**.
   b. Enter a user name and password.
4. In the **Receiver email address** box, type valid email addresses that you want to receive the notifications.
5. In the **Sender email address** box, type a valid email address that you want to send the alerts from.
6. Click the **Test Connection** button.
7. When your settings are correct, click the **Apply** button to save the **SMTP Server** 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 558.

Prerequisites

- The IP address of the SNMP trap recipient, a Network Management Station where Unity will send SNMP traps.

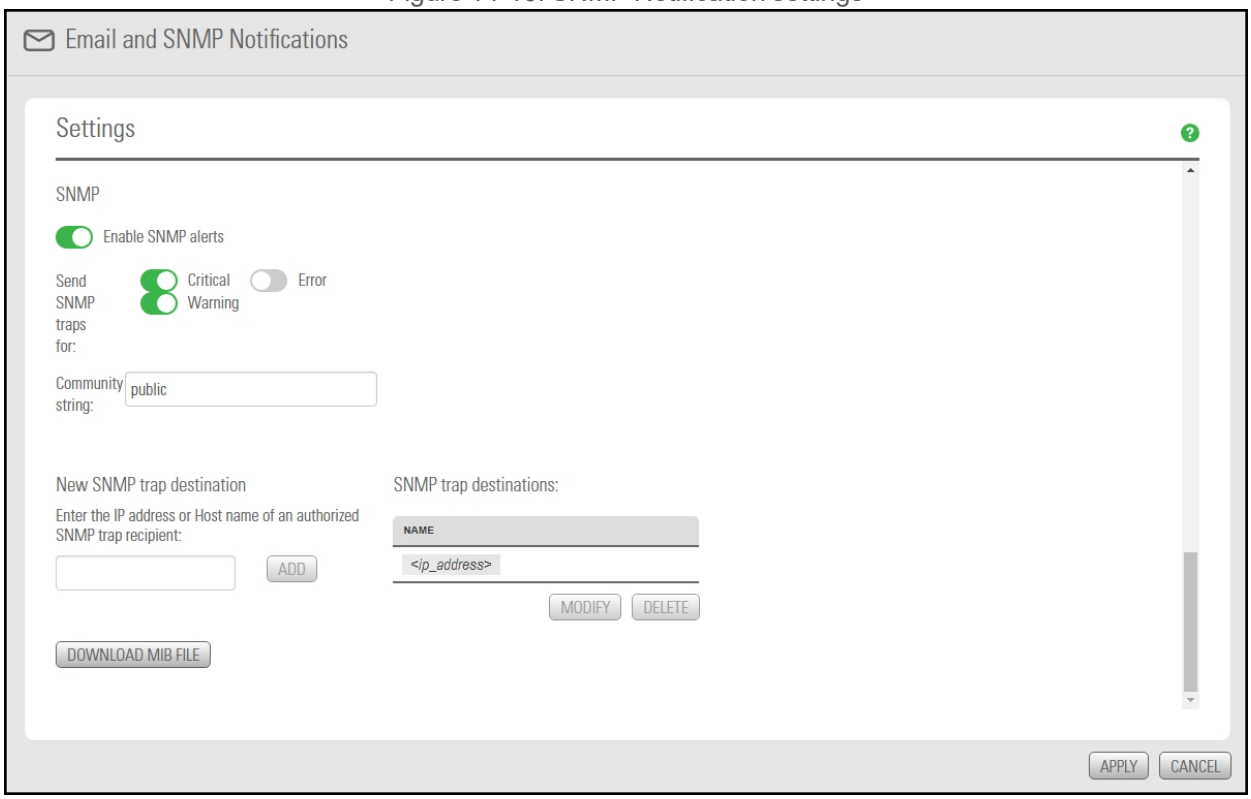
- The community string used by the Network Management Station. The community string is a text string that acts as a password. It is used to authenticate messages that are sent between the Network Management Station and SNMP agents and it is included in every packet that is transmitted between the SNMP 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. On the **Unity navigation bar**, select **System > Notifications**. The **Email and SNMP Notifications Settings** panel opens.
2. Scroll down to the **SNMP** section of the panel.

Figure 14-10: SNMP Notification settings



3. Click the **Enable SNMP alerts** button
4. In the **Send SNMP traps** section, enable at least one trap type (Critical, Warning, Error).
5. Enter a **Community string**. Community strings are defined in your trap manager.
6. Enter the IP address or Host name of an authorized SNMP trap recipient.
7. Click **Add**. You can click Modify or Delete if you need to add or change trap recipients.

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 Stations where SNMP traps will be received.
9. Click the **Apply** button to save your changes.

14

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 572

Understanding how using chmod in NFS creates allow and deny entries in CIFS ACLs 573

Examples of CIFS permissions after applying chmod in NFS 575

Mapping UNIX accounts on Unity to corresponding Microsoft Active Directory accounts 580

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 the facing page);
- 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	
• Write attributes • Take ownership • Change permissions • Write extended attributes • Read permissions • Read attributes • Read extended attributes	• **List folder / read data file** access control entry is added for *owner* in CIFS if **Read (r)** access is set for user in NFS • **Create files / write data** access control entry is added for *owner* in CIFS if **Write (w)** access is set for user in NFS • **Traverse folder / execute file** access control entry is added for *owner* in CIFS if **Execute (x)** access is set for user in NFS
Group	
• Read permissions • Read attributes • Read extended attributes	• **List folder / read data** file access control entry is added for *group* in CIFS if **Read (r)** access is set for group in NFS • **Create files / write data** access control entry is added for *group* in CIFS if **Write (w)** access is set for group in NFS • **Traverse folder / execute file** access control entry is added for *group* in CIFS if **Execute (x)** access is set for group in NFS

Default entries always set in CIFS	Entries set in CIFS only if the corresponding permission is set in NFS3
Everyone	
• Read permissions • Read attributes • Read extended attributes	• **List folder / read data** file access control entry is added for *everyone* in CIFS if **Read (r)** access is set for *others* in NFS • **Create files / write data** access control entry is added for *everyone* in CIFS if **Write (w)** access is set for *others* in NFS • **Traverse folder / execute file** access control entry is added for *everyone* in CIFS if **Execute (x)** access is set for *others* 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 *user*	*allow* access control entry added for owner 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 *user*	NFS permissions set for *group* or *others*	*allow* access control entry added for *owner* 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 *user*	NFS permissions set for *others*	*allow* access control entry added for *group* 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: rwx to owner, rx to everyone

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
owner allow entry	• 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
group allow entry	• List folder / read data • Read extended attributes • Traverse folder / execute file • Read attributes • Read permissions
everyone allow entry	• List folder / read data • Read extended attributes • Traverse folder / execute file • Read attributes • Read permissions

Example 2: rw to owner and others

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
owner **allow** entry 1	• List folder / read data • Create files / write data • Create folders / append data
group **deny** entry	• List folder / read data • Create files / write data • Create folders / append data
owner **allow** entry 2	• 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
group **allow** entry	• Read extended attributes • Read attributes • Read permissions
everyone **allow** entry	• List folder / read data • Create files / write data • Create folders / append data • Read extended attributes • Write extended attributes • Read permissions

Example 3: rwx to group only

This command grants Read (r), Write (w), and Execute (x) 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
group **deny** entry	• List folder / read data • Create files / write data • Create folders / append data
owner **allow** entry	• Read extended attributes • Write extended attributes • Read attributes • Write attributes • Read permissions • Change permissions • Take ownership
group **allow** entry	• List folder / read data • Create files / write data • Create folders / append data • Read extended attributes • Traverse folder / execute file • Read attributes • Read permissions
everyone **allow** entry	• Read extended attributes • Read attributes • Read permissions

Example 4: CIFS ACL entries preserved after chmod on NFS files

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 files 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**
owner **allow** entry	• 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	*lily@win.domain* **allow** entry	• List folder / read data • Read extended attributes • Traverse folder / execute file • Read attributes • Read permissions
group **allow** entry	• List folder / read data • Read extended attributes • Traverse folder / execute file • Read attributes • Read permissions	*bob* **allow** entry	• List folder / read data • Read extended attributes • Traverse folder / execute file • Read attributes • Read permissions

Original entries		New entries	
CIFS ACL entries	**Permissions**	**CIFS ACL entries**	**Permissions**
everyone **allow** entry	None	*owner* **allow** entry	• 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
lily@win.domain **allow** entry	• List folder / read data • Read extended attributes • Traverse folder / execute file • Read attributes • Read permissions	*group* **allow** entry	• List folder / read data • Read extended attributes • Traverse folder / execute file • Read attributes • Read permissions
bob **allow** entry	• List folder / read data • Read extended attributes • Traverse folder / execute file • Read attributes • Read permissions	*everyone* **allow** entry	• 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*.

Topics in this section:

nstusermaps 581

15

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 file system on the Unity Storage System, you must map the user or group accounts that you add to the Unity Storage System 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	**`nstusermaps add winuser:<useraccount@AD.net> unixuser:<username>`**
remove a mapping	**`nstusermaps remove winuser:<user_account@domain.xxx> unixuser:<user_name>`**
map multiple user and/or group accounts	The `nstusermaps` command includes a wildcard (*) option that enables you to map multiple user and/or group accounts on the Unity Storage System with their corresponding domain accounts in the Microsoft Active Directory. To map a user account, type: **`nstusermaps add winuser:*@AD.net unixuser:*`** To map a group account, type: **`nstusermaps add wingroup:*@AD.net unixgroup:*`** where `@AD.net` represents the Microsoft Active Directory domain containing the user or group accounts that you want to specify mapping for.

To...	Type this

exclude a user or group from identity mapping	When mapping user or group accounts between Microsoft Active Directory and the Unity Storage System, the system processes name-based mappings in this order of precedence:
	1. Exclusions:
	`cwindows-name@domain` to `" "`, or
	`unix-name` to `" "`
	2. Name-to-name mappings:
	`windows-name@domain` to `unix-name`
	3. Wild-card mappings: `*@domain` to `*`
	Type one of these variations of the `nstusermaps` command:
	`nstusermaps add unixuser:<user> " "`
	`nstusermaps add unixgroup:<group> " "`
	Where `<user/group>` represents the user or group account on the Unity Storage System that you do not want to map to its corresponding account in the Microsoft Active Directory domain.
	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 the Unity Storage System. For example, type one of these variations:
	`nstusermaps add winuser:*@AD.net " "`
	`nstusermaps add wingroup:*@AD.net " "`
	Where `@AD.net` represents the Microsoft Active Directory domain containing the user or group account you do not want to map to its corresponding account on the Unity Storage System.

display identity mapping information for a specific user and/or group	Type one of these commands: **`nstusermaps show -c winuser:<user>`** **`nstusermaps show -c unixuser:<user>`** **`nstusermaps show -c wingroup:<group>`** **`nstusermaps show -c unixgroup:<group>`** Where `<user/group>` represents the user or group account in Microsoft Active Directory domain and/or on the Unity Storage System.

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 the Unity Storage System.

`nstusermaps add winuser:<bob.summers@AD.net> unixuser:<bsummers>`

Appendix A

Unity nxadmin account access permissions

This table lists the access permissions for the built-in Unity **nxadmin** account, Unity System, and Pool administrative roles. Unity users created by the nxadmin account are allowed only file system permissions and CIFs-share permissions.

Access permissions	Unity Administrator (nxadmin)	Unity Site Administrator
Perform initial Unity setup	✓	×
Run CLI commands	✓	×
Unity System-level tasks		
• Change network settings for the Unity System	✓	✓
• Modify name and the DNS entry for the Unity System	✓	✓
• Enable the NDMP (Network Data Management Protocol) backup service and set the user name and password for the service	✓	✓
• Shut down/restart Unity	✓	✓
• Give Unity Site Administrator access to users and/or groups	×	×
• Revoke Unity Site Administrator access from users and/or groups	×	×
• Allocate new storage systems to the Unity System	✓	✓
• Shut down/restart external storage systems	✓	✓
• Perform firmware updates (using Unity firmware upgrader)	✓	×
• Customize date and time formats	✓	✓

Access permissions	Unity Administrator (nxadmin)	Unity Site Administrator
• Customize the server time and time zone (in the Unity System's properties panel)	✓	×
• Access the Performance Monitor to view performance metrics for the system	✓	✓
• 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 access to storage pools	✓	✓
• Revoke a user's and/or group's access	✓	✓
• Add volumes	✓	✓
• Replace a volume	✓	✓
• Perform scrub operations on storage pools and set a scrub schedule	✓	✓
• Configure FASTier cache assignments for the storage pool	✓	✓
File System tasks		
• Create new file system	✓	✓

Access permissions	Unity Administrator (nxadmin)	Unity Site Administrator
• Delete file system	✓	✓
• Modify a file system's name	✓	✓
• Adjust space usage settings	✓	✓
• Change the sharing method (CIFS, NFS, FTP, and/or anonymous access)	✓	✓
• Assign file system-level access permissions (Read, Read/Write, or Full, and Inherit) to users and/or groups	✓	✓
LUN-level tasks		
Create new LUNs	✓	✓
Delete LUNs	✓	✓
Create new iSCSI targets	✓	✓
Change CHAP authentication for LUNs and iSCSI targets	✓	✓
Manage CHAP authentication for the Unity System, include adding new CHAP users	✓	✓
Add, edit, and delete LUN masks	✓	✓
Add, edit, and delete Initiator Groups	✓	✓
Snapshots-related tasks		
Set schedules for snapshots	✓	✓
Take manual snapshots	✓	✓
Roll-back the data in a share to a specific snapshot	✓	✓
• Delete snapshots and configure auto-deletion settings	✓	✓
• Start/stop snapshot browsing	✓	✓
Data replication operations		
• Add a secondary Unity System and configure data replication	✓	✓
• Set data replication schedules (Asynchronous data replication)	✓	✓
• Perform offline replications (Asynchronous data replication)	✓	✓

Access permissions	Unity Administrator (nxadmin)	Unity Site Administrator
• Import data from the secondary Unity System or from a USB device (Asynchronous data replication)	✓	✓
• Failover all Unity System-level operations to the secondary system (Asynchronous data replication)	✓	✓
• Failover a storage pool to the secondary Unity System (Asynchronous data replication)	✓	✓
• Promote/demote the primary and/or secondary Unity System (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	✓	✓
• 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	✓	✓
• Manage groups (for example, add and/or remove users from a group)	✓	✓
• Change a user password	✓	✓ *Their own passwords ; not other Unity Site Administrators' passwords*
Manage a remote Unity System		
• Add a remote Unity System to manage	✓	✓
• View nodes and objects on the remote Unity System	✓	✓
• Configure/manage nodes and objects on the remote Unity System	✓	✓
Manage system events		
• Retrieve and view system events	✓	✓

A

Access permissions	Unity Administrator (nxadmin)	Unity Site Administrator
• Email and/or save event logs	✓	✓
• Configure event logging	✓	✓
Manage SNMP and email alerts		
• Configure SNMP alerts	✓	✓
• Configure email alerts	✓	✓

Terminology

1 A B C D E F G H I J L M N O P R S T U V

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 3: Configuring the access protocol on page 122 and Modifying file system sharing methods on page 145.

Active/Active Clustering

The Unity Storage System has built-in Active/Active Clustering capability, whereby both controller nodes on the Unity Storage System 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 Storage System'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 375.

ACL

An Access Control List (ACL) in server storage technology is a security mechanism consisting of a table of rules (Access Control Entries - ACEs) that define which users, groups, or systems are permitted or denied access to specific data objects, such as files, folders, or directories. It provides granular, fine-grained control over permissions, going beyond standard owner/group/other settings to enable

specific access rights like read, write, modify, or delete for multiple users.

ACoU

Assureon Client on Unity, a feature in Nexsan Unity storage systems that integrates with Nexsan Assureon archive storage. It allows the Unity system to archive data to Assureon to ensure data integrity, compliance, and storage efficiency.

Key aspects and functions of ACoU (Assureon Client on Unity) include: Archiving & Shortcutting, Data Integrity & Protection, Performance & Scalability, Restore Functionality, Integration with Assureon. In essence, ACoU is the bridge that allows Nexsan Unity to leverage the advanced secure archiving capabilities of Nexsan Assureon.

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.

ARC

Adaptive Replacement Cache (ARC) in ZFS and high-performance file systems is a sophisticated caching algorithm used to manage system memory (DRAM). It tracks both "recency" (recently used data) and "frequency" (frequently used data) to predict what should stay in the cache for better performance.

Level 2 Adaptive Replacement Cache (L2ARC) is a specific feature of the ZFS file system. While the primary ARC lives in a server's high-speed RAM (DRAM), the L2ARC acts as an extension that lives on faster secondary storage, typically SSDs or NVMe drives.

Asynchronous data replication

The asynchronous data replication function provides off-site disaster recovery protection for the Unity Storage System. 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 Storage System'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 Unity Storage System and sends either the entire contents up to the snapshot to the secondary Unity Storage System —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 Unity Storage System.

See .

Authentication mode

See User authentication mode on page 609.

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 Unity Storage System; as a result, to browse the contents of a replicated file system, you must set up a CIFS or NFS mapping to the remote Unity Storage System 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 184.

See the *Nexsan Unity Snapshots and Replication Guide*.

Bucket

A bucket is a basic container that holds data. It can be used to organize and control access to the data.

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 82.

In addition to CHAP authentication, Unity provides LUN masking for added security see Host connectivity: LUN masks and Initiator Groups on page 322.

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

See Clustering overview on page 376.

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 375.

D

Dataset

A dataset is any file system, iSCSI LUN, or CIFS share.

Dashboard

Unity's dashboard view interface presents the same data as the property panels in Unity, but for the entire Unity Storage System. The dashboard displays performance data, system 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 Unity's other panels and wizards to change data configuration settings.

See Finding Unity features on page 26.

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 473.

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.”

EUI

(Extended Unique Identifier) An identifier that is formed by concatenating the OUI with a 24-bit extension identifier that is assigned by Unity– the resulting identifier is represented as a set of octets separated by dashes (hexadecimal notation) or colons (bit-reversed notation).

The OUI (Organizationally Unique Identifier) is a 24-bit number that uniquely identifies a vendor, manufacturer, or other organization globally or worldwide. See Fibre Channel initiator.

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 Storage System 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 Unity 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 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 557.

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. .

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 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.

Unity Storage System or pool failover: Typically, you use the failover function to transfer data and system operations to a remote Unity Storage System 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 enables 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 enables you to forcefully promote the remote Unity Storage System to primary status in your Unity deployment in the event of a complete system failure—due to a catastrophic disaster—on the primary Unity Storage System.

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.

See Adding a storage pool on page 90 and Disabling Read caching on page 252.

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.

You can expose LUNs over Fibre Channel using a unified Fibre Channel target. The Fibre Channel ports are configured as targets. Fibre Channel is supported by the UNITY3100, UNITY3300, and UNITY7900.

Fibre Channel initiator

An application system end-point that is capable of initiating a session with a Fibre Channel target, sending SCSI commands and I/O requests. When a LUN is associated with a specific initiator, the LUN will only be visible to this initiator.

The initiator for Fibre Channel must be identified by the HBA port World Wide Name (WWN) or the Extended Unique Identifier (EUI). For added security, Unity provides LUN masking; see Host connectivity: LUN masks and Initiator Groups on page 322.

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).

File System

Subfolders of storage pools, file systems are Unity organizational structures available as shares

exposed on the network via CIFS protocol and/or the NFS protocol.

Each file system is identified on the network by its file system name, which you specify when you add the file system to the system. Client computers then access the file system (over the CIFS and/or NFS protocols). Only those users on the network that you authorize to access the file system (by setting file system-level access permissions for them) can either view and/or perform Read/Write operations on the data in the file system. See also Sharing methods

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 enables 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 Unity nxadmin account access permissions and Users and access rights on page 69.

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

(Host Bus Adaptor) is a hardware circuit or expansion card that connects a host server to external storage devices or network storage systems. It acts as an translator, converting the server's internal bus protocols (usually PCIe) into storage-specific protocols.

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 initator and Creating a LUN mask on page 324.

HDD

Hard Disk Drives (HDDs) remain crucial in server storage for high-capacity, cost-effective, and reliable mass storage, often used for data archiving, backups, and large database systems. They offer the lowest cost per TB, with enterprise-grade models providing 24/7 reliability, high capacity (20TB+), and stable performance for sequential workloads, despite being slower than SSDs.

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 Unity System on page 406 and Resetting the RAID configuration for storage on page 416.

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 Unity 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 enables you to manage user accounts and passwords on Windows and UNIX systems using Network Information Service (NIS). IDMU also enables you to automatically synchronize passwords between Windows and UNIX operating systems.

Immutable snapshot

An snapshot is immutable when it cannot be changed or modified after its creation. With Unity, immutable snapshots cannot be deleted or extended until after the expiration date set by the system administrator. These capabilities enable organizations to access or recover all of their data without paying a ransom.

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

You use the IPMI (Intelligent Platform Management Interface) interface to perform administrative tasks to remotely manage Unity in the event that you are unable to connect from within 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.

On a clustered system, you must set a separate IPMI IP address for each controller node.

See Setting or modifying IPMI settings on page 398.

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 Storage System 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 (Unity Storage System) 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 231 and Managing iSCSI targets on page 315.

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

You can configure iSCSI targets on Unity to use 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.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 320.

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 Storage System is actually 1500 bytes. For the Unity Storage System, 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 using Unity on page 399 and Enabling jumbo frames using the nxadmin CLI on page 400.

Adding an iSNS server on page 320.

K

Kerberos

Kerberos is a critical network authentication protocol used in server storage technology to secure access to data, particularly in enterprise NAS (Network Attached Storage) and SAN (Storage Area Network) environments. It acts as a trusted third party that uses "tickets" to authenticate users and services without transmitting passwords over the network, ensuring that data access is restricted to verified principals.

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" in the *nxcmd Command Line Interface Reference Guide*..

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 Storage System. 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, and **1024** LUNs.

LUNs can be exposed over iSCSI or Fibre Channel. 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. When exposed to targets over Fibre Channel, a LUN forms a block device identified by a unique HBA port WWN that can be accessed by one or more FC initiators.

See LUNs on page 231.

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 Creating a LUN on page 236 and Creating a LUN mask on page 324.

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.

The Management target is used for both iSCSI and Fibre Channel targets.

Manual replication

In asynchronous replication, a manual, replication is a replication process that you start manually on a storage pool. With manual 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.

Mb

(Megabit) Approximately one million (1,000,000) bits.

Mb/s

(Megabits per second) Used to describe the speed of network data transmission.

MFA

Multi-Factor Authentication (MFA) in server storage technology is a critical security layer that requires users to provide two or more verification factors—such as passwords, security tokens, or biometrics—to access storage systems, backups, and data management consoles. As ransomware threats increase, MFA is considered essential for protecting data stored on-premise, in Storage Area Networks (SAN), Network Attached Storage (NAS), and cloud environments.

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 enables you to take manual or automatic backup copies or snapshots of data.

If Unity is joined to a Microsoft Active Directory domain, Unity automatically exposes all the snapshots for each file system/LUN on 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 Changing a pool resource group on page 107.

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 enables 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 46.

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 enables 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 file systems on Unity, and uses background snapshots for fast backups. See Setting NDMP configuration options on page 439.

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 nxadmin 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 185.

NFSv4

(Network File System version 4) NSFv4 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 186.

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.

NTLM

NTLM (NT LAN Manager) is a legacy suite of Microsoft security protocols used for authentication, integrity, and confidentiality in Windows networks and server storage environments. While primarily an authentication protocol, NTLM is heavily integrated into server storage technology for managing access to network file shares (CIFS/SMB), particularly for legacy systems, workgroups, and scenarios where modern protocols like Kerberos are not available.

NTP

(Network Time Protocol) A protocol designed to synchronize the clocks of devices over a network. See Time server.

NVDIMM

(Non-Volatile Dual In-line Memory Module) is a type of hybrid computer memory that retains data even when electrical power is completely lost. It installs into a standard motherboard memory slot and operates at standard system RAM speeds, serving as a bridge between high-speed volatile memory and persistent storage.

NVMe

(Non-Volatile Memory express) is an open, logical-device interface specification for accessing a computer's non-volatile storage media usually attached via the PCI Express bus.

O

Object

An object is a file or a discreet unit of data. In Unity, objects also contain metadata that describes that file.

Object Lock

Object Lock is a feature that makes data immutable by preventing a file from being changed or deleted until a given date. Unity enables bucket or object level protection for a specified retention period to create immutable copies of data. This can be important to address compliance, regulatory, and other data protection requirements.

Object Store

An object store holds data in small pieces called objects and is useful for storing large amounts of unstructured data. Object storage is the most recent of the three main forms of data storage. The other forms are file storage and block storage. Unity object storage is based on the S3 protocol.

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

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 system, peer site, or replication peer. In asynchronous replication, a peer represents an Unity Storage System that you set up data replication to/from.

Pool

A storage pool (also referred to as a "pool") groups disks into volumes, to which you can add file systems, LUNS, and object stores. Pools allow you to expose file systems and shares to CIFS clients (Windows-based systems) and NFS clients (UNIX/Linux-based systems). You can replicate all the data in the pool, or just a subset of it, for disaster recovery.

Unity™ enables you to create as many storage pools as there are available volumes (RAID sets) on the system.

If the Unity Storage System is connected to one or more Unity Storage Expansions, storage pools can combine volumes from both—provided that the RAID level configurations are the same on all device in the pool.

Pool Resource Group

When you create a storage pool on the Unity Storage System, 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 Storage System. 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 386.

See Clustering overview on page 376

Primary system

See Unity Storage System.

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 Unity System on page 406 and Resetting the RAID configuration for storage on page 416.

RAID 5

RAID 5 provides redundancy by writing data and parity information across three or more drives, thereby increasing performance. You need at least three 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 four 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 two drives, instead of four, 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 two drives and striping will automatically be applied across two 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 92.

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 Unity Storage System.

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 enables you to replicate data between two sites —a primary and a remote Unity—over a LAN or WAN connection. See Asynchronous data replication.

Resilvering

Resilvering is the process of rebuilding data onto a new or replacement drive within a mirrored or RAID-Z storage pool, primarily associated with the ZFS file system. It involves copying data from existing, healthy disks in the pool to a new disk to restore the array to a healthy, fully redundant state after a drive failure.

Rollback function

Unity enables 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.

RPC

Remote Procedure Call (RPC) in server storage technology is a protocol that allows a program on a client machine to request services or execute procedures on a remote server as if it were a local function call. It abstracts the complexities of network communication (like TCP/IP), making it essential for distributed storage systems, file systems, and database management.

S

S3 Protocol

The S3 (Simple Storage Service) protocol is a REST-based API developed by Amazon Web Services (AWS) that has become the de facto industry standard for object storage, allowing applications to store, manage, and retrieve data over HTTP/HTTPS. While AWS offers a managed implementation of this service, the protocol itself is widely implemented in on-premises server storage systems, hybrid clouds, and by third-party storage vendors, making it a crucial component for interoperability in modern IT infrastructure.

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 Storage System provides a disk scrubbing mechanism that checks the physical hard disks, which comprise the volumes in a storage pool on the Unity Storage System, 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 94

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 system

In asynchronous replication, a remote or secondary system 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.

Secret Key

A secret key is used to sign requests by the user to gain access to data and programmatic services. Unity uses an access key and a private key to grant authorization. The pair of keys are similar to the concept of a user name and password pair.

SED

A Self-Encrypting Drive (SED) is a hard drive or SSD with a built-in controller that automatically encrypts all data written to the media and decrypts it upon reading. This hardware-based security ensures data is always encrypted at rest without using CPU resources. SEDs offer instant secure erase capabilities and prevent data theft, as the data is inaccessible without the authentication key.

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 methods

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 195
- 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 systems 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, 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 195
- 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 enables 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 3: Configuring the access protocol on page 122 and Modifying file system sharing methods on page 145.

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 186.

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 185.

Site

See Unity Storage System

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 enables 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 567.

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 Unity System on page 566

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 enables 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

Unity provides a mechanism that enables 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 snapshotssee 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 66.

Storage expansion

On Unity, a storage expansion is a Nexsan external storage system: this refers to a Nexsan Unity or E-Series storage device connected externally to Unity via a SAS (or Fibre Channel) add-on card (optional).

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.

System name

A system name enables 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 third floor.

The system name is particularly useful in identifying Unity Storage Systems in multi-system environments, where a single Unity session manages multiple sites on the network (remote site management).

See Step 1: Configuring Unity System properties on page 56 and Changing the Unity Storage System name on page 438.

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 used on page 438.

Thin Provisioning

Thin Provisioning enables 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 enables 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 Step 1: Setting the LUN name and block size on page 237.

Thread management

Thread management refers to the methods to create, schedule, and coordinate multiple execution paths (threads) within a process to handle concurrent I/O requests, data processing, and system operations efficiently. It involves utilizing thread pools, kernel-level threads, and asynchronous I/O to maximize hardware utilization, such as SSDs, while minimizing latency and avoiding bottlenecks caused by idle threads waiting on disk input/output.

TRIM

TRIM is a crucial Advanced Technology Attachment (ATA) command used in server storage technology—specifically for Solid State Drives (SSDs) that allows an operating system to notify the SSD controller which data blocks are no longer in use, such as those belonging to deleted files. In enterprise environments, this command is essential for maintaining high write performance and extending the lifespan of SSDs by optimizing garbage collection.

U

Unity Storage System (also Unity System, Site)

A Unity Storage System—also referred to as the local Unity Storage System, active Unity Storage System, or primary Unity Storage System (in a replicated environment)—represents a geographic location that hosts a Unity Storage System. More specifically, a Unity Storage System can contain either:

- a Unity System with no external storage;
- a Unity System with one or multiple Unity Storage Systems connected to it (via Fibre Channel or SAS).

A remote Unity Storage System—also referred to as a secondary site or a replication site (in a replicated environment)—represents either:

- a Unity Storage System that is designated as the data replication site for the local site;
- a Unity Storage System that is being managed remotely from the local site.

A Unity Storage System can be the primary site in a replicated environment and also perform double-duty as the remote data replication site for another Unity.

See Understanding multi-site implementation on page 46.

UNMAP

UNMAP is a critical SCSI command in server storage technology used to reclaim physical storage space from thinly provisioned storage arrays. When data is deleted from a host operating system, the underlying storage array often remains unaware of this change, continuing to reserve that space. UNMAP notifies the array that specific Logical Block Addresses (LBAs) are no longer in use, allowing the storage to be returned to the free pool for reuse. It is the SAS/SCSI equivalent of the ATA TRIM command for SSDs.

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 file system-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 enables 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 Unity nxadmin account access permissions and Users and access rights on page 69.

User authentication mode

During initial system configuration, Unity authentication is applied to the built-in nxadmin user account.

Unity supports these user authentication modes:

- **Unity authentication (default):** Unity verifies that, when a user enters a user name and password to log on to Unity, they match the corresponding user name and password stored locally.
- **Microsoft Windows Active Directory domain:** When a user enters a user name and password in the same Unity login window, Unity checks the Microsoft Windows Active Directory server for a matching user record. See Joining a Microsoft Active Directory domain on page 458
- **CHAP authentication:** Challenge-Handshake Authentication users can be set up to restrict iSCSI access to LUNs on Unity Storage Systems. See Configuring and managing CHAP authentication on page 82

CLI only

- **LDAP Directory service (in UNIX/Linux environments):** When a user enters a user name and password in the same Unity login window, Unity checks the LDAP Directory server for a matching user record. See "Connecting to an LDAP directory service" in the *nxadmin Command Line Interface Reference Guide* on the Nexsan.com/support webpage

Regardless of the type of authentication, Unity uses the information in your configuration to determine the file system-level access permissions that are granted to the user.

See User authentication modes on page 70 and Administrator and user permissions on page 70.

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 enables 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: enables 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 plugin

Unity includes a built-in VMware 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 Storage System 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 254.

Volume

A volume represents a subset of the aggregated disk space available on Unity, or on a Nexsan E-Series or a Nexsan Expansion System connected to Unity. Unity presents available disk space as volumes.

The total number of volumes available on Unity Storage Systems and Unity Storage Expansions depends on the RAID level (5, 6, or 10) and RAID sets that you specify during system setup.

See Storage and Pool. See also Mixing volumes with different RAID levels on page 92, and Resetting the RAID configuration for storage on page 416.

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 Storage System's VSS Hardware Provider serves as the interface between Windows Volume Shadow Copy Service running on a host system and the Unity Storage System. Upon receiving instructions from a VSS host to create, mount, and restore snapshots, the VSS Hardware Provider sends the appropriate commands to the Unity Storage System 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.

Z

ZFS

ZFS (Zettabyte File System) is an enterprise-grade file system and logical volume manager that provides near-limitless storage capacity, automated data repair, and advanced management features like snapshots and compression. Unlike traditional storage technologies that separate the file system from the volume manager, ZFS combines these layers to eliminate the need for hardware RAID controllers and simplify storage administration.

B

Index

A

Access Control Lists (ACLs) 195
Access permissions 70, 173, 177, 194, 583
    shares 176, 194
access permissions
    file systems or CIFS shares
managing 197
Access Time mode 103, 144
Accessing a CIFS share 181
Accessing an NSTshare 184
Accessing the IPMI web-based interface 398
ACLs 173, 195, 458, 472, 475, 573, 575, 605
Active Archive menu 40
Active Directory 70, 502, 609
    Configuring the host for Kerberos support 468
    creating computer objects 453
    domain requirements 452
    joining 458
    time server 608
Active node 378
Active/Active clustering 22, 375, 589
    defintion 377
Add a secondary site for asynchronous data replication 506
Adding
    users 76
Adding a file system 117
Adding a group 78
Adding a host for each Resource Controller in DNS Manager 467
Adding a LUN 236
Adding a Reverse Lookup Zone in DNS Manager 463
Adding a secondary site 442
Adding a share 174
Adding a storage pool 90
Adding a user account 76
Adding a user to a group 79
Adding an iSCSI target 315
Adding an iSNS server 320-321
Adding cloud storage configurations 539
Adding new drives 414
Adding volumes to a pool 98
Adding volumes to a replicated pool 99
All ports / All LUNs feature 22, 590
Allocating FASTier cache devices 513
Allocating new storage 406
Alternate primary/secondary domain controllers 471
Anonymous access 194
Anonymous Write access 177, 197
APAL status 481
Applications 238
Applying configuration settings 64
Assigning access permissions for file systems or CIFS shares 197
Asynchronous Replication 501
    before you begin 502
    compression 530
    disabling 518
    enabling 518
    encryption 530
    features 504
    network settings 528
    one-to-one 505
    removing 532
    starting 506
    step 1 506
    step 2 509
    step 3 510
    step 4 513
    step 5 514
    step 6 515
    terminology 287, 500
    usage 501
Authentication modes
    Active Directory 458
    LDAP 473
Auto-deletion 243

Auto-deletion settings of snapshots 100
Automatic collection and transfer of system logs 484
Automatic replication 501
Automatic snapshots 208, 302
Automatically assing a name 212, 297

B

Before adding LUNs 236
Before creating pools 90
Benefits of authenticating users 610
Browsing a LUN snapshot 297
Browsing a share snapshot 212
Browsing contents of a replicated share 536
Browsing snapshots 205, 212, 215, 273, 288, 290, 292, 294-295, 297, 535, 591

C

Call Home settings 56
CallHome
  understanding 484
CallHome settings 56
Changing a user's password 80
Changing the Unity Administrator (nxadmin) password 81
CHAP 232
CHAP authentication 82
  Configuring CHAP for iSCSI targets 317
  Deleting a CHAP user 85, 87
  For a target 86
CIFS 214
CIFS and NFS sharing 180
CIFS sharing 24, 30, 33, 42, 49, 51, 53, 66, 70, 76, 88-89, 115-117, 122, 131, 145, 147, 151, 155, 162, 171, 173-176, 178-182, 189-190, 192, 194-197, 216, 286, 290, 386, 431, 439, 458, 463, 472, 475, 520, 535, 550, 571-573, 575-578, 585, 589, 605
Clearing event logs 562
Clearing pool errors 110
Cloud Connector 539
Cloud Connector menu 41
Cluster
  Active node 378
  chassis inter-connect card status 386
  Components and terminology 377
  Controller information 386
  Health status 386
  License information 386
  Managing active/active clustering 375
  Moving cluster resources 387
  Passive node 378
  Restarting cluster nodes 389
  Shutting down cluster nodes 391
  Typical cluster implementation 386
  When a node is down 387
Cluster resources definition 377
Cluster Settings menu 34
Cluster-level access rights 584
Collecting logs 560
Collection of system logs 484
Complete system failure 524
Compression settings 530
Computer objects 453, 459
Concepts and terminology
  Cluster 377
  E-Centre 42
  Replication 287, 500
Configurable RAID 22
Configuring a data replication schedule 509
Configuring asynchronous replication for a dataset 518
Configuring IPMI settings 398
Configuring LACP 402
Configuring logging options 559
Configuring LUNs in Disk Management 267
Configuring network settings 58
Configuring new drives 414
Configuring RAID settings 407
Configuring SMTP server settings 566
Configuring storage 62
Configuring the host in Active Directory 468
Configuring the network type for data replication 536
Connecting to a specific domain controller 459
Connecting to an iSCSI LUN from a Windows-based initiator 318
Connecting to the Internet
  using a direct LAN link 494
  using a workstation 496
  using an HTTP proxy server 495
Connectivity to the Internet 493
Controller definition 42, 45, 377
Controller IP addresses 394
Convention for a site name 438
CPU 550
createlogpackage 560
Creating
  snapshots 37, 204, 285
Creating a storage pool 90
Creating an Initiator group 330
Creating file systems for home directories 155
Critical
  pool 105
Current and accurate copy of production data 539

D

Dashboard panel 26
Data backup 232, 501, 539
Data compression for Async Replication 530
Data encryption 530
Data management functions on LUNs 232
Data migration 502, 524, 539
Data protection 232
Data Protection menu 31
Data Protection menu and panels 40
Data Replication 90, 116, 122, 160, 173, 232, 502, 506, 514-515, 558, 593
Data replication
  access rights 585
  asynchronous 501
  LUN 241
Data sharing disabled 134
Data type 238
Dataset replication 504, 510, 518
Date and time formats 441
DEGRADED 110
Deleting a CHAP user 85, 87
Deleting a share 192
Deleting a storage pool 114
Deleting a user or a group 80
Deleting an Initiator group 333
Deleting cloud storage configuration 543
Deleting LUN snapshots manually 301
Deleting share snapshots manually 218
Device I/O 550
Direct LAN link 494
Disabling a storage pool's replication schedule 521
Disabling asynchronous data replication for a dataset 518
Disabling data sharing for a share 134
Disabling Read caching 252
Disabling SED encryption 427
Disabling the Access Time mode 144
  pool 103
Disaster recovery 232, 501, 523, 539
Disconnecting a site 443
Discovering new domain controllers 470
Discovering new storage 407
Disk Management 267
Disk properties 269
distinguedName 459
DNS alias 452
DNS Manager
  Adding a host for each Resource Controller 467
  Adding a Reverse Lookup Zone 463
DNS mappings 527
dNSHostName 456
Domain
  Unjoining 472
Domain controller
  Alternate primary/secondary 471
Domain controller discovery 470
Domain controller management 469
Domain name 458

E

Editing cloud storage configuration 542
Editing IP restrictions 150
Emailing events 563
  Space usage threshold violations 565
Enable NDMP 439
Enable snapshot scheduling 243
Enabling client-side space usage notifications for a LUN 254
Enabling compression
  LUN 251
  share 142
  storage pool 102
Enabling FTP sharing 483
Enabling FTP support 482
Enabling Internet Connectivity 493
Enabling IPMI 398
Enabling jumbo frames 400
Enabling jumbo frames using Unity 399
Enabling Kerberos 463
Enabling LACP 403
Enabling Read caching 252
Enabling SED encryption 425
Enabling the Access Time mode 144
Enabling the security mode for NFS shares at the site level 479
Enabling VMWare VAAI hardware acceleration 254
Enabling ZFS Encryption
  File Systems 199, 280
Encryption settings 530
Error event
  pool 106, 110
E-Series storage systems 413
Ethernet switches for LACP 401, 403
Event logs 557
  access rights 586
  Clear 562
  Collecting logs 560
  Configuring logging options 559
  Viewing events 558
Event notifcation 557
  Setting up emails 563
  Setting up notifications 563
Example of cluster implementation 386
Expandable storage 22
Expanding capacity for a pool 98
Export encryption keys 426

F

Failover 504
  Definition 379
  disaster recovery 523
  of the entire site 525
  Site failover vs. pool failover 524
  versus promote 523
FASTier cache devices 108-109, 513
FASTier I/O statistics 551
FASTier Read caching 252
FAULTED 110
Fibre Channel 24
File locks 606
File name representation 606
File system 115
  adding 117
  considerations 117
  data management functions 116
  renaming 133
  viewing space usage 130
File System
  Snapshots Properties panel
Snapshots tab 293
File Systems menu 37
Filtering live performance metrics 553
Filtering snapshots in the grid 205, 295
Find Domain Controllers 471
Firmware version of E-Series 413
Folder name representation 606
FTP 482
FTP sharing 180
  system 483
Full access
  shares 196
Full-Duplex 401

G

GID 78, 186, 601
Global catalog 452
groupadd 185
GUID Partition Table 268
Guidelines for LUNs 232

H

Help menu 31
Hidden CIFS share 145, 176
High availabity 376
home directories
  about 154
  adding 155
  example in Windows 172
  managing 154
  Managing group assignments 169
Host Connectivity menu 34
Hot spares 63, 409, 415, 417
HTTP proxy server 495

I

IDMU 185-186, 459
igb# 397
Imminent system failure 524
Immutable snapshots for file systems 220
Immutable snapshots for LUNs 304
Incremental updates 500, 504
Initializing a LUN 319
Initializing LUNs in Disk Management 267
Initiator group
  create 330
  delete 333
  modify 331
Internet connection
  with a direct LAN link 494
  with a workstation 496
  with an HTTP proxy server 495
Intersite Virtual IP address 395, 442
Intersite virtual IP address 507
IP address requirements 394
IP permission precedence on shares 151
IP restrictions
  editing or removing 150
  setting 147
IPMI console 400, 402
IPMI settings 398
IPMI web-based interface 398
IQN 316
iSCCI target
  Adding 315
  Configuring CHAP authentication 317
  Managing 315
  Specifying IQN and public alias 316
iSCSI initiators 82
iSCSI LUN definition 44
iSCSI target definition 42
iSCSI Targets menu 38
iSNS 320-321
ixgbe# 397

J

Joining
  Active Directory 458
  LDAP 473
Jumbo frames 400

K

Kerberos
  Adding a host for each Resource Controller in DNS Manager 467
  Adding a Reverse Lookup Zone in DNS Manager 463
  Configuring the host in Active Directory 468
KVM console 402

L

LACP
  configuring 402
  Requirements and guidelines 401
  Understanding link aggregation 402
Layout of the Manage Users and Groups panel 75
LDAP 25, 29, 66, 70, 73, 122, 145, 162, 176, 182, 194, 197, 438-439, 452, 469, 473, 475, 502, 571, 578, 580, 609
LDAP catalog 452
LDAP Directory server 452
LDAP directory service 473
LDAP Domain 473
LDAP server 608
License status for the cluster 386
Link aggregation 402
Link layers 396
Linux 238
Live performance metrics 553
Load balancing 376, 524
Logging options 559
Logical Unit Number (LUN) 237
Logs 484
LUN
  Adding a target 315
  Connecting to an iSCSI LUN from a Windows-based initiator 318
  Data management functions 232
  Deleting snapshots 301
  Enabling client-side space usage notifications 254
  Enabling VMWare VAAI hardware acceleration 254
  guidelines 232
  Initializing a LUN 319
  LUN-level access rights 585
  Managing 231
  mgmt target 258
  renaming 250
  Snapshots 285
  Snapshots Properties panel 291
Settings tab 302
  viewing space usage 105, 248
LUN compression 251
LUN definition 42, 44
LUN name 237
LUNs menu 38

M

Maintenance update plan 447
Manage Users
  access rights 586
Manage Users and Groups panel 75
Management interface IP addresses 394
Management network interface 22, 58, 61
Management Virtual IP address 394
managing FASTier cache devices 108
Managing snapshots for LUNs
  using Properties panel 291
Managing snapshots for shares 204
  using Properties panel 204, 207
Managing users and access rights 73
Managing users and groups 79
Manual pool scrub 95
Manual replication 501
Manual snapshots 211, 296
Manually deleting LUN snapshots 301
Manually deleting share snapshots 218
Manually refreshing site-level or share-level information 442
Mapping a CIFS share 182
Master Boot Record 268
Maximum number of targets per pool 315
Memory 550
Menu-driven nxadmin CLI
  Change network type setting 536
mgmt target 258
Microsoft Active Directory 29, 73, 83, 88, 130, 155, 160-161, 163, 176, 185, 194, 216, 289-290, 438-439, 452-453, 458, 469, 472, 475, 571, 578, 580-581, 595
Microsoft Exchange 238
Microsoft Volume Shadow Copy Service 216, 289
Mixed mode operation 606
Mixing of volumes 92
Modifying a storage pool's replication schedule 520
Modifying an Initiator group 331
Modifying data and time formats 441
Modifying network settings 393
Modifying sharing methods 145
Modifying space usage settings 136
Modifying user authentication settings 452
Mount points
  shares 185, 192

Moving a storage pool
from pool's properties panel 107
Moving cluster resources 387
msDS-SupportedEncryptionTypes 456
MTU 598
Multi-site management 442
Mutual CHAP authentication 82, 86

N

NDMP configuration 439
NDMP support for data backup 232
NESTHOSTNAME 456
NestOS 42
NestOS Admin Menu
Shutdown and Reboot menu 400
NestOS Replication Bandwidth menu
Change network type setting 536
Network interfaces
IP addresses 395
link layers 396
naming convention 397
Network performance 550
Network settings 58, 61, 412
modifying 393
Network settings for asynchronous replication 528
Network Time Protocol (NTP) 452
New drives 414
New features and enhancements 18
New Simple Volume 268, 319
New storage allocation 406
New storage discovery 407
New user for E-Cemtre authentication 76
Nexsan storage system 412
NFS 214
NFS security mode
site 479
NFS sharing xiv, 17-18, 24, 33, 42, 49, 51, 53, 89, 115-117, 122, 131, 145, 147, 151, 155, 162, 173, 175, 180, 184-186, 192, 194-196, 286, 386, 431, 439, 458, 472, 475, 479, 520, 535, 539, 550, 571-573, 575, 577-578, 581, 589, 605
NFS Version 480
NFSv3 185, 196
NFSv4 196
nic
modify-aggr 403
set-linkprop 400
nic show-link 396
No access IP restrictions 147
Node definition 45, 377
Non-Administrator user account 453
Non-Optimized Path 22, 49, 51, 53, 380, 385, 481, 590
Notification thresholds 140
Notifications panel 35
nstndmp 439
nstusermaps 185, 581
Number of RAID sets 409, 414, 417
NVDIMM 481
nx# 397
nx0 58, 61, 403
IP addresses 394-395
Network interface 395
nx1 403
nx99 58, 61, 396
IP addresses 394
Network interface 395
nxadmin access rights 583
nxadmin credentials 443

O

Object Store 45, 335
Object Store properties 39
OFFLINE 110
Offline disks 267
Offline replication 501
on-board LAN1 port 395
One-to-one replication 505
One-way CHAP authentication 82, 86
Opening the Manage Users and Groups panel 75
Optimized path 22, 49, 51, 53, 380, 385, 481, 590
Oracle OLTP 238
Order of precedence for pool and dataset properties 93
Organizational Unit (OU) 459

P

Passive node 378
Password change 80
Peer site 602
Peer system 500
Performance metrics 553
Performance Monitor
Starting 551
Performing a failover 525
Permissions 66, 88, 116, 149, 151, 177, 196-197, 360, 363, 575-578
Pool
property settings order of precedence 93
Pool compression 102
Pool definition 42, 44
Pool resource group 378
Virtual IP address 395
Pools
Adding volumes to a pool 98
Adding volumes to a replicated pool 99

creating a storage pool 90
Deleting 114
Disabling a storage pool's replication schedule 521
Disabling the Access Time mode 103
Manual scrub 95
Modifying a storage pool's replication schedule 520
pool level access rights 584
Removing asynchronous data replication for a storage pool 532
Replacing a volume 99
replica 500
Setting the scrub schedule 96
Snapshot auto-deletion 100
Space usage notification thresholds 105
Powering down Unity storage system 419, 423
Powering on 421
Powering on Unity 421, 424
Powering Unity back on 421, 424
Pre-defined computer objects 459
Primary system 500
private0 396
Promote 524
Proxy DN 473
Proxy server 495
Public alias 316

Q

Quiesce the system 391
Quota 136

R

RAID configuration 407
Resetting 416
RAID level 409, 414, 416
Read access
shares 196
Read caching 252
Read/Write access
shares 196
Read/Write anonymous access 589
Read-only access IP restrictions 147
Read-only anonymous access 214, 589
Read-write access IP restrictions 147
Rebooting E-Series 422, 425
Rebooting Unity controllers 422
Refreshing site-level or share-level information 442
Remote access to replicated data 504
Remote connectivity 484
Remote site
access rights 586
adding 442
disconnecting 443
Removing a Unity Storage System 417
Removing a user from a group 79
Removing asynchronous data replication for a storage pool 532
Removing IP restrictions 150
Renaming a file system 133
Renaming a LUN 250
Renaming a share 189
Renaming a storage system 413
Replacing a volume in a pool 99
Replica 500
Replicated datasets 290, 534
Replicated pool 99
Replicated share 536
Replication
compression settings 530
encryption settings 530
network settings 528
Replication schedule
configuring 509
disabling 521
Modifying 520
Replications menu 40
Requirements and guidelines for implementing LACP 401
Reserved space 136
Resetting RAID configuration 416
Resilvering operation 110
Resource Group 91
Restarting cluster nodes 389
Restarting Unity after power failure 421, 424
Restore previous versions 216
Reverse Lookup Zone 463
Revoking access permissions
file systems or CIFS shares 197
Role-based administration in Unity 70
Rollback function 215-216, 289, 300, 604
Run a command
nstusermaps 581

S

Scheduled automatic updates 504
Scheduled replication 501
Scheduling automatic data transfer to cloud storage 546
Scheduling immutable snapshots for File System 225
Scheduling immutable snapsots for LUN 311
Scrubbing a pool
manual 95
scheduling 96
Searching for a snapshot 207, 294
secondary site 523-524
Adding 442
definition of 500

offline replication 516
Security and Permissions 75
Selecting alternate primary/secondary domain controllers 471
Selecting datasets to replicate 510
Self-Encrypting Drives (SEDs)
using 425
Send critical notification when space usage reaches 141
Server time zone 56
servicePrincipalName 456
Set the Subnet Mask, Default Gateway, and DNS on all externally-attached Nexsan storage systems 394
Setting
quota 120, 158, 353, 355, 610
reservation 136, 239
Setting a schedule for automatic snapshots 208, 302
Setting auto-deletion settings for share snapshots 217
Setting IP restrictions 147
Setting up asynchronous replication 506
Setting up SNMP notification 567
Settings tab, snapshots 208, 302
Share
considerations 117
Deleting snapshots 218
Disabling data sharing for a share 134
Enabling the Access Time mode 144
Managing snapshots 204
mapping a CIFS share to a drive 182
Rollback function 289, 604
point-in-time snapshot 215, 300
using VSS 216
searching for a snapshot 207, 294
Setting a schedule for automatic snapshots 208, 302
setting space usage 140
Snapshots Properties panel 204, 207
Settings tab 208
Sorting the list of snapshots 205, 294
Stopping snapshot browsing 214
viewing mount points 192
Share compression 142
Share definition 42, 44
Share-level refresh 442
Shares
access permissions 176
adding 174
deleting 192
name 175
Renaming 189
Sharing method
FTP 482
modifying 145
NVDIMM 481
Shutting down cluster nodes 391
Shutting down Unity storage enclosures 419, 423
Site 56
Site Administrator access 71, 583
Site definition 42-43
Site failover vs. pool failover 524
Site name 438
Site-level refresh 442
Site-level troubleshooting 477
Size of block 238
SMTP 35, 48, 106, 140, 395, 563-564, 566, 593
SMTP server settings 566
Snapshot
access rights 585
Auto-deletion settings 100
browsing a LUN snapshot 297
browsing a share snapshot 212
filtering 205, 295
LUNs 285
Manually deleting LUN snapshots 301
Manually deleting share snapshots 218
Properties panel
Settings tab 208, 302
Snapshots tab 293
Rollback function 289, 604
point-in-time snapshot 215, 300
using VSS 216
searching for 207, 294
Setting a schedule for automatic snapshots 208, 302
Setting auto-deletion settings 217
sorting 205, 294
Stopping share snapshot browsing 214
Taking a snapshot 211, 296
Snapshots
Properties panel 204, 207, 291
scheduling 241
viewing replicated snapshots 290
Snapshots menu 41
SNMP 24, 29, 35, 48, 395, 563-565, 567, 587, 593
SNMP notification 567
access rights 587
Software upgrades 447
Sorting the list of snapshots 205, 294
Source storage system 500
Space usage for a file system
viewing 130
Space usage for a LUN 105, 232, 239, 248, 254
Space usage for a share 136
Modifying 136
notification thresholds 140
Space usage notification thresholds 105
Space usage threshold violations 565
Specific domain controller 459

SQL Server 238
SSH 484
Starting aysnchronous replication 506
Starting the Performance Monitor 551
Starting Unity 421, 424
Static IP addresses 63
Stopping share snapshot browsing 214
Storage allocation 406
Storage configuration 62
Storage Configurator 408
Storage enclosures 92
  definition 42
  shutting down E-Series 419, 423
Storage menu 30
Storage panels and menus 35
Storage pool
  access rights 584
  compression 102
  creating a storage pool 90
  definition 44
  deleting 114
  Disabling a storage pool's replication schedule 521
  Manual scrub 95
  Modifying a storage pool's replication schedule 520
  Moving a pool 107
  property settings order of precedence 93
  Removing asynchronous data replication for a storage pool 532
  Replacing a volume 99
  replica 500
  Setting the scrub schedule 96
  Space usage notification thresholds 105
Storage pool I/O 550
Storage Pools menu 36
Storage systems
  renaming 413
Storage Systems menu 35
Synchronous replication
  features 538
  usage 539
System events 558
System maintenance 524
System Management definition 377
System menu 29
System menu panels and menus 33
System Preferences 29

T

Taking a snapshot 211, 296
Target CHAP authentication 86
Target storage system 500
Tasks and operations when a cluster node is down 387
Terminate asynchronous replication 532
Testing on non-production storage systems 539
Thin Provisioning 232
Time server 438
Time Server 458, 473
Time server support 452
Time zone 56, 442
Transfer of system logs 484
Transferring data manually to cloud storage 544
Troubleshooing site-level warnings and errors 477
Typical cluster implementation 386

U

UID 77, 186, 601
Unallocated disk 319
Unallocated disks 267
UNAVAILABLE 110
Understanding access rights 70
Understanding link aggregation 402
Understanding link layers 396
Understanding the CallHome feature 484
Unity 2.0 features in this release 22
Unity authentication 70, 475, 609
  Adding a group 78
  Adding a user account 76
  Adding a user to a group 79
  Changing a user's password 80
  Changing the nxadmin password 81
  Deleting a user or a group 80
Unity Authentication 73, 83, 458, 472-473
Unity definition 42
Unity navbar 28, 32
Unity roles and access rights 583
Unity Storage Systems
  remove 417
Unity system name and time zone 56
Unity System-level access rights 583
Unity System-level CHAP authentication 82
Unity Systems menu 33
Unity UI
  dashboard panel 26
  Unity navbar 28, 32
Unity, shutting down 419, 423
UNIX Access Control Lists (ACLs) 195
Unjoining a domain 472
Unlimited quota 136
Upgrading software 447
USB 447
User and Group permissions 70
User authentication modes 70
User authentication settings 452
User Management panel 35
userAccountControl 456
useradd 185
userPrincipalName 456
Using an NFS version 3 (NFSv3) client to

access an NFS share 185
Using an NFS version 4 (NFSv4) client to access an NFS share 186
Using Self-Encrypting Drives (SEDs) 425

V

Verifying
settings 128, 167, 245, 317, 410, 514
Verifying configuration settings 64
Video Streaming 238
Viewing
Events 33, 477, 484
Viewing APAL status 481
Viewing cluster health status 386
Viewing cluster license status 386
Viewing controller information 386
Viewing events 558
Viewing file system usage
file system 130
Viewing mount points 192
Viewing NVDIMM status 481
Viewing pool errors 110
Viewing replicated datasets 290, 534
Viewing snapshots 290
Viewing space usage
LUN 105, 248
Viewing user or group access rights 72, 88
Virtual volume size 239
VMWare VAAI hardware acceleration 254
Volume defintion 42, 44
Volume mixing 92
Volume replacement 99
Volume Shadow Copy Service 216, 289
VSS Hardware Provider 25, 285, 289-290
vStorage APIs for Array Integration 254, 610

W

Warning event
pool 106
When a cluster node is down 387
Windows 238
Windows Access Control Lists (ACLs) 195
Windows-based initiator 318
Workstation used to connect to the Internet 496

Z

Zero data loss and downtime 538



Nexsan Headquarters

1287 Anvilwood Avenue
Sunnyvale, CA 94089
United States of America

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 Support page:
www.nexsan.com/support

Worldwide Web
www.nexsan.com

Copyright © 2010-2026 Nexsan, Inc. All Rights Reserved.

Nexsan® is a trademark or registered trademark of Nexsan, Inc. The Nexsan logo is a registered trademark of Nexsan, Inc.

All other trademarks and registered trademarks are the property of their respective owners.

Document Reference: 20261103AM083232

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