NEXSAN

HYPER-UNIFIED STORAGE

nxadmin Command Line Interface Reference Guide v. 7.3

NEXSAN | 1287 Anvilwood Avenue | Sunnyvale, CA 94089 USA
Printed March 23, 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

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)

CE Safety: 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.

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 ..... **ix**

Audience ix
Conventions ix
Contacting Nexsan ix
Notes, Tips, Cautions, and Warnings x
Related documentation x
Safety notices xi

Chapter 1: Accessing the nxadmin and nxcmd CLIs **13**

Connecting to the Unity Storage System using SSH 13
Connecting to the Unity Storage System from the IPMI Web-based interface 14
Prerequisites 14
Connecting to the Unity Storage System via remote console 16

Chapter 2: Using the nxadmin CLI's command-based shell **17**

aclpropagate 17
arp 19
audit 21
autolog 22
bedit 23
callhome 24
cap 26
cat 27
cd 27
changeenclosureid 28
changenameservices 29
chmod 30
cleandev 36
clearjbodflags 37
cloudconnector 38
cloudcron 41
clustering 42
createlogpackage 43
dataproperty 44
date 46

diskhbcfg 48
domainname 49
drives 49
echo 50
edit 51
enforcessl 51
errorlog 52
eventflag 53
exit 53
fcstat 54
firewall 54
format 56
ftpconfig 57
groupadd 59
groupdel 60
help 60
hostname 61
ifconfig 61
immutablecron 62
info 64
intmonitoring 64
iostat 65
ipgroups 67
ipmi 69
ipmitool 70
isainfo 73
kill 74
led 74
listfcclients 77
listug 78
logrotate 78
ls 83
lun 89
maintenance 90
man 91
md5sum 91
menu 92
modgid 92
moduid 93
mpstat 93
netstat 95
ndmpsnap 99
network 100
nfs 101
nfsstat 102
nic 103
nics 113
nicstat 113
nmp 115
nscacherestart 115
nstds 116
nstfcdata 116

nstls 118
nstndmp 118
nstpool 123
nstsasdata 125
nstsharectl 128
nstusermaps 130
nstvault 133
ntpdate 134
nvram 135
nxcmd 136
nxservices 137
passwd 139
peer 139
perfmon 140
performance 142
ping 142
prompt 145
ps 146
ptree 149
pwd 150
reboot 151
replication 151
resetcache 152
resilver 152
route 153
sensors 155
services 157
setdefaultdomain 158
setip 159
sha256sum 160
shareacl 160
shares 164
showmount 164
showroutes 165
shutdown 166
siteinfo 166
smbadm 167
smbrestart 171
smbserver 171
snmpadm 173
snmpproperty 175
snmptosyslog 175
svc 176
term 178
top 178
trace 181
traceroute 186
ui 189
uptime 190
useradd 190
userdel 191
userquota 192

vmstat ... 193
vssadm ... 194
whoami ... 194
wwn ... 195
ypcat ... 196
ypinit ... 197
ypwhich ... 198

Chapter 3: Using the menu-driven nxadmin CLI ... 201

Network menu ... 202
Setting or modifying network settings ... 202
Displaying aggregation information for network interfaces ... 203
Configuring data replication settings ... 204
Configuring the network bandwidth for data replication ... 205
Configuring compression settings for data replication ... 205
Configuring the network interface for data replication ... 205
Configuring the network type for data replication ... 206
Configuring encryption settings for data replication ... 207
Configuring the buffer size for High Performance Networks (HPN) ... 207
Setting the maximum number of concurrent replications per controller ... 208
Changing the replication priority adjustment ... 208
Running a network performance test ... 209
Running a network connectivity test ... 209
Modifying IPMI settings ... 210
Switching between DHCP and Static IP addressing for the IPMI interface ... 211
Setting the IPMI password ... 211
Resetting the IPMI password to default ... 212
Clearing IPMI network settings ... 212
Setting an IP address for the Update Server ... 212
Configuring iSCSI targets ... 213
Displaying iSCSI target allocations ... 213
Recalculating iSCSI target allocations ... 214
Changing the network interface for iSCSI targets ... 215
Shut down and Reboot menu ... 216
Restarting the Unity Storage System or one of its controller nodes ... 216
Shutting down the Unity Storage System or one of its controller nodes ... 217
Obtaining the status and location of a controller node ... 218
Powering down or powering up the peer node ... 220
Restart the Web service ... 221
Run a command ... 221
chown ... 224
createlogpackage ... 224
date ... 225
fcinfo ... 226
firewall ... 227
groupadd ... 228
ifconfig ... 229
iostat ... 229
ipmitool ... 230
listug ... 231
modgid ... 232
moduid ... 232

nestpool clear ... 233
nestpool iostat ... 233
nestpool status ... 234
nfs ... 235
nic ... 236
nscacherestart ... 237
nstfcdata ... 237
nstsasdata ... 238
nstusermaps ... 240
resetcache ... 242
restartldapclient ... 242
route ... 242
sasinfo ... 243
showmount ... 244
showroutes ... 245
smbrestart ... 245
useradd ... 246
Fault Repair menu ... 247
Configure file systems and Active Directory ... 248
Setting IP-based access restrictions on a file system ... 249
Setting IP-based restrictions on a CIFS file system ... 249
Setting IP-based restrictions on an NFS file system ... 252
Enabling the no_root_squash property on an NFS file system ... 254
Setting a space usage quota on a file system ... 257
Displaying space usage quotas on file systems ... 258
Disabling the Offline Files function for a file system ... 260
Enabling the Offline Files function for a file system ... 260
Configuring the Active Directory client ... 261
Modifying the block size of a file system or a storage pool ... 261
Enabling access-based enumeration of folders and files in a CIFS file system ... 262
Configuring the LDAP Client in AD mode ... 263
Showing current LDAP client information ... 263
Initializing LDAP to Active Directory mapping ... 263
Uploading a Certification Authority (CA) certificate ... 264
Removing a Certification Authority (CA) certificate ... 265
Setting the LDAP Client configuration ... 265
Configuring the file system group lookup ... 265
Resetting the LDAP Client configuration ... 265
Clearing the nstusermaps cache ... 266
Viewing instructions on using nstusermaps for LDAP to AD mapping ... 266
Showing ACLs on file systems ... 266
Setting ACLs on file systems ... 266
Restarting the LDAP Client service ... 267
Reset the Unity Storage System ... 267
System menu ... 268

Appendix A: Enabling LACP ... 271

Understanding link aggregation ... 272
Requirements and guidelines for implementing LACP ... 272
Enabling LACP using the nxadmin CLI ... 272
Troubleshooting LACP ... 273
Disabling LACP on the Unity Storage System ... 274

Appendix B: Enabling jumbo frames using the nxadmin CLI **275**

Appendix C: Integrating with Network Information Service (NIS) **277**

Appendix D: SNMP Management Information Bases **279**

Host Resources 280
Interface 286
LM Sensor 294
RFC1213 295
SNMP Framework 295
SNMPv2 Framework 296
UCD Disk I/O 297
UCD SNMP 297

Glossary **299**

Index **311**

About this document

The *nxadmin Command Line interface Reference Guide* documents the NestOS command shell, which includes a menu-driven format, as well as a command-based shell for more advanced users. You access the NestOS CLI from any client computer with network access to the Unity Storage System, or from a console connected directly via KVM.

Audience

This guide has been prepared for the following audience:

- IT system administrators
- Engineers
- Technicians
- Any qualified NST/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.com/support Web page, 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.

Worldwide Web site:
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 Software User Guide*
- *NexsanUnity nxadmin Command-line Interface Reference Guide*
- *NexsanUnity nxcmd Command-line Interface Reference Guide*
- *NexsanUnity VMware Best Practices Guide*
- *NexsanUnity NFS Interoperability*
- *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

Accessing the nxadmin and nxcmd CLIs

The Unity Storage System provides the nxadmin and nxcmd command-line interface (CLI), which enable you to perform specific configuration and management functions from within the native NestOS command shell. You access the nxadmin CLI from any client machine with network access to the Unity Storage System, or from a console connected directly via KVM.

The nxadmin CLI includes

- a menu-driven format, as well as a command-based shell for more advanced users.
- the nxcmd command line interface, which enables you to create Nexsan storage pools, file systems, and LUNs issuing specific commands from within the NestOS command shell.

To access the nxadmin and nxcmd CLIs, see:

- Connecting to the Unity Storage System using SSH below
- Connecting to the Unity Storage System from the IPMI Web-based interface on the next page
- Connecting to the Unity Storage System via remote console on page 16

Connecting to the Unity Storage System using SSH

the Unity Storage System supports Secure Shell (SSH) connections to its operating system command shell.

To access the nxadmin CLI, you can open an SSH session to the Unity Storage System using an SSH client—for example, *Putty*—running on a client machine with network connectivity to the Unity Storage System.

Prerequisites

- Download and install an SSH client of your choice on a client machine that has network connectivity to the Unity Storage System. 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

To access the nxadmin CLI using an SSH client:

1. Launch an SSH client and enter the management virtual IP address (on the management or nx99 interface) for the Unity Storage System.
2. When the login prompt displays, type `nxadmin`, and press Enter.
3. When you are prompted for the password, type the nxadmin (Nexsan Unity Administrator) password configured on the Unity Storage System, and press Enter. This displays the nxadmin CLI prompt.

4. Type `menu` to access the menu-driven nxadmin CLI (NestOS Admin Menu), or type `help` to display the list of available commands.

Note If you are connecting to a system that has not yet been configured using the Nexsan Unity System Configuration wizard—that is, an uninitialized the Unity Storage System—you must type the default password for the nxadmin (Nexsan Unity Administrator) account: **PASSWORD** (all upper-case).

Connecting to the Unity Storage System from the IPMI Web-based interface

Use this method if you want to open a remote session to the Unity Storage System from the IPMI Web-based interface. The recommended method is using SSH or a remote console. Please see "Connecting to the Unity Storage System using SSH" (page 13)

Prerequisites

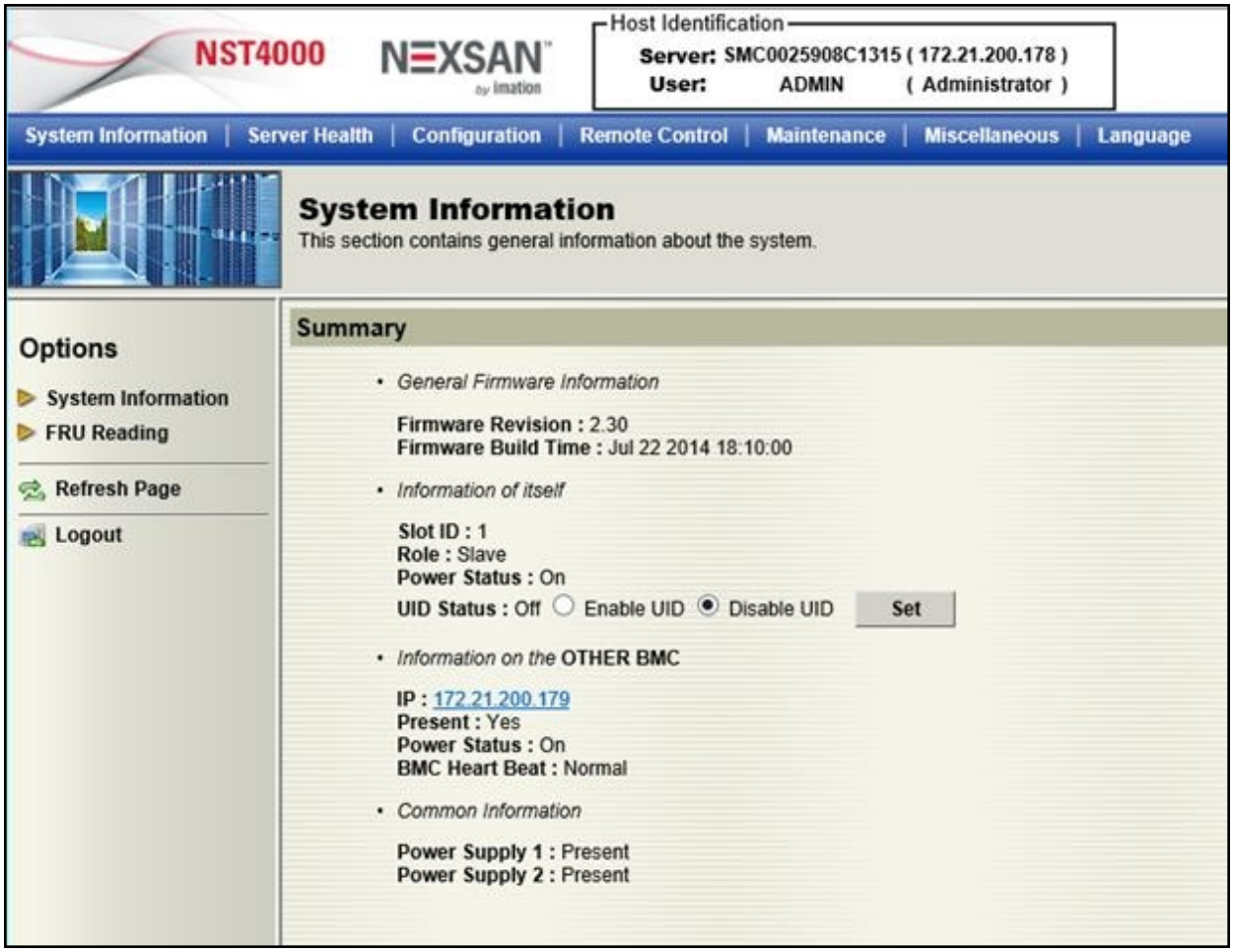
- To perform this task, you must first configure IPMI network settings for the Unity Storage System. See "Setting up the Unity Storage System" in *Nexsan Unity Software User Guide* on the Nexsan.com/support Web page.

To open a remote session to IPMI:

1. Open a Web browser on a system that is installed on the same network (and subnet) as the Unity Storage System.
2. In the Web browser's address bar, type the IPMI IP address on the Unity Storage System.
3. Once you enter the Unity Storage System's IPMI IP address in Web browser's address bar, press Enter; this launches the Unity Storage System's IPMI Web-based interface, and displays the log on dialog.
4. In the **Username** field, type **ADMIN** (all upper case).

5. Type the IMPI password in the **Password** field (the default password is **ADMIN**—all upper case). This displays the IPMI Web-based interface's main screen.

Figure 1-1: Opening an SSH session from the Unity Storage System's IPMI Web-based interface



6. To launch a remote session to the Unity Storage System, click the **Remote Control**button at the top of the IPMI Web-based interface's main screen. This opens the Remote Control page.
7. Click the **Launch Console** button on the Remote Control page.
8. The Unity Storage System's IPMI Web-based interface launches a remote session to the Unity Storage System using a Java™ viewer. If you do not have the Java™ Web launcher installed on your system, you are prompted to download and install it. Or, if you have the Java™ Web launcher installed, you are prompted to open the viewer. Install the Java™ Web launcher, or click **Yes** to continue when prompted.
9. When the remote session to the Unity Storage System opens, press Enter to display the login prompt.

► Login as to the nxadmin command shell:

1. At the login prompt, type `nxadmin`, and press Enter.
2. When you are prompted for the password, type the nxadmin (Nexsan Unity Administrator) password configured on the Unity Storage System, and press Enter. This displays the nxadmin CLI prompt.

3. Type `menu` to access the menu-driven nxadmin CLI (NestOS Admin Menu), or type `help` to display the list of available commands.

Note If you are connecting to a system that has not yet been configured using the Nexsan Unity System Configuration wizard—that is, an uninitialized the Unity Storage System—you must type the default password for the nxadmin (Nexsan Unity Administrator) account: **PASSWORD** (all upper-case).

Connecting to the Unity Storage System via remote console

The Unity Storage System provides two KVM ports (one on each controller node), which provide USB, VGA and Serial connections to the Unity Storage System. You can use these connections for a console access to the Unity Storage System.

► To connect to the Unity Storage System using KVM:

1. Plug a KVM device's cable into the KVM ports on the back of the Unity Storage System's chassis.
2. Open a remote session via KVM to the *active* node on the Unity Storage System. To determine which node is *active* on a clustered Unity Storage System (Unity versions 1.x through 2.x):
   a. Start Nexsan Unity.
   b. In Nexsan Unity's tree view, click the Unity Storage System node to display its child nodes.
   c. Click the Clusters node to display its child nodes.
   d. Click the node representing the Unity Storage System, and then open its Properties panel.
   e. Select the **Cluster Resources** tab. The Cluster Resources tab indicates the controller node where cluster resources are currently hosted: the *active* controller node will have the System Management component assigned to it.
3. When the remote session to the Unity Storage System opens, press Enter to display the login prompt.
4. At the login prompt, type `nxadmin`, and press Enter.
5. When you are prompted for the password, type the nxadmin (Nexsan Unity Administrator) password configured on the Unity Storage System, and press Enter. This displays the nxadmin CLI prompt.
6. Type `menu` to access the menu-driven nxadmin CLI (NestOS Admin Menu), or type `help` to display the list of available commands.

Note If you are connecting to a system that has not yet been configured using the Nexsan Unity System Configuration wizard—that is, an uninitialized the Unity Storage System —you must type the default password for the nxadmin (Nexsan Unity Administrator) account: **PASSWORD** (all upper-case).

Chapter 2

Using the nxadmin CLI's command-based shell

CAUTION: The section describes advanced functions and features intended for use by system administrators. If you are unsure of a specific command or function, and how it may impact your storage infrastructure, please contact Nexsan Support for assistance, or to obtain more information.

The nxadmin CLI's command-based shell provides a full set of command-based options for configuring advanced settings on Unity, as well as for displaying information about the system (such as, network and disk I/O metrics, disk information, etc.) and the status and health of specific system components.

To use a command, simply type the command using the appropriate syntax. This section uses this syntax format:

```
command name [-option] [-option parameter|parameter] [-option <user input>]
```

- options are enclosed within square brackets: [ ]
- options having a choice of parameters use a vertical bar to separate the choices: |
- user input required for some options is enclosed within angle brackets: < >

For most commands, you can display usage syntax and available options and switches by simply typing the corresponding command at the prompt; for example, to display usage syntax for the `nstpool` command, type `nstpool` at the nxadmin CLI's prompt.

In addition, you can display help information for each command:

- type `help` before the command to display extensive help content; for example, `help eventflag`. Alternatively, you can use `man` before the command; for example, `man eventflag`.
- type `-?` after the command to view usage information.

aclpropagate

To run this command:

1. Access the CLI command shell—see Accessing the nxadmin and nxcmd CLIs on page 13.
2. Type the command using the syntax provided in this topic.
3. Press Enter.

Description	This command propagates file system-level ACL permissions to all folders, sub-folders, and files in the file system. You can use the command to either propagate all file system-level ACL permissions to the file system's contents, or only a single ACL.

Notes:

- You can only run this command for file systems currently hosted on this controller node. To modify file systems on the peer controller, log on to the corresponding node (or use the peer command to access the node directly).
- To modify file system ACL permissions, use the shareacl command (or Nexsan Unity).

Controller — Run this command on both controllers.

Syntax

```
aclpropagate
[-s <file system name>]
[-n <acl name>]
[-c <command>]
```

Options

`-s <file system name>`

This option specifies the name of the file system to modify.

`-n <acl name>`

This option specifies the file system's ACL permission to propagate.

`-c <command>`

This option specifies the sub-command to be executed by the `aclpropagate` command. The allowed sub-commands are:

- `show` displays the file system(s) on the current controller and their corresponding ACL permissions. It can be used optionally with `-n`.
- `propagateall` recursively overwrites all ACLs permissions for folders, sub-folders, and files in the specified file system, to correspond with the ACL permissions of the file system. It must be used with the `-s` option.
- `add` recursively propagates a specific ACL permission to the file system's contents. It must be used with the `-s` and `-n` options.

  CAUTION: This will not check if an entry already exists, a duplicate is created if an entry already exists.
- `remove` removes a specific ACL permission from the file system, and also (recursively) from all folders, sub-folders, and files in the file system. It must be used with the `-s` and `-n` options.

  CAUTION: If multiple entries exist with the same name and permissions, all entries are removed. If there are multiple instances of an entry with different permissions, only the first instance is removed.

Example 1 — We display the current ACL permissions for a file system.

```
aclpropagate -c show -s file system1
pool: pool1 file system: file system1
Permissions Name
rwxpdDaARWcCos:fd-----:allow owner@
--------------:fd-----:allow group@
```

```
rwxpdDaARWc--s:fd-----:allow everyone@
------a-------:-------:allow user:nobody
r-x---a-R-c--s:fd-----:allow user:admin-user@mydomain.net
r-x---a-R-c--s:fd-----:allow user:richard@mydomain.net
r-x---a-R-c--s:fd-----:allow group:Users Of Backup
System@mydomain.net
```

Example 2 We propagate an entry to the files and folders in the file system.

```
aclpropagate -c add -s file system1 -n "group:Users Of Backup
System@mydomain.net"
pool: pool1 file system: file system1
Permissions Name
r-x---a-R-c--s:fd-----:allow group:Users Of Backup
System@mydomain.net
```

arp

To run this command:

1. Access the CLI command shell—see Accessing the nxadmin and nxcmd CLIs on page 13.
2. Type the command using the syntax provided in this topic.
3. Press Enter.

Description This command enables you to display and modify the Internet-to-MAC address translation tables used by the address resolution protocol (ARP).

With no options, this command displays the current ARP entry for a specific host. The host can be specified using a name or an IP address.

Controller Run this command on the controller where you want to view or change the Internet-to-MAC address translation tables.

Syntax

```
arp
<host name>
[-a [-n]]
[-d <host name>]
[-f <file name>]
[-s <host name> <MAC address> [temp] [pub] [trail] [permanent]]
```

Options

`<host name>`

This option is used to specify the host for which you wish to perform ARP commands. The host can be specified by name or by IP address.

`-a`

This option displays all of the current ARP entries. The definitions of the flags in the table are:

- d: Unverified. This is a local IP address that is currently undergoing Duplicate Address Detection. ARP cannot respond to requests for this address until Duplicate Address Detection is complete.
- o: Old. This entry is aging. If the IP requests it again, a new ARP query is generated. This state is used for detecting peer address changes.
- y: Delayed. Periodic address defense and conflict detection was unable to send a packet due to internal network use limits for non-traffic-related messages (100 packets per hour per interface). This occurs only on interfaces with a large number of aliases.
- A: Authority. This machine is authoritative for this IP address. ARP does not accept updates from other machines for this entry.
- L: Local. This is a local IP address configured on one of the machine's logical interfaces. ARP defends this address if another node attempts to claim it.
- M: Mapping. Only used for the multicast entry for 244.0.0.0.
- P: Publish. Includes IP addresses for the machine and the addresses that have explicitly been added by the -s option. ARP responds to ARP requests for this address.
- S: Static. Entry cannot be changed by learned information. This indicates that the permanent flag was used when creating the entry.
- U: Unresolved. Waiting for an ARP response.

The option -n can be added to -a to disable the automatic numeric IP-address-to-name translation. Use arp -an or arp -a -n to display numeric IP addresses only.

-d <host name>

This option is used to delete an entry for the specified host.

-f <file name>

This option is used to read the specified file and set multiple entries in the ARP tables. Entries in the file should be in the form of:

<host name> <MAC address> [temp] [pub] [trail] [permanent]

See -s for argument definitions.

-s <host name> <MAC address>

This option is used to create an ARP entry for the specified host using its MAC address. This option takes the following optional arguments:

- temp: Used to allow the entry to be subject to deletion by aging.
- pub: Used to publish the entry, meaning that the system responds to arp requests for this host even though the <host name> is not its own.
- permanent: Used to make the entry permanent, meaning that the system does not accept MAC address changes for the host from the network.

Note: The system does not implement trailer encapsulation, and the word trail is accepted on entries for compatibility purposes only.

Example

We delete an ARP entry for the host named Finance1.

```
arp -d Finance1
Finance1 (172.21.12.33) deleted
```

audit

To run this command:

1. Access the CLI command shell—see Accessing the nxadmin and nxcmd CLIs on page 13.
2. Type the command using the syntax provided in this topic.
3. Press Enter.

Description

This command displays a history of commands run by the nxadmin user. The system displays audit history for multiple sessions, but only a limited amount of history is retained.

Controller

Run this command on the controller for which you wish to view the command history.

Syntax

```
audit
[-c <command> [-n <number of lines>] [-u <user name>]]
```

Options

`-c`

This option specifies the command to run. Currently, the only supported command is `show`. Nevertheless, this option is required.

`-n`

This option specifies the number of lines of history to retrieve. When not specified, `audit` returns all available history.

`-u`

This option specifies the user name. Currently, the only user supported is **nxadmin**. When not specified, `audit` returns the history for **nxadmin**.

Example

```
audit -c show -n 5
2013.07.30-20.08.44.844 - nxadmin 172.21.11.29 54937
172.21.12.100 - userquota
2013.07.30-20.19.08.567 - nxadmin 172.21.11.29 54937
172.21.12.100 - exit
2013.07.31-20.36.25.251 - nxadmin 172.21.11.29 56999
172.21.12.100 - exit
2013.08.01-13.32.20.649 - nxadmin 172.21.11.29 53415
172.21.12.100 - menu
2013.08.01-14.16.19.986 - nxadmin 192.168.200.131 49845
172.21.12.1 - audit -c show -n 5
```

autolog

To run this command:

1. Access the CLI command shell—see Accessing the nxadmin and nxcmd CLIs on page 13.
2. Type the command using the syntax provided in this topic.
3. Press Enter.

Description

This command enables you to upload logs to Nexsan Technical Support based on a pre-defined or customized schedule.

Notes:

- It must first be enabled on our License Servers for your Unity Storage System. Please contact Nexsan Support for details; for contact information to our Support group, please visit our Web site: https://www.nexsan.com/support.
- This command can only be run when the CallHome service is stopped. Use the `callhome stop` command to stop the CallHome service.
- The current version of `callhome`, which is 0.1, does not display the `autolog` command. You must update `callhome` to the new version to be able to view and use the `autolog` command.

2

Controller

Run this command on the controller having the issue.

Syntax

```
autolog
[-c enable|update|reset|disable|status]
[-t time]
[-d day(s)]
```

Options

`-c enable`

This option enables the `autolog` command to send logs.

`-c update`

This option updates the days and time if the `autolog` command is already enabled. Optionally, use `-t` and `-d` to set custom time values. If you do not use custom time values, the default recommended values are used.

`-c reset`

This option resets the days and time to the default recommended values.

`-c disable`

This option disables the `autolog` command. No logs will be sent anymore.

`-c status`

This option provides status of the automatic sending of logs for both controller nodes.

`-t <time>`

This option specifies the time to upload the logs. Use a 24-hour format.

`-d <day(s)>`

This option specifies the days to send the logs. The default is every day. The format is a number from `0` to `6`, `0` being Sunday. You can specify multiple days; for example:

- To specify only weekdays, use `-d 1,2,3,4,5`
- To specify only weekends, use `-d 6,0`

Example

We enable the `autolog` command and we configure the schedule settings to send logs to Technical Support automatically every day of the week, at 8:30 p.m.

1. Update the `callhome` command to the new version.
2. Try the `autolog` command:

   `autolog`

   The command should display the available options.
3. Stop the CallHome service:

   `callhome stop`
4. Enable the `autolog` command:

   `autolog -c enable`

   The command retrieves the recommended schedule settings from the License Server over the Internet.
5. Configure the schedule using custom values:

   `autolog -c update -d 1,2,3,4,5 -t 20:30`

bedit

To run this command:

1. Access the CLI command shell—see Accessing the nxadmin and nxcmd CLIs on page 13.
2. Type the command using the syntax provided in this topic.
3. Press Enter.

Description

This command opens a basic file viewer/editor that enables you to open and modify a file.

To exit the file, press the **Tab** key to highlight `Save and Quit` or `Quit without Saving` and press Enter.

Notes:

- The editor used by the `bedit` command is different from the one used by the `edit` command.
- When opening a read-only file, `bedit` will not allow you to save any changes.

Controller

Run this command on the controller where the file you wish to edit is stored.

Syntax

```
bedit [<file name>]
```

Options

`<file name>`

This option specifies the file that you wish to open and edit. To open a file in a different directory, specify the full path name; for example, `bedit /etc/hosts`.

callhome

To run this command:

1. Access the CLI command shell—see Accessing the nxadmin and nxcmd CLIs on page 13.
2. Type the command using the syntax provided in this topic.
3. Press Enter.

Description

This command provides access to the Call Home service. It allows Nexsan Technical Support personnel to connect to the Unity Storage System and troubleshoot issues remotely.

To use the CallHome service, the Unity Storage System must have Internet access and at least one of these ports must be open and allowed between the Unity Storage System and the network firewall:

- 20022
- 80

CAUTION: Run this command only if requested by Nexsan Technical Support.

Note: To send logs automatically to Technical Support, you must stop the Call Home service and then enable the `autolog` command.

Controller

Run this command on the controller having the issue.

Syntax

```
callhome
[start]
[stop]
[status]
[setclient <IP> <port>]
[test]
[hosts]
[monitor]
[sendlogs]
[update]
[suspend]
[resume]
[reset]
[version]
```

Options

`start`

This option starts the CallHome service.

`stop`

This option stops the CallHome service.

`status`

This option displays the status of the CallHome service.

`setclient <IP> <port>`

This option enables you to connect to the CallHome service from a workstation. Enter the IP address and the port number of the client.

`test`

This option tests connectivity to all known CallHome service hosts.

`hosts`

This option lists all SSH and HTTP CallHome servers to which the CallHome service is connected. It lists the server's IP address or domain name and the SSH port number. The connection is always over SSH. If a direct SSH connection is not possible, the system will connect to CallHome servers using SSH over HTTP. In this case, this option will also display the HTTP server's IP address and port number.

`monitor`

This option monitors the I/O traffic during a CallHome session. It displays the Sent and Received packets approximately once per second. Press any key to stop the monitoring session and return to the prompt.

`sendlogs`

This option packages and sends logs to the CallHome server.

Note: This command can only be run when the CallHome service is stopped.

`update`

This option checks if there are updates of the CallHome version.

`suspend`

This option pauses the sending of event driven logs to the Unity Storage System.

`resume`

This option resumes the sending of event driven logs to the Unity Storage System.

`reset`

This option resets the triggers to send event driven logs to the Unity Storage System.

`version`

This option returns the CallHome service version. This command is enabled after updating the `callhome` command to its latest version, if you are running an older build of Unity [[[Undefined variable Unity.Firmware Version]]] and you have never used the `callhome`command. See the example below to enable and run this command.

Example 1 We check the status of the CallHome service.

```
callhome status
The CallHome service is not running.
```

Example 2 We start the CallHome service.

```
callhome start
Starting CallHome service... Done.
```

Example 3 We update the `callhome` command to the new version, then we check if the version is higher than `0.1`.

1. Start the CallHome service:

   `callhome start`

2. Wait for a few minutes, until the nxadmin CLI restarts automatically:

   ```
   SSH shell interrupted.
   The connection to the SSH shell was broken. The system will attempt to reconnect in 5 seconds.
   Copyright 2010-2014 Nexsan Technologies Inc. All Rights Reserved.
   Loading shell... Ready.
   Type 'help' for command list.
   Type 'menu' for system menu.
   ```

3. The `callhome` command is now updated. Verify the new version:

   `callhome version`

   ```
   Version: 5.38.0.0
   ```

2

cap

To run this command:

1. Access the CLI command shell—see Accessing the nxadmin and nxcmd CLIs on page 13.
2. Type the command using the syntax provided in this topic.
3. Press Enter.

Description This command performs a capture of logging information and saves it in a log package to be sent to Nexsan Support. The log files are rotated as each one fills up.

Controller Run this command on the controller where the logging information you want to capture is stored.

Syntax `cap <argument>`

In the NestOS nxadmin, enter `callhome sendlogs cap` or `createlogpackage cap`. Also, you can enter `cap` on the NestOS command line for details.

Arguments `-c command`

Commands to run:

`capture` Starts a capture.

`show` Shows the currently running capture.

`stop` Stops the currently running capture.

`-p port` Port to capture.

Examples:

`80` Useful for the UI.

`-h host`

The hostname to filter. IP address or resolvable name.

`-t time`

Amount of time to capture in seconds, or suffix `m` for minutes, `h` for hours.
The default is 5 minutes.

`-P size`

Packet Size. Default is 0 which grabs the entire packet. Some protocols will benefit from a lower size.

`-i interface`

Interface to capture. Make sure that routing is taken into account when deciding which interface to capture from.
Examples:
`nx99` management interface, useful for the UI.
`nx0` data interface.

cat

To run this command:

1. Access the CLI command shell—see Accessing the nxadmin and nxcmd CLIs on page 13.
2. Type the command using the syntax provided in this topic.
3. Press Enter.

Description	This command displays the contents of a file in the terminal window.
Controller	Run this command on the controller where the file you wish to view is stored.
Syntax	`cat <filename>`
Options	`<filename>` This option is used to specify the name of the file to be displayed in the terminal window. If you are in a different directory than the file you wish to display, enter its full path name; for example, `cat /etc/hosts`.

cd

To run this command:

1. Access the CLI command shell—see Accessing the nxadmin and nxcmd CLIs on page 13.
2. Type the command using the syntax provided in this topic.
3. Press Enter.

Description	This command enables you to change working directories. The accessible directories are `etc`, `bin`, `log`, and `pools`. To go up a level, use a double period (`..`).

Controller — Run this command on the controller where the directory you wish to navigate to is located.

Syntax — `cd <directory> | ..`

Options — `<directory>`

This option specifies the name of the directory that you wish to navigate to.

`..`

This option tells the `cd` command to go up one level in the directory hierarchy.

Example —
```
ES156190-001-01:P:/> cd log
ES156190-001-01:P:/log>
```

changeenclosureid

To run this command:

1. Access the CLI command shell—see Accessing the nxadmin and nxcmd CLIs on page 13.
2. Type the command using the syntax provided in this topic.
3. Press Enter.

Description — This command enables you to change the storage system (enclosure) ID after replacing its chassis. When you add a storage system to Unity, its configuration, including the chassis ID, is saved in the system.

If you replace the chassis of a storage system, the new chassis will have a different ID. The Unity Storage System detects the new chassis but does not have any configuration saved for it. The old chassis is still configured on the Unity Storage System but it cannot be detected anymore since it is no longer connected. For this reason, when you replace a storage system's chassis, you need to run the `changeenclosureid` command to update the chassis ID in the configuration file.

Controller — Run this command on any controller.

Syntax — `changeenclosureid`

Options — None

Example —

1. Type **`changeenclosureid`**.

2. The Unity Storage System will display output similar to this:

```
Loading...
Storage enclosure ID replacement:
Storage enclosures that have a stored configuration but are no longer detected:
2152: US224 (2152) (US224)
Storage enclosures that do not have a stored configuration and are detected:
2153: US224 (2153) (US224)
Press enter to choose the default value (ex.: [default])
Which storage enclosure would you like to replace? [2152]:
```

3. In most cases, the Unity Storage System will detect one storage system. (If you changed two chassis, the system will detect two new storage systems.) Press Enter to select the old storage system.
4. You are then prompted to select the new storage system.

```
Which storage system would you like to replace it with? [2153]:
```

   Press enter to select it. The Unity Storage System updates the configuration files.

```
Applying changes to configuration files.
Changes applied successfully.
```

5. Refresh Unity to view the replaced storage system.

changenameservices

To run this command:

1. Access the CLI command shell—see Accessing the nxadmin and nxcmd CLIs on page 13.
2. Type the command using the syntax provided in this topic.
3. Press Enter.

Description	This command defines the properties of naming services. You can add or remove switches, or show if the switch is configured. For NIS integration, this command reconfigures the `etc/nsswitch.conf` file after changing the authentication mode in the user interface so that the NIS authentication settings are added to the password and group files. For steps to integrate NIS, see Integrating with Network Information Service (NIS).
Controller	Run this command on both controllers.

Syntax	`changenameservices`
	`-c <command>`
	`-s <switch>`

Options	`-c`

This option lets you run one of the following commands:

- `add`: Adds the specified switch to nameservices.
- `remove`: Removes the specified switch from nameservices.
- `show`: Shows whether or not the switch is configured.

`-s`

This option lets you specify a switch to run a command on. Currently, the only supported switch is `nis`, which is used for NIS integration.

Example

```
changenameservices -c add -s nis
Setting the current node...
Setting the peer node...
```

chmod

To run this command:

1. Access the CLI command shell—see Accessing the nxadmin and nxcmd CLIs on page 13.
2. Type the command using the syntax provided in this topic.
3. Press Enter.

Description

This command changes file permissions.

TIP: Use `helpacl` to view help on this command, as follows: `chmod helpacl`.

NOTE: This command is intended for advanced users, and thus should be used with caution.

Controller

Run this command on the controller where the files are located.

Syntax

```
chmod [-fR] absolute-mode file
chmod [-fR] symbolic-mode-list file
chmod [-fR] acl_operation file
chmod [-fR] [-@ named_attribute] attribute_specification_list
file
chmod [filesystems]
chmod [helpacl]
chmod [help]
```

Options

`-f`

This is the Force option. `chmod` does not complain if it fails to change the mode of a file.

`-R`

This option recursively descends through directory arguments, setting the mode for each file. When symbolic links are encountered, the mode of the target file is changed, but no recursion takes place.

`-@ named_attribute`

Performs the attribute operation on the named extended attribute file of each file operand instead of the file operand itself. If multiple `-@` operations are supplied, the attribute specification mode is applied to each of the named attribute files.

A named attribute of `*` carries meaning to `chmod`, and is considered to mean all extended attribute files associated with a file operand. This does not refer to the special files `.` and `...`

A named attribute of `..` carries special meaning to `chmod`, and is considered to mean the file operand itself. This allows the command to apply the attribute specification mode to the specified named attribute file of the file operand and the file operand itself.

Absolute Mode

```
chmod [-fR] absolute-mode file
```

The `absolute-mode` argument is specified using octal numbers `nnnn` defined as `n`, a number from 0 to 7. An absolute mode is constructed from the OR of any of the following modes:

- `4000`: Sets user ID on execution.
- `20#0`: Sets group ID on execution if `#` is 7, 5, 3, or 1. Enables mandatory locking if `#` is 6, 4, 2, or 0. For directories, files are created with BSD semantics for propagation of the group ID. With this option, files and subdirectories created in the directory inherit the group ID of the directory, rather than of the current process. For directories, the setgid bit can only be set or cleared by using symbolic mode.
- `1000`: Turns on sticky bit.
- `0400`: Allows read by owner.
- `0200`: Allows write by owner.
- `0100`: Allows execute (search in directory) by owner.
- `0700`: Allows read, write, and execute (search) by owner.
- `0040`: Allows read by group.
- `0020`: Allows write by group.
- `0010`: Allows execute (search in directory) by group.
- `0070`: Allows read, write, and execute (search) by group.
- `0004`: Allows read by others.
- `0002`: Allows write by others.
- `0001`: Allows execute (search in directory) by others.
- `0007`: Allows read, write, and execute (search) by others.

Symbolic Mode

```
chmod [-fR] symbolic-mode-list file
```

The symbolic-mode-list argument is a comma-separated list (with no intervening white space) of symbolic mode expressions of the form:

`[who]` *operator* `[permissions]`

Operations are performed in the order given. Multiple permissions letters following a single operator cause the corresponding operations to be performed simultaneously.

- `who`: zero or more of the characters `u` (user's permissions), `g` (group's permissions), `o` (others' permissions), and `a` (all permissions for users, groups and others) specifying whose permissions are to be changed or assigned.
- `+`, `-` or `=` operator, signifying how permissions are to be changed:
  - `+`: Add permissions. If permissions are omitted, nothing is added. If `who` is omitted, adds the file mode bits represented by permissions, except for the those with corresponding bits in the file mode creation mask. If `who` is present, adds the file mode bits represented by the permissions.
  - `-`: Take away permissions. If permissions are omitted, do nothing. If `who` is omitted, clear the file mode bits represented by permissions, except for those with corresponding bits in the file mode creation mask. If `who` is present, clear the file mode bits represented by permissions.
  - `=`: Assign permissions absolutely. If `who` is omitted, clears all file mode bits; if `who` is present, clears the file mode bits represented by `who`. If permissions are omitted, does nothing else. If `who` is omitted, adds the file mode bits represented by permissions, except for the those with corresponding bits in the file mode creation mask. If `who` is present, add the file mode bits represented by permissions.
- The permission can be any compatible combination of the following letters. Permissions to a file can vary depending on your user identification number (UID) or group identification number (GID). Permissions are described in three sequences each having three characters rwx.
  - `l`: mandatory locking
  - `r`: read permission
  - `s`: user or group set ID
  - `t`: sticky bit
  - `w`: write permission
  - `x`: execute permission
  - `X`: execute permission if the file is a directory or if there is execute permission for one of the other user classes
  - `u`, `g`, `o`: indicates that permission is to be taken from the current user, group or other mode respectively.

ACL Operation `chmod [-fR] acl_operation file`

An Access Control List (ACL) is a list of Access Control Entries (ACEs), each of which define access permissions for a particular class of user. The list of ACEs is numbered, starting from zero. The position of an ACE within an ACL is called an *index*. This index is used as an argument in many of the chmod commands described below.

An ACL operation ommand line has the following format:

```
chmod [options]A[index]- file ...
chmod [options]A-acl_specification file ...
chmod [options]A[index]{+|=}acl_specification file ...
```

Where `acl_specification` is a comma-separated list (with no intervening whitespace) of the form:

- `A[index]+acl_specification`: Prepends the access control entries (ACE) specified in acl_specification to the beginning of the file's ACL. Depending on the file system, the ACL can be reordered when applied to the file. If the optional index is specified, then new ACEs are inserted before specified index.
- `A-`: Removes all ACEs for current ACL on file and replaces current ACL with new ACL that represents only the current mode of the file.
- `Aindex-`: Removes ACE specified by index number.
- `A-acl_specification`: Removes ACEs specified by *acl_specification*, if they exist in current file's ACL.
- `A=acl_specification`: Replaces a files entire ACL with *acl_specification*.
- `A [index]=acl_specification`: Replaces ACEs starting at a specific index number in the current ACL on the file. If multiple ACEs are specified, then each subsequent ACE in acl_specification replaces the corresponding ACE in the current ACL.

The permissions argument is a (`/`) separated string of the following flags:

Note: Other flags may appear but are not supported.

- `read_data (r)`: Permission to read the data of a file.
- `list_directory (r)`: Permission to list the contents of a directory.
- `write_data (w)`: Permission to modify a file's data anywhere in the file's offset range.
- `add_file (w)`: Permission to add a new file to a directory.
- `add_subdirectory (p)`: Permission to create a subdirectory to a directory.
- `read_xattr (R)`: Ability to read the extended attributes of a file.
- `write_xattr (W)`: Ability to create extended attributes or write to the extended attribute directory.
- `execute (x)`: Permission to execute a file.
- `read_attributes (a)`: The ability to read basic attributes (non-ACLs) of a file.
- `write_attributes (A)`: Permission to change the times associated with a file or directory to an arbitrary value.
- `delete (d)`: Permission to delete a file.
- `delete_child (D)`: Permission to delete a file within a directory.
- `read_acl (c)`: Permission to read the ACL of a file.
- `write_acl (C)`: Permission to write the ACL of a file.
- `write_owner (o)`: Permission to change the owner of a file.

There are permissions aliases that set multiple flags using the following:

- `full_set`: All permissions.

- modify_set: All permissions except write_acl and write_owner.
- read_set read_data, read_acl, read_attributes, and read_xattr.
- write_set write_data, append_data, write_attributes, and write_xattr.

The inheritance argument is a / separated string of the following flags:

- file_inherit (f): Inherit to all newly created files.
- dir_inherit (d): Inherit to all newly created directories.
- inherit_only (i): When placed on a directory, do not apply to the directory, only to newly created files and directories. This flag requires that either file_inherit and/or dir_inherit is also specified.
- no_propagate (n): Indicates that ACL entries should be inherited to objects in a directory, but inheritance should stop after descending one level. This flag is dependent upon either file_inherit and/ or dir_inherit also being specified.

Attribute Operation

```
chmod [-fR] [-@ named_attribute] attribute_specification_list file
```

The attribute_specification_list argument is the character S followed by a comma-separated list of one or more attribute_specifications. Each attribute_specification is of the form [operator]attribute_specifier.

An operator is one of the following:

- +: Each attribute specified by the associated attribute_specifier is adjusted to match the value specified by the attribute_specifier.
- -: Each attribute specified by the associated attribute_specifier is adjusted to match the inverse of the value specified by the attribute_specifier.
- =: Each attribute specified by the associated attribute_specifier is adjusted to match the value specified by the attribute_specifier. Any boolean read-write extended system attributes associated with the current file that are not specified by attribute_specifier is cleared.

If an operator is not specified in an attribute_specification, chmod behaves as if + had been specified.

An attribute_specifier takes one of the following values:

- a: Sets all boolean read-write extended system attributes associated with the current file.
- c[*compact_attribute_setting*]: Sets each boolean read-write extended system attribute identified by compact_attribute_list. A compact_attribute_list is a list of zero or more adjacent attribute abbreviation characters from list of Attribute Names and Abbreviation Characters later in this section. An arbitrary number of hyphen (-) characters can be included in a compact_attribute_list. These are ignored.

- `v[verbose_attribute_setting]`: Sets each boolean read-write extended system attribute identified by `verbose_attribute_setting`. A `verbose_attribute_setting` is an attribute name from the list of Attribute Names and Abbreviation Characters later in this section, optionally, immediately preceded by no. If the attribute name is used without no, the attribute is set; otherwise the attribute is cleared.
- A `verbose_attribute_setting_list` is zero or more comma-separated `verbose_attribute_settings`.

Multiple operations specified for a file are accumulated and are all set for a file operand as a single attribute setting operation. If an attribute is specified more than once in an `attribute_specification_list`, the last specified operation is applied.

List of Attribute Names and Abbreviation Characters:

- `hidden (H)`
- `sparse (s)`
- `system (S)`
- `readonly (R)`
- `archive (A)`
- `nounlink (u)`
- `immutable (i)`
- `appendonly (a)`
- `nodump (d)`
- `av_quarantined (q)`
- `av_modified (m)`

file systems

Displays all Unity Storage System file systems and their folders. To change permissions on a file system, you must enter the exact path of the file system; for example, `/pools/pool name/file system name`.

`helpacl`

Displays the complete help for the `chmod` command.

`help`

Displays the basic help for the `chmod` command.

Example

► To display the Unity Storage System's file systems:

```
chmod file systems
```

```
File system            Node      Folder
s2p1                   1         /pools/p1/s2p1
```

► To change permission on a file in a file system:

```
chmod o+x /pools/pool1/filesystem1/file1
```

cleandev

To run this command:

1. Access the CLI command shell—see Accessing the nxadmin and nxcmd CLIs on page 13.
2. Type the command using the syntax provided in this topic.
3. Press Enter.

Description

This command manually rediscovers connected Unity Storage Systems. It does so by first attempting to load every driver in the system and attach to all possible device instances, then creating logical links to device nodes in the `dev` and `devices` directories, then loads the device policy.

Controller

Run this command on the controller to which the Unity Storage Systems you wish to rediscover are attached.

Syntax

```
cleandev
[-c <deviceclass>]
[-C]
[-i <drivername>]
[-l <modulepath>]
[-n]
[-r <rootdir>]
[-s]
[-t <devlinktablefile>]
[-v]
```

Options

`-c <deviceclass>`

This option restricts `cleandev` operations to devices of the specified class. The possible values are `disk`, `port`, or `pseudo`. This option can be used multiple times to specify multiple types.

`-C`

This option cleans up dangling `dev` links that are not normally removed. If a device class is specified using the `-c` option, this option only cleans up `dev` links for the specified device class or classes.

`-i <drivername>`

This option restricts the cleaning process to devices for the named driver.

`-n`

This option prevents drivers from being loaded or new nodes from being added to the kernel device tree.

`-r <rootdir>`

This option looks for the `dev` directory trees in the specified root directory rather than at the root itself.

`-s`

This option suppresses any changes to the `dev` folder. When used with the `-v` option, this can be useful for debugging.

`-t <devlinktablefile>`

This option reads the named `devlink.tab` file instead of the default file, which is `/etc/devlink.tab`.

`-v`

This option displays changes in verbose mode.

Example **`cleandev -C -v`**

```
devfsadm[13519]: verbose: removing file: /dev/smp/expd0
devfsadm[13519]: verbose: removing file: /dev/cfg/c5
devfsadm[13519]: verbose: removing file: /dev/cfg/c6
devfsadm[13519]: verbose: removing file: /dev/usb/device1
devfsadm[13519]: verbose: removing file: /dev/usb/device0
devfsadm[13519]: verbose: removing file: /dev/usb/hub1
devfsadm[13519]: verbose: removing file: /dev/usb/hub6
devfsadm[13519]: verbose: removing file: /dev/usb/hub2
devfsadm[13519]: verbose: removing file: /dev/usb/hub5
devfsadm[13519]: verbose: removing file: /dev/usb/hub7
devfsadm[13519]: verbose: removing file: /dev/usb/hub0
devfsadm[13519]: verbose: removing file: /dev/usb/hub4
devfsadm[13519]: verbose: removing file: /dev/usb/hub3
devfsadm[13519]: verbose: removing file:
/dev/rdsk/c2t5000C50025F85083d0s2
devfsadm[13519]: verbose: removing file:
/dev/rdsk/c2t5000C50025F85083d0s8
devfsadm[13519]: verbose: removing file:
/dev/rdsk/c2t5000C50025F8741Fd0s13
devfsadm[13519]: verbose: removing file:
/dev/rdsk/c2t5000C50025F869DBd0p4
devfsadm[13519]: verbose: removing file:
/dev/rdsk/c2t5000C50025F870ABd0s12
```

clearjbodflags

To run this command:

1. Access the CLI command shell—see Accessing the nxadmin and nxcmd CLIs on page 13.
2. Type the command using the syntax provided in this topic.
3. Press Enter.

Description This command resets failure and predicted failure flags on external JBODs.

Note: This command does not display a confirmation message.

Controller Run this command on either controller.

Syntax	`clearjbodflags`
Options	None

cloudconnector

To run this command:

1. Access the CLI command shell as described in "Accessing the nxadmin and nxcmd CLIs" (page 13)
2. Type the command using this syntax.
3. Press Enter. TheUnity displays your current prompt settings and the available variables you can choose to change the prompt display.
4. Enter the new prompt format.
5. Press Enter.

Description	The Cloud Connector command enables you to sync and to manage files between local file systems and remote cloud storage.
Controller	You can run these commands on any controller
Command Groups	There are three different groups of commands, • Config management commands • Job management commands • Functional commands Within each group, there is a set of sub-commands described below.

Config Management Commands	To access a cloud storage system, first you need to create a configuration with a unique name, as well as access information including a login id and password. This config is stored in the Unity local controller.
config create syntax	`cloudconnector config create <name> <AWS|UnityCloud|AzureBlob|AzureFiles|.> -a access_key -s secret_access_key -e endpoint <endpoint|Azure share URL>` The config create command is used to create a config for S3 compatible cloud storage, in this example using AWS and Unity Object Store.
config delete syntax	`cloudconnector config delete <name>` The config delete command is used to delete the config, specified by the name.

config show syntax	`cloudconnector config show`
	The config show command is used to show all the configs that have been created. For each config, it shows the name, type, provider, and endpoint. It does not show password and access key. For example,
	`> cloudconnector config show`

```
[myunity]
type = s3
provider = <provider name>
endpoint = https://<ip address>
```

config showkeys syntax

```
cloudconnector config showkeys
```

The config showkeys command is used to show all the information of all the configurations, including password and access keys. This command is hidden, so not exposed to the users.

Job Management Commands

The main functions of Cloud Connector are to sync, copy, or move files; between a local file system and cloud storage, between two file systems, or between two cloud storage systems. When working on a large amount of files, this command may take some time to complete, making it inconvenient to run in the foreground. Therefore by default, the cloudconnector will automatically create a job for the command to run in the background.

syntax

```
cloudconnector <copy|sync|move> source:path dest:path [-F|-N jobname]
```

The option [-F], is to run this command in foreground.

The option [-N jobname], is to set a name for the job. The name will be part of the final name of the job, which is in this format:

YYYYmmdd_HHMMSS_<jobname>_<unique-code>

Note: The program only uses the first 10 characters of the jobname input by the user. If no [-N jobname] is applied, Cloud Connector will automatically create a name in this default format: YYYYmmdd_HHMMSS_<cmd>_<unique-code>. The automated method makes the name unique and easily recognizable.

jobs syntax

```
cloudconnector jobs
```

The cloudconnector jobs command lists all jobs,including job name, status, and other info, sorted by most to the least recent job, and automatically assigns an id number. The list is sequenced starting with id number 1 for the most recent job. This id number is used as a job id in the other commands.

For example, the following job list contains the columns: job id, job name, type (manual or scheduled), starting time, status(eg.done), and job command.

```
[1] 20241107_114016_sync_88f5 manual 2024-11-07_11:40:16 Done sync
'FileSystem2/mybuckst' 'myunity:mybucket'
[2] 20241107_114000_OSbackup_6c7c scheduled 2024-11-07_11:40:00 Done sync
'FileSysteml/SysTools' 'myunity:osbackup'
[3] 20241107_112931_OSbackup_6c7c manual 2024-11-07_11:29:31 Done sync
'FileSysteml/SysTools' 'myunity:osbackup'
[4] 20241107_112646_sync_756f manual 2024-11-07_11: Done sync
'FileSystem2/awsbackup' 'FileSystenl/SysTools'
[5] 20241107_112435_sync_88f5 manual 2024-11-07_11: Done sync
'FileSystem2/mybucket' 'myunity:mybucket'
```

jobs log <id> syntax

```
cloudconnector jobs log <id>
```

The jobs log <id> command shows the log of the job, specified by the job id. It shows the last log/status of the job.

jobs delete <id> syntax

```
cloudconnector jobs delete <id>
```

The jobs delete <id> deletes the job, specified by the job id. This command deletes the job from the job list, including the job's log and other associated info.

jobs cancel <id> syntax

```
cloudconnector jobs cancel <id>
```

The jobs cancel <id> command stops the job, specified by the job id, if it is not started or not finished running.

Note

- Each time the Cloud Connector jobs command runs it lists all current available jobs, and reassigns the id numbers to each job. Those job id numbers will associate with their corresponding jobs, and stay unchanged, until the user runs the cloudconnector jobs command again.
- Each time a job runs, it will be given a new job name, which is unique.
- When a sync (copy, or move) command, with the same arguments and the same job name executes multiple times, even if each of job has a unique name, it will be recognized as the same job. The Cloud Connector will only keep the recent five runs. The remaining runs will be deleted automatically.
- All other jobs in the job list will remain until deleted by the jobs delete command.

2

Functional Commands

Cloud Connector supports the following most frequently used functional commands, to sync and manage files betweem local and cloud storage systems.

syntax

```
cloudconnector <copy|sync|move> source:path dest:path [flags] [-F|-N jobname]
cloudconnector <check> source:path dest:path [flags]
cloudconnector <ls|lsd|lsf|lsl|lsjson> source:path [flags]
cloudconnector <mkdir|rmdir|rmdirs> source:path [flags]
cloudconnector <cat|md5sum|sha1sum|size|touch|tree> source:path [flags]
cloudconnector <delete|purge> source:path [flags]
cloudconnector help [flags]
cloudconnector <command> [--help|-h]
```

path

Local Path

- To access user created file systems.
- Format: `file-system-name/subfolder`. Example: `FileSystem1/subfolder`
- Alternate format: `full path name to the file system`. Example: `/pools/Pool1/FileSystem1/subfolder`
- With exception of user created file systems, access to other local file systems are forbidden and prevented by the program.

Cloud Path

• Also known as the remote path.

• Format: `cloud-config-name:bucket/subfolder`. Example: `myunity:mybucket/subfolder`

Note:

• The command argument: 'source:path' and 'dest:path' can be either one of Local Path or Cloud Path.

• For more information about flags, use syntax `cloudconnector help [flags]`

• For the detailed usage of a command, use syntax `cloudconnector [command] -help`, or the abbreviated version `cloudconnector [command]-h`

cloudcron

To run this command:

1. Access the CLI command shell as described in "Accessing the nxadmin and nxcmd CLIs" (page 13)
2. Type the command using this syntax.
3. Press Enter. TheUnity displays your current prompt settings and the available variables you can choose to change the prompt display.
4. Enter the new prompt format.
5. Press Enter.

Description

Cloud Cron is used to setup scheduled jobs for recurrent actions. It can create/manage cron jobs to run sync/copy/move commands, with a user defined schedule.

Controller

You can run these commands on any controller

Syntax

```
cloudcron {command}
<copy|sync|move> source:path dest:path [flags] [-N jobname]
[-E recur] [-M minute -H hour -D day -m month -d DoW]
```

The sync/copy/move commands use the same syntax as the Cloud Connector.

Schedule options

`[-E recur] [-M minute -H hour -D day -m month -d DoW]`

`-E` : the recur frequency, format {number}[MHDmY], default every minute e.g. 5M: every 5 minutes; 4H: every 4 hours; 3D: every 3 days; 1m: every month; 1Y: every year;

`-M` : the minute (0-59), or multiple minutes separated by comma (,)

`-H` : the hour (0-23), or multiple hours separated by comma (,)

`-D` : the day of month (1-31), or multiple days separated by comma (,)

`-m` : the month (1-12), or multiple months separated by comma (,)

`-d` : the day of week, (0-7), or multiple days separated by comma (,)

Scheduling capabilities are comprehensive: by combining occurance and recur frequency, by specifying the minute/hour/day/month/day-of-week, and by supporting multiple values in each item.

The program also provides a human readable description for the schedule setting of each job. For example:

```
[ES20014-0-999-01]:A: /> cloudcron add sync FileSysteml/SysTools
myunity:osbackup -N OSbackup -E 5M
[ES20014-0-999-01]:
adding cron entry: "*/5 * * * *", schedule: Every 5 minutes, every hour, every
day
for command: 'sync FileSysteml/SysTools myunity:osbackup -N OSbackup'...
[ES200140-999-02]:
adding cron entry: "*/5 * * * *", schedule: Every 5 minutes, every hour, every
day
for command: 'sync FileSysteml/SysTools myunity:osbackup -N OSbackup'...
```

Management commands

`cloudcron show`,

show current cron jobs for all commands.

`cloudcron add`,

add a cron job for the specific command.

`cloudcron remove`,

remove a cron job for the specific command.

2

clustering

To run this command:

1. Access the CLI command shell—see Accessing the nxadmin and nxcmd CLIs on page 13.
2. Type the command using the syntax provided in this topic.
3. Press Enter.

Description

This command enables you to display the status of cluster resources and to move cluster resources from one cluster to the other.

Controller

Run this command on either controller.

Syntax

```
clustering
[show]
[config]
[mgmt <Controller number>]
[rg1 <Controller number>]
[rg2 <Controller number>]
```

Options

`show`

This command displays the current states of all cluster resources.

`config`

This command checks the status of the configuration files for both clusters and reports any discrepancies.

`mgmt <Controller number>`

This command moves the management cluster service to the specified Controller (1 or 2).

`rg1 <Controller number>`

This command moves the Resource Group 1 (rg1) cluster service to the specified Controller (1 or 2).

`rg2 <Controller number>`

This command moves the Resource Group 2 (rg2) cluster service to the specified Controller (1 or 2).

Example

We display the current status of all cluster resources.

```
clustering show
2013-05-21.12:55:22 - Clustering Service Information:
Node             Service     State       MonitorInt  Startup
ES260786-176-01  mgmt        running     nx0         auto
                 rg1         running     nx0         auto
                 rg2         stopped     nx0         auto
ES260786-176-02  mgmt        stopped     nx0         auto
                 rg1         stopped     nx0         auto
                 rg2         running     nx0         auto
```

2

createlogpackage

To run this command:

1. Access the CLI command shell—see Accessing the nxadmin and nxcmd CLIs on page 13.
2. Type the command using the syntax provided in this topic.
3. Press Enter.

Description

This command collects all system log files on the Unity Storage System and creates an encrypted package that you download from the Unity Storage System, using a specific URL provided during command execution.

This command is similar to the `nxcmd Event CollectLogs` command in the nxcmd command-line interface (CLI). This feature is also available in Nexsan Unity's Event Viewer, using the **Collect Logs** button.

Controller

Run this command on the controller where the logs you wish to package are located.

Syntax

`createlogpackage`

Options

None

Example

```
createlogpackage
Generating local logs...
..................................................
Finished local logs.
```

```
About to request the logs from the cluster peer...
Generating remote logs...
....................................................
Finished remote logs.
Retrieving remote logs...
Cleaning up remote logs...
Archiving...
done.
Preparing the cluster peer to have the logs...
Copying the logs to the cluster peer...
Finished copying the log package to the peer node web folder.
Main URL(s) to retrieve the log package(note that most likely
any of the IPs can be used):
http://172.21.156.190/Help/ecentrelogs_ES156190-001_2013-06-07_
14-21-11.zip
or
http://172.21.156.191/Help/ecentrelogs_ES156190-001_2013-06-07_
14-21-11.zip
```


dataproperty

To run this command:

1. Access the CLI command shell—see Accessing the nxadmin and nxcmd CLIs on page 13.
2. Type the command using the syntax provided in this topic.
3. Press Enter.

Description

This command enables you to display or set various properties of pool data on the Unity Storage System.

Controller

Run this command on the controller that contains the resource group where the file systems or pools you wish to view or configure are located.

Syntax

```
dataproperty
[-c <command>]
[-p <property>]
[-n <name>]
[-v <value>]
[-t <type>]
```

Options

`-c <command>`

This option specifies the sub-command to be executed by the `dataproperty` command. The allowed sub-commands are:

- `show`: Displays existing file systems, luns, and pools.

- `list`: Displays a list of properties that can be configured.
- `get`: Displays the value of one or more properties, depending on syntax:
  - `-n <name>`: Lists values of all properties of the named file system, LUN, or pool.
  - `-p <property>`: Lists the values of the specified property for all file systems, LUNs, and pools.
  - `-t <type>`: Lists the values of all properties for all data stores of the specified type: `share`, `lun`, or `pool`.

  These options can be combined to narrow the results. For instance, `dataproperty -c get -n <name> -p <property>` gets the value of the specified property for the named data store.
- `set`: Sets the value of a property. For this sub-command, `-n <name>`, `-p <property>`, `-t <type>`, and `-v <value>` are all required.

`-p <property>`

This option specifies a property. When used with `-c get`, it displays the current value of the property. When used with `-c set`, it sets the property to a specified value.

The properties supported by this option are:

- `aclinherit`: This property controls how access control lists (ACLs) are inherited when files and directories are created. The supported values are:
  - `restricted`: Removes the `write_acl` and `write_owner` permissions when the ACL entry is inherited.
  - `passthrough`: The file system inherits all inheritable ACL entries without modification.
  - `keeptrivial`: Same as `passthrough`, but trivial ACL entries are not destroyed when using `chmod`.
- `compression`: This property controls the compression algorithm for this dataset. Changing this property only affects newly-written data. The supported values are:
  - `off`: Turns off compression.
  - `on`: Turns on LZJB compression. Same as `lzjb`.
  - `lzjb`: Turns on LZJB compression. The lzjb compression algorithm is optimized for performance while providing decent data compression.
  - `gzip`: Turns on GZIP compression.
  - `gzip-`*`N`*: Turns on GZIP compression at the specified level. `N` can be an integer from `1` (fastest) through `9` (most compression). The `gzip` value, above, is equivalent to `gzip-6`.
  - `lz4`: Turns on LZ4 compression.

`-n <name>`

This option specifies a file system are, LUN, or pool name.

`-v <value>`

This option specifies the value that you wish to set a property to. It is required when

using the `set` sub-command. It is not used by any other sub-command.

`-t <type>`

This option specifies a data storage type: `share`, `lun`, or `pool`.

Example 1 — We display existing file systems, LUNs, and storage pools.

```
dataproperty -c show
Type Name
pool FinancePool1
file system FinanceMTL
```

Example 2 — We display the current settings of access control lists (ACLs) inheritance.

```
dataproperty -c get -p aclinherit
name : FinancePool1
     type : pool
     aclinherit : restricted
name : FinanceMTL
     type : file system
     aclinherit : passthrough
```

Example 3 — We set the access control lists (ACLs) inheritance to *Restricted* for any new file system created on storage pool `FinanceMTL`.

```
dataproperty -c set -p aclinherit -n FinanceMTL -t share -v
restricted
Setting property aclinherit in share FinanceMTL to [restricted]
(previous value was [passthrough])
```

Example 4 — We change the compression setting for a file system to LZ4.

```
dataproperty -c set -p compression -t share -n filesystem1 -v
lz4
Setting property compression in File system filesystem1 to [lz4]
(previous value was [off])
```

date

To run this command:

1. Access the CLI command shell—see Accessing the nxadmin and nxcmd CLIs on page 13.
2. Type the command using the syntax provided in this topic.
3. Press Enter.

Description — This command writes the date and time to standard output or attempts to set the system date and time. With no arguments, the current date and time is written.

Controller — Run this command on either controller.

Syntax

```
date
[-u [-R] [+format]]
[-a [-]<sss.fff>]
```

```
[-u][<mm>][<dd>]<HHMM>[<.SS>] | <mmddHHMM>[<cc>][<yy>][<.SS>]]
```

Options

`-u`

This option displays (or sets) the date in Greenwich Mean Time (GMT—universal time), bypassing the normal conversion to (or from) local time.

`-R`

This option displays the time in RFS 2822 format; for example: `Wed, 19 Jun 2013, 19:13:20 -0400`.

By default (without this option), the time is displayed in this format: `Wed June 19 12:13:20 EDT 2013`.

`-a [-]<sss.fff>`

This option slowly adjusts the time by `sss.fff` seconds (where `fff` represents fractions of a second). This adjustment can be positive (no notation) or negative (adding - before `sss.fff`). The system's clock is sped up or slowed down until it has drifted by the number of seconds specified.

`[[<mm>][<dd>]<HHMM>[<.SS>] | <mmddHHMM>[<cc>][<yy>][<.SS>]]`

These options allow you to set the time and/or date.

- Used without `-u`, it sets the time/date in local time.
- Used with `-u`, it sets the time/date in GMT.

The individual operands are:

- `<mm>`: The month
- `<dd>`: The date of the month
- `<HH>`: The hour, in 24-hour time format
- `<MM>`: The minute
- `<.SS>`: The second
- `<cc>`: The century (a year divided by 100 and truncated to an integer) as a decimal number (`00-99`). For example, `<cc>` is `19` for the year 1988 and `20` for the year 2007.
- `<yy>`: The last two digits of the year number. If century (`<cc>`) is not specified, then values in the range `69-99` shall refer to years 1969 to 1999 inclusive, and values in the range `00-68` shall refer to years 2000 to 2068, inclusive.

The month, day, year number, and century may be omitted; the current values are applied as defaults.

Example 1

We set the unit to July 7th, 2014 at 12:23:30 a.m., local time.

```
date 07071223302014.30
Mon Jul 07 12:23:30 EDT 2014
```

Example 2

We set the date and time in GMT without changing the current year.

```
date -u 07070423.30
Sun Jul 07 04:23:30 GMT 2013
```

diskhbcfg

To run this command:

1. Access the CLI command shell—see Accessing the nxadmin and nxcmd CLIs on page 13.
2. Type the command using the syntax provided in this topic.
3. Press Enter.

Description

This command is used for configuring disk heartbeats. This allows communication between the two cluster nodes via the disks.

CAUTION: You should only run this command if requested by Nexsan Technical Support.

Controller

Run this command on either controller.

Syntax

```
diskhbcfg
[set <parameter> <argument>]
[get]
[update]
[check]
```

Options

`set <parameter> <argument>`

This option configures disk heartbeats using the following parameters:

- `persistentreservation enable|disable` enables or disables persistent reservations.
- `reserveddevicesperpool #` sets the maximum number of devices to reserve per storage pool.
- `diskHBPerEnclosure #` sets the maximum number of disk heartbeats per storage system.
- `vlunHb enable|disable` enables or disables the use of virtual LUNs for disk heartbeats. This parameter only applies to persistent reservation.

`get`

This option displays the current settings for disk heartbeats and reservations.

`update`

This option updates the current disk heartbeats and reservations, according to current system state and settings.

`check`

This option checks the current status of disk heartbeats and reservation.

Example

```
diskhbcfg get
Persistent reservation: Enabled
Reserved devices per pool: 3
Disk heartbeats per enclosure: 2
```

```
Use virtual LUNs: true
Update configuration on changes: true
```

domainname

To run this command:

1. Access the CLI command shell—see Accessing the nxadmin and nxcmd CLIs on page 13.
2. Type the command using the syntax provided in this topic.
3. Press Enter.

Description	This command displays or sets the domain name used for NIS integration. For steps to integrate NIS, see Integrating with Network Information Service (NIS).
Controller	Run this command on both controllers.
Syntax	`domainname` `[<domain> | -s]`

Options	`<domain>`
	This is the domain name that you wish to assign for NIS integration.
	`-s`
	This option displays the current domain name.

Example	**`domainname -s`** `qadomain.net`

drives

To run this command:

1. Access the CLI command shell—see Accessing the nxadmin and nxcmd CLIs on page 13.
2. Type the command using the syntax provided in this topic.
3. Press Enter.

Description	This command displays a list of all disk drives in the Unity Storage System as well as in any Unity Storage Systems connected to the Unity Storage System. The command provides the serial number of each drive and indicates the storage system (enclosure) that each drive is associated with.
Controller	Run this command on either controller.
Syntax	`drives` `[paths]`
Options	`paths` This option displays FC or SAS connections to the drives.
Example	**`drives`**

```
Enumerating drives...
Drives in NST6000 (000001) (Chassis ID: 100000001, Slots: 24):
* Slot 1: No drive.
* Slot 2: TOSHIBA-MBF2600RC 0108 (Serial: N07R341NUM83R, Size:
600.1 GB)
* Slot 3: No drive.
* Slot 4: No drive.
* Slot 5: No drive.
* Slot 6: No drive.
* Slot 7: No drive.
* Slot 8: No drive.
* Slot 9: No drive.
* Slot 10: No drive.
* Slot 11: No drive.
* Slot 12: No drive.
* Slot 13: No drive.
* Slot 14: No drive.
* Slot 15: No drive.
* Slot 16: No drive.
* Slot 17: No drive.
* Slot 18: No drive.
* Slot 19: No drive.
* Slot 20: No drive.
* Slot 21: No drive.
* Slot 22: No drive.
* Slot 23: No drive.
* Slot 24: No drive.
Volumes in E18 (3d34d2c) (Chassis ID: 3d34d2c):
* Volume: 7A3276274D2C, LUN 0 (Size: 6.0 TB)
* Volume: 7A3276234D2C, LUN 1 (Size: 6.0 TB)
* Volume: 7A3276204D2C, LUN 2 (Size: 6.0 TB)
* Volume: 7A3276194D2C, LUN 3 (Size: 6.0 TB)
```


echo

To run this command:

1. Access the CLI command shell—see Accessing the nxadmin and nxcmd CLIs on page 13.
2. Type the command using the syntax provided in this topic.
3. Press Enter.

Description: This command prints entered text to the output or displays the numeric exit code for the last operation that was run. This can be useful in scripting.

Controller: Run this command on either controller.

Syntax:
```
echo
[<text> | $?]
```

Options:

`<text>`

Entering text after `echo` tells the command to display that text in the output. This is useful in scripting for when you want a script to display text.

`$?`

This option tells the `echo` command to return the numeric exit code for the last operation that was run. This can be useful in scripting for when you need to determine if the previously-run command was successful.

Example:
```
echo Command completed successfully.
Command completed successfully.

echo $?
0
```

edit

To run this command:

1. Access the CLI command shell—see Accessing the nxadmin and nxcmd CLIs on page 13.
2. Type the command using the syntax provided in this topic.
3. Press Enter.

Description: This command enables you to view or edit a file; for example, to view a log file.

Notes:

- The editor used by the `edit` command is different from the one used by the `bedit` command.
- When opening a read-only file, `edit` will not allow you to save any changes.

Controller: Run this command on the controller where the file you wish to edit is stored.

Syntax: `edit <file name>`

Options: `<file name>`

This option specifies the file that you wish to open and edit. To open a file in a different directory, specify the full path name; for example, `edit /etc/hosts`.

enforcessl

To run this command:

1. Access the CLI command shell—see Accessing the nxadmin and nxcmd CLIs on page 13.
2. Type the command using the syntax provided in this topic.

3. Press Enter.

Description — Nexsan Unity 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 Nexsan Unity is running. This command enables you to turn off this feature and turn it back on.

Controller — Run this command on any controller

Syntax — `enforcessl <true|false>`

Options — `true`

This option enforces the SSL encryption.

`false`

This option removes the SSL encryption.

errorlog

To run this command:

1. Access the CLI command shell—see Accessing the nxadmin and nxcmd CLIs on page 13.
2. Type the command using the syntax provided in this topic.
3. Press Enter.

Description — This command displays the most recent error logs.

Controller — Run this command on the controller where the errors you wish to view occurred.

Syntax — `errorlog [<number of lines>]`

Options — `<number of lines>`

This option enables you to specify how many lines of the error log that you want returned. The default is 1000.

Example — **`errorlog 10`**

```
Aug 04 2015 01:00:02.333402296
ereport.nexsan.log.com.nexsan.scheduling nvlist version: 0
            event_id = 16033
            Class = ereport.nexsan.debug.com.nexsan.nest.data
            date = 2015-08-03 T 11:38:49
            level = warning
            message = Failed to update the Unity Vault
            Protection
Module information: com.nexsan.NxException: Failed validate the
active host status
            mainclass = com.nexsan.nest.manager.
```

```
Main trace = Failed validate the active host status
Com.nexsan.nest.NestException: Failed validate the
active host status
Com.nexsan.NxException.fixEmbeddedException
(NxException.java:62)
...
```

eventflag

To run this command:

1. Access the CLI command shell—see Accessing the nxadmin and nxcmd CLIs on page 13.
2. Type the command using the syntax provided in this topic.
3. Press Enter.

Description	This command enables you to show or clear event flags on the Unity Storage System on both controller nodes.
Controller	Run this command on either controller.
Syntax	`eventflag [show] | [clear <event flag number>]`

Options	`show`
	This option displays the event flags for both controller nodes. It first displays event flags for the controller that you are accessing the unit through. It then displays event flags for the other controller in the unit.
	`clear <event flag number>`
	This option clears the specified event flag.

exit

To run this command:

1. Access the CLI command shell—see Accessing the nxadmin and nxcmd CLIs on page 13.
2. Type the command using the syntax provided in this topic.
3. Press Enter.

Description	This command exits the nxadmin CLI and closes the SSH session. It accepts no options or arguments.
Controller	Run this command on either controller.
Syntax	`exit`
Options	None

fcstat

To run this command:

1. Access the CLI command shell—see Accessing the nxadmin and nxcmd CLIs on page 13.
2. Type the command using the syntax provided in this topic.
3. Press Enter.

Description — This command displays Fibre Channel statistics based on the Fibre Channel clients connected to the Unity Storage System. This command can help troubleshooting Fibre Channel issues, such as multipathing and unoptimized path access issues.

Controller — Run this command on either controller.

Syntax — `fcstat [-T d|u] [interval [count]]`

Options — `-T d|u`

This option displays a time stamp before each statistics block, either:

- in date format (`d`), or
- as an alphanumeric representation of the value returned by time (`u`).

`interval`

This option sets the number of seconds between reports.

`count`

This option sets the number of reports to be displayed.

Example — **`fcstat 5`**

```
FC Port WWN              RBYTES     READS       WBYTES    WRITES
50003A400000241B          44212       137            0         0
50003A400000241C           7025       155        19824       106
50003A400000241A          19213        58            0         0
50003A400000241D      275436723     11492   35243625247    149978
50003A400000241B          44212       137            0         0
50003A400000241C           7025       155        19824       106
50003A400000241A          19213        58            0         0
50003A400000241D      275436723     11492    3566241823    150316
```

firewall

To run this command:

1. Access the CLI command shell—see Accessing the nxadmin and nxcmd CLIs on page 13.
2. Type the command using the syntax provided in this topic.
3. Press Enter.

Description — The firewall command enables you to enable, disable, and configure the firewall on the Unity Storage System. the Unity Storage System's firewall service prevents both

port.

You can also use this command to open all dynamic ports on the Unity Storage System for specific IP addresses; this is particularly useful for NDMP-based backups where you may want to grant an NDMP server access to the Unity Storage System through the firewall.

Controller — Run this command on both controllers.

Syntax

```
firewall
[startservice]
[stopservice]
[status]
[reloadconfig]
[custom add <port number> <udp | tcp> <description>]
[custom remove <port number | all> <udp | tcp>]
[custom show]
[dynamic add <IP> <udp | tcp> <description>]
[dynamic remove <IP | all> <udp | tcp>]
[dynamic show]
```

Options

`startservice`

This command starts the firewall service.

Note: When you start the firewall service, anything that uses a dynamic port may be disconnected.

`stopservice`

This command stops the firewall service.

`status`

This command shows the current status of the firewall service, including all port routings.

`reloadconfig`

This command reloads the firewall configuration file.

`custom add <port number> <udp | tcp> <description>`

This command adds a custom port with the specified port number, type, and description. The description must NOT contain quotes or spaces. Underscores are permitted.

`custom remove <port number | all> <udp | tcp>`

This command removes one or all custom ports. To remove a specific port, specify its port number and protocol. To remove all custom ports, type **`all`** and the protocol.

`custom show`

This command displays all custom ports, their port numbers, and their descriptions.

`dynamic add <IP> <udp | tcp> <description>`

This command adds a dynamic port with the specified IP address, type, and description. The description must NOT contain quotes or spaces. Underscores are permitted.

```
dynamic remove <IP | all> <udp | tcp>
```

This command removes one or all dynamic ports. To remove a specific port, specify its IP address and protocol. To remove all custom ports, type **all** and the protocol.

```
dynamic show
```

This command displays all dynamic ports, their IP addresses, and their descriptions.

Example

We display all custom ports using the `firewall custom show` command.

```
firewall custom show
pass in quick proto udp from any to any port = 2131 keep state # Acct_svc
pass in quick proto tcp from any to any port = 2141 keep state # Finance
pass in quick proto udp from any to any port = 2151 keep state # Mktg_svc
```

format

2

To run this command:

1. Access the CLI command shell—see Accessing the nxadmin and nxcmd CLIs on page 13.
2. Type the command using the syntax provided in this topic.
3. Press Enter.

Description

This command displays available disk drives on the system, including drives on Unity Storage Systems connected externally.

Controller

Run this command on either controller.

Syntax

```
format
```

Options

None

Example

```
format
0. c0t5000A72A3006A49Ed0 <STEC-Z16IZF2E-200UCV-E46F-186.31GB> - /pci@0,0/pci8086,3c06@2,2/pci8086,3516@0/iport@ff/disk@w5000a72a3006a49e,0
1. c2t600144F0DA938E000000519FE37F0001d0 <NEXSAN_lun-0100-1.00GB> - /scsi_vhci/disk@g600144f0da938e000000519fe37f0001
2. c2t600144F040F3C0000000519FE3950001d0 <NEXSAN_lun-0100-1.00GB> - /scsi_vhci/disk@g600144f040f3c0000000519fe3950001
3. c2t500003934C8801FCd0 <TOSHIBA-MK1001GRZB-0106-93.16GB> - /scsi_vhci/disk@g500003934c8801fc
4. c2t5000039308113B14d0 <TOSHIBA-MBF2600RC-0108 cyl 107099 alt 2 hd 6 sec 1824> - /scsi_vhci/disk@g5000039308113b14
```

```
5. c2t6000402002D84D2F7B2321A100000000d0 <NEXSAN-NXS-B01-000-Q011-
3.64TB> - /scsi_vhci/disk@g6000402002d84d2f7b2321a100000000
6. c2t6000402002D84D2F7B2321A200000000d0 <NEXSAN-NXS-B01-000-Q011-
3.64TB> - /scsi_vhci/disk@g6000402002d84d2f7b2321a200000000
7. c2t6000402002D84D2F7B2321A600000000d0 <NEXSAN-NXS-B01-000-Q011-
5.46TB> - /scsi_vhci/disk@g6000402002d84d2f7b2321a600000000
8. c2t6000402002D84D2F7B2321AA00000000d0 <NEXSAN-NXS-B01-000-Q011-
5.46TB> - /scsi_vhci/disk@g6000402002d84d2f7b2321aa00000000
9. c3t0d0 <ATA-INTELSSDSA2VP02-0379 cyl 3736 alt 2 hd 224 sec 56>
- /pci@0,0/pci8086,3582@1f,2/disk@0,0
10. c3t1d0 <ATA-INTELSSDSA2CW30-0362 cyl 46719 alt 2 hd 224 sec
56> - /pci@0,0/pci8086,3582@1f,2/disk@1,0
```

ftpconfig

To run this command:

1. Access the CLI command shell—see Accessing the nxadmin and nxcmd CLIs on page 13.
2. Type the command using the syntax provided in this topic.
3. Press Enter.

Description

This command enables you to configure and enable group access tofile systems s using the File Transfer Protocol (FTP). The FTP service can be configured to grant local authentication groups access to file systems via FTP on the selected resource group. By default, the FTP service is not enabled on the Unity Storage System.

NOTES:

- The FTP service only authenticates to the Unity Storage System using local authentication. However, if you selected Active Directory authentication in Nexsan Unity, you can still use the `ftpconfig` command to enable local authentication for users and groups.

  You can also assign access permissions using the shareacl command for the file systems to be accessible to the local user.
- Enabling FTP support will create additional folders in the `/var/opt/nest/users/` directory. It is recommended to leave these folders untouched for proper FTP behavior.
- Dynamic ports for FTP passive mode are 32768 to 33768.

Controller

Run this command on either controller.

Syntax

```
ftpconfig [-c <command>] [-f <flag>] [-s <ecosystem name>]
[-p <pool name>] [-r 1|2] [-g <group name>] [-G <GID>]
```

Options

`-c <command>`

This option specifies the sub-command to run:

- `enable`: Turns on the FTP service. It also creates a default group called `ftpgroup`. If the FTP service is already set up, the current configuration will not be overwritten, unless you use the `-f setupoverwrite` option.
- `disable`: Turns off the FTP service without removing any existing configuration.
- `uninstall`: Uninstalls the FTP service and completely removes the configuration.
- `addshare`: Adds a file systems to be accessible via FTP. You must use the `-s` and `-p` options with this sub-command.

  TIP: To list all file systems, use the shares command.
- `removeshare`: Removes a file system from being accessible via FTP. You must use the `-s` and `-p` options with this sub-command.
- `listshares`: Displays the list of file systems that are currently accessible via FTP.
- `addgroup`: Enables the specified group to have access to file systems on a resource group. You must use the `-g` and `-r` options with this sub-command.
- `removegroup`: Disables access for the specified group to file systems on a resource group. You must use the `-g` and `-r` options with this sub-command.
- `listgroups`: Displays the list of groups that have access to the file systems on the resource group.

  NOTE: To manage groups and users that belong to a group, use the modgid and groupadd commands.

`-f <flag>`

You can use the `-f` option multiple times within the same command:

- `setupoverwrite`: Overwrites the existing configuration when enabling the FTP service.
- `nopeer`: Forces the configuration settings to be applied even if the peer is currently down.

`-s <ecosystem name>`

This option specifies the name of the file system for which you want to grant or revoke access via FTP. This option is required when using the `addshare` or `removeshare` sub-command.

`-p <pool name>`

This option specifies the name of the pool to which the file system belongs. This option is required when using the `addshare` or `removeshare` sub-command.

`-r 1|2`

This option specifies which resource group to use with the `addgroup`, `removegroup`, or `listgroup` sub-command.

`-g <group name>`

This option specifies the group name to use with the `addgroup`, `removegroup`, or `listgroup` sub-command.

`-G <GID>`

This option specifies the group ID to use for the default group, `ftpgroup`. The default is `1021`.

Example

We make sure that FTP is enabled, then we make file system `MTLFinance1` visible via FTP.

```
ftpconfig -c enable
ftpconfig -c addshare -p FinancePool1 -s MTLFinance1
```

groupadd

To run this command:

1. Access the CLI command shell—see Accessing the nxadmin and nxcmd CLIs on page 13.
2. Type the command using the syntax provided in this topic.
3. Press Enter.

Description

This command enables you to add local group accounts on the Unity Storage System that correspond to UNIX/Linux Microsoft Active Directory domain accounts. The members of the group accounts that you add to the Unity Storage System can then access NFS file systems in a Microsoft Active Directory environment.

Note: This command does not display a confirmation message.

Controller

Run this command on either controller.

Syntax

```
groupadd -g <gid> [-o] <group name>
```

Options

`-g <gid>`

This option assigns the specified group ID `<gid>` to the group being added. This group ID must be a non-negative decimal integer below 2147483647.

You cannot use these group ID numbers because they are reserved:

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

If there are conflicting IDs, please contact Nexsan Technical Support.

`-o`

This option, when used with `-g`, allows the group ID to be non-unique.

`<group name>`

This option specifies the group name to be added.

Example

```
groupadd -g 1002 users
```

groupdel

To run this command:

1. Access the CLI command shell—see Accessing the nxadmin and nxcmd CLIs on page 13.
2. Type the command using the syntax provided in this topic.
3. Press Enter.

Description: This command enables you to delete local user accounts on the Unity Storage System that correspond to UNIX/Linux Microsoft Active Directory domain accounts.

Note: No output gets displayed, except in the case of error.

Controller: Run this command on either controller.

Syntax:

```
groupdel <group name>
```

```
<group name>
```

This option specifies the group name to be deleted.

Example:

```
groupdel Accounting
```

help

To run this command:

1. Access the CLI command shell—see Accessing the nxadmin and nxcmd CLIs on page 13.
2. Type the command using the syntax provided in this topic.
3. Press Enter.

Description: This command displays a list of all available commands in the nxadmin CLI's command-based shell.

Controller: Run this command on either controller.

Syntax:

```
help
```

Options: None

Example:

```
help
```

```
arp         Address resolution display and control.
audit       Auditing.
bedit       Basic file viewer/editor.
callhome    Manages the CallHome service.
cat         Print the contents of a file.
...
```

hostname

To run this command:

1. Access the CLI command shell—see Accessing the nxadmin and nxcmd CLIs on page 13.
2. Type the command using the syntax provided in this topic.
3. Press Enter.

Description	This command enables you to display or temporarily set the host name of the Unity Storage System.
Controller	Run this command on either controller.
Syntax	`hostname <host name or IP address>`
Options	`<host name or IP address>` This option temporarily sets the name or IP address of the host to the value entered after the command. The host name reverts to what it was before when the controller is rebooted.

Example 1	**`hostname`**
	`ES600000-001-01`
	`hostname Finance1`
	`Finance1:A:/>`

Example 2	**`hostname`**
	`ES156180-001-01`
	`hostname 172.21.156.180`
	`172.21.156.180:A:/>`

ifconfig

To run this command:

1. Access the CLI command shell—see Accessing the nxadmin and nxcmd CLIs on page 13.
2. Type the command using the syntax provided in this topic.
3. Press Enter.

Description	This command displays the configuration for network interfaces on the Unity Storage System.
Controller	Run this command on the controller where the network connections you wish to view are located.

Syntax	`ifconfig`
	`[-a | <netname>]`
	CAUTION: The `ifconfig` command provides additional options for managing the Unity Storage System's network interfaces. However, it is NOT recommended that you use these additional options unless you are instructed to do so by Nexsan Technical Support.

Options `-a`

This option displays the configuration for all detected network interfaces.

`<netname>`

This option displays the configuration for the specified network interface.

Example **`ifconfig nx0`**

```
nx0: flags=1000843<UP,BROADCAST,RUNNING,MULTICAST,IPv4> mtu 1500
index 3
     inet 172.21.200.10 netmask ffff0000 broadcast
172.21.255.255
     ether 0:1e:67:54:9a:3a
```

immutablecron

To run this command:

1. Access the CLI command shell as described in "Accessing the nxadmin and nxcmd CLIs" (page 13)
2. Type the command using this syntax.
3. Press Enter. TheUnity displays your current prompt settings and the available variables you can choose to change the prompt display.
4. Enter the new prompt format.
5. Press Enter.

Description The Immutablecron command enables you to manage cron jobs for scheduled immutable snapshots on a Share or a LUN..

Controller You can run this command on any controller

Syntax `immutablecron -c command [-F Share/LUN-name -R retention-days] [-E recur] [-M minute -H hour -D day -m month -d DoW] [-S cron-expression`

Options -c add

Add a cron job with specified schedule, to create immutable snapshots with specified retention days on the specified Share/LUN, allow to add multiple corn jobs with different schedules for the same Share/Lun and retention days.

-c remove

Remove cron jobs for the specified Share/LUN and retention days.

-c show

Show current cron jobs for immutable snapshots.

-c clear

Delete all the cron jobs for the specified Share/Lun.

-c test

Test and verify the schedule.

-F

Name of Share or LUN

-R

The number of days of the retention period (1-9999)

-E

The recur frequency, format {number}[MHDmY], default every minute e.g. 5M: every 5 minutes; 4H: every 4 hours; 3D: every 3 days; 1m: every month; 1Y: every year;

-M

The minute (0-59), or multiple minutes separated by comma (,)

-H

The hour (0-23), or multiple hours separated by comma (,)

-D

The day of month (1-31), or multiple days separated by comma (,)

-m

The month (1-12), or multiple months separated by comma (,)

-d

The day of week, (0-7), or multiple days separated by comma (,)

-s

cron expression (only support 5 fields format)

Examples

• Show current cron jobs for all Shares and LUNs

-c show

• Add a cron job at every Sunday at 0:00, to create an immutable snapshot onFileSystem1, with 10 days of retention

```
-c add -F FileSystem1 -R 10 [Scheduling Arguments]
```

• Delete the immutable snapshot cron job for FileSystem1 with 10 days of retention

```
-c remove -F FileSystem1 -R 10
```

• Test and verify the schedule formed by scheduling arguments

```
-c test [Scheduling Arguments]
```

Examples of 'Scheduling Arguments'

[-E recur] [-M minute -H hour -D day -m month -d DoW] [-S cron-expression]

Default is set to run every minute, every hour, every day

-E 1D , Set to run every day, at 0:00

-E 1D, -d 0 Set to run every day, on Sunday at 0:00

-E 1D, -d 0,3 Set to run every day, on Sunday and Wednesday at 0:00

-E 2D, -D 2 -H 1 Set to run every 2 days, starting on day 2 of month, at 1:00

-E 1m , Set to run every month, on day 1 of the month, at 0:00

-E 1Y , Set to run every year, on January 1st, at 0:00

-E 1H -M 30, Set to run every hour, at 30 minutes past the hour

-E 1D -M 30, -H 1 Set to run every day, at 1:30

-E 1m -M 30 -H 1 -D 1,15, Set to run on day 1 and 15 of each month, at 1:30

info

To run this command:

1. Access the CLI command shell—see Accessing the nxadmin and nxcmd CLIs on page 13.
2. Type the command using the syntax provided in this topic.
3. Press Enter.

Description: This command displays version information for the software components installed on the Unity Storage System.

Controller: Run this command on either controller.

Syntax: `info`

Options: None

Example:

```
info
NeSTOS Version : 16541
Application Version : 3.0.0.44779
Application buildinfo : d
Clustering Version : 3.0.0.44779
Clustering buildinfo : d

Clustering information:
ES600000-001-01:
nest_syspool running auto unblocked ES600000-001-mgmt-nx99-vip
nx99 60 10
C01_NONE stopped auto unblocked ES600000-001-rg1-vip nx0 60 10
C02_NONE running auto unblocked ES600000-001-rg2-vip nx0 90 10
ES600000-001-02:
nest_syspool stopped auto unblocked ES600000-001-mgmt-nx99-vip
nx99 90 10
C01_NONE running auto unblocked ES600000-001-rg1-vip nx0 90 10
C02_NONE stopped auto unblocked ES600000-001-rg2-vip nx0 60 10
```

intmonitoring

To run this command:

1. Access the CLI command shell—see Accessing the nxadmin and nxcmd CLIs on page 13.
2. Type the command using the syntax provided in this topic.
3. Press Enter.

Description: This command configures interface monitoring for resource groups. It enables you to change the behavior of the cluster so that when a Resource Group is in this list, the link state of the network interface is not monitored and no event gets generated to switch over the resource group to the peer node.

This is useful for environments using Fibre Channel LUNs; it enables you to unplug a

network interface and connect new Fibre Channel cards without triggering a cluster switchover.

Controller — Run this command on any controller.

Syntax
```
intmonitoring -c <command> -s <service>
```

Options

`-c <show|forceexclude|default>`

This option specifies the sub-command to run:

- `show` displays the current settings.
- `forceexclude` sets the resource group to exclude from network monitoring; it must be used with the `service` option.
- `default` sets the resource group back to the default value; it must be used with the `service` option.

`-s <rg1|rg2>`

This option specifies the service to run:

- `rg1` is for Resource Group 1
- `rg2` is for Resource Group 2

Example — We are excluding Resource Group 2 from network monitoring.

```
intmonitoring -c forceexclude -s rg2
```


iostat

To run this command:

1. Access the CLI command shell—see Accessing the nxadmin and nxcmd CLIs on page 13.
2. Type the command using the syntax provided in this topic.
3. Press Enter.

Description — This command displays input/output statistics for the Unity Storage System, including terminal and disk I/O activity and CPU utilization.

Controller — Run this command on either controller.

Syntax
```
iostat
[-cCdDeEiImMnpPrstxXYz]
[-l <number of disks>]
[-T d|u]
[<interval rate> [<update count>]]
```

Options

`-c`

This option tells the `iostat` command to report the percentage of time that the unit has spent in user, system, wait, and idle mode.

`-C`

This option tells the `iostat` command to report disk statistics by Controller.

`-d`

This option tells the `iostat` command to display disk I/O in kilobits per second and transfers per second, plus the average service time in miliseconds.

`-D`

This option tells the `iostat` command to display disk I/O in reads per second and writes per second, plus the percentage of disk utilization.

`-e`

This option tells the `iostat` command to report device error summary statistics.

`-E`

This option tells the `iostat` command to report extended device error statistics.

`-i`

Used with the `-E` option, this option tells the `iostat` command to show the device IDs for the device statistics output by `-E`.

`-I`

This option tells the `iostat` command to report the counts of each interval instead of rates, where applicable.

`-l <number of disks>`

This option tells the `iostat` command to limit the number of disks to the specified number.

`-m`

This option tells the `iostat` command to display mount points. This option is most useful in conjunction with `-p`.

`-M`

This option tells the `iostat` command to display data throughput in megabits per second instead of kilobits per second.

`-n`

This option tells the `iostat` command to convert device names to `cXdYtZ` format.

`-p`

This option tells the `iostat` command to report per-partition disk statistics as well as per-device disk statistics.

`-P`

This option tells the `iostat` command to report only per-partition disk statistics without per-device disk statistics.

`-r`

This option tells the `iostat` command to display data in a comma-separated format.

`-s`

This option tells the `iostat` command to suppress state change messages.

`-T d|u`

This option tells the `iostat` command to display a time stamp in date (`d`) format or UNIX time_t (`u`) format.

`-t`

This option tells the `iostat` command to display characters read from and written to terminals.

`-x`

This option tells the `iostat` command to display extended disk statistics.

`-X`

This option tells the `iostat` command to display I/O path statistics.

`-Y`

This option tells the `iostat` command to display I/O path I/T/L statistics.

`-z`

This option tells the `iostat` command to suppress entries with all zero values.

`<interval rate>`

This option specifies the rate at which to display updated statistics. It is expressed as the number of seconds between updates; for example, `iostat 5` displays the statistics once every five seconds. If this option is not specified, statistics are display only once.

`<update count>`

This option specifies the total number of updates to display. It is only used with the `<interval rate>` option; for example, `iostat 5 10` displays the statistics once every five seconds, ten times. If this option is not specified, statistics are displayed continuously.

Example **`iostat`**

```
   tty        sd1          sd2          sd3          sd4          cpu
tin tout kps tps serv kps tps serv kps tps serv kps tps serv us sy wt id
  0    6  24  17    4  24   6    1   0   0    0   0   0    0  3  2  0 95
```

ipgroups

CAUTION: DO NOT use this command in combination with any other IP restrictions-based mechanism in Unity, such as the **IP Restrictions** option in the Unity user interface and all IP restrictions-based commands under the nxcmd `share` option. Doing so will override configuration changes made using the `ipgroups` command. In addition, this command DOES NOT support entries containing IP prefixes and IPs with masks; you can only add IP addresses to a group.

▶ **To run this command:**

1. Access the CLI command shell—see Accessing the nxadmin and nxcmd CLIs on page 13.
2. Type the command using the syntax provided in this topic.

3. Press Enter.

Once you create a group using the `ipgroups` tool, you must then add the group name to a share access-list using the relevant options in the menu command. For example, you can create a group called `IPG_share1_ro` containing all the IPs of host systems that you want to give read-only (`ro`) access to `share1`. You would then add the `IPG_share1_ro` group to the `ro` share access-list for `share1`.

Description

The `ipgroups` tool enables you to group multiple host IPs into an alias (group name). This name can be used in the IP restrictions and will be associated with all the IPs in the share access-list.

Note Using `ipgroups` is only recommended if you have reached the limit of entries permitted in a share access-list. The command allows you to group multiple IPs into an alias (group name) that you can then add to a share access-list.

Controller

Run this command on either controller.

Syntax

► **To add a group to a share access-list:**

1. Under the nxadmin CLI, type `menu`.
2. Select `6 - Configure Shares and Active Directory`.
3. Select `1 - Configure Share Access Lists`.

Note The Unity user interface will NOT display share access-lists containing groups that were created using the `ipgroups` tool.

```
ipgroups
[-c | <command>]
```

The command is one of the following:

`show-name`	Show by group name. Optionally use `-i` and/or `-n`
`show-ip`	Show by IP. Optionally, use `-i` and/or `-n`
`add`	Requires `-i` and/or `-n` Multiple `-i` and `-n` arguments are supported.
`remove`	Requires `-i` and `-n` Multiple `-i` and `-n` arguments are supported. **Notes:** If you specify one or more IPs without any groups, all those IPs will be removed from all groups. If you specify one or more groups without any IPs, all the groups will be removed from all IPs.

Options

`-i IP`

The host IP address that you want to add, remove, or show.

This option can be used multiple times.

Only full IP addresses are supported, no CIDS (that is, prefixes).

`-n IPG_name`

The group name that is used in IP restrictions.

The group name must start with `IPG_`

Although not mandatory, it is good practice to create group names based on the share names and access list type.

This option can be used multiple times.

`-C`

Disable colors (-C).

`-S`

Show one entry per line for `show-ip` and `show-name`

Examples

Example for adding an IP address to two groups:

```
ipgroups -c add -i 181.54.54.55 -n IPG_public_rw -n IPG_
payrolldata_ro
```

Example for removing an IP from a group:

```
ipgroups -c remove -i 181.54.54.55 -n IPG_payrolldata_ro
```

ipmi

To run this command:

1. Access the CLI command shell—see Accessing the nxadmin and nxcmd CLIs on page 13.
2. Type the command using the syntax provided in this topic.
3. Press Enter.

Description

This command enables you to reset IPMI settings for the Unity Storage System.

Controller

Run this command on the controller for which you wish to reset IPMI settings.

Syntax

```
ipmi updatesettings | fullcheck
```

Options

`updatesettings`

The `ipmi updatesettings` command resets the settings of IPMI configuration for the Unity Storage System. For example, if you changed the IP address of a Controller node in the IPMI interface, this command will update the password on the Unity Storage System.

Note: If you accidentally changed the password for the CLUSTERCONTROL IPMI user in the IPMI interface, this command will reset the password. The CLUSTERCONTROL IPMI user is used by the system for power control operations between the controllers node on the Unity Storage System; for example, powering on, powering off, or restarting a controller node from the other node. That user requires a specific password that MUST NOT be changed.

`fullcheck`

This option resets and rechecks all IPMI settings. This action can take a long time, so it is only recommended if IPMI has a serious problem.

ipmitool

To run this command:

1. Access the CLI command shell—see Accessing the nxadmin and nxcmd CLIs on page 13.
2. Type the command using the syntax provided in this topic.
3. Press Enter.

Description

This program lets you manage Intelligent Platform Management Interface (IPMI) functions of either the local system (via a kernel device driver) or a remote system (using IPMI v1.5 and IPMI v2.0). These functions include printing FRU information, configuring the LAN, getting sensor readings, and controlling remote chassis power.

CAUTION: With IPMI remote access enabled, a remote station has the ability to control a system's power state. To reduce vulnerability, it is strongly advised that the IPMI LAN interface only be enabled in 'trusted' environments where system security is not an issue or where there is a dedicated, secure 'management network'.

Furthermore, it is strongly advised that you should not enable IPMI for remote access without setting a password, and that the password should not be the same as any other password on that system.

CAUTION: When an IPMI password is changed on a remote machine, the new password is sent across the network as clear text. This could be observed and then used to attack the remote system. It is thus recommended that IPMI password management only be performed on the local station.

Controller

If you are using the `chassis` sub-command, run this command on either controller.

If you are using the `lan` sub-command, run this command on the controller that the LAN is connected to.

Syntax

```
ipmitool
[-c]
[-v]
[-V]
-I lan | lanplus | open
-H <host name>
[-p <port>]
[-U <user name>]
[-f <password file>]
<command>
```

CAUTION: The `ipmitool` command provides additional options for managing the Unity Storage System's IPMI interface. However, it is NOT recommended that you use these additional options unless you are instructed to do so by Nexsan Technical Support.

Options

`-c`

This option presents the output in CSV (comma-separated variable) format.

`-v`

This option is used to increase the level of verbosity in the debug output. It can be entered multiple times. If entered three times, the system returns hexdumps of all incoming and outgoing packets.

`-V`

This option displays version information.

`-I lan | lanplus | open`

This option selects the IPMI interface to use: `lan`, `lanplus`, or `open`.

`-H <host name>`

This option specifies the remote server address. This can be either an IP address or host name. This option is required for `lan` and `lanplus` interfaces. It is not used for `open`IPMI interfaces.

`-p <port>`

This option selects the remote port. The default port is 623.

`-U <user name>`

This option specifies the user name for the remote system. The default user name is NULL.

`-f <password file>`

This option specifies the name of the file that contains the remote server password. If this option is absent, or the password file is empty, ipmitool prompts the user for a password. If no password is entered at the prompt, the remote server password defaults to NULL.

IPMI 1.5 supports a password length of up to 16 characters. IPMI 2.0 supports a password length of up to 20 characters on `lanplus` interfaces. Longer passwords are truncated.

`<command>`

See the **Sub-Commands**, below.

Sub-Commands

The `ipmitool` CLI command provides several sub-commands that perform various actions on the IPMI interface. The two most commonly used are `chassis` and `lan`.

CAUTION: It is NOT recommended that you use any additional sub-commands unless you are instructed to do so by Nexsan Technical Support.

`chassis`

This sub-command performs various actions on the Unity Storage System's chassis, including querying status, setting power cycling policy, and starting and stopping the unit. The supported operations are `poh`, `policy`, `power`, `restart_cause`, `selftest`, and `status`.

- `poh` queries the Power On Hours counter (which tracks the time since the unit was last turned on) and displays its current value.

- `policy` sets the Unity Storage System's power policy in the event of a power failure. The supported values of `policy` are:
  - `always-off` tells the unit to remain powered down when power is restored.
  - `always-on` tells the unit to always power on when power is restored.
  - `previous` tells the unit to return to its previous state when power is restored.
- `power` enables you to view or change the Unity Storage System's power state . The supported operands are :
  - `cycle` cycles power to the unit by turning it off for at least one full second.
  - `diag` sends a diagnostic interrupt (NMI) to the processor or processors.
  - `off` turns power to the unit off.
    CAUTION: This operation does not initiate a clean shutdown of the operating system before turning power off.
  - `on` turns unit power on.
  - `reset` performs a hard reset of the unit.
  - `soft` initiates a soft shutdown of the operating system by emulating a fatal over temperature.
  - `status` displays the unit's current power status.
- `restart_cause` displays the cause of the most recent system restart.
- `selftest` checks the basic health of the `open` IPMI interface by initiating a self test and displaying the results.
- `sensor` displays CPU temperature and voltage, and fan status for the controller on which you are running the command.
- `status` displays information regarding the high-level status of the system chassis and main power subsystem.

CAUTION: The `chassis` sub-command provides additional options for managing the Unity Storage System's chassis. However, it is NOT recommended that you use these additional options unless you are instructed to do so by Nexsan Technical Support.

`lan`

This sub-command performs various actions on the Unity Storage System's local area network. The supported operations are `print` and `set`.

- `print [<channel>]` displays the current configuration of the specified LAN channel. If no channel is specified, it displays the configuration of the first found LAN channel.

- `set <channel> <action> <parameter>` enables you to set various settings on the specified LAN channel. The settings that can be set are:
  - `ipaddr <n.n.n.n>` sets the IP address for the LAN channel.
  - `netmask <n.n.n.n>` sets the subnet mask for the LAN channel.
  - `defgw ipaddr <n.n.n.n>` sets the default gateway IP address.
  - `bakgw ipaddr <n.n.n.n>` sets the backup gateway IP address.
  - `password <password>` sets the session password for this channel.
  - `user` enables the default user for this channel. It requires no parameter.

CAUTION: The `lan` sub-command provides additional options for managing the Unity Storage System's LAN channels. However, it is NOT recommended that you use these additional options unless you are instructed to do so by Nexsan Technical Support.

Example 1 — We get the power status for a remote unit.

```
ipmitool -I lan -H 172.116.12.10 chassis power status
Chassis Power is on.
```

Example 2 — We set the IP address for a LAN channel connected to the local unit.

```
ipmitool lan set 1 ipaddr 172.115.15.12
Setting LAN IP Address to 172.115.15.12
```


isainfo

To run this command:

1. Access the CLI command shell—see Accessing the nxadmin and nxcmd CLIs on page 13.
2. Type the command using the syntax provided in this topic.
3. Press Enter.

Description — This command is used to identify various attributes of the CPU on the currently running system. When used with no options, `isainfo` displays the names of the native instruction sets for applications supported by the current version of the operating system.

Controller — Run this command on either controller.

Syntax

```
isainfo
[-v [-b | -k | -n]]
[-x]
```

Options

`-v`

This option displays more detailed information, including applications.

`-b`

This option displays the number of bits in the address space of the native instruction set.

`-k`

This option displays the name of the instruction sets used by the operating system kernel components, such as device drivers and STREAMS modules.

`-n`

This option displays the name of the native instruction set used by portable applications supported by the current version of the operating system.

`-x`

This option displays instruction extensions to the native ABI which are supported by the platform.

Example

```
isainfo
amd64 i386
```

```
isainfo -k
amd64
```

```
isainfo -x
amd64: vmx avx xsave pclmulqdq aes sse4.2 sse4.1 ssse3 popcnt
tscp cx16 sse3 sse2 sse fxsr mmx cmov amd_sysc cx8 tsc fpu
i386: vmx avx xsave pclmulqdq aes sse4.2 sse4.1 ssse3 popcnt
tscp ahf cx16 sse3 sse2 sse fxsr mmx cmov sep cx8 tsc fpu
```


kill

To run this command:

1. Access the CLI command shell—see Accessing the nxadmin and nxcmd CLIs on page 13.
2. Type the command using the syntax provided in this topic.
3. Press Enter.

Description

This command terminates a running process. It requires the process ID, which can be obtained using the `ps` command.

CAUTION: Use this command with extreme caution, as it may terminate vital system processes.

Controller

Run this command on the active controller.

Syntax

`kill <process ID>`

Note: This command does not display a confirmation.

Options

`<process ID>`

This option specifies the ID of the process that you wish to terminate or quiesce.

Example

```
kill 24010
```

led

To run this command:

1. Access the CLI command shell—see Accessing the nxadmin and nxcmd CLIs on page 13.
2. Type the command using the syntax provided in this topic.

3. Press Enter.

Description

This command enables you to configure LED beacons for the Unity Storage System's chassis and drives. It also enables to view LED status for troubleshooting purposes when you do not have physical access to the chassis.

There are two LED modes: `ident`(normal state) and `fail`(failed state).

The `led` command monitors the drive LED status. On the Unity Storage System, drive carriers display the drive status as follows:

- A steady red or orange LED indicates a drive failure.
- A blinking red or orange LED indicates that a user turned on the identification LED.

Controller

Run this command on any controller.

Syntax

```
led
[-c <command>]
[-p <property>]
[-n <chassis number>]
[-d <disk>]
[-s <slot>]
[-m <ledtype>]
```

Options

`-c <command>`

This option specifies the sub-command to be executed by the `led` command. The allowed sub-commands are:

- `list` displays the chassis and drives of the Unity Storage System.
- `get` obtains the LED status(es) of the specified drive or chassis. `get` must be used with `-p` and its associated arguments.
- `set` configures the LED status(es) to the specified value (with `-m`) for the specified drive. `set` must be used with `-p` and its associated arguments.
- `unset` reverts the LED status(es) back to their default value for the specified chassis or drive. `unset` must be used with `-p` and its associated arguments.

`-p <property>`

This option specifies a property. When used with `-c get`, it displays the current value of the property. When used with `-c set`, it sets the property to the specified value(s). When used with `-c unset`, it reverts the value(s) back to its(their) default value(s) for the property.

The properties supported by this option are:

- `chassis` identifies the chassis on which to run the command. The command displays, sets or unsets the LED status of all disks in the chassis.

  `chassis` must be used with `-c` and `-n`.
- `drive` identifies the drive on which to run the command. The command displays, sets or unsets the LED on the drive.

  `drive` must be used with `-c`, `-n`, `-d` or `-s`, and optionally `-m`.

- `faileddrive` identifies a drive that has failed. The command sets or unsets the LED status on the failed drive. In cases where the LED is off for unknown reasons, this command enables you to turn the LED back on.

  `faileddrive` must be used with `-c`. No other arguments are required; the `led` command will automatically detect the faulted drives.

  Note: When replacing a faulty drive, the drive does not appear in the output of `-c list` anymore. To see the disk LED status, run the `led -c get -p chassis -n chassis_number` command.

`-n <chassis number>`

This option specifies the Unity Storage System's chassis number (not the chassis ID).

`-d <disk>`

This option specifies the disk(s) on which to perform the action. You separate the disk IDs with commas; for example, `c2t5000C5002607817Bd0,c2t5000C5002607A75Bd0`.

`-s <slot>`

This option specifies the slot(s) on which to perform the action. You separate the slot numbers with commas; for example, `1,2,5`.

`-m <ledtype>`

This option configures the LED type—`ident` or `fail` when used with `-c set`. It displays the current LED mode when used with `-c get`. `ident` means the LED status reflects a normal state, and `fail` indicates a LED status of failed. The default is `ident`.

Example 1

We display the list of chassis and disks for an NST6000connected to an NST224X. Note that this example only displays an excerpt of the first chassis output. You notice that the disk numbering starts at 03; this means that there are no disks in slots 01 and 02.

```
led -c list
2 Chassis found
Chassis - 01: JBOD 500093d001b23000 NEXSAN-NST224X 0450 /dev/es/ses0
(tier 1) 22 disks
03 c2t500003946818C130d0 hc://:product-id=NEXSAN-NST224X:chassis-
id=500093d001b23000:serial=EAA0PCB05WR7:part=TOSHIBA-
MBF2450RC:revision=0109/bay=3/disk=0
04 c2t500003946818C104d0 hc://:product-id=NEXSAN-NST224X:chassis-
id=500093d001b23000:serial=EAA0PCB05WR0:part=TOSHIBA-
MBF2450RC:revision=0109/bay=4/disk=0
05 c2t500003946818C1D8d0 hc://:product-id=NEXSAN-NST224X:chassis-
id=500093d001b23000:serial=EAA0PCB05WS5:part=TOSHIBA-
MBF2450RC:revision=0109/bay=5/disk=0
06 c2t500003946818C0F4d0 hc://:product-id=NEXSAN-NST224X:chassis-
id=500093d001b23000:serial=EAA0PCB05WPU:part=TOSHIBA-
MBF2450RC:revision=0109/bay=6/disk=0
07 c2t500003942800F7B4d0 hc://:product-id=NEXSAN-
NST224X:chassis-
id=500093d001b23000:serial=EAA0PC705T95:part=TOSHIBA-
```

```
MBF2450RC:revision=0109/bay=7/disk=0
...
23 c2t50000393F8211684d0 hc://:product-id=NEXSAN-NST224X:chassis-
id=500093d001b23000:serial=EAA0PC405RVF:part=TOSHIBA-
MBF2450RC:revision=0109/bay=23/disk=0
24 c2t50000393F821152Cd0 hc://:product-id=NEXSAN-NST224X:chassis-
id=500093d001b23000:serial=EAA0PC405RTW:part=TOSHIBA-
MBF2450RC:revision=0109/bay=24/disk=0
Chassis - 02: UNITY4400 5001e674e35e3fff Intel-RES2CV360 0b00
/dev/es/ses1 (tier 1) 2 disks
02 c2t5000039308138DE4d0 hc://:product-id=Intel-RES2CV360:chassis-
id=5001e674e35e3fff:serial=EA00PB109GWG:part=TOSHIBA-
MBF2600RC:revision=0108/bay=1/disk=0
11 c2t50000394BC88F5D4d0 hc://:product-id=Intel-RES2CV360:chassis-
id=5001e674e35e3fff:serial=43U0A002TVL6:part=TOSHIBA-
PX02SMF020:revision=0103/bay=10/disk=0
```

Example 2 — We obtain the LED status for all disks in the first chassis.

```
led -c get -p chassis -n 01
```

Example 3 — We obtain the LED status for drives in the first four slots in first chassis. Following our first example, the Unity Storage System indicates that there are no disks in slots 01 and 02.

```
led -c get -p drive -s 1,2,3,4 -n 01
No disk in slot 01
No disk in slot 02
03 c2t500003946818C130d0 - fail: (OFF) - ident: (OFF)
04 c2t500003946818C104d0 - fail: (OFF) - ident: (OFF)
```

Example 4 — We replaced a failed drive and change the new drive's LED mode to `ident` (normal state).

```
led -c unset -p faileddrive -d c2t5000C5002607A75Bd0
```

listfcclients

To run this command:

1. Access the CLI command shell—see Accessing the nxadmin and nxcmd CLIs on page 13.
2. Type the command using the syntax provided in this topic.
3. Press Enter.

Description	This command lists the connected Fibre Channel clients, their initiator WWN, target WWN, status, and connection information.
Controller	Run this command on either controller.
Syntax	`listfcclients`
Options	None

Example **listfcclients**

```
Fibre channel clients:
 + Initiator WWN:21000024ff4da7aa
   Target WWN: 50003a4000057801
   Status: online
   Connection: 3/pci1077,15e@0 of the QLogic QLE2562 2-Port
   Fibre Channel Card
```

listug

To run this command:

1. Access the CLI command shell—see Accessing the nxadmin and nxcmd CLIs on page 13.
2. Type the command using the syntax provided in this topic.
3. Press Enter.

Description This command displays local user and group accounts configured on the Unity Storage System.

Controller Run this command on the active controller.

Syntax `listug [users | groups]`

Options `users`

This option displays local user accounts configured on the Unity Storage System.

`groups`

This option displays local group accounts configured on the Unity Storage System.

Example **listug users**

```
testuser(10100) : ecenterusers(99999)
```

listug groups

```
testgroup (10100) :
```

logrotate

To run this command:

1. Access the CLI command shell—see Accessing the nxadmin and nxcmd CLIs on page 13.
2. Type the command using the syntax provided in this topic.
3. Press Enter.

Description This command rotates log entries. When used with no options, it reads the `/etc/logadm.conf` file and, for every entry found in that file, checks the corresponding log file to see if it should be rotated.

Controller Run this command on the controller where the logs you wish to rotate are stored.

Syntax `logrotate`

```
<log file>
[-e <email address>] [-F <timestamps>] [-f <conf-file>] [-h] [-N]
[-n] [-r] [-V [<logname>]] [-v] [-w <entryname>]
[-p <period>] [-P <timestamp>] [-s <size>]
[-a <post-command>] [-b <pre-command>] [-c] [-g <group>] [-l] [-m
<mode>] [-M <command>] [-o <owner>] [-R <log file name>] [-t
<template>] [-z <count>]
[-A <age>] [-C <count>] [-E <command>] [-S <size>] [-T <pattern>]
```

General options

`<log file>`

This option specifies a log file to perform the rotation operation upon. By default, `logrotate` reads the `/etc/logadm.conf` file.

`-e <email address>`

This option sends errors by email to the specified address.

`-F <timestamps>`

This option uses `timestamps` instead of `/var/logadm/timestamps`.

`-f <conf-file>`

This option uses the specified file instead of `/etc/logadm.conf`. This allows non-root users to keep their own `logrotate` configuration files.

`-h`

This option displays help for the `logrotate` command.

`-N`

This option prevents the creation of an error message if the specified log file does not exist. Normally, `logrotate` produces an error message if the log file is not found. With `-N`, if the log file doesn't exist, `logrotate` moves on to the expire rules (if any) and then to the next log file (if any), without creating the empty replacement log file.

`-n`

This option displays the actions that the command will perform without actually performing them. This option is useful for checking arguments before making any changes to the system.

It is important to remember, however, that since log rotating actions are only printed with this option, `logrotate` might not find files that need expiring. But if subsequently run without the `-n` option, `logrotate` might create a file that needs expiring by performing the log rotating actions. Therefore, if you see no files being expired with the `-n` option, files still might be expired without it.

`-r <logname>`

This option removes any entries corresponding to the `<logname>` from `/etc/logadm.conf`.

`-V [<logname>]`

This option validates that an entry for `<logname>` exists in `/etc/logadm.conf` and is

syntactically correct. If <logname> is not specified, all entries in the configuration are validated.

-v

This option displays information about the operations being performed in verbose mode.

-w <entryname> [<logfile>]

This option updates the configuration file (by default /etc/logadm.conf) with the specified entry name and consisting of all options preceding -w. The entry name can be a simple word or it can be the path name of the log file. If a path name rather than a name is used, it must be a fully qualified path name.

If the <logfile> is not specified, the <entryname> is assumed to be the name of the log file.

For example, the following command creates an entry in the configuration file that rotates the /var/adm/exacct/proc file, keeping ten previous versions in /var/adm/exacct/proc.0 through /var/adm/exacct/proc.9.

% logadm -c 10 /var/adm/exacct/proc -w proc-rotate /etc/logadm.conf

Options controlling when a log file is rotated

-p <period>

This option specifies the amount of time to preserve a log file. The period can be specified as a number followed by one of the following:

- h: hours
- d: days
- w: weeks
- m: months
- y: years

The period can also be specified as either now or never. Specifying now forces log rotation. Specifying never prevents log rotation.

If this option is not used, the Unity Storage System assumes a period of 1w.

-P <timestamp>

This option uses <timestamp> instead of the current system time to determine if the log rotation period has passed. The <timestamp> should be entered as it would in the date command. The <timestamp> is always recorded in Coordinated Universal Time (UTC).

-s <size>

This option only rotates a log file when its size is equal to or greater than the specified size. The size must be specified using a number followed by one of the following:

- b: bytes
- k: kilobytes
- m: megabytes
- g: gigabytes

If this option is not used, the Unity Storage System assumes a size of `1b`.

Options controlling how a log file is rotated

`-a <post-command>`

This option executes a command after the log rotation is complete. The `<post-command>` must be a valid CLI command. Use quotes around `<post-command>` if it contains spaces or special characters.

When rotating multiple logs with one `logrotate` command, `<post_command>` is executed only once after all the logs are rotated, not once per rotated log.

`-b <pre-command>`

This option executes a command before the log rotation is complete. The `<pre-command>` must be a valid CLI command. Use quotes around `<pre-command>` if it contains spaces or special characters.

When rotating multiple logs with one `logrotate` command, `<pre_command>` is executed only once before all the logs are rotated, not once per rotated log.

`-c`

This option rotates the log file by copying it and truncating the original log file to zero length instead of renaming the log file.

`-g <group>`

This option specifies the new group to use when renaming log files.

`-l`

This option uses local time rather than Coordinated Universal Time (UTC) when renaming log files.

`-m <mode>`

This option specifies the new mode to use when renaming log files.

`-M <command>`

This option uses the specified command to rename the log file. If the keyword `$file` is specified, it is expanded to the name of the log file. Similarly, the keyword `$nfile` is expanded to the new name of the log file. The `$nfile` keyword is only available with commands provided with the `-M` option. After the command completes, the log file is replaced by the rotate file. The default `<command>` is `/bin/mv $file$nfile`.

The `<command>` must be a valid CLI command. Use quotes around `<command>` if it contains spaces or special characters.

`-o <owner>`

This option creates the new empty log file with the specified owner as the owner of the file instead of preserving the previous owner.

`-R <command>`

This option runs the specified command whenever `logrotate` rotates an old log file. This option is useful for processing log file contents after rotating the log (sorting it, removing blank lines, etc.).

The `<command>` must be a valid CLI command. Use quotes around `<command>` if it

contains spaces or special characters.

When rotating multiple logs with one `logrotate` command, the `<command>` supplied with `-R` is executed once every time a log is rotated.

`-t <template>`

This option specifies a template to use when renaming log files. A template can be a simple name, such as `/bin/adm/oldfile`, or it can contain special keywords that are expanded by `logrotate`. Allowed keywords are:

- `$basename`: The log file name without the directory.
- `$dirname`: The name of the directory where the log to be rotated is located.
- `$domain`: The domain name (see domain name).
- `$file`: The full path and file name of the log to be rotated.
- `$n`: Version number. 0 is the most recent version, 1 is the next most recent, etc.
- `$N`: The same as `-n`, but starts at 1 instead of 0.
- `$secs`: The number of seconds since 00:00:00 UTC, January 1, 1970.

If no `-t` option is specified, the default template is `$file.$n`. Actual rotation of log files, where each version is shifted up until it expires, is done using the `$n` keyword. If the template does not contain the `$n` keyword, the log file is simply renamed to the new name, and then the expiration rules, if any, are applied.

`-z <count>`

This option compresses all old log files except for the most recent `<count>` number. If `<count>` is set to `0`, all old log files are compressed.

Log files are compressed with gzip and have an extension of `.gz`.

Options controlling the expiration of old log files

`-A <age>`

This option deletes any versions that are older than the specified age. The age variable must be a number followed by one of the following:

- `h`: hours
- `d`: days
- `w`: weeks
- `m`: months
- `y`: years

`-C <count>`

This option deletes old versions of the log files until there are not more than `<count>` files left. The `<count>` variable must be an integer.

If no expiration options (`-A`, `-C`, or `-S`) are specified, the default `<count>` is 10. To prevent the default expiration rule from being applied automatically, specify `-C 0`.

`-E <command>`

This option executes the specified command to expire a file instead of deleting it. This can be useful if you wish to preserve older log files by emailing them to administrators or

by copying them into an archive.

The command must be a valid CLI command. Use quotes around the command if it contains spaces or special characters.

If the old log file is not removed or renamed by the command, `logrotate` considers it for expiration the next time that it runs on the specified log file. If present, the keyword `$file` is expanded in the specified command to the name of the file being expired.

`-S <size>`

This option deletes old log files until the total disk space used is less than the specified size. The size must be specified using a number followed by one of the following:

- `b`: bytes
- `k`: kilobytes
- `m`: megabytes
- `g`: gigabytes

`-T pattern`

This option uses the specified pattern to find old log files.

Example

We rotate `syslog` and keep eight log files. Old log files are put in the directory `/var/oldlogs` instead of `/var/log`:

```
logadm -c 8 -t'/var/oldlogs/syslog.$n' /var/log/syslog
```

ls

To run this command:

1. Access the CLI command shell—see Accessing the nxadmin and nxcmd CLIs on page 13.
2. Type the command using the syntax provided in this topic.
3. Press Enter.

Description

This command lists the files in the file systems only. Folder names are displayed in square brackets. The output is sorted alphabetically by default.

- The default format for output directed to a terminal is multi−column with entries sorted down the columns.
- The `-1` option allows single column output.
- The `-m` option enables stream output format.
- To determine output formats for the `-C`, `-x`, and `-m` options, `ls` uses an environment variable, `COLUMNS`, to determine the number of character positions available on one output line. If this information cannot be obtained, 80 columns are assumed.
- If the `-w` option is used, the argument overrides any other column width.

When setting permissions, the user or group must be set as well as the `allowdeny` argument. The user can be the following string to reference everyone: `everyone@`.

TIP: Use `helpacl` to view help on this command, as follows: `ls helpacl`.

Controller

Run this command on the controller where the directory you wish to view the contents of

is located.

Syntax

```
ls [-aAbcCdeEfFghHiklLmnopqrRsStuUwvVx1@]
ls [-/c|v] [-%atime|crtime|ctime|mtime|all]
ls [--block-size size] [--color[=when]] [--file-type]
ls [--si] [--time-style style] [file]
ls [filesystems]
ls [helpacl]
ls [help]
```

Options

`-aAbcCdeEfFghHiklLmnopqrRsStuUwvVx1@`

The mode printed when the `-e`, `-E`, `-g`, `-l`, `-n`, `-o`, `-v`, `-V`,or `-@` option is in effect consists of eleven characters. The first character can be one of the following:

- `d`: directory
- `D`: door
- `l`: symbolic link
- `b`: block special file
- `c`: character special file
- `p`: FIFO special file
- `P`: event port
- `s`: AF_UNIX address family socket
- `-`: ordinary file

The next 9 characters are interpreted as three sets of three bits each. The first set refers to the owner's permissions; the next to permissions of others in the user-group of the file; and the last to all others. Within each set, the three characters indicate permission to read, to write, and to execute the file as a program, respectively.

For a directory, execute permission is interpreted to mean permission to search the directory for a specified file. The character after permissions is an ACL or extended attributes indicator. This character is an `@` if extended attributes are associated with the file and the `-@` option is in effect. Otherwise, this character is a plus sign (`+`) character if a non-trivial ACL is associated with the file or a space character if not.

If `-/` and/or `-%` are in effect, then the extended system attributes are printed when the file system supports extended system attributes.

The following options are supported:

- `-a`: Lists all entries, including those that begin with a dot (.), which are normally not listed.
- `-A`: Lists all entries, including those that begin with a dot (.), with the exception of the working directory (.) and the parent directory (..).
- `-b`: Forces printing of non-printable characters to be in the octal \ddd notation.
- `-B`: Do not display any files ending with a tilde (~).

- `-c`: Uses time of last modification of the i-node (file created, mode changed, and so forth) for sorting (`-t`) or printing (`-l` or `-n`).
- `-C`: Multi-column output with entries sorted down the columns. This is the default output format.
- `-d`: If an argument is a directory, lists only its name (not its contents). Often used with `-l` to get the status of a directory.
- `-e`: The same as `-l`, except displays time to the second, and with one format for all files regardless of age: *mmm dd hh:mm:ss yyyy*.
- `-E`: The same as -l, except displays time to the nanosecond and with one format for all files regardless of age: yyyy-mm-dd hh:mm:ss.nnnnnnnnn.
- `-f`: Forces each argument to be interpreted as a directory and list the name found in each slot. This option turns off -l, -t, -s, -S, and -r, and turns on -a. The order is the order in which entries appear in the directory.
- `-F`: Appends a symbol after certain types of files to indicate the file type. The following symbols are used: `/` directory, `>` door file, `|` named pipe (FIFO), `@` symbolic link, `=` socket, `*` executable.
- `-g`: The same as `-l`, except that the owner is not printed.
- `-h`: All sizes are scaled to a human readable format, for example, 14K, 234M, 2.7G,or 3.0T. Scaling is done by repetitively dividing by 1024. The last `--si` or `-h` option determines the divisor used.
- `-H`: If an argument is a symbolic link that references a directory, this option evaluates the file information and file type of the directory that the link references, rather than those of the link itself. However, the name of the link is displayed, rather than the referenced directory.
- `-i`: For each file, prints the i-node number in the first column of the report.
- `-k`: All sizes are printed in kbytes. Equivalent to --block-size=1024.
- `-l`: Lists in long format, giving mode, ACL indication, number of links, owner, group, size in bytes, and time of last modification for each file.
- `-L`: If an argument is a symbolic link, this option evaluates the file information and file type of the file or directory that the link references, rather than those of the link itself. However, the name of the link is displayed, rather than the referenced file or directory.
- `-m`: Streams output format. Files are listed across the page, separated by commas.
- `-n`: The same as -l, except that the owner's UID and group's GID numbers are printed, rather than the associated character strings.
- `-o`: The same as -l, except that the group is not printed.
- `-p`: Puts a slash (/) after each filename if the file is a directory.
- `-q`: Forces printing of non-printable characters in file names as the character question mark (?).
- `-r`: Reverses the order of sort to get reverse alphabetic, oldest first, or smallest file size first as appropriate.

- `-R`: Recursively lists subdirectories encountered.
- `-s`: Indicates the total number of file system blocks consumed by each file displayed.
- `-S`: Sorts by file size (in decreasing order) and for files with the same size by file name (in increasing alphabetic order) instead of just by name.
- `-t`: Sorts by time stamp (latest first) instead of by name. The default is the last modification time. See `-c`, `-u` and `-%`.
- `-u`: Uses time of last access instead of last modification for sorting (with the `-t` option) or printing (with the `-l` option).
- `-U`: Output is unsorted.
- `-v`: The same as `-l`, except that verbose ACL information is displayed as well as the `-l` output. ACL information is displayed even if the file or directory doesn't have an ACL.
- `-V`: The same as `-l`, except that compact ACL information is displayed after the `-l` output. The format of the displayed ACL is as follows:

  ```
  entry_type : permissions : inheritance_flags : access_type
  ```

- `-w`: Multi-column output where the column width is forced to cols.
- `-x`: Multi-column output with entries sorted across rather than down the page.
- `-1`: Prints one entry per line of output.
- `-@`: The same as `-l`, except that extended attribute information overrides ACL information. An @ is displayed after the file permission bits for files that have extended attributes.

Permissions argument

The permissions argument is a (`/`) separated string of the following flags:

Note: Other flags may appear but are not supported.

- `read_data (r)`: Permission to read the data of a file.
- `list_directory (r)`: Permission to list the contents of a directory.
- `write_data (w)`: Permission to modify a file's data anywhere in the file's offset range.
- `add_file (w)`: Permission to add a new file to a directory.
- `add_subdirectory (p)`: Permission to create a subdirectory to a directory.
- `read_xattr (R)`: Ability to read the extended attributes of a file.
- `write_xattr (W)`: Ability to create extended attributes or write to the extended attribute directory.
- `execute (x)`: Permission to execute a file.
- `read_attributes (a)`: The ability to read basic attributes (non-ACLs) of a file.
- `write_attributes (A)`: Permission to change the times associated with a file or directory to an arbitrary value.
- `delete (d)`: Permission to delete a file.
- `delete_child (D)`: Permission to delete a file within a directory.

- `read_acl (c)`: Permission to read the ACL of a file.
- `write_acl (C)`: Permission to write the ACL of a file.
- `write_owner (o)`: Permission to change the owner of a file.

There are permissions aliases that set multiple flags using the following:

- `full_set`: All permissions.
- `modify_set`: All permissions except `write_acl` and `write_owner`.
- `read_set read_data, read_acl, read_attributes`, and `read_xattr`.
- `write_set write_data`, `append_data`, `write_attributes`, and `write_xattr`.

Inheritance argument

The inheritance argument is a `/` separated string of the following flags:

- `file_inherit (f)`: Inherit to all newly created files.
- `dir_inherit (d)`: Inherit to all newly created directories.
- `inherit_only (i)`: When placed on a directory, do not apply to the directory, only to newly created files and directories. This flag requires that either `file_inherit` and/or `dir_inherit` is also specified.
- `no_propagate (n)`: Indicates that ACL entries should be inherited to objects in a directory, but inheritance should stop after descending one level. This flag is dependent upon either `file_inherit` and/ or `dir_inherit` also being specified.

```
[-/c|v] [-%atime|crtime|ctime|mtime|all]
```

- `/`: The `-/` option supports two option arguments `c` (compact mode) and `v` (verbose mode). Displays the long listing, same as `-l`. In addition, displays the extended system attributes associated with the file when extended system attributes are fully supported by the underlying file system.

  The attributes are as follows:

  - `atime`: Equivalent to `-u`.
  - `crtime`: Equivalent to `-u`.
  - `ctime`: Equivalent to `-c`.
  - `mtime`: Uses the last modification time of the file contents for sorting or printing. If extended system attributes are not supported or if the user does not have read permission on the file or if the crtime extended attribute is not set, crtime is treated as a synonym for mtime.
  - `all`: all available timestamps are printed.
  - The option `-%` all does not effect which timestamp is displayed in long format and does not affect sorting.

```
[--block-size size] [--color[=when]] [--file-type]
```

- `--block-size size`: Displays sizes in multiples of size. Size can be scaled by suffixing one of YyZzEePpTtGgMmKk. Additionally, a B can be placed at the end to indicate powers of 10 instead of 2. For example, `.10mB` means blocks of 10000000 bytes while `10m` means blocks of 10*2^20 -- 10485760 -- bytes. This is mutually exclusive with the `-h` option.
- `--color[=when]`: Displays file names using color on color-capable terminals. when is an optional argument that determines when to display color output. Possible values for `when` are `always`, `yes`, `force` (always use color), `auto`, `tty`, `if-tty` (use color if a terminal is present), `no`, `never`, `none` (never use color; default).
- `--file-type`: Displays a suffix after a file depending on its type, similar to the `-F` option, except `*` is not appended to executable files.

`[--si] [--time-style style] [file]`

- `--si`: Displays human scaled sizes similar to the -h option, except values are repeatedly divided by 1000 instead of 1024. The last option `--si` or `-h` determines the divisor used.
- `--time-style style`: Displays times using the specified style. This does not effect the times displayed for extended attributes (`-%`).

  Possible values for style are:

  - `full-iso`: Equivalent to -E.
  - `long-iso`: Displays in YYYY-MM-DD HH:MM for all files.
  - `iso`: Display older files using YYYY-MM-DD and newer files with MM-DD HH:MM.
  - `locale`: Use the default locale format for old and new files. This is the default.
  - `+FORMAT`: Use a custom format.
- `file`: A path name of a file to be written. If the file specified is not found, a diagnostic message is output on standard error.

`file systems`

Displays all the Unity Storage System file systems and their folders.

`helpacl`

Displays the complete help for the `ls` command.

`help`

Displays the basic help for the `ls` command.

Example 1 We display extended attributes.

```
ls -/v /pools/p1/s1s1
```

Example 2 We display time stamps.

```
ls -%all /pools/p1/s1s1
```

Example 3 We display file systems.

```
ls shares
```

This example shows one file system:

```
File system             Node      Folder
s2p1                    1         /pools/p1/s2p1
```

lun

To run this command:

1. Access the CLI command shell—see Accessing the nxadmin and nxcmd CLIs on page 13.
2. Type the command using the syntax provided in this topic.
3. Press Enter.

Description — This command enables or disables Write Protection on a LUN, and also sets the space usage threshold warning.

Controller — Run this command on any controller.

Syntax

```
lun
[-c <command>]
[-l <lun name>]
[-p <percentage>]
[-v]
```

Options

`-c <command>`

This option specifies the sub-command to be executed by the `lun` command. The allowed sub-commands are:

- `show` displays all LUNs on the Unity Storage System and their settings.
- `enablewriteprotect` sets the specified LUN to read-only mode.

  Note: When changing the write protection for a LUN mounted on a Windows client via iSCSI, it is strongly recommended that you first OFFLINE the corresponding disk on the client.
- `disablewriteprotect` sets the specified LUN to read-write.
- `setwarn` enables the threshold warning at the percentage specified with `-p`. This sub-command also modifies the percentage. If the percentage is not specified, the default value will be used, which is at 100%. It must be used with `-l` and optionally `-p`.

  Note: Before using this command, it is recommended that you:
  - remove the mask at the target level in Nexsan Unity or use the `nxcmd lun DeleteMask` command (see the *Nexsan nxcmd CLI Reference Guide*).
  - disconnect the LUN at the client level.
- `disablewarn` disables the warning threshold. It must be used with `-l`.

`-l <lun name>`

This option specifies the name of the LUN. It must be used with `-c enablewriteprotect` and `-c disablewriteprotect`.

`-p <percentage>`

The percentage of the LUN used between 1 and 99.

`-v`

This option enables verbose mode.

Example

We allow the Windows host to write data to a LUN.

1. Put the disk offline in Windows Disk Management.
2. Run the CLI command: `lun -c disablewriteprotect -l FinanceLUN`.
3. Put the disk back online in Windows Disk Management.

maintenance

To run this command:

1. Access the CLI command shell—see Accessing the nxadmin and nxcmd CLIs on page 13.
2. Type the command using the syntax provided in this topic.
3. Press Enter.

Description

This command sets the Controller resource nodes to maintenance mode, meaning that the startup mode for the cluster resource groups is set to `manual`. This prevents resource groups from being automatically migrated from one Controller node to another when a Controller fails or is taken offline. This can be useful for certain troubleshooting and maintenance procedures.

Controller

Run this command on the controller where the resource nodes you wish to put into maintenance mode are located.

Syntax

```
maintenance
[show]
[on]
[off]
```

Options

`show`

This command displays the current status of maintenance mode (either `Enabled` or `Not enabled`) and of each cluster resource.

Note: If some of the cluster service startup values are not available because the passive node is not accessible, you must check the passive node separately.

`on`

This command activates maintenance mode, which sets the startup mode for resource groups to `manual`.

`off`

This command deactivates maintenance mode, which sets the startup mode for resource groups to `auto`, which is the default operating mode.

Example

We enable maintenance mode.

```
maintenance on
Setting C01_NONE to manual on Node 1
Setting C02_NONE to manual on Node 1
Setting C01_NONE to manual on Node 2
Setting C02_NONE to manual on Node 2
```

man

To run this command:

1. Access the CLI command shell—see Accessing the nxadmin and nxcmd CLIs on page 13.
2. Type the command using the syntax provided in this topic.
3. Press Enter.

Description	This command enables you to open the man page for a specific command. The man page provides online help for a command that you are not familiar with. It provides a description, usage and syntax details, as well as examples on how to use the command.
Controller	Run this command on any controller.
Syntax	`man <command name>`
Options	`<command name>` This option specifies the command for which you want to display help.
Example	We display the help for the `nstusermaps` command. `man nstusermaps`

md5sum

To run this command:

1. Access the CLI command shell—see Accessing the nxadmin and nxcmd CLIs on page 13.
2. Type the command using the syntax provided in this topic.
3. Press Enter.

Description	This command checks and displays the MD5 (128-bit) checksums of the specified file.
Controller	Run this command on the controller where the file you wish to checksum is located.
Syntax	`md5sum <file name>`
Options	`<file name>` This option specifies the name of the file to be checked. The name must be entered as a full path. For example, `/etc/hosts`.
Example	**`md5sum /etc/passwd`** `852321ab589d1561f9c9765c9b77be7b /etc/passwd`

menu

To run this command:

1. Access the CLI command shell—see Accessing the nxadmin and nxcmd CLIs on page 13.
2. Type the command using the syntax provided in this topic.
3. Press Enter.

Description	This command displays the menu-driven nxadmin CLI. For more information see Using the menu-driven nxadmin CLI .
Controller	Run this command on either controller.
Syntax	`menu`
Options	None

modgid

To run this command:

1. Access the CLI command shell—see Accessing the nxadmin and nxcmd CLIs on page 13.
2. Type the command using the syntax provided in this topic.
3. Press Enter.

Description	This command enables you to modify the group ID (GID) or the group name of a local user account that you added to the Unity Storage System using the `useradd` command. This command adds the user to the group.
Controller	Run this command on the active controller.
Syntax	`modgid <uid> <new gid 1|group name>[,<new gid 2|group name>,...]` **Note**: This command does not display a confirmation.

Options	`<uid>`
	This option identifies the user by its current UID.
	`<new gid>`
	This option specifies the GID for the group to which you wish to assign the user. Multiple GIDs can be entered, separated by commas, to assign a user to multiple groups.
	`<group name>`
	This option specifies the name of the group to which you wish to assign the user. Multiple group names can be entered, separated by commas, to assign a user to multiple groups.

Example 1	We add user *Bob* who has a user ID of *214* to three groups using their GID numbers (*324*,*303*, and *128*). **`modgid 214 324,303,128`**
Example 2	We add user *Bob* who has a user ID of *214* to two groups using their group names

(*FinanceMTL* and *FinanceQC*).

```
modgid 214 FinanceMTL,FinanceQC
```

moduid

To run this command:

1. Access the CLI command shell—see Accessing the nxadmin and nxcmd CLIs on page 13.
2. Type the command using the syntax provided in this topic.
3. Press Enter.

Description — This command enables you to modify the user ID (UID) of a local user account that you added to the Unity Storage System using the `useradd` command.

Controller — Run this command on the active controller.

Syntax — `moduid <uid> <new uid>`

Note: This command does not display a confirmation.

Options — `<uid>`

This option identifies the user account by its current UID.

`<new uid>`

This option specifies the new UID that you wish to assign to the user account.

Example — **`moduid 213 284`**

mpstat

To run this command:

1. Access the CLI command shell—see Accessing the nxadmin and nxcmd CLIs on page 13.
2. Type the command using the syntax provided in this topic.
3. Press Enter.

Description — This command reports processor statistics in tabular form. Each row of the table represents the activity of one processor. The first table summarizes all activity since boot. Each subsequent table summarizes activity for the preceding interval. All values are rates listed as events per second unless otherwise noted.

During execution of the kernel status command, the state of the kernel can change. If relevant, a state change message is included in the `mpstat` output, in one of the following forms:

- `<<processor 3 moved from pset: -1 to: 1>>`
- `<<pset destroyed: 1>>`
- `<<pset created: 1>>`
- `<<processors added: 1, 3>>`
- `<<processors removed: 1, 3>>`

The `mpstat` command reports the following information:

- `CPU` or `SET`: Without the `-a` option, mpstat reports CPU statistics for a processor ID. With the `-a` option, mpstat reports SET statistics for a processor set ID.
- `minf`: Number of minor faults.
- `mjf`: Number of major faults.
- `xcal`: Inter-processor cross-calls.
- `intr`: Interrupts.
- `ithr`: Interrupts as threads (not including clock interrupts).
- `csw`: Context switches,
- `icsw`: Involuntary context switches.
- `migr`: Thread migrations (to another processor).
- `smtx`: Spins on mutexes (lock not acquired on first try).
- `srw`: Spins on reader/writer locks (lock not acquired on first try).
- `syscl`: System calls.
- `usr`: Percent user time.
- `sys`: Percent system time.
- `wt`: Percent I/O wait time (no longer calculated -- this statistic will always return a value of zero).
- `idl`: Percent idle time.

Controller

Run this command on either controller.

Syntax

```
mpstat [-a] [-p | -P <set>] [-q] [-T u | d] [<interval>]
[<count>]
```

Options

`-a`

This option aggregates output by processor set and sorts the output by set number.

`-p`

This option reports the set membership of each CPU and sorts the output by set number.

`-P <set>`

This option displays only the CPUs that are members of the specified processor set.

`-q`

This option suppresses the state change messages.

`-T u | d`

This option displays the system time and date at the top of the output table.

- Use `u` to output the time and date in the format of the system's internal representation (example: `1370961134`).
- Use `d` to output the time and date in the standard display format (example: `Tue Jun 11 10:31:22 EDT 2013`).

`<interval>`

This option displays output on an ongoing basis, separated by the specified number of seconds. Without this option, `mpstat` displays output only once.

`<count>`

This option specifies the number of reports to display. Without this option, `mpstat` reports statistics for all processors.

Example **`mpstat -q -T d 10`**

```
Tue Jun 11 10:31:22 EDT 2013
CPU minf mjf xcal intr ithr csw icsw migr smtx srw syscl usr sys wt idl
  0 2971   0  112  768  220 881    3   95   96   0  3475   2   5  0  95
  1  951   0   83  436  130 453    1   68   96   0   923   1   3  0  96
  2  354   0   63  243   41 286    1   45   68   0   389   1   1  0  98
  3  213   0   54  189   17 264    1   36   59   0   306   1   1  0  98
  4  137   0   36  127   12 181    1   30   50   0   201   1   1  0  98
  5   96   0   29  140   14 216    1   30   50   0   226   1   1  0  98
  6   89   0   19  102   10 160    1   27   45   0   167   1   1  0  98
  7   76   0   21  131   13 211    1   29   49   0   213   1   1  0  98
  8 2931   0  113  288   11 645    3   56   95   0  3323   2   4  0  94
  9 1059   0   78  233   13 343    1   48   99   0  1055   1   2  0  97
```

2

netstat

To run this command:

1. Access the CLI command shell—see Accessing the nxadmin and nxcmd CLIs on page 13.
2. Type the command using the syntax provided in this topic.
3. Press Enter.

Description This command displays the contents of certain network-related data structures in various formats, depending on the options you select.

With no options, `netstat` displays connected sockets for `PF_INET`, `PF_INET6`, and `PF_UNIX`, unless otherwise modified by the `-f` option.

Controller Run this command on the controller for which you wish to view network data.

Syntax

```
netstat
[-a | -n |-v | -R]
[-f <address-family> | <filter>]
[-P <protocol]
[-g | -p | -s | -m | -i | -r | -M | -D]
[-I <interface>]
[<interval> [<count>]]
[-T u | d]
```

Options

`-a`

This option displays the state of all sockets, all routing table entries, or all interfaces, both physical and logical. Normally, listener sockets used by server processes are not shown. Under most conditions, only interface, host, network, and default routes are shown and only the status of physical interfaces is shown.

`-n`

This option displays network addresses as numbers. Normally, `netstat` displays network addresses as symbols.

`-v`

This option displays additional information for the sockets, STREAMS memory statistics, routing table, and multicast group memberships.

`-R`

This option displays extended security attributes for sockets and routing table entries. The `-R` option is available only if the system is configured with the OS Trusted Extensions feature.

When used with `-r`, this option displays the gateway security attributes for the routing entries.

When used with no display modifiers (none of `[-g | -p | -s | -m | -i | -r | -M | -D]`), this option displays additional information for Multi-Level Port (MLP) sockets. This includes the label for the peer if the socket is connected.

The following flags can be appended to the socket's 'State' output:

- `P`: The socket is an MLP on a zone-private IP addresses.
- `S`: The socket is an MLP on an IP addresses shared between zones.

`-f <address-family> | <filter>`

When used with `<address-family>`, this option limits the information displayed to that of the specified address family. The value of <address-family> can be one of the following:

- `inet`: For the `AF_INET` address family showing IPv4 information.
- `inet6` : For the `AF_INET6` address family showing IPv6 information.
- `unix`: For the `AF_UNIX` address family.

When used with `<filter>` (available for the `-r` option only), this option limits the display of routes to those matching the specified filter. A filter rule consists of a <keyword>:<value> pair. The known keywords and the value syntax are:

- `af:{inet|inet6|unix|number}`: Selects an address family. This is identical to `-f address_family`, and both syntaxes are supported.
- `outif:{name|ifIndex|any|none}`: Selects an output interface. You can specify the interface by name or by ifIndex number. If `any` is used, the filter matches all routes having a specified interface (anything other than NULL). If `none` is used, the filter matches all routes having a NULL interface.

- `dst:{ip-address[/mask]|any|none}`: Selects a destination IP address. If specified with a mask length, any routes with matching or longer (more specific) masks are selected. If `any` is used, then all addresses but `0` are selected. If `none` is used, then address `0` is selected.
- `flags:[+ -]?[ABDGHLMSU]+`: Selects routes tagged with the specified flags. By default, the flags as specified must be set in order to match. With a leading `+`, the flags specified must be set but others are ignored. With a leading `-`, the flags specified must not be set and others are permitted.

You can enter multiple instances of `-f` to specify multiple filters.

`-P <protocol>`

This option limits the display of statistics or sockets states to those applicable to `<protocol>`. The protocol can be one of `ip`, `ipv6`, `icmp`, `icmpv6`, `igmp`, `udp`, `tcp`, or `rawip`; `rawip` can also be specified as `raw`. This option only accepts protocol options entered in all lowercase.

`-g`

This option displays the multicast group memberships for all interfaces. If the `-v` option is included, source-specific membership information is also displayed.

`-p`

This option displays the net-to-media tables.

`-s`

This option displays per-protocol statistics.When used with the `-M` option, it shows multicast routing statistics instead. When used with the `-a` option, per-interface statistics are displayed, when available, in addition to statistics global to the system.

`-m`

This option displays the STREAMS memory statistics.

`-i`

This option displays the state of the interfaces that are used for IP traffic. Normally this shows statistics for the physical interfaces. When combined with the `-a` option, it also reports information for the logical interfaces.

`-r`

This option displays the routing tables. Normally, only interface, host, network, and default routes are shown, but when this option is combined with the `-a` option, all routes are displayed, including cache. If you have not set up a multicast route, `-ra` might not show any multicast routing entries, although the kernel will derive such an entry if needed.

`-M`

This option displays the multicast routing tables. When used with the `-s` option, it shows multicast routing statistics instead.

`-D`

This option displays the status of DHCP-configured interfaces.

`-I <interface>`

This option displays the state of a particular interface. The `<interface>` variable can be any valid interface such as `hme0` or `eri0`. Normally, the status and statistics for physical interfaces are displayed. When this option is combined with the `-a` option, information for the logical interfaces is also reported.

`<interval>`

This option displays statistics accumulated since last display every `<interval>` seconds, repeating forever, unless `<count>` is specified. This option may be used with `-i`, `-m`, `-s`, and `-M -s`. Some values are configuration parameters which are simply redisplayed at each interval.

`<count>`

This option displays interface statistics the number of times specified by `<count>`, at the interval specified by `<interval>`.

`-T u | d`

This option displays the system time and date at the top of the output. Use `u` to output the time and date in the format of the system's internal representation (example: `1370961134`). Use `d` to output the time and date in the standard display format (example: `Tue Jun 11 10:31:22 EDT 2013`).

2

Example

netstat

```
TCP:ipv4
   Local Address        Remote Address    Swind Send-Q Rwind
Recv-Q    State
---------------- ----------- ------ ----- ------ -----------
ES600000-001-01-private0.60813 ES600000-001-02-rmi.http 4194816
0 4194856       0 ESTABLISHED
ES600000-001-mgmt-vip.http 172.21.12.175.52738   65700       0
4194580       0 ESTABLISHED
ES600000-001-01.55636 ES600000-001-01.39478 4198400      0
4196340      0 CLOSE_WAIT
ES600000-001-01.ssh 172.21.12.175.50151   65024      0 4194580
0 ESTABLISHED
...
```

netstat -g

```
Group Memberships: IPv4
Interface Group                RefCnt
--------- -------------------- ------
lo0        all-systems.mcast.net     1
ntb0       rip2-routers.mcast.net    1
ntb0       all-systems.mcast.net     2
nx0        rip2-routers.mcast.net    1
nx0        all-systems.mcast.net     4
nx99       rip2-routers.mcast.net       1
nx99       all-systems.mcast.net         3
private0  rip2-routers.mcast.net           1
```

```
private0   all-systems.mcast.net                3

Group Memberships: IPv6
If    Group                         RefCnt
----- ----------------------------- ------
lo0   ff02::1:ff00:1                    1
lo0   ff02::1                          1
```

netstat -i

```
Name  Mtu  Net/Dest      Address        Ipkts  Ierrs Opkts
 Oerrs Collis Queue
lo0   8232 loopback      ES600000-001-01 94103104 0     94103104
0     0       0
ntb0 1500 ES600000-001-01-ntb0 ES600000-001-01-ntb0 13893  0
13849 0     0      0
nx0   1500 ES600000-001-01 ES600000-001-01 55461067 0
29931931 0     0      0
nx99 1500 ES600000-001-nx99-01 ES600000-001-nx99-01 10271573 0
    8679984 0     0      0
```

ndmpsnap

To run this command:

1. Access the CLI command shell—see Accessing the nxadmin and nxcmd CLIs on page 13.
2. Type the command using the syntax provided in this topic.
3. Press Enter.

Description

This command is used to manage ndmp snapshots. With this command you can:

- List snapshots
- Remove or clear snapshots
- Setup cron jobs to autodelete snapshot

Controller

Run this command on the controller where the snapshots you wish to manage are located.

Syntax

```
ndmpsnap [-option] [command]
kill <process ID>
```

Options

The following options are supported:

- `-c`: command
- `-l`: only execute on local mode
- `-f` forcefully clear self-locked ndmp snapshots
- `-F` forcefully clear any-locked ndmp snapshots
- `-p` specific pool from which ndmp snapshots are listed or cleared
- `-T` time The time to clear the snapshots. The default is 3:30am. Use 24 hour time format, such as 3:30 for 3:30am

- `-d`day(s) The days to clear the snapshots. The default is Sunday. The format to specify the days is a number 0 to 6 (0=Sunday) and multiple days can be specified. For example only the weekdays would be 1,2,3,4,5 and only the weekends would be 6,0.

Example `ndmpsnap -c list`

network

To run this command:

1. Access the CLI command shell—see Accessing the nxadmin and nxcmd CLIs on page 13.
2. Type the command using the syntax provided in this topic.
3. Press Enter.

Description This command enables you to do the following:

- Display link status information for each network interface on the Unity Storage System (such as `up` or `down`)
- Set source-based routing rules to route network traffic back through the source interface
- Enable link aggregation
- Enable jumbo frames for interfaces (see Enabling jumbo frames on the Unity Storage System)

Controller Run this command on the controller where the network interfaces you wish to view or configure are located.

Syntax

```
network
[get lacp <interface name>]
[get sbr]
[get link <interface name>]
[get mtu <interface name>]
[set lacp <interface name> <off | active | passive>]
[set sbr <source-then-any | source-only | any>]
[set mtu <interface name> <new value>]
```

Options

`<get | set> lacp`

This command enables you to get or set the link aggregation mode of the specified interface. When using `get`, only the interface name needs to be specified. When using `set`, the mode (`off`, `active`, or `passive`) must be specified .

`<get | set> sbr`

This command lets you get or set the source-based routing rule. When using `get`, no other parameter needs to be entered. When using `set`, the new rule (`source-then-any`, `source-only`, or `any`) must be specified.

`get link`

This command enables you to display link information such as the MAC address, the link status, the link speed, i/o information, and the duplex setting.

`<get | set> mtu`

This command lets you get or set the jumbo frames setting for iSCSI interfaces. When using `get`, only the interface name needs to be specified. When using `set`, the new value (in Kb/s) must be specified.

Example

We use the `link` command to display link information for nx0.

```
network get link nx0
INT          PORT         PROPERTY           VALUE
-------------------------------------------------
nx0                       -                  0:c:29:10:8a:9b
                          LACP               off
                          MTU                1500
             e1000g2      -                  0:c:29:10:8a:9b
                          Link Speed         1000Mb
                          Link Duplex        full
                          Link State         up
                          Link AggrState     connected
                          Link InBytes        2184193204
                          Link OutBytes      234704415
```

nfs

To run this command:

1. Access the CLI command shell—see Accessing the nxadmin and nxcmd CLIs on page 13.
2. Type the command using the syntax provided in this topic.
3. Press Enter.

Description

This command enables you to change or set the NFS version 4 (NFSv4) domain on the Unity Storage System, and also set the maximum version for NFS, either 3 or 4.

Notes:

- NFSv3 uses UID/GID based permissions mapping. This means users must have the same UID/GID on both the client and the Unity Storage System.
- NSFv4 uses name-based permissions mapping. This means users must have the same name on both the client and the Unity Storage System.

Controller

Run this command on either controller.

Syntax

```
nfs
[domain show | set <domain name>]
[maxversion show | set {3 | 4}]
```

Options

`domain`

This option enables you to show or set the NFS domain on the Unity Storage System.

- Specifying `show` displays the current domain.
- Specifying `set` and a `<domain name>` sets the domain name to the specified value.

`maxversion`

This options enables you to show or set the maximum version for NFS.

- Specifying `show` displays the current maximum version.
- Specifying `set` and either `3` or `4` sets the maximum version to the value entered.

Example

```
nfs maxversion show
=4
```

nfsstat

To run this command:

1. Access the CLI command shell—see Accessing the nxadmin and nxcmd CLIs on page 13.
2. Type the command using the syntax provided in this topic.
3. Press Enter.

Description

This command displays NFS statistics. If entered with no options, it displays all NFS, RPC, and NFS_ACL information for both the server and the client side.

Controller

Run this command on either controller.

Syntax

```
nfsstat
[-c|-n|-r|-s|-z|-a]
[-T u|d]
[-v <version>]
[<interval> [<count>]]
[-m <path name>]
```

Options

`-c`

This option displays information for the client only. Can be combined with `-a`, `-n`, or `-r` to filter the information further.

`-n`

This option displays only NFS information (not NFS_ACL or RPC). Can be combined with `-c` to display NFS information for the client only, or with `-s` to display NFS information for the server only.

`-r`

This option displays only RPC information. Can be combined with `-c` to display RPC information for the client only, or with `-s` to display RPC information for the server only.

`-s`

This option displays information for the server only. Can be combined with `-a`, `-n`, or `-r`

to filter the information further.

`-a`

This option displays only NFS_ACL information. Can be combined with `-c` to display NFS_ACL information for the client only, or with `-s` to display NFS_ACL information for the server only.

`-T u|d`

This option displays the system time and date at the top of the output. Use `u` to output the time and date in the format of the system's internal representation (example: `1370961134`). Use `d` to output the time and date in the standard display format (example: `Tue Jun 11 10:31:22 EDT 2013`).

`-v <version>`

This option specifies which NSF version to display information for. The value of `<version>` can be `2`, `3`, or `4`.

`<interval>`

This option displays the statistics once every `<interval>` seconds.

`<count>`

This option displays only the `<count>` number of reports. Can only be used with `<interval>`.

`-m <path name>`

This option displays the information for each NFS-mounted file system for the specified path. This includes the server name and address, mount flags, current read and write sizes, the retransmission count, the attribute cache timeout values, failover information, and the timers used for dynamic retransmission.

The `-m` option cannot be combined with any other option. If you try to combine `-m` with any other option, an error message is displayed.

Example **`nfsstat -s -r`**

```
Server rpc:
Connection oriented:
calls    badcalls   nullrecv   badlen     xdrcall    dupchecks  dupreqs
0          0          0        0          0            0        0
Connectionless:
calls    badcalls   nullrecv   badlen     xdrcall    dupchecks  dupreqs
486361          0          0        0          0         1565        3
```

nic

To run this command:

1. Access the CLI command shell—see Accessing the nxadmin and nxcmd CLIs on page 13.
2. Type the command using the syntax provided in this topic.
3. Press Enter.

Description This command enables you to display and configure advanced network settings on the

Unity Storage System, such as link properties, usage, and aggregation (including creating, adding, modifying, and removing aggregations).

Note: The `nic` command provides several administrative functions for configuring data-link interfaces on the Unity Storage System. This command is intended for advanced users and/or for Nexsan Technical Support personnel; some options available with this command should only be executed with the assistance of a Nexsan Support Engineer.

Controller

You must run this command on both controller nodes.

Syntax

```
nic
[create-aggr [-t] [-P <policy>] [-L <mode>] [-T <timer>] [-u <address>] -l <linkname1> [-l <linkname2>...] <aggrname>]
[add-aggr [-t] -l <linkname1> [-l <linkname2>...] <aggrname>]
[delete-aggr [-t] <aggrname>]
[modify-aggr [-t] [-P <policy>] [-L <mode>] [-T <time>] [-u <address>] <aggrname>]
[remove-aggr [-t] -l <linkname1> [-l <linkname2>...] <aggrname>]
[show-aggr [-L] [-x] [-o <field>,...] [-p] [-P] [-s [-i <interval>]] [<aggrname>]]
[rename-link <oldlinkname> <newlinkname>]
[show-link -o <field>,... [-p] [-P] [-s [-i <interval>]] <linkname>]
[set-linkprop [-t] -p <prop>=<value>[,...] <linkname>]
[reset-linkprop [-t] [-p <prop>,...] <linkname>]
[show-linkprop [-o <field>,...] [-c] [-P] [-p <prop>,...] [<linkname>]]
[show-phys -H [-o <field>,..] [-p] [-P] [<physlinkname>]]
[show-usage [-a] [-p <plotfile>] [-F <format>] [-s <DD/MM/YYYY,HH:MM:SS>] [-e <DD/MM/YYYY,HH:MM:SS>] -f <logfile> <linkname>]
create-vlan [-ft] -l <link> -v <vid> [link]
delete-vlan [-t] <link>
show-vlan [-pP] [-o <field>,..] [<link>]
```

Options

`create-aggr`

This command enables you to create a link aggregation, which treats two or more physical network connection as a single connection with the specified link name. This option accepts the following arguments:

- `-t`: Specifies that the aggregation is temporary. The aggregation lasts until the system is next rebooted.
- `-L <mode>`: Specifies whether LACP should be used and, if used, the mode in which it should operate. Supported values are `off`, `active`, or `passive`. Default is `off`.

- `-l <linkname>`(required): Each Ethernet link (or port) in the aggregation is specified using an `-l` option followed by the name of the link to be included in the aggregation. Multiple links are included in the aggregation by specifying multiple `-l` options.
- `<aggrname>` (required): Sets the name of the link aggregation.

`add-aggr`

This command enables you to add one or more links to an existing aggregation. It accepts the following arguments:

- `-t`: Specifies that the addition is temporary. The addition lasts until the system is next rebooted, at which time the aggregation returns to its previous configuration.
- `-l <linkname>` (required): Specifies an Ethernet link to add to the aggregation. Multiple links can be added by supplying multiple `-l` options.
- `<aggrname>` (required): Specifies the aggregation to which you wish you add links.

`delete-aggr`

This command enables you to delete a specified aggregation. It accepts the following arguments:

- `-t`: Specifies that the deletion is temporary. The aggregation is restored when the system is next rebooted.
- `<aggrname>` (required): Specifies the aggregation to be deleted.

`modify-aggr`

This command enables you to modify the parameters of a link aggregation. It accepts the following arguments:

- `-t`: Specifies that the modification is temporary. The modification lasts until the system is next rebooted, at which time the aggregation returns to its previous configuration.
- `-L <mode>`: Specifies whether LACP should be used and, if used, the mode in which it should operate. Supported values are `off`, `active`, or `passive`. The default is `off`.
- `<link name>` (required): Specifies the aggregation that you wish to modify.

`remove-aggr`

This command enables you to remove one or more links from a specified aggregation. It accepts the following arguments:

- `-t`: Specifies that the removal is temporary. The removal lasts until the system is next rebooted, at which time the aggregation returns to its previous configuration.
- `-l <linkname>` (required): Specifies the link that you wish to remove from the aggregation. Multiple links can be removed by supplying multiple `-l` options.
- `<link name>` (required): Specifies the aggregation from which you wish to remove links.

`show-aggr`

This command displays aggregation information, LACP information, or statistics, either

for all aggregations or for a specified aggregation.

By default, with no arguments, this command displays the following fields for all aggregations:

- `LINK`: The name of the aggregation.
- `POLICY`: The LACP policy of the aggregation.
- `ADDRPOLICY`: Either `auto`, if the aggregation is configured to automatically configure its unicast MAC address (the default), or `fixed`, if `-u` was used to set a fixed MAC address.
- `LACPACTIVITY`: The LACP mode of the aggregation. Possible values are `off`, `active`, or `passive`, as set by the `-L` option for `create-aggr` or `modify-aggr`.
- `LACPTIMER`: The LACP timer value, as set by the `-T` option for `create-aggr` or `modify-aggr`. Possible values are `short` or `long`.
- `FLAGS`: A set of state flags associated with the aggregation. Currently, no flags are supported; therefore, this field should always be `-----`.

The `show-aggr` command supports the following arguments:

- `-L`: Displays detailed LACP information for the aggregation link and each underlying port. By default, with no additional arguments, it displays the following fields for each aggregation and port:
  - `LINK`: The name of the aggregation.
  - `PORT`: The name of one of the underlying ports.
  - `AGGREGATABLE`: Whether or not the port can be added to an aggregation.
  - `SYNC`: If yes, the system considers the port to be synchronized as part of the aggregation.
  - `COLL`: If yes, collection of incoming frames is enabled on the associated port.
  - `DIST`: If yes, distribution of outgoing frames is enabled on the associated port.
  - `DEFAULTED`: If yes, the port has not received LACP data from the LACP partner and is therefore using default partner information.
  - `EXPIRED`: If yes, the receive state of the port is EXPIRED.

- `-x`: Displays additional aggregation information, including detailed information on each underlying port. This command displays the following fields for each aggregation and port:
  - `LINK`: The name of the aggregation.
  - `PORT`: The name of one of the underlying ports.
  - `SPEED`: The speed of the aggregation or port in megabits per second (Mbps).
  - `DUPLEX`: Displays the duplex setting (`full` or `half`) of the aggregation or port if the aggregation `STATE` is `up`. Displays `unknown` in all other cases.
  - `STATE`: The state of the aggregation. The possible values are `up`, `down`, or `unknown`.
  - `ADDRESS`: The MAC address of the aggregation or port.
  - `PORTSTATE`: Displays the state of the individual port. The possible values are `attached` or `standby`.
- `-o <field>,...`: A case-insensitive, comma-separated list of output fields to display. The field names must be taken from those listed above, or `all` to display all fields. The fields applicable to the `-o` option are limited to those listed under each output mode. For instance, if `-L` is used, only the fields listed under `-L` can be specified.
- `-p`: Displays the command output in a stable, machine-parseable format. The `-o` argument is required when using `-p`.
- `-P`: Displays the persistent aggregation configuration rather than the state of the running system.
- `-s`: Displays aggregation statistics.
- `-i`: Used with `-s`, used to set an interval, in seconds, at which statistics should be displayed. If this argument is not used, statistics will be displayed only once.
- `<aggrname>`: Used to indicate a specific aggregation for which to display information.

`rename-link`

Used to rename a link. The first argument is the current link name. The second argument is the new name you wish to assign to the link.

`show-link`

This command displays link configuration or statistics, for one or more data links (network interfaces).

By default, with no arguments, this command displays the following fields for all data links:

- `LINK`: The name of the data link.
- `CLASS`: The class of the data link. The possible values are `phys`, which is a physical link, or `aggr`, which is an aggregation. The `show-phys` command displays more detailed information for physical links, and the `show-aggr` command displays more detailed information for aggregations.

- MTU: The maximum transmission unit (frame) size for the link, in bytes.
- STATE: The link state of the data link. Possible values are up, down, or unknown.
- OVER: The physical link over which the data link is operating. This applies to aggregations.

The show-link command accepts the following arguments:

- -o <field>,...: A case-insensitive, comma-separated list of output fields to display. If the -s option is not used, the field names must be taken from those listed above, or all to display all fields.
- -p: Displays the command output in a stable, machine-parseable format. The -o argument is required when using -p.
- -P: Displays the persistent link configuration.
- -s: Displays link statistics. The following fields are displayed by default:
  - LINK: The name of the data link.
  - IPACKETS: The number of packets received on this link.
  - RBYTES: The number of bytes received on this link.
  - IERRORS: The number of input errors.
  - OPACKETS: The number of packets sent on this link.
  - OBYTES: The number of bytes sent on this link.
  - OERRORS: The number of output errors.

  The -o option can be used to display specific fields.
- -i: Used with -s, used to set an interval, in seconds, at which statistics should be displayed. If this argument is not used, statistics will be displayed only once.
- <linkname>: Used to indicate a specific link for which to display information.

set-linkprop

This command is used to set one or more properties on the specified link. The list of properties and their values depends on the link type, the network device driver, and the networking hardware. Use the show-linkprop command to display these properties.

This command takes the following arguments:

- -t: Specifies that the changes are temporary. Temporary changes last until the system is next rebooted.
- -p <prop>=<value>[,...]: A comma-separated list of properties to set to the specified values.
- <linkname>: Used to specify the link for which you wish to set properties.

reset-linkprop

This command is used to reset one or more properties on a specified link to the value that they had at startup. If no properties are specified, all properties are reset. This command takes the following arguments:

- -t: Specifies that the resets are temporary. Temporary resets last until the system is next restarted.

- `-p <prop>[,...]`: A comma-separated list of properties to reset.
- `<linkname>`: Used to specify the link for which you wish to reset properties.

`show-linkprop`

This command is used to display the current or persistent values of one or more link properties, either for one data link or for all data links.

By default, with no arguments, this command displays the current values of the following fields for all properties on all data links:

- `LINK`: The name of the data link.
- `PROPERTY`: The name of the property.
- `PERM`: The read/write permissions of the properties. Possible values are `ro` (read-only) or `rw` (read/write).
- `VALUE`: The current property value. If the value is not set, it is displayed as `--`. If the value is unknown, it is displayed as `?`.
- `DEFAULT`: The default value of the property. If the property has no default value, it is displayed as `--`.
- `POSSIBLE`: A comma-separated list of values that the property can have. If the possible property values are unknown or unbounded, it is displayed as `--`.

The `show-linkprop` command accepts the following arguments:

- `-o <field>,...`: A case-insensitive, comma-separated list of fields to display. The field names must be taken from those listed above, or `all` to display all fields.
- `-c`: Displays the command output in a stable, machine-parseable format. The `-o` argument is required when using `-c`.
- `-P`: Displays persistent link property information instead of current values.
- `-p prop<[,...]>`: A comma-separated list of properties to show.
- `<linkname>`: Used to specify a link for which to display properties.

`show-phys`

This command enables you to display information about the device and attributes of a specified physical link or of all physical links.

By default, with no arguments, this command displays the following fields:

- `LINK`: The name of the data link.
- `MEDIA`: The media type provided by the physical data link.
- `STATE`: The state of the physical link. Possible values are `up`, `down`, or `unknown`.
- `SPEED`: The current speed of the link in megabits per second (Mbps).
- `DUPLEX`: For Ethernet links, displays the duplex setting (`full` or `half`) of the physical link if the link `STATE` is `up`. Displays `unknown` in all other cases.
- `DEVICE`: The name of the physical device under this link.

The `show-phys` command takes the following arguments:

- `-H`: Displays hardware resource usage as returned by the network interface card (NIC) driver. The following fields are displayed by default:
  - `LINK`: A physical device corresponding to a NIC driver.
  - `GROUP`: A collection of `RINGS`.
  - `GROUPTYPE`: Receive (`RX`) or transmit (`TX`). All `RINGS` in a `GROUP` are of the same type.
  - `RINGS`: A hardware resource used by a data link, subject to assignment by a driver to different `GROUP`s.
  - `CLIENTS`: MAC clients that are using the `RINGS` within a `GROUP`.
- `-o <field>[,...]`: A case-insensitive, comma-separated list of output fields to display. The field names must be taken from those listed above, or `all` to display all fields. The fields applicable to the `-o` option are limited to those listed under each output mode. For instance, if `-H` is used, only the fields listed under `-H` can be specified.
- `-p`: Displays the command output in a stable, machine-parseable format. The `-o` argument is required when using `-p`.
- `-P`: Displays the persistent configuration for all links, including those that have been removed from the system. When `-P` is specified, an additional field, `FLAGS`, is displayed. If a link has `FLAGS` value of `r`, it means the physical device associated with a physical link has been removed.
- `<physlinkname>`: Used to specify a physical link for which you wish to display information.

`show-usage`

This command is used to display historical network usage from a stored extended accounting file. The default output is the summary of network usage for all current links for the entire period for which extended accounting is available. This command takes the following arguments:

- `-a`: Displays all network usage during the period for which extended accounting is available, including usage for links that are no longer present.
- `-f <filename>`: The name of the file from which to read the extended accounting records of network usage.
- `-p <plotfile>`: Writes the network usage data to a file of the format specified by `-F`, which is required.
- `-F <format>`: Specifies the format of the plot file defined by `-p`. Currently, `gnuplot` is the only supported format.
- `-s <time>`: The time, in DD/MM/YYYY,HH:MM:SS format, from which to begin retrieving network usage data from the extended accounting records. If `-s` is not specified, retrieval begins at the earliest time for which data is available.
- `-e <time>`: The time, in DD/MM/YYYY,HH:MM:SS format, at which to stop retrieving network usage data from the extended accounting records. If `-e` is not specified, retrieval continues through the most recent available data.

- `<linkname>`: Used to specify a particular link for which to retrieve network usage data. If no link is specified, this command retrieves network usage data for all links.

`create-vlan [-f] -l <link> -v <vid> [link]`

This command creates a virtual LAN with an ID (that is not currently used); for example, `nx2`, `nx3`, etc. VLANs are isolated networks that are configured through switches or router devices. All VLANs created will use the same physical port as `nx0`. You can create as many VLANs as you want.

Note: The `nic create-vlan` command must be run on both nodes.

All packets going over the new interface that you created with `create-vlan` will be tagged with the ID specified with `-v`.

Note: `nx0` and `nx1` are always untagged by default; you must untag them on the switch manually.

After creating a VLAN, the new virtual interface displays when you run the `setip` command. You must enter the IP addresses, as needed, to configure the VLAN.

This command takes the following arguments:

- `-f`: Forces the creation of the VLAN link. Some devices do not allow frame sizes large enough to include a VLAN header. When creating a VLAN link over such a device, the -f option is needed, and the MTU of the IP interfaces on the resulting VLAN must be set to 1496 instead of 1500.
- `-l`: Specifies the link over which the VLAN is created (for example, `nx0`).
- `-v`: Specifies the virtual ID of the VLAN.
- `link`: Name of the VLAN link (for example, `nx1`).

`delete-vlan <link>`

This command deletes the specified VLAN.

`show-vlan [-pP] [-o <field>,..] [<link>]`

This command displays the VLAN configuration for all VLAN links or for the specified VLAN link.

This command accepts these arguments:

- `-p`: Displays output using a stable machine-parseable format. You must use it with the `-o` option. The output format is one or more lines of colon (:) delimited fields. The fields displayed are specific to the sub-command used and are listed under the entry for the -o option for a given sub-command. Output includes only those fields requested by means of the -o option, in the order requested. When you request multiple fields, any literal colon characters are escaped by a backslash (\) before being output. Similarly, literal backslash characters will also be escaped (\\).
- `-P`: Displays the persistent VLAN configuration rather than the state of the running system.

- `-o`: Displays a case-insensitive, comma-separated list of output fields. The field name must be one of the fields listed below, or the special value all, to display all fields. For each VLAN link, the following fields can be displayed:
  - `link`: Name of the VLAN link (for example, `nx1`).
  - `vid`: ID associated with the VLAN.
  - `over`: Name of the physical link over which this VLAN is configured.
  - `flags`: Set of flags associated with the VLAN link. Possible flags are `f` (the VLAN was created using the `-f` option to `create-vlan`), and `i` (the VLAN was implicitly created when the DLPI link was opened. These VLAN links are automatically deleted on last close of the DLPI link).
- `link`: Name of the VLAN link (for example, `nx1`).

Example 1 We display the CLASS, MTU, and STATE of the *nx0* network interface.

```
nic show-link -o class,mtu,state nx0
CLASS                MTU                  STATE
aggr                 1500                 up
```

Example 2 We add an additional port, *igb6*, to the secondary network interface, *nx1* by running this command on both nodes:

```
nic add-aggr -l igb6 nx1
```

Then, it is recommended to verify that the link layer configuration is identical on both nodes:

```
nic show-link
```

Example 3 We delete a secondary network interface, *nx1*, by running this command on both nodes:

```
nic delete-aggr nx1
```

Then, it is recommended to verify that the link layer configuration is identical on both nodes:

```
nic show-link
```

Example 4 We create a VLAN called *nx2* to which we assign tag *397*. *nx2* will use the *nx0* link, and will send tagged packets with a vlan ID of *397* so the switch will know that tagged packets of *397* will go to VLAN *397*.

On Controller 1:

```
create-vlan -l nx0 -v 397 nx2
```

On Controller 2:

```
create-vlan -l nx0 -v 397 nx2
```

Then, we configure the VLAN by assigning a new subnet and set of IP addresses to the new interface using the `setip` command. This command will open the Unity Storage System network configuration utility.

```
setip
```

nics

To run this command:

1. Access the CLI command shell—see Accessing the nxadmin and nxcmd CLIs on page 13.
2. Type the command using the syntax provided in this topic.
3. Press Enter.

Description	This command displays the physical locations of the network ports on the current Controller node.
Controller	Run this command on the controller where the network ports you wish to view information for are located.
Syntax	`nics`
Options	None

Example	**`nics`**
	`System Chassis : UNITY3300`
	`System Node # : 2`
	`igb0 : 1000 RJ45 - 1G Copper Network Port onboard, first port from the left`
	`igb1 : 1000 RJ45 - 1G Copper Network Port onboard, second port from the left`
	`igb2 : 1000 RJ45 - 1G Copper Network Port onboard, third port from the left`
	`igb3 : 1000 RJ45 - 1G Copper Network Port onboard, fourth port from the left`

nicstat

To run this command:

1. Access the CLI command shell—see Accessing the nxadmin and nxcmd CLIs on page 13.
2. Type the command using the syntax provided in this topic.
3. Press Enter.

Description	This command provides statistics on the network interfaces used by the Unity Storage System.
Controller	Run this command on either controller.

Syntax	`nicstat`
	`[-hvnsxpztual]`
	`[-i interface[,interface...]]`
	`[interval [count]]`

Options

`-h`

This option provides help content for the `nicstat` command.

`-v`

This option displays the `nicstat` version (1.90).

`-n`

This option displays statistics for non-local interfaces only (it excludes `lo0`).

`-s`

This option displays summary statistics only.

`-x`

This option displays extended statistics.

`-p`

This option displays parseable statistics.

`-z`

This option displays statistics without lines containing only zero values.

`-t`

This option displays TCP statistics.

`-u`

This option displays UDP statistics.

`-a`

This option displays statistics without lines containing only zero values, and combines the TCP and UDP statistics. It is the equivalent of running `-x -u -t`.

`-l`

This option displays Loopback, Mbit/s, Duplex, and State statistics for the network interfaces.

`-i interface`

This option displays statistics on the specified network interface(s) only.

`interval [count]`

This option displays statistics based on the specified interval, and optionally the number of seconds using the `count` option; for example:

- `nicstat 1` displays statistics every 1 second;
- `nicstat 1 5` displays statistics 5 times only;
- `nicstat -z 1` displays statistics every 1 second, and skips lines with zero values;
- `nicstat -i hme0 1` displays statistics for the `hme0` interface only every 1 second.

Example

We display summary statistics since the Unity Storage System's boot time, by not specifying any options.

```
nicstat
Time       Int       rKB/s wKB/s rPk/s wPk/s rAvs  wAvs  %Util Sat
13:32:16   lo0       0.00  0.00  0.06  0.06  0.00  0.00  0.00  0.00
13:32:16   nx0       0.11  0.00  0.34  0.00  336.0 206.3 0.00  0.00
13:32:16   private0  0.01  0.01  0.03  0.03  275.7 203.1 0.00  0.00
```

nmp

To run this command:

1. Access the CLI command shell—see Accessing the nxadmin and nxcmd CLIs on page 13.
2. Type the command using the syntax provided in this topic.
3. Press Enter.

Description	This command connects to a Unity Storage System using the Nexsan Management Protocol. This protocol is used for configuration and monitoring of Nexsan RAID systems. For complete information on NMP, please refer to the *Nexsan Management Protocol Specification* document on the Nexsan portal.
Controller	You can run this command on any controller.
Syntax	`nmp <host name>|ip`

Options	`host name`
	This command specifies the host name of the E-Series system.
	`IP`
	This command specifies the IP address of the E-Series system.

Example	We connect to the Unity Storage System using the host name. **`nmp ES260786-176-01`**

nscacherestart

To run this command:

1. Access the CLI command shell—see Accessing the nxadmin and nxcmd CLIs on page 13.
2. Type the command using the syntax provided in this topic.
3. Press Enter.

Description	This command clears the DNS client cache on the the Unity Storage System. Use this command if you want to reset, or flush, cached DNS entries on the Unity Storage System after you make changes to the DNS server on your network. **Note**: No output is displayed during this process. If an error appears, please contact Nexsan Technical Support.
Controller	Run this command on the controller having the issue.

Syntax `nscacherestart`

Options None

nstds

To run this command:

1. Access the CLI command shell—see Accessing the nxadmin and nxcmd CLIs on page 13.
2. Type the command using the syntax provided in this topic.
3. Press Enter.

Description This command displays property information for datasets (LUNs and file systems) and system datasets.

Controller Run this command on the controller where the directory of which you want to view the contents is located.

Syntax `nstds list`

Options None

Example `nstds list`

```
NAME                      USED  AVAIL  REFER  MOUNTPOINT

nest_syspool              200M  776M   32K    /nest_syspool
nest_syspool/config       2.25M 974M   2.25M  /nest_
                                              syspool/config
nstbootpool               8.98G 6.64G  46K    /nstbootpool
nstbootpool/ROOT          4.79G  6.64G 31K    legacy
nstbootpol/ROOT/nestos    4.79G 6.64G  4.01oG /
nstbootpool/export/home   87.7M 6.64G  32K    /export/home
nstbootpool/logs          10.5M 3.99G  31K    none
...
```

nstfcdata

To run this command:

1. Access the CLI command shell—see Accessing the nxadmin and nxcmd CLIs on page 13.
2. Type the command using the syntax provided in this topic.
3. Press Enter.

Description This command displays administrative information for the Fibre Channel host bus adapter (HBA) ports on the Unity Storage System. It also displays information for any Fibre Channel targets that might be connected to the ports.

Controller Run this command on the controller where you want to see fibre channel information.

Syntax

```
nstfcdata
[hba-port <port WWN>]
[remote-port <port WWN>]
[logical-unit | lu <device path>]
[-?]
[-V]
[--help]
```

Options

`hba-port <arguments> <port WWN>`

This option displays information for all initiator mode and target mode fibre channel HBA ports on the Unity Storage System. If you don't specify a port WWN, all initiator mode and target mode fibre channel HBA ports on the host are displayed.

Note: World Wide Name (WWN) are unique 8 byte (64-bit) identifiers in SCSI or fibre channel similar to that of MAC Addresses on a Network Interface Card (NIC).

You can use these optional arguments with `hba-port`:

- `-i` displays all initiator mode fibre channel HBA ports.
- `-t` displays all target mode fibre channel HBA ports.
- `-e` displays information for all FCoE ports.
- `-l` displays the link error statistics information for the HBA ports.

`remote-port <arguments> <port WWN>`

This option displays information for HBA ports on a remote Unity Storage System. If you don't specify a port, all initiator mode and target mode fibre channel HBA ports on the remote host are displayed.

You can use these optional arguments with `remote-port`:

- `-s` displays SCSI target information for the remote ports.
- `-l` displays the link error statistics information for the remote ports.

`logical-unit | lu <device path>`

This option displays the logical unit referenced by the specified device path. If you don't specify a device path, all fibre channel logical units are listed. This option applies only to the initiator mode.

`-V`

This option displays version information for the fibre channel driver.

`--help`

This option displays help content for the `nstfcdata` command.

Example

We list all HBA ports on the Unity Storage System.

`nstfcdata hba-port`

nstls

To run this command:

1. Access the CLI command shell—see Accessing the nxadmin and nxcmd CLIs on page 13.
2. Type the command using the syntax provided in this topic.
3. Press Enter.

Description	This command displays the files and directories in the current working directory for Nexsan Configuration Files. Folder names are displayed in square brackets.
Controller	Run this command on the controller where the directory you wish to view the contents of is located.
Syntax	`nstls`
Options	None

Example	**`nstls`**
	`[etc]`
	`[log]`
	`[bin]`

nstndmp

The `nstndmp` command enables you to query the NDMP (Network Data Management Protocol) service on the Unity Storage System to get the status of active sessions, terminate a session, query backup devices, and set or get the current NDMP service variables and properties.

To run this command:

1. Access the CLI command shell—see Accessing the nxadmin and nxcmd CLIs on page 13.
2. Type the command using the syntax provided in this topic.
3. Press Enter.

See also "Enabling NDMP for the Unity Storage System" in the *Nexsan nxcmd Command Line Interface Reference Guide*.

Recommended settings

Nexsan recommends that you use the default and recommended settings for NDMP listed in this topic.

NAS name

Resolves via DNS. Set to either the name of an interface on the Unity Storage System designated for backups or the IP address of the resource group. Set the `mover-nic` property on the NAS to the IP address of the resource group or applicable Unity name.

User name and password

Set user name and password in the Unity Storage System interface.

Backup level

Nexsan Unity supports incremental backups.

Description

This command enables you to query the NDMP service on the Unity Storage System to get the status of active sessions, terminate a session, query backup devices, and set or get the current NDMP service variables and properties.

CAUTION: This command is intended for advanced users and/or for Nexsan Technical Support personnel; some options available with this command should only be executed with the assistance of a Support Engineer, or with explicit instructions provided by a Support Engineer.

Controller

You must run this command on both controllers.

Syntax

```
nstndmp
[get -p <property> [-p <property>]...]
[set -p <property value> [-p <property value>]...]
[show-devices]
[show-sessions [-i tape,scsi,data,mover] [session id]...]
[kill-sessions <session id...>]
[enable -a <authentication type> -u <user name>]
[disable -a <authentication type>]
```

Options

`get -p <property> [-p <property>]...`

This command displays information for the specified properties:

- `backup-quarantine`

  Backs up the files marked as quarantined by AV. Acceptable values are `yes` or `no`. The default is `no`.

- `dar-support`

  Sets the Direct Access Recovery. DAR enables you to restore specific files from a backup set, instead of having to restore all backed up files, or having to read the entire backup tape/disc to locate the file(s). When using DAR, NDMP can find the exact location of a file using the NDMP file history interface, which reduces the amount of information processed and reduces recovery time. Acceptable values are `yes` or `no`. The default is `yes`. Nexsan recommends using DAR. DAR requires NDMP version 3 or later. DDAR is not supported.

- `<altmount>`

  Set `altmount=true` if you are using path names longer than 900 characters.

- `<UTF-8>`

  Set `UTF-8=true` to support Unicode variable width character encoding.

- `extract_acl`

  Use EXTRACT_ACL to extract Windows ACLs (Access Control Lists).

- `debug-path`

  Specifies the path where the debug log is saved. The default is `/var/ndmp`.

- `drive-type`

  Specifies either SystemV or BSD tape drives for the data management application. Valid values are `sysv` and `bsd`. The default is `sysv`.

- `dump-pathnode`

  Enables or disables backing up the directories containing modified files or directories in dump(1) backup format. Acceptable values are `yes` or `no`. The default is `no`. Nexsan recommends using tar for backups, based on recent updates.

- `fs-export`

  Specifies an optional list of mount points that are only exported paths for backup. This has no effect if you leave it empty.

- `ignore-ctime`

  Determines whether the change timestamp (ctime) of files and directories is used to determine whether a file should be backed up in level backup. If this parameter is set to yes, only the modification time (mtime) of the file or directory determines whether it should be backed up. Acceptable values are `yes` or `no`. The default is `no`.

- `restore-quarantine`

  Restores the files that had been marked as quarantined by AV and are backed up. Acceptable values are `yes` or `no`. The default is `no`.

- `tar-pathnode`

  Enables or disables backing up the directories containing modified files or directories in tar backup format. Acceptable values are `yes` or `no`. The default is `no`. Nexsan recommends using tar for backups.

- `token-maxseq`

  Sets the maximum sequence number for subsequent token-based incremental backup in NDMP-V4. The default value is 9. There are two limits for this value: soft-limit, which is 59, and hard-limit, equal to 64. If the token sequence number, passed by the DMA, is between the soft and hard limits, a warning message is issued to the DMA. The token sequence number can never exceed the hard-limit value.

- `type-override`

  Override the value of TYPE. Valid values are `zfs` and `off`. By default, type-override has a value of off and does not override TYPE. Invalid values are treated as `off`. If it is set to `zfs`, make sure that the path format used in the data management application is consistent with the zfs backup type.

- `version`

  Sets the maximum active NDMP protocol version. Valid values are currently `2`, `3`, and `4`. The default is `4`.

- `zfs-token-support`

  Enables or disables token based method for ZFS backup type. Acceptable values are `yes` or `no`. The default is `no`.

- `zfs-force-override`

  Overrides the value of ZFS_FORCE. yes forces a value of y. no forces a value of n. By default, zfs-force-override has a value of off and does not override ZFS_FORCE.

- `debug-path`

  Specifies the path where the debug log is saved. The default is `/var/ndmp`.

- `drive-type`

  Specifies either SystemV or BSD tape drives for the data management application. Valid values are `sysv` and `bsd`. The default is `sysv`.

- `dump-pathnode`

  Enables or disables backing up the directories containing modified files or directories in dump(1) backup format. Acceptable values are `yes` or `no`. The default is `no`. Nexsan recommends using tar for backups.

- `fs-export`

  Specifies an optional list of mount points that are only exported paths for backup. This has no effect if you leave it empty.

- `ignore-ctime`

  Determines whether the change timestamp (ctime) of files and directories is used to determine whether a file should be backed up in level backup. If this parameter is set to yes, only the modification time (mtime) of the file or directory determines whether it should be backed up. Acceptable values are `yes` or `no`. The default is `no`.

- `restore-quarantine`

  Restores the files that had been marked as quarantined by AV and are backed up. Acceptable values are `yes` or `no`. The default is `no`.

- `tar-pathnode`

  Enables or disables backing up the directories containing modified files or directories in tar backup format. Acceptable values are `yes` or `no`. The default is `no`. Nexsan recommends using tar for backups, based on recent updates.

- `token-maxseq`

  Sets the maximum sequence number for subsequent token-based incremental backup in NDMP-V4. The default value is 9. There are two limits for this value: soft-limit, which is 59, and hard-limit, equal to 64. If the token sequence number, passed by the DMA, is between the soft and hard limits, a warning message is issued to the DMA. The token sequence number can never exceed the hard-limit value.

- `type-override`

  Override the value of TYPE. Valid values are `zfs` and `off`. By default, type-override has a value of off and does not override TYPE. Invalid values are treated as `off`. If it is set to `zfs`, make sure that the path format used in the data management application is consistent with the zfs backup type.

- `version`

  Sets the maximum active NDMP protocol version. Valid values are currently `2`, `3`, and `4`. The default is `4`.

- `zfs-token-support`

  Enables or disables token based method for ZFS backup type. Acceptable values are `yes` or `no`. The default is `no`.

- `zfs-force-override`

  Overrides the value of ZFS_FORCE. yes forces a value of y. no forces a value of n. By default, zfs-force-override has a value of off and does not override ZFS_FORCE.

- `set -p <property value> [-p <property value>]...`

This command sets a value for the specified property. The values are the same as those provided for `get`.

- `show-devices`

This option lists the name, vendor, serial number, and other information about the storage connected to the Unity Storage System.

`show-sessions [-i tape,scsi,data,mover] [session id]...`

This option displays details of an NDMP session. You can use these arguments with `show-sessions`:

- `-i tape,scsi,data,mover` identifies a type of interface about which to obtain data. If you don't specify an interface,information for all types of interfaces is displayed.
- `ID` specifies a particular session about which to display data. If you don't specify an ID, data for all sessions is displayed.

`kill-sessions <session id...>`

This option enables you to terminate the specified session, which is identified by a number.

`enable -a <authentication type> -u <user name>`

This option prompts for the user's password twice for confirmation and activates the specified authentication type with the given user name and password for NDMP client access. Authentication type values can be `cram-md5` or `cleartext`.

`disable -a <authentication type>`

This option disables the specified authentication type for an NDMP client's remote access. Authentication type values can be `cram-md5` or `cleartext`.

Example

We display the current properties set for NDMP support on the Unity Storage System:

```
nstndmp get
debug-path=/var/ndmp
dump-pathnode=no
tar-pathnode=no
ignore-ctime=no
token-maxseq=9
version=4
dar-support=no
tcp-port=10000
backup-quarantine=no
```

```
restore-quarantine=no
overwrite-quarantine=no
nstfs-force-override=off
drive-type=sysv
vendor-name=Nexsan Technologies
product-name=NestOS v2
mover-nic=
debug-enable=false
```

nstpool

To run this command:

1. Access the CLI command shell—see Accessing the nxadmin and nxcmd CLIs on page 13.
2. Type the command using the syntax provided in this topic.
3. Press Enter.

Description	This command allows you to list storage pools on the Unity Storage System. It displays storage pool status, and view I/O statistics for a specific storage pool.
Controller	You can run this command from any controller node.
Syntax	`nstpool [status|iostat|clear|list|online] <pool> <device>`

Options	`status`
	This option displays the status for the specified pool(s): the pool state, the number of READ, WRITE, and CKSUM operations. It also displays the used disks, cache disks, and spare disks present in the pool, and specifies if any errors occurred.
	`iostat`
	This option displays I/O statistics for the specified pool(s): disk capacity (allocated and free), the number of operations (read and write), and network bandwidth (read and write).
	`clear`
	This option clears device errors in a pool.
	`list`
	This option displays the pool properties: pool name(s), size, amount of space allocated, amount of free space, capacity, health status, and altroot.
	`list`
	This option displays the pool properties: pool name(s), size, amount of space allocated, amount of free space, capacity, health status, and altroot.
	`online`
	This option brings the physical device online. It is not applicable to spares or cache devices.

<pool>

This parameter specifies the pool name. If you do not use this parameter, the `nstpool` command displays information for all storage pools existing on the Unity Storage System.

<device>

This parameter specifies the device name. Run the `nstpool status` command to display available devices.

Example

We display status information for all pools on the Unity Storage System.

```
nstpool status
pool: FinancePool1-93ecfe85-eb00-4675-b83e-22513fe5d1b7
state: ONLINE
scan: scrub repaired 0 in 0h0m with 0 errors on Sat Jul 27
00:00:36 2013
config:
        NAME                STATE     READ    WRITE    CKSUM
        FinancePool1        ONLINE    0       0        0
        raidz2-0            ONLINE    0       0        0
              c10t0d0       ONLINE    0       0        0
              c10t1d0       ONLINE    0       0        0
              c10t2d0       ONLINE    0       0        0
              c10t3d0       ONLINE    0       0        0
        raidz2-1            ONLINE    0       0        0
              c10t4d0       ONLINE    0       0        0
              c10t5d0       ONLINE    0       0        0
              c10t6d0       ONLINE    0       0        0
              c10t8d0       ONLINE    0       0        0
        spares
              c10t9d0       AVAIL
             c10t10d0       AVAIL
errors: No known data errors

pool:nstbootpool
state:ONLINE
scan:none requested
config:
        NAME                STATE     READ    WRITE    CKSUM
        nstbootpool         ONLINE    0       0        0
             c3t0d0s0       ONLINE    0       0        0
errors: No known data errors
```

nstsasdata

To run this command:

1. Access the CLI command shell—see Accessing the nxadmin and nxcmd CLIs on page 13.
2. Type the command using the syntax provided in this topic.
3. Press Enter.

Description — This command displays administrative information for the Serial Attached SCSI-2 (SAS-2) host bus adapter (HBA) on the Unity Storage System.

Controller — Run this command on the controller where you want to see SAS information.

Syntax

```
nstsasdata
[hba <hba name>]
[hba-port <hba port name>]
[expander <expander device sas address>]
[target-port <target port SAS address>]
[logical-unit|lu <operating system device>]
[-V]
[--help]
```

Options

`hba <hba_name> [-v]`

This option displays information for a specific HBA, by its HBA name. You can use the `-v` option to display additional information.

`hba-port <hba_port_name> [-y] [-v] [-a] [-l]`

This option displays information for the specified HBA port name.

Note: If you do not specify a name, the `nstsasdata hba-port` command lists all HBA ports.

You can use these arguments with the `nstsasdata hba-port` command:

- `-y` displays the physical information on the HBA port.
- `-v` displays details on hardware information, such as SAS address, topology device, and so on.
- `-a` displays the HBA port information from the HBA name of an HBA.
- `-l` displays the link error statistics information for the HBA port.

`expander <expander device sas address> [-v] [-t] [-p <hba port name>]`

This option displays the hierarchical view of the expander, referenced by the specified Expander Device SAS address.

Note: If you do not specify an Expander Device SAS address, the `sasinfo expander` command displays all expanders that are visible across all HBA ports.

You can use these arguments with the `nstsasdata expander` command:

- `-v` displays detailed information for all expanders that are visible through the specified HBA port.
- `-t` displays all target ports that are attached to expanders connected to the specified HBA port.
- `-p` displays expander information for a specific port; you must specify the HBA port name.

`target-port [-v] [-s] <target port SAS address>`

This option displays information for a specific target port, by its Target Port SAS Address.

Note: If you do not specify a Target Port SAS Address, the `sasinfo target-port` command displays all discovered target ports.

You can use these arguments with the `nstsasdata target-port` command:

- `-v` displays target ports with the HBA port and expander that they are connected to.
- `-s` displays the SCSI attributes for target ports.

`logical-unit | lu [-v] <operating system device>`

This option displays the logical unit information for a device.

Note: If you do not specify a device, the `sasinfo logical-unit` or `lu` command displays all SAS logical units, including the SAS Management Protocol (SMP) target port.

You can use the `-v` option to display additional information about the logical unit.

2

Example 1 We display all information for existing HBAs.

```
nstsasdata hba -v
HBA Name: NXSN-mpt_sas-0
Manufacturer: LSISAS2008
Model: LSI SAS2008
Firmware Version: 10.0.2.0
FCode/BIOS Version: not available
Serial Number: LSISAS2008ALL:LSI SAS2008
Driver Name: mpt_sas
Driver Version: MPTSAS HBA Driver 00.00.00.24e
Number of HBA Ports: 1
```

Example 2 We display physical information for HBA ports without specifying a port name.

```
nstsasdata hba-port -y
HBA Name: NXSN-mpt_sas-0
HBA Port Name: /dev/cfg/c5
Phy Information:
Identifier: 0
State: enabled
```

```
HardwareLinkRate(Min/Max): 1.5Gbit/6Gbit
ProgrammedLinkRate(Min/Max): 1.5Gbit/6Gbit
NegotiatedLinkRate: 6Gbit
Identifier: 1
State: enabled
HardwareLinkRate(Min/Max): 1.5Gbit/6Gbit
ProgrammedLinkRate(Min/Max): 1.5Gbit/6Gbit
NegotiatedLinkRate: 6Gbit
Identifier: 2
State: enabled
HardwareLinkRate(Min/Max): 1.5Gbit/6Gbit
ProgrammedLinkRate(Min/Max): 1.5Gbit/6Gbit
NegotiatedLinkRate: 6Gbit
```

Example 3 We display all target ports attached to all expanders.

```
nstsasdata expander -t
HBA Name: NXSN-mpt_sas-0
HBA Port Name: /dev/cfg/c5
Expander SAS Address(Tier 1): 5003048000ec12ff
Target Port SAS Address: 5000c50025de569e
Target Port SAS Address: 5000c50025de91de
Target Port SAS Address: 5000c50025de93be
Target Port SAS Address: 5000c50025dfa84e
```

Example 4 We display the SCSI attributes of all target ports.

```
nstsasdata target-port -s
Target Port SAS Address: 5000c50025de569e
Type: SAS Device
HBA Port Name: /dev/cfg/c5
Expander Device SAS Address: 5003048000ec12ff
LUN : 0
OS Device Name : /dev/rdsk/c2t5000C50025DE569Fd0s2
Vendor: SEAGATE
Product: ST32000444SS
Device Type: Disk Device
Target Port SAS Address: 5000c50025de91de
Type: SAS Device
HBA Port Name: /dev/cfg/c5
Expander Device SAS Address: 5003048000ec12ff
```

```
LUN : 0
OS Device Name : /dev/rdsk/c2t5000C50025DE91DFd0s2
Vendor: SEAGATE
Product: ST32000444SS
Device Type: Disk Device
```

Example 5 We display logical unit information for a device without additional data.

```
nstsasdata lu
OS Device Name: /dev/es/ses1
OS Device Name: /dev/rdsk/c2t5000C50025DF9693d0s2
OS Device Name: /dev/rdsk/c2t5000C50025DFB2F3d0s2
OS Device Name: /dev/rdsk/c2t5000C50025DF9B63d0s2
OS Device Name: /dev/rdsk/c2t5000C50025DE9303d0s2
```

nstsharectl

To run this command:

1. Access the CLI command shell—see Accessing the nxadmin and nxcmd CLIs on page 13.
2. Type the command using the syntax provided in this topic.
3. Press Enter.

Description This command enables you to perform advanced administrative functions on file system protocols.

Syntax

```
nstsharectl
[get [-h | -p <property> <protocol>]]
[set [-h | -p <property value>... <protocol>]]
[status [-h | <protocol]]
```

Controller You must run this command on both controllers.

Options

```
get [-h | -p <property> <protocol>]
```

This command displays the property values for the specified file sharing protocol. If you do not provide the `-p` option, the command displays all properties for the specified protocol. The protocol can be `NFS` or `SMB`. For the list of properties, see the examples below.

```
set [-h | -p <property value>... <protocol>]
```

This command sets properties for the specified file sharing protocol.

```
status [-h | <protocol>]
```

This command displays status of the specified protocol. If you do not specify any protocol, the status for all file-sharing protocols is displayed.

Example 1 We display all property values for the NFS protocol.

```
nstsharectl get nfs
servers=256
lockd_listen_backlog=32
lockd_servers=256
lockd_retransmit_timeout=5
grace_period=90
server_versmin=2
server_versmax=4
client_versmin=2
client_versmax=4
server_delegation=on
nfsmapid_domain=
max_connections=-1
protocol=ALL
listen_backlog=32
device=
```

Example 2 We display all property values for the CIFS (SMB) protocol.

```
nstsharectl get smb
system_comment=
max_workers=1024
netbios_scope=
lmauth_level=2
keep_alive=5400
wins_server_1=
wins_server_2=
wins_exclude=
signing_enabled=true
signing_required=false
restrict_anonymous=false
pdc=
ads_site=
ddns_enable=false
autohome_map=/etc
ipv6_enable=false
print_enable=false
map=
unmap=
disposition=
```

Example 3 We change the minimum version of the server NFS protocol.

```
nstsharectl set -p server_versmin=3 nfs
```

Example 4 We display status information on for all protocols used on our Unity Storage System.

```
nstsharectl status
nstcifs online
nfs online
autofs online client
smbfs online client
```

Example 5 We set the NTML authentication level to `5`. By default, the Unity Storage System uses NTML level 2 authentication (`lmauth_level` is set to `2`). If your Active Directory Domain Controller uses a different authentication level, you will have to change this setting to another value.

Refer to the table below for an explanation of the security level values supported by Nexsan.

```
nstsharectl set -p lmauth_level=5 smb
```

Setting	Description	Security Level
Send NTLM response only	Client computers use NTLMv1 authentication, and they use NTLMv2 session security if the server supports it. Domain controllers accept LM, NTLM, and NTLMv2 authentication.	2
Send NTLM2 response only	Client computers use NTLMv2 authentication, and they use NTLMv2 session security if the server supports it. Domain controllers accept LM, NTLM, and NTLMv2 authentication.	3
Send NTLM response only. Refuse LM.	Client computers use NTLMv2 authentication, and they use NTLMv2 session security if the server supports it. Domain controllers refuse to accept LM authentication, and they will accept only NTLM and NTLMv2 authentication.	4
Send NTLM response only. Refuse LM and NTLM.	Client computers use NTLMv2 authentication, and they use NTLMv2 session security if the server supports it. Domain controllers refuse to accept LM and NTLM authentication, and they will accept only NTLMv2 authentication.	5

nstusermaps

To run this command:

1. Access the CLI command shell—see Accessing the nxadmin and nxcmd CLIs on page 13.
2. Type the command using the syntax provided in this topic.
3. Press Enter.

Description — This command enables you to map local users to Microsoft Active Directory users.

Controller — Run this command on both controllers for changes to take effect.

Syntax

```
nstusermaps
[-f <command file>]
[add [-d] <name 1> <name 2>...
[dump [-n] [-v]
[export [-f <file name>] <format>]
[flush [-a]]
[get-namemap <name>]
[help]
[import [-F] [-f <file name>] <format>]
[list]
[remove [-a] | [-f|-t <name>] | [-d <name 1> <name2>...]]
[set-namemap [-a <authentication method>] [-D <bind DN>]
[-j <password file>] <name 1> <name 2>
[show [-c] [-v] identity <target type>]
[unset-namemap [-a <authentication method>] [-D <bind DN>]
[-j <password file>]
```

Options

`[-f <command file>]`

This option reads and executes sub-commands from the specified command file. The `nstusermaps -f` command reads from standard input.

`add [-d] <name 1> <name 2>`

This command creates a mapping to the corresponding user or group account in the Microsoft Active Directory domain.

```
nstusermaps add -d <windowsuser@AD.net> <unixusername>
```

`dump [-n] [-v]`

This command displays identity mapping information for users and groups existing on the Unity Storage System. It show the user or group SID (security ID) and the corresponding GID and UID.

- `-n` displays the Windows group maps.
- `-v` displays Windows group security IDs (SID) and their corresponding GIDs.

`export [-f <file name>] <format>`

This command exports user maps to the specified file and format.

`flush [-a]`

Flushes the identity mapping cache so that future mapping requests will be fully processed based on the current rules and directory information. This is a non-disruptive operation. A rule change automatically flushes the cache; this manual operation can be used to force newly changed directory information to take effect.

`get-namemap <name>`

This option displays the directory-based name mapping information from the specified name. The name can be a AD or native LDAP user or group object.

`help`

This command displays the help for the `nstusermaps` command.

`import [-F] [-f <file name>] <format>`

This command imports user maps from the specified file and format. The `-f` file option reads the rules from the specified file. The `-F` option flushes existing name-based mapping rules before adding new ones.

`list`

This command displays existing user idmaps. If there is no idmap, there is no output.

`remove [-a] | [-f|-t <name>] | [-d <windowsuser@AD.net> <unixusername>]`

This command removes a mapping from the corresponding user or group account in the Microsoft Active Directory domain. Use `-a` to remove all mapping information.

`set-namemap [-a <authentication method>] [-D <bind DN>] [-j <password file>] <windowsusername> <unixusername>`

This option sets name mapping information in the AD or native LDAP user or group object.

You can use these arguments with `set-namemap`:

- `-a` specifies the authentication method when modifying native LDAP entry. The default value is sasl/GSSAPI.
- `-D` uses the distinguished name to bind to the directory.
- `-j` specifies the file containing the password for authentication to the directory.

`show [-c] [-v] identity <target type>`

This option shows the identity of type, target-type, that the specified name maps to. If you do not specify the target type, the non-diagonal mapping is shown. By default, it shows only mappings that have been established already.

- `-c` forces the evaluation of name-based mapping configurations or the dynamic allocation of IDs.
- `-v` shows how the mapping was generated and also whether the mapping was just generated or was retrieved from the cache.

`unset-namemap [-a <authentication method>] [-D <bind DN>] [-j <password file>]`

This option unsets directory-based name mapping information from the specified name and optional target type. The name can be AD or native LDAP user or group object.

Example 1

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>`

Example 2 We display user maps to view GIDs and UIDs.

```
nstusermaps dump
usid:S-1-5-21-3198797834-3143126336-2597567724-501 ==
gid:2147483789
usid:S-1-5-21-3198797834-3143126336-2597567724-501 ==
uid:2147483649
gsid:S-1-5-21-3198797834-3143126336-2597567724-513 ==
gid:2147483650
gsid:S-1-5-2 == gid:2147483651
```

Example 3 We display Windows group GID and UID.

```
nstusermaps dump -n
wingroup:Domain Users@ES260786-176-01 == gid:2147483650
wingroup:Network == gid:2147483651
wingroup:Guests@BUILTIN == gid:2147483652
winuser:Guest@es260786-176-01.qadomain.net == gid:2147483790
winuser:Guest@ES260786-176-01 == uid:2147483649
```

Example 4 We display Windows group security IDs (SID) and their corresponding GIDs.

```
nstusermaps dump -v
gsid:S-1-5-21-3198797834-3143126336-2597567724-513 ==
gid:2147483650
Method: Ephemeral
gsid:S-1-5-2 == gid:2147483651
Method: Ephemeral
gsid:S-1-5-32-546 == gid:2147483652
Method: Ephemeral
usid:S-1-5-21-3198797834-3143126336-2597567724-501 ==
gid:2147483790
Method: Ephemeral
usid:S-1-5-21-3198797834-3143126336-2597567724-501 ==
uid:2147483649
Method: Ephemeral
```

nstvault

To run this command:

1. Access the CLI command shell—see Accessing the nxadmin and nxcmd CLIs on page 13.
2. Type the command using the syntax provided in this topic.
3. Press Enter.

Description This command displays the status of the Unity Vault Protection Modules connected to

NST6000.

Controller — Run this command from any controller.

Syntax — `nstvault`

Options — None

Example — This example displays the Unity Vault Protection Modules functioning properly.

```
nstvault
Name: NST Vault 1
Status: OL
Battery: 100.00%
Output Load: 1.00A (15.00%)
Name: NST Vault 2
Status: OL
Battery: 90.00%
Output Load: 1.00A (15.00%)
```

This example displays one of the Unity Vault Protection Modules having a failure.

```
nstvault
Name: NST Vault 1
Status: OL
Battery: 100.00%
Output Load: 1.00A (15.00%)
NST Vault 2 unreachable
```

2

ntpdate

To run this command:

1. Access the CLI command shell—see Accessing the nxadmin and nxcmd CLIs on page 13.
2. Type the command using the syntax provided in this topic.
3. Press Enter.

Description — This command enables you to set the Network Time Protocol (NTP) server for time and date synchronization with the Unity Storage System. This ensures that the date and time settings on the Unity Storage System 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.

Controller — You can run this command on any controller.

Syntax — `ntpdate -c <command> -l -h`

Options — `-c <force|status>`

The `c-` option uses one of these two parameters:

- `force` will force time synchronization with the first server on the list.
- `status` will display the current date, server list, and NTP service status.

`-l>`

The `-l` option includes local servers for date and time synchronization.

`-h>`

This option displays the help for the `ntpdate` command.

Example

We display the current NTP server setttings.

```
ntpdate -c status
... NODE[01] ...
DATE: Wed May 21 14:59:06 EDT 2014
STATE           STIME       FMRI
online          May_15      svc:/network/ntp:default
SERVERS:
time.nist.gov
... NODE[02] ...
DATE: Wed May 21 14:59:11 EDT 2014
STATE           STIME       FMRI
online          May_15      svc:/network/ntp:default
SERVERS:
time.nist.gov
```

nvram

To run this command:

1. Access the CLI command shell—see Accessing the nxadmin and nxcmd CLIs on page 13.
2. Type the command using the syntax provided in this topic.
3. Press Enter.

Description

This command enables you to view information about the FASTier write cache devices used by the Unity Storage System.

Controller

Run this command on any controller

Syntax

`nvram [-c nvdimm|info] [-v]`

Options

`-c nvdimm`

This option displays information about the power management state and the size of FASTier NVDIMM write cache devices on each controller.

`-c info`

This option displays information about the type of FASTier write cache device, the device health and activation status, and the number of virtual devices and their size.

`-v`

When specified, this option displays technical details about the FASTier write cache device, such as the number of chunks and the buffer addresses.

Example 1 — We display NVDIMM information.

```
nvram -c nvdimm
NVDIMM device 0 on Controller 1:
Power Management Unit state: Charged
Size: 8 GB
NVDIMM device 0 on Controller 2:
Power Management Unit state: Charged
Size: 8 GB
```

Example 2 — We display FASTier write cache information (NVDIMM).

```
nvram -c info
enable: 1
writecache mode: NVDIMM
solid state device health: N/A
virtual device size: 1073741824
number of virtual device: 8
local state: enabled
remote state: peer ready
```

Example 3 — We display FASTier write cache information (system memory).

```
nvram -c info
enable: 1
writecache mode: SYS RAM
solid state device health: good
virtual device size: 536870912
number of virtual device: 16
local state: enabled
remote state: peer ready
```

nxcmd

To run this command:

1. Access the CLI command shell—see Accessing the nxadmin and nxcmd CLIs on page 13.
2. Type the command using the syntax provided in this topic.
3. Press Enter.

Description — This command starts the nxcmd command line interface, which enables you to create storage pools, file systems, and LUNs on the Unity Storage System by issuing specific

commands from within the Unity Storage System NestOS command shell. The `nxcmd` command entered by itself displays a list of its available options. For complete details on `nxcmd`, see the *Nexsan Unity nxcmd Reference Guide*.

Controller — You can run this command on any controller.

Syntax — `nxcmd <option> <action> <parameter> <parameter configuration setting> [optional parameter]`

Options

- `Cluster` moves a Pool Resource Group from one controller node to the other.
- `Event` configures event notifications on the Unity Storage System, including the configuration of SMTP settings, email alerts, and system notifications.
- `FibreTarget` displays Fibre Channel target configuration.
- `InitiatorGroup` configures global LUN presentation.
- `iSCSITarget` adds and manages iSCSI targets.
- `LUN` adds and manages LUNs.
- `NestedShare` adds and manages file systems.
- `PerformanceMetric` records, monitors and manages Performance Monitor recordings.
- `Pool` adds a storage pool to the system and perform pool-level tasks.
- `Replication` sets up and manage asynchronous replication.
- `Share` adds and manages file systems.
- `Site` sets up a Unity Storage System and performs other Unity Storage System-level tasks.
- `Snapshot` manage file systems and LUN snapshots.
- `StorageDevice` displays storage device information.
- `SyncReplication` configures storage pool mirrors for data replication.
- `System` enables you to verify the Unity Storage System's version installed and perform software upgrades as well as feature updates.
- `UserManager` adds and manages CHAP users, and local user/group accounts (for Nexsan Unity authentication).

nxservices

To run this command:

1. Access the CLI command shell—see Accessing the nxadmin and nxcmd CLIs on page 13.
2. Type the command using the syntax provided in this topic.
3. Press Enter.

Description — This command enables you to configure and manage the Unity Storage System's services.

Controller

You can run this command on any controller.

Syntax

```
nxservices <listservices|service name
[debug|pid|coredump|restartrmi|signal #|build_type|friendly_
name|service_name]>
```

Options

`listservices`

This option displays all services you can configure with the `nxservices` command.

See below for information on these services.

`service name` can be any of these services. You must use a sub-command with the specified service.

- `SHAREDRESOURCE`
- `SYSTEMMANAGER`
- `SCHEDULER`
- `ZILMANAGER`
- `CALLJAVA`
- `DATASETMANAGEMENT`
- `QUERYSTORAGELOGS`
- `WEBSERVICE`
- `RESOURCEMONITOR`
- `PERFORMANCEMONITOR`: This service runs the Performance Monitor feature. The Performance Monitor provides multiple graph views that enable you to visually examine real-time performance metrics for the Unity Storage System.
- `SITERESET`: This service runs the Site Reset feature. The reset process deletes all storage pools and file systems from the Unity Storage System; unjoins the Unity Storage System from the Microsoft Active Directory Server or LDAP Directory Service, or if the Unity Storage System is configured with Nexsan Unity Authentication, it deletes all local users and groups on the system.

Sub-commands

`debug`

This sub-command fixes issues encountered with a specific service. You can use this sub-command if the Event Viewer displays error messages about a service.

Note: This command does not display a confirmation message.

`pid`

This sub-command displays the process ID of the specified service.

`coredump`

This sub-command displays the recorded state of the specified service for debugging and troubleshooting purposes.

`restartrmi`

`signal #`

`build_type`

`friendly_name`

`service_name`

This sub-command displays the path and full name of the specified service.

Example — We display the path and full name for the `calljava` service.

```
nxservices calljava service_name
system/nest-calljava
```

passwd

To run this command:

1. Access the CLI command shell as described in Accessing the nxadmin and nxcmd CLIs on page 13.
2. Type the command using this syntax.
3. Press Enter.
4. Type the new password when prompted.
5. Press Enter.

Description — This command changes the password of the **nxadmin** account on the Unity Storage System.

Controller — Run this command on the active controller for the change to take effect. (The active controller has the System Management component running on it.)

Syntax — `passwd <user>`

Options — `user`

This option specifies the name of the user for whom to change the password. If you do not specify a user name, the Unity Storage System will prompt you to change the **nxadmin** password.

peer

To run this command:

1. Access the CLI command shell as described in Accessing the nxadmin and nxcmd CLIs on page 13.
2. Type the command using this syntax.
3. Press Enter.

4. The peer name prompt will change to the controller name and display **P** next to the name. For example,

   ```
   ES260786-176-01:A:/> peer
   ES260786-176-02:P:/>
   ```

   Type your command(s) on the peer node.
5. To go back to the primary node, type `peer` again.
6. Press Enter.

Description — This command connects to the peer controller node on the Unity Storage System via SSH.

Controller — You can run this command on any controller.

Syntax — `peer`

Options — None

Example — We connect to the other controller node, then we view the existing folder and files on that node.

```
ES260786-176-02:A:/> peer
FinanceSite176:P> ls
```


perfmon

To run this command:

1. Access the CLI command shell—see Accessing the nxadmin and nxcmd CLIs on page 13.
2. Type the command using the syntax provided in this topic.
3. Press Enter.

Description — This command sets which performance metrics (accessors) will be used to monitor system performance. You can then view these performance metrics using in Nexsan Unity, using the Dashboard or the Performance Monitor.

Note: This command may cause system performance degradation.

Controller — Run this command on any controller.

Syntax —

```
perfmon
[-c <command>]
[-a <accessor>]
```

Options — `-c <command>`

This option specifies the sub-command to be executed by the `perfmon` command. The allowed sub-commands are:

- `show` displays the performance accessors.
- `enable` enables one or more performance accessor(s). It must be used with `-a`.
- `disable` disables one or more performance accessor(s). It must be used with `-a`.

- `none` disables all performance accessors.
- `all` enables all performance accessors.

`-a accessor[,accessor,accessor...]`

This option specifies the metric(s) against which the command will run. You need to separate each accessor with a comma from the following list:

`site,devices,cifs,fastier,latency,luns,nfs`

Example 1 — We display the current configuration for performance metrics

```
perfmon -c show
Node 01:
luns Disabled
nfs Disabled
devices Disabled
site Disabled
cifs Disabled
fastier Disabled
latency Disabled
Node 02:
luns Disabled
nfs Disabled
devices Disabled
site Disabled
cifs Disabled
fastier Disabled
latency Disabled
```

Example 2 — We enable performance metrics for the devices and FASTier devices on the Unity Storage System.

```
perfmon -c enable -a devices,fastier
Node 01:
enabling devices,fastier...
Node 02:
enabling devices,fastier...
```

Example 3 — We disable all performance metrics.

```
perfmon -c none
Node 01: Disabling all Accessors...
Node 02: Disabling all Accessors...
```

performance

To run this command:

1. Access the CLI command shell—see Accessing the nxadmin and nxcmd CLIs on page 13.
2. Type the command using the syntax provided in this topic.
3. Press Enter.

Description: This command gathers system performance data for troubleshooting purposes. The command launches a script for the specified duration while the system collects performance data and generates the corresponding Excel files. To go back to the shell, hit Control-C.

Controller: Run this command on any controller.

Syntax:

```
performance
[-c run -t <time>]
[-c status]
[-c stop]
[-c clean]
```

Options:

`-c run -t <time>`

This option starts monitoring and collecting system performance data for the specified duration. The time can be `1`, `6`, `12`, or `24` hours.

`-c status`

This option displays the state of the system monitoring.

`-c stop`

This option stops the monitoring of the system performance.

`-c clean`

This option removes the generated Excel files from the Unity Storage System.

Example: We collect system performance data for 12 hours.

```
performance -c run -t 12
```

ping

To run this command:

1. Access the CLI command shell—see Accessing the nxadmin and nxcmd CLIs on page 13.
2. Type the command using the syntax provided in this topic.
3. Press Enter.

Description: This command tests the reachability of a host on the network.

Controller: You can run this command on any controller.

Syntax:

```
ping host [timeout]
```

```
ping -s [-l|-U]
 [-a|-d|-b|-D|-L|-n|-R|-r|-v]
 [-A <address family>]
 [-c traffic class]
 [-g <gateway>] [-g <gateway>]]
 [-N <next hop>]
 [-F <flow label>]
 [-I <interval>]
 [-i <network interface>]
 [-P <type of service>]
 [-p <port number>]
 [-t ttl]
 [host <data size> <number of packets>]
```

Options

`-s [-l | -U]`

The `-s` option sends one datagram per second and collect statistics. The `-l` option displays the value of the hop limit field in each packet received. The `-U` option sends UDP packets instead of ICMP (ICMP6) packets.

`-a`

The `-a` option pings all addresses of a multi-homed destination. The output looks like a ping has been run once for each IP address of the destination.

If this option is used together with `-A`, `ping` probes only the addresses that are of the specified address family.

When used with the `-s` option and you do not specify the number of packets, `ping` continuously probes the destination addresses in a round robin fashion. If you specify the number of packets, `ping` sends the specified number of probes to each IP address of the destination and then exits.

`-d`

The `-d` option sets the `SO_DEBUG` socket option.

`-b`

The `-b` option bypasses the global IPsec policy and sends and receives packets in the clear for this connection only. This option can be used to troubleshoot network connectivity independent of IPsec. You must be a superuser or a user granted the `sys_net_config` privilege to use this option.

`-D`

The `-D` option turns off fragmentation. For IPv4 and IPv6, fragmentation will not be allowed when datagrams are sent. If the `packetlen` exceeds the MTU, the `ping` command may report that sending failed due to the message being too long.

`-L`

The `-L` option turns off loopback of multicast packets. Normally, members are in the

host group on the outgoing interface, a copy of the multicast packets is delivered to the local machine.

`-n`

The `-n` option shows network addresses as numbers. The `-n` option blocks the reverse lookup, so the `ping` command displays IP addresses instead of host names.

`-R`

The `-R` option stores the route of the packet inside an IPv4 header. The contents of the record route are only printed if you use the `-v` and `-s` options. They are only set on return packets if the target host preserves the record route option across echos, or if you use the `-l` option.

`-r`

The `-r` option bypasses the normal routing tables and sends directly to a host on an attached network. If the host is not on a directly-attached network, an error is returned. This option can be used to ping a local host through an interface that has been dropped by the router daemon.

`-v`

The `-v` option displays verbose output.

`-A <address family>`

The `-A` option specifies the address family of the target host; can be either `inet` or `inet6`. Address family determines which protocol to use. For an argument of inet, IPv4 is used. For inet6, IPv6 is used.

`-c <traffic class>`

The `-c` option specifies the traffic class of probe packets. The value must be an integer in the range from 0 to 255. Gateways along the path may route the probe packet differently depending upon the value of `traffic_class` set in the probe packet. This option is valid only on IPv6.

`-g <gateway>`

The `-g` option specifies a loose source route gateway. The user can specify more than one gateway by using `-g` for each gateway. The maximum number of gateways is 8 for IPv4 and 127 for IPv6.

`-N <next hop>`

The `-N` option specifies a next-hop router so that the probe packet goes through the specified router along its path to the target host. This option bypasses the system routing table and leaves the probe packet header unmodified. You can only specify one next-hop router.

`-F <flow label>`

The `-F` option specifies the flow label of probe packets. The value must be an integer in the range from 0 to 1048575. This option is valid only on IPv6.

`-I <internal>`

The `-I` option turns on the statistics mode and specifies the interval between successive transmissions. The default is one second. See the `-s` option.

`-i <network interface>`

The `-i` option specifies the outgoing interface address to use for multicast packets for IPv4 and both multicast and unicast packets for IPv6. The interface address can be a literal IP address, for example, `10.123.100.99`, or an interface name, for example, `eri0`, or an interface index, for example `2`.

`-P <type of service>`

The `-P` option sets the type of service in probe packets to the specified value. The default is zero. The value must be an integer in the range from 0 to 255. This option is valid only on IPv4.

`-p <port number>`

The `-p` sets the base UDP port number used in probes. You must use this option with the `-U` option. The default base port number is 33434. The `ping` command starts setting the destination port number of UDP packets to this base and increments it by one at each probe.

`-t <ttl>`

The `-t` option specifies the IPv4 time to live, or IPv6 hop limit, for unicast and multicast packets. The default time to live (hop limit) for multicast is one hop.

`host <data size> <number of packets>`

This option specifies the host name. You can specify a data size; the default data size is 56 bytes. If you specify the number of packets, the `ping` command sends ping requests until it either sends the number of requests or receives the number of replies.

Example

We set the `ping` command to send probe packets to all the IPv4 addresses of the host `FinanceSite`, one at a time. It sends an ICMP6 ECHO_REQUEST every second until the user interrupts it.

```
ping -s -A inet -a FinanceSite
```

prompt

To run this command:

1. Access the CLI command shell as described in "Accessing the nxadmin and nxcmd CLIs" (page 13)
2. Type the command using this syntax.
3. Press Enter. TheUnity displays your current prompt settings and the available variables you can choose to change the prompt display.
4. Enter the new prompt format.
5. Press Enter.

Description

This command changes the system prompt. The prompt uses variables so that any Unity Storage System or node change is automatically reflected in the prompt. You can also enter text in the prompt; the text will not change.

Controller — Run this command on both controllers so that the prompt remains consistent.

Syntax — `prompt ${hostname} ${site} ${node} ${active} ${path}`

Options

`${hostname}`

This option specifies the host name; for example `ES123456-001-01`. The variable must be entered as written above.

`${site}`

This option specifies the Unity Storage System friendly name; for example, `FinanceSite`. The variable must be entered as written above.

`${node}`

This option specifies the controller node, either `01` or `02`. The variable must be entered as written above.

`${active}`

This option specifies the active or passive controller, as either `:A` or `:P`. The variable must be entered as written above.

`${path}`

This option specifies the current directory. The variable must be entered as written above.

Example — We change our current prompt to display the Unity Storage System name, the node number, and the active node on the cluster.

1. Type **`prompt`**. The Unity Storage System displays the current prompt and available variables.

```
es260786-176-01:P:>
Current prompt: ${hostname}${active}:${path}
Available variables:
 ${hostname} hostname (ex. ES123456-001-01)
 ${site} site friendly name
 ${node} 01 or 02
 ${active} :A or :P on cluster nodes, blank on single nodes
 ${path} current directory
New prompt:
```

2. At the New prompt line, enter **`${site}-${node}${active}`**. Here we separate the Unity Storage System name from the node number by typing a dash.
3. Press Enter. The prompt now displays `FinanceSite176-02:P>`.

ps

To run this command:

1. Access the CLI command shell—see Accessing the nxadmin and nxcmd CLIs on page 13.
2. Type the command using the syntax provided in this topic.

3. Press Enter.

Description

This command displays all running processes on the Unity Storage System. Use this command in conjunction with the `kill` command to kill/quiesce a process, if needed.

Without options, `ps` displays information about processes that have the same effective user ID and the same controlling terminal as the invoker. The output contains only the process ID, terminal identifier, cumulative execution time, and the command name. Otherwise, the information displayed is controlled by the options.

Controller

Run this command on the active controller. (The active controller has the System Management component running on it.)

Syntax

```
ps [-aAcdefjHlLPyZ]
[-g <group list>]
[-h <lgroup list>]
[-n <name list>]
[-o <format>]
[-p <process list>]
[-s <session leader IDs>]
[-t terminal]
[-u <UID list>]
[-U <UID list>]
[-G <GID list>]
```

Options

`-a`

This option displays information about all processes most frequently requested, except session leaders and processes not associated with a terminal.

`-A`

This option lists information for all processes (identical to `-e`).

`-c`

This option displays information in a format that reflects scheduler properties. The `-c` option affects the output of the `-f` and `-l` options

`-d`

This option lists information for all processes, except session leaders.

`-e`

This option displays information about each process currently running.

`-f`

This option generates a full listing.

`-j`

This option displays session IDs and process group IDs.

`-H`

This option displays the home `lgroup` of the process under an additional column header, LGRP.

`-l`

This option generates a long listing.

`-L`

This option displays information about each light weight process in each selected process.

`-P`

This option displays the number of the processor to which the process or lwp is bound, if any, under an additional column header, PSR.

`-y`

Under a long listing (`-l`), this option omits the obsolete F and ADDR columns and includes an RSS column to report the resident set size of the process. Both RSS and SZ are reported in units of kilobytes instead of pages.

`-Z`

This option displays the name of the zone with which the process is associated under an additional column header, ZONE. This column is limited to 8 characters. To view more characters, use `ps -eZ`.

`-g <group list>`

This option displays information on the specified group leader IDs. (A group leader is a process whose process ID number is identical to its process group ID number.)

`-h <lgroup list>`

This option displays the home `lgroup`of the process under an additional column header, LGRP.

`-n <name list>`

This option specifies the name of an alternative system file in place of the default.

`-o <format>`

This option displays information according to the specified format.

`-p <process list>`

This option displays only process data for the specified ID numbers (PID).

`-s <session leaders IDs>`

This option displays information for the specified session leaders IDs.

`-t <terminal>`

This option displays only process data associated with a terminal identifier.

`-u <UID list>`

This option displays only process data for the specified user ID number or login name.

`-U <UID list>`

This option displays process information for the specified user ID numbers or login names. Use a comma to separate the UIDs or names.

`-G <GID list>`

This option displays information for processes for the specified group IDs.

Example **ps**

```
PID          TTY                      Time       CMD
24010        pts/3                    0:00       ps
```

ptree

▶ **To run this command:**

1. Access the CLI command shell—see Accessing the nxadmin and nxcmd CLIs on page 13.
2. Type the command using the syntax provided in this topic.
3. Press Enter.

Description This command displays the process tree on the Unity Storage System, including hierarchies and dependencies, for the specified process IDs or users.

Controller Run this command on the controller where you want to see the information.

Syntax `ptree [-a] [-c] [-z <zone>] [PID|<user name>]`

Options `-a`

This option displays all processes.

`-c`

This option displays process contract memberships in addition to parent-child relationships. You must use this option with `-a`.

`-z <zone>`

This option displays only process for the specified zone. The zone can be specified as either a zone name or numerical ID.

`PID | <user name>`

You must specify either the process ID (or a list of process IDs), or one or more user names.

Example ▶ **Output excerpt:**

ptree

```
10 /lib/svc/bin/svc.startd
 493 /usr/lib/saf/sac -t 300
 497 /usr/lib/saf/ttymon
 502 /usr/lib/saf/ttymon -g -d /dev/console -l console -m
ldterm,ttcompat -h -
```

```
 23228 /usr/lib/saf/ttymon -g -d /dev/vt/2 -l console -m
ldterm,ttcompat -h -p E
 23243 /usr/lib/saf/ttymon -g -d /dev/vt/3 -l console -m
ldterm,ttcompat -h -p E
 23257 /usr/lib/saf/ttymon -g -d /dev/vt/4 -l console -m
ldterm,ttcompat -h -p E
 23270 /usr/lib/saf/ttymon -g -d /dev/vt/5 -l console -m
ldterm,ttcompat -h -p E
 23284 /usr/lib/saf/ttymon -g -d /dev/vt/6 -l console -m
ldterm,ttcompat -h -p E
23322 /usr/lib/vtdaemon -s -c 16
12 /lib/svc/bin/svc.configd
44 /lib/inet/ipmgmtd
49 /lib/inet/netcfgd
51 /sbin/dlmgmtd
172 /usr/lib/pfexecd
181 /usr/lib/inet/in.mpathd -a
215 /usr/lib/zones/zonestatd
230 /usr/lib/power/powerd
233 /usr/lib/ldap/ldap_cachemgr
258 /usr/lib/dbus-daemon --system
```


pwd

To run this command:

1. Access the CLI command shell—see Accessing the nxadmin and nxcmd CLIs on page 13.
2. Type the command using the syntax provided in this topic.
3. Press Enter.

Description	This command displays the full path of the current, working directory.
Controller	Run this command on the controller where you want to see the information.
Syntax	`pwd`
Options	None
Example	We are working in the `FinancePool1` directory. **`pwd`** `/pools/FinancePool1`

reboot

To run this command:

1. Access the CLI command shell—see Accessing the nxadmin and nxcmd CLIs on page 13.
2. Type the command using the syntax provided in this topic.
3. Press Enter.

Description	This command reboots the controller node that you are currently accessing.
Controller	Run this command on the controller that you want to reboot.
Syntax	`reboot`
Options	None

replication

To run this command:

1. Access the CLI command shell—see Accessing the nxadmin and nxcmd CLIs on page 13.
2. Type the command using the syntax provided in this topic.
3. Press Enter.

Description	This command enables you to display the progress of asynchronous data replication on a dataset, to view the replication properties, and to display the current replication status of storage pool and its datasets. This command is useful if you have a large amount of data to replicate and you want to know how much data has been transferred and the estimated time remaining to complete the replication.
Controller	Run this command on the controller hosting the storage pool.

Syntax	`replication`
	`[progress <dataset name>]`
	`[get_ds <pool name|dataset name>]`
	`[show <pool name|dataset name>]`

Options	`progress <dataset name>`
	This option displays the current progress of a dataset being replicated.
	`get_ds <pool name|dataset name>`
	This option displays replication configuration properties for the specified storage pool or dataset (LUN or file system).
	`show <pool name|dataset name>`
	This option displays the replication status for the specified storage pool or dataset (LUN or file system); for example, whether the replication state is idle or replicating, or the last error message.

Example	We display the replication progress for `FinanceFileSystem2015`. You can use the

nstds list command to get the full name of the dataset.

```
replication progress financepool-240daeec-c1a0-49f0-a8de-
91a6a0aa753f/financefilesystem2015
```

Amount Sent	Percentage	Current Speed	Remaining Time
175GB	11%	4.18MB/s	0:05:23

resetcache

To run this command:

1. Access the CLI command shell—see Accessing the nxadmin and nxcmd CLIs on page 13.
2. Type the command using the syntax provided in this topic.
3. Press Enter.

Description — This command resets the system cache. The Unity Storage System caches system-level configuration settings at the server-level, and then delivers cached information on demand at the management level through Nexsan Unity. This ensures that the system performs optimally.

You may be required, under certain circumstances, to manually refresh the system cache; for example, if Nexsan Unity appears to be out of sync with configuration settings on the Unity Storage System. This command is equivalent to the **Refresh System Cache** option available from Nexsan Unity's global toolbar.

Controller — Run this command on the active controller. (The active controller has the System Management component running on it.)

Syntax — `resetcache`

Options — None

resilver

To run this command:

1. Access the CLI command shell—see Accessing the nxadmin and nxcmd CLIs on page 13.
2. Type the command using the syntax provided in this topic.
3. Press Enter.

Description — This command displays the current state of a resilvering operation and enables you to improve resilvering performance if needed.

The Unity Storage System 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, the Unity Storage System copies the data from one disk (or volume) to another.

Controller — Run this command on the controller hosting the storage pools affected by the resilvering operation.

Syntax — `resilver [improve|default|show]`

Options — `improve`

This option improves the performance of resilvering on the fly for storage pools with a lot of data. However, data access performance will be reduced as a result. Once the resilvering operation is complete, revert back to the default state.

`default`

This option sets the default resilvering state.

`show`

This option displays the current resilvering state.

Example —

```
resilver default
zfs_resilver_delay: 0x2 = 0x2
zfs_scrub_delay:0x4 = 0x2
zfs_top_maxinflight: 0x20 = 0x20
zfs_resilver_min_time_ms: 0xbb8 = 0xbb8
updating //platform/i86pc/boot_archive
updating //platform/i86pc/amd64/boot_archive
```


route

To run this command:

1. Access the CLI command shell—see Accessing the nxadmin and nxcmd CLIs on page 13.
2. Type the command using the syntax provided in this topic.
3. Press Enter.

Description — This command enables you to add TCP/IP routing entries to the routing table on the Unity Storage System. On an the Unity Storage System with both the (onboard) 1Gb network interface and the (optional) 10Gb interface, if you configured the 1Gb interface as a secondary network connection, you can use the route command to add a routing entry to the routing table on the Unity Storage System, in order for the system to route data requests to the subnet that you configured for the secondary 1Gb interface.

When adding a routing entry to the routing table using the route command, you need the:

- destination host IP or destination network Subnet/Mask
- IP address of the router (on the same subnet as the 1Gb interface) that will route to the destination host/subnet

Controller — You must run this command on both controllers.

Syntax — `route [-f|-n|-p|-q|-v] [[-sub-commands] arguments]`

Options — `-f`

This option flushes the routing tables of all gateway entries. If you use the `-f` option with any of the route sub-commands, `route` flushes the gateways before performing the sub-command. Specify the table to flush by entering `inet` or `inet6` immediately after the `-f` option. If you do not specify a table, IPv4 (`inet`) routes is the default.

`-n`

This option prevents attempts to print host and network names symbolically when reporting actions. This option is useful when name servers are unavailable.

`-p`

This option makes changes to the network route tables persistent across system restarts. The operation is applied to the network routing tables first and, if successful, is then applied to the list of saved routes associated with the currently active Network Configuration Profile.

`-q`

This option suppresses all output.

`-v`

This option displays additional details in verbose mode.

2

Sub-commands

`add`

Adds a route.

`change`

Changes aspects of a route (such as its gateway).

`delete`

Deletes a specific route.

`flush`

Removes all gateway entries from the routing table.

`get`

Displays the route for a destination.

`monitor`

Continuously reports any changes to the routing information base, routing lookup misses, or suspected network partitioning.

`show`

Displays the list of routes to be applied at system start-up. `show` can only be used in conjunction with `-p`.

Example 1

We add a route to a subnet. The IP address for the 1Gb interface is set to 10.1.1.100, the router is 10.1.1.1, and the destination subnet is 30.40.20.0 255.255.255.0.

```
route -p add -net 30.40.20.0 -netmask 255.255.255.0 10.1.1.1
```

Example 2

We add a route to a specific host. The IP address for the 1Gb interface is set to 10.1.1.100, the router is 10.1.1.1, and the destination host is 30.40.20.15.

```
route -p add -host 30.40.20.15 10.1.1.1
```

Example 3 — We display all currently configured routes on the Unity Storage System.

```
route -p show
```

Example 4 — We remove a subnet. After displaying all configured routes on the Unity Storage System (using the `route -p show` command), you want to disable a specific routing entry, for example: **persistent: route add -net 30.40.20.0 -netmask 255.255.255.0 10.1.1.1**, type:

```
route -p delete -net 30.40.20.0 -netmask 255.255.255.0 10.1.1.1
```

Example 5 — We remove a host. After displaying all configured routes on the Unity Storage System (using the `route -p show` command), you want to remove a specific host entry, for example: **persistent: route add -host 30.40.20.15 10.1.1.1**, type:

```
route -p delete -host 30.40.20.15 10.1.1.1
```

sensors

To run this command:

1. Access the CLI command shell—see Accessing the nxadmin and nxcmd CLIs on page 13.
2. Type the command using the syntax provided in this topic.
3. Press Enter.

Description — This command displays chassis/system sensor information for the current controller node, as well as for available sensor information for Nexsan expansion units connected to the Unity Storage System.

Information provided by sensors includes fan, CPU, power supply status, and more; you can use the data to identify hardware and/or component faults.

Controller — You can run this command on any controller.

Note: Sensor information for Nexsan expansion units can be seen from any controller.

Syntax — `sensors`

Options — None

Example —

```
sensors
Polling sensors...
Node: ES200030-001-01
Location: right (from the front)
Sensors for E4400:
* CPU 1 status (discrete): normal
* CPU 2 status (discrete): normal
* CPU 1 core voltage (voltage): normal [1.03 V]
* CPU 2 core voltage (voltage): normal [0.94 V]
* CPU 1 voltage status (voltage): normal [1.54 V]
* CPU 2 voltage status (voltage): normal [1.54 V]
```

```
* 5V supply voltage (voltage): normal [5.08 V]
* 12V supply voltage (voltage): normal [12 V]
* 1.5V supply voltage (voltage): normal [1.51 V]
* 3.3V supply voltage (voltage): normal [3.29 V]
* 3.3V standby supply voltage (voltage): normal [3.34 V]
* 5V standby supply voltage (voltage): normal [5.04 V]
* Battery voltage (voltage): normal [3.36 V]
* System temperature (temperature): normal [31 C]
* DIMM temperature, slot 1A for CPU 1 (temperature): normal [37 C]
* DIMM temperature, slot 2A for CPU 1 (temperature): normal [37 C]
* DIMM temperature, slot 3A for CPU 1 (temperature): normal [37 C]
* DIMM temperature, slot 1A for CPU 2 (temperature): normal [32 C]
* DIMM temperature, slot 2A for CPU 2 (temperature): normal [32 C]
* DIMM temperature, slot 3A for CPU 2 (temperature): normal [32 C]
* Lower Layer Fan 1 (fan): normal [8500 RPM]
* Lower Layer Fan 2 (fan): normal [8500 RPM]
* Lower Layer Fan 3 (fan): normal [8500 RPM]
* Upper Layer Fan 1 (fan): normal [8160 RPM]
* Upper Layer Fan 2 (fan): normal [8400 RPM]
* Upper Layer Fan 3 (fan): normal [8280 RPM]
Node: ES200030-001-02
Location: left (from the front)
Sensors for E4400:
* CPU 1 status (discrete): normal
* CPU 2 status (discrete): normal
* CPU 1 core voltage (voltage): normal [1.01 V]
* CPU 2 core voltage (voltage): normal [1.02 V]
* CPU 1 voltage status (voltage): normal [1.39 V]
* CPU 2 voltage status (voltage): normal [1.38 V]
* 5V supply voltage (voltage): normal [5.04 V]
* 12V supply voltage (voltage): normal [12 V]
* 1.5V supply voltage (voltage): normal [1.51 V]
* 3.3V supply voltage (voltage): normal [3.26 V]
* 3.3V standby supply voltage (voltage): normal [3.31 V]
* 5V standby supply voltage (voltage): normal [5.00 V]
* Battery voltage (voltage): normal [3.36 V]
* System temperature (temperature): normal [28 C]
* DIMM temperature, slot 1A for CPU 1 (temperature): normal [37 C]
* DIMM temperature, slot 2A for CPU 1 (temperature): normal [38 C]
* DIMM temperature, slot 3A for CPU 1 (temperature): normal [37 C]
* DIMM temperature, slot 1A for CPU 2 (temperature): normal [36 C]
* DIMM temperature, slot 2A for CPU 2 (temperature): normal [36 C]
```

```
* DIMM temperature, slot 3A for CPU 2 (temperature): normal [37 C]
* Lower Layer Fan 1 (fan): normal [9384 RPM]
* Lower Layer Fan 2 (fan): normal [9384 RPM]
* Lower Layer Fan 3 (fan): normal [9384 RPM]
* Upper Layer Fan 1 (fan): normal [7680 RPM]
* Upper Layer Fan 2 (fan): normal [8160 RPM]
* Upper Layer Fan 3 (fan): normal [8400 RPM]
Sensors for E5110 chassis:
* Power Supply (right from front) (discrete): normal
* Power Supply (left from front) (discrete): normal
* Temperature (right from front) (temperature): normal [30 C]
* Temperature (left from front) (temperature): normal [35 C]
* 5V supply voltage (voltage): unknown [0.00 V]
* 12V supply voltage (voltage): unknown [0.00 V]
* 5V supply current (misc): unknown
* 12V supply current (misc): unknown
```

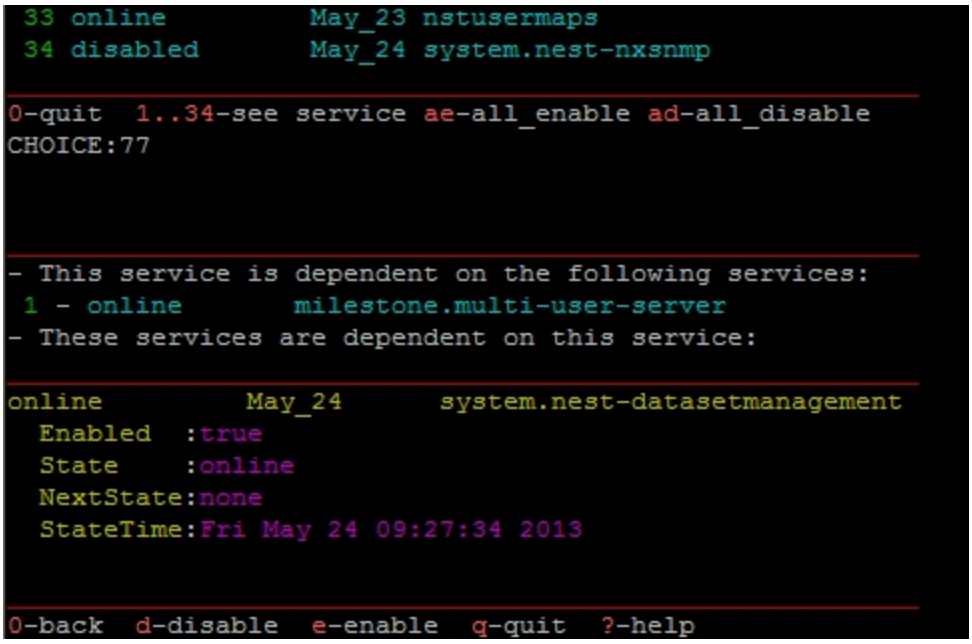
services

To run this command:

1. Access the CLI command shell—see Accessing the nxadmin and nxcmd CLIs on page 13.
2. Type the command using the syntax provided in this topic.
3. Press Enter.

Description	This command enables you to view status of specific services, and stop or restart the services through a menu. It also displays the dependency with other services. **CAUTION**: Some services are dependent on other services to function properly. Only disable a service if requested by Nexsan Technical Support.
Controller	Run this command on the controller having an issue.
Syntax	`services`
Options	None
Example	1. Type **`services`**. 2. Enter the number corresponding to the service.

3. Press Enter. If the service is dependent on other services, or if services depend on the selected service, a message will display to inform you. It is not recommended to disable services that have dependencies with other services.



4. At the Choice line, type:
   - **d** for disable, or
   - **e** for enable.
5. Press Enter.

setdefaultdomain

To run this command:

1. Access the CLI command shell—see Accessing the nxadmin and nxcmd CLIs on page 13.
2. Type the command using the syntax provided in this topic.
3. Press Enter.

Description	This command defines the default domain used with your the Unity Storage System. You can create, remove, or show the default domain. This command can also be used for NIS domain integration. For steps to integrate NIS, see Integrating with Network Information Service (NIS).
Controller	You can run this command on any controller.
Syntax	`setdefaultdomain [-d] [-s] [<domain name>]`

Options	`-d`
	This option deletes the current default domain.
	`-s`

This option displays the current default domain.

`domain name`

This command sets the default domain to the domain name you specify.

Example — We change the default domain to **qadomain.net**.

`setdefaultdomain qadomain.net`

setip

To run this command:

1. Access the CLI command shell—see Accessing the nxadmin and nxcmd CLIs on page 13.
2. Type the command using the syntax provided in this topic.
3. Press Enter.

Description — This command displays the the Unity Storage System network configuration utility, where you can modify network settings for the management interface (nx99) and the primary data network interface (nx0), or configure IP addresses for a new network interface.

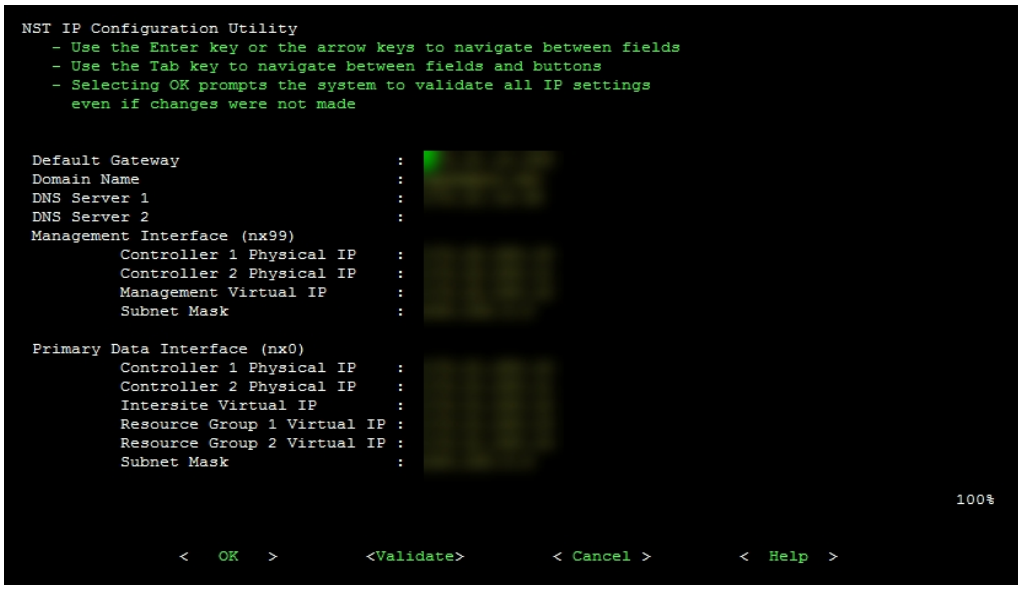
1. Type the network settings in each of the corresponding fields; use the Tab key to navigate between fields.
2. When finished, tab to the <Validate> option and press Enter. The Unity Storage System validates the new or updated network settings.
3. Once the validation process completes, tab to the <OK> option and press Enter to apply the network settings to the system.

Controller — You can run this command on any controller.

Syntax — `setip`

Options — None

Example



sha256sum

To run this command:

1. Access the CLI command shell—see Accessing the nxadmin and nxcmd CLIs on page 13.
2. Type the command using the syntax provided in this topic.
3. Press Enter.

Description: This command checks and displays the Secure Hash Algorithm (SHA-256) hash of the specified file.

Controller: Run this command on the controller hosting the file.

Syntax:
```
sha256sum <file name>
```

Options:
```
<file name>
```
This option specifies the file name.

shareacl

To run this command:

1. Access the CLI command shell—see Accessing the nxadmin and nxcmd CLIs on page 13.
2. Type the command using the syntax provided in this topic.
3. Press Enter.

Description: This command enables you to assign local user and/or group accounts (that you added to the Unity Storage System) access permissions (Read, Read/Write, or Full) to NFS file systems on the system.

TIP: If you only have CIFS file systems in your environment, you can set the file systems for both CIFS and NFS sharing in Nexsan Unity. The file system will be accessible from the CLI and you will be able to configure the CIFS file systems using the `shareacl` command.

Controller: Run this command on the controller hosting the file systems.

Syntax:
```
shareacl
[-c shares | get | resetall | deleteindex | replaceall | replace
| insert | append | help]
[-i <index name>]
[-p <pool name>]
[-s <file system name>]
[-u <user name>]
[-g <group name>]
[-a permission]
[-d allow | deny]
[-f inheritance]
```

Options

`-c shares`

This option lists existing file systems on the Unity Storage System, along with their type and the pool name.

`-c get`

This option displays permissions and the indexes. You must provide the:

- pool name (with the `-p` option) and
- file systems name (with the `-s` option).

`-c resetall`

This option resets all permissions for the specified file systems. You must provide the:

- pool name (with the `-p` option), and
- file systems name (with the `-s` option).

`-c deleteindex`

This option removes a permission entry from the file systems access index. You must provide the:

- pool name (with the `-p` option),
- file systems name (with the `-s` option), and
- index name (with the `-i` option).

`-c replaceall`

This option replaces all access control lists with the specified list. You must provide the:

- pool name (with the `-p` option),
- file systems name (with the `-s` option),
- user name (with the `-u` option) or group name (with the `-g` option), and
- permission status (with the `-d` option).

Optionally, you can provide the inheritance using the `-f` option.

`-c insert`

This option inserts a permission entry at the specified index. You must provide the:

- pool name (with the `-p` option),
- file systems name (with the `-s` option),
- user name (with the `-u` option) or group name (with the `-g` option), and
- permission status (with the `-d` option).

Optionally, you can provide the inheritance using the `-f` option.

`-c append`

This option adds a permission for the specified entry, which can be the:

- pool name (with the `-p` option),
- file systems name (with the `-s` option),

- user name (with the `-u` option) or group name (with the `-g` option), or
- permission status (with the `-d` option).

Optionally, you can provide the inheritance using the `-f` option.

`-c help`

This option display help content for the `shareacl` command.

`-i <index name>`

This option specifies the index name of a permission entry.

`-p <pool name>`

This option specifies the name of the pool where the file system resides.

`-s <file system name>`

This option specifies the name of the file systems to which we grant or revoke permissions.

`-u <user name>`

This option specifies the name of the user to whom we grant or revoke permissions.

`-g <group name>`

This option specifies the name of the group to which we grant or revoke permissions.

`-a permission`

This option specifies which permissions to grant or revoke. These permission arguments are supported:

- `read_data (r)`: Permission to read the data of a file.
- `list_directory (r)`: Permission to list the contents of a directory.
- `write_data (w)`: Permission to modify a file's data anywhere in the file's offset range.
- `add_file (w)`: Permission to add a new file to a directory.
- `add_subdirectory (p)`: Permission to create a subdirectory to a directory.
- `read_xattr (R)`: Permission to read the extended attributes of a file.
- `write_xattr (W)`: Permission to create extended attributes or write to the extended attribute directory.
- `execute (x)`: Permission to execute a file.
- `read_attributes (a)`: Permission to read basic attributes (non-ACLs) of a file.
- `write_attributes (A)`: Permission to change the times associated with a file or directory to an arbitrary value.
- `delete (d)`: Permission to delete a file.
- `delete_child (D)`: Permission to delete a file within a directory.
- `read_acl (c)`: Permission to read the ACL of a file.
- `write_acl (C)`: Permission to write the ACL of a file.

- `write_owner (o)`: Permission to change the owner of a file.

These permission aliases are supported; they allow you so set multiple permissions concurrently:

- `full_set`: All permissions.
- `modify_set`: All permissions except `write_acl` and `write_owner`.
- `read_set`: `read_data`, `read_acl`, `read_attributes`, and `read_xattr`.
- `write_set`: `write_data`, `append_data`, `write_attributes`, and `write_xattr`.

`-d allow | deny`

This option gives or removes the permissions specified with the `-a` option.

`-f inheritance`

This option provides inheritance settings based on a file or directory.

These inheritance arguments are supported:

- `file_inherit (f)`: Inherit to all newly created files.
- `dir_inherit (d)`: Inherit to all newly created directories.
- `inherit_only (i)`: When placed on a directory, do not apply to the directory, only to newly created files and directories. This flag requires that either `file_inherit` or `dir_inherit` be also specified.
- `no_propagate (n)`: Indicates that ACL entries should be inherited to objects in a directory, but inheritance should stop after descending one level. This flag requires that either `file_inherit` or `dir_inherit` is also specified.

Example 1

We provide user `Bob` full access to a file systems named `PayRollData` in a storage pool named `FinancePool1`, with an index number of `5`.

```
shareacl -c insert -p FinancePool1 -s PayRollData -u Bob
-d allow -i 5 -a full_set
```

Example 2

We disable the file and directory inheritance for user `Bob` in storage pool `poola`, for file systems `file systems3` at index number `4`. The other permissions, which are listed in the command, remain the same.

```
shareacl -c replace -p poola -s file systems3-i 4 -u bob -a
list_directory/read_data/add_file/write_data/add_
subdirectory/append_data/read_xattr/write_xattr/execute/delete_
child/read_attributes/write_attributes/delete/read_acl/write_
acl/write_owner/synchronize -d allow
```

Example 3

We enable the file and directory inheritance for user `bob` in storage pool `poola`, for `c3` at index number `4`.

```
shareacl -c replace -p poola -s filesystem3 -i 4 -u bob -a list_
directory/read_data/add_file/write_data/add_subdirectory/append_
data/read_xattr/write_xattr/execute/delete_child/read_
attributes/write_attributes/delete/read_acl/write_acl/write_
owner/synchronize -d allow -f file_inherit/dir_inherit
```

shares

To run this command:

1. Access the CLI command shell—see Accessing the nxadmin and nxcmd CLIs on page 13.
2. Type the command using the syntax provided in this topic.
3. Press Enter.

Description: This command enables you to display existing file systems on the Unity Storage System.

Controller: Run this command on the controller hosting the file systems.

Syntax: `shares`

Options: None

Example:

```
shares
Share         : PayRollData1
      Pool    : FinancePool1
      Type    : sharenfs
      Node    : 2
```


showmount

To run this command:

1. Access the CLI command shell—see Accessing the nxadmin and nxcmd CLIs on page 13.
2. Type the command using the syntax provided in this topic.
3. Press Enter.

Description: This command lists the UNIX/Linux clients that have remotely mounted an NFS file system on the Unity Storage System. It is important to note that the `showmount` command caches mount information, and as such, it may not immediately display information for file systems that were recently mounted, or it may continue to display information for file systems that are no longer remotely mounted.

In addition, the `showmount` command does not return information about NFS version 4 (NFSv4) clients.

Controller: You must run this command on the active controller. (The active controller has the System Management component running on it.)

Syntax: `showmount [-a|-d|-e] <host name>`

Options:

`-a`

This option displays remote mounts on the Unity Storage System, in the format `host name:directory`.

`-d`

This option displays the directories on the controller you are connected to.

`-e`

This option displays the list of shared file systems.

`<host name>`

This option specifies the host name.

Example 1 — We display the mount points from both nodes. We are connected to the active controller.

```
showmount
ES260786-176-001-01
ES260786-176-001-02-rmi
qa-ad.qadomain.net
```

Example 2 — We display mounted file systems that are shared.

```
showmount -e
export list for ES260786-176-01:
/config @127.0.0.1,@200.200.200.0
/pools/FinancePool/FinanceQC (everyone)
```

showroutes

To run this command:

1. Access the CLI command shell—see Accessing the nxadmin and nxcmd CLIs on page 13.
2. Type the command using the syntax provided in this topic.
3. Press Enter.

Description — This command displays the routing table on the Unity Storage System. More specifically, this command shows the routes currently configured on all (active) network interfaces on the system.

Controller — You must run this command on both controllers.

Syntax — `showroutes`

Options — None

Example

```
showroutes
Routing Table: IPv4
Destination     Gateway         Flags  Ref  Use          Interface
--------------  --------------  -----  ---  ----------   ---------
default         172.21.12.254   UG     3    397660
127.0.0.1       127.0.0.1       UH     28   685271097    lo0
172.21.12.0     172.21.14.176   U      11   1135049      nx0
172.21.12.0     172.21.12.101   U      61   48482243     nx0
200.200.200.0   200.200.200.3   U      3    1292470976   private0
200.200.200.0   200.200.200.2   U      3    1659118791   private0
```

```
Routing Table: IPv6
 Destination      Gateway         Flags  Ref  Use         If
--------------   -------------   -----  ---  ---------   -------
::1              ::1             UH     2    19970       lo0
```

shutdown

To run this command:

1. Access the CLI command shell—see Accessing the nxadmin and nxcmd CLIs on page 13.
2. Type the command using the syntax provided in this topic.
3. Press Enter.

Description

This command quiesces (or stops), in sequential order, all services on the Unity Storage System before shutting down the controller node.

CAUTION: When you shut down the controller node, it does NOT physically turn the power off. You must press and hold the power button on the front panel of the Unity Storage System chassis to power off the system. If you shut down only a controller node on the Unity Storage System, you must remove the power cable corresponding to the node from the back of the Unity Storage System chassis before attempting to physically access the controller node.

Controller

Run this command on the controller that you want to shut down.

Syntax

```
shutdown
```

Options

None

siteinfo

To run this command:

1. Access the CLI command shell—see Accessing the nxadmin and nxcmd CLIs on page 13.
2. Type the command using the syntax provided in this topic.
3. Press Enter.

Description

This command enables you to update stored configuration settings for any remote Unity Storage Systems that the primary Unity Storage System is connected to; specifically, you can change the stored intersite virtual IP, system name, and system serial number of a remote system. This command does not modify settings on the remote system; it only updates corresponding settings on the primary system.

You should use this command only if you changed the intersite virtual IP or name of a remote Unity Storage System while the primary system was inaccessible; and the updated configuration was not propagated.

To update the stored intersite virtual IP, system name, or system serial number of a remote system to the primary system:

1. Run this command on the remote system to display the relevant information.

2. Run this command on the local system to update/modify the information for the corresponding remote the Unity Storage System.

Controller — Run this command on the active controller. (The active controller has the System Management component running on it.)

Syntax — `siteinfo -c [show] [change -i -n|-s]`

Options — `-c show`

This command displays the local system's name, IP address and system serial, and peer sites IP addresses.

`-c change -i -n | -s`

This command changes the IP address of a secondary system; specify the new IP address with the `-i` option, and specify either the secondary system name with the `-n` option or serial number with the `-s` option.

Example — We change the IP address of the secondary system `FinanceSiteQC`.

`siteinfo -c change -i 172.21.14.175 -n FinanceSiteQC`

smbadm

To run this command:

1. Access the CLI command shell—see Accessing the nxadmin and nxcmd CLIs on page 13.
2. Type the command using the syntax provided in this topic.
3. Press Enter.

Description — This command enables you to configure and manage CIFS local groups and users, and manage domain membership.

CAUTION: Only run the `smbadm` command if requested by Nexsan Technical Support.

Controller — You must run this command on both controllers.

Syntax —

```
smbadm
[add-member -m <user name> [-m <user name>]... <group name>]
[create -d <description> <group name>]
[delete <group name>]
[disable-user <user name>]
[enable-user <user name>]
[get [[-p <property>]...] <group>]
[-h]
[join -u <user name> <domain>]
[join -w workgroup]
[list * . - +]
[remove-member -m <user name> [[-m user name]...] <group name>]
[rename <group name> <new group name>]
```

```
[set -p <property value> [[-p <property value>]...] <group
name>]
[show -m|-p|group]
```

Options

```
add-member -m <user name> <group>
```

This command specifies the name of users to add for the specified group.

```
create -d <description> <group name>
```

This command creates a new group. Provide a one-word description for the group and then type the name.

The 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 name cannot consist solely of periods (.) and spaces. Be consistent in the way you enter names because when Nexsan Unity™ presents lists of user and group accounts, they are displayed in alphabetic order.

```
delete <group name>
```

This command deletes the specified group.

```
disable-user <user name>
```

This command disables access for the specified user. The name is not case-sensitive.

```
enable-user <user name>
```

This command enables access for an existing user. The name is not case-sensitive.

```
get [[-p <property>]...] <group name>
```

This command displays information on the property for the specified group; the property can be access rights, file system permissions, or group members.

```
-h
```

This command displays the help for the `smbadm` command.

```
join -u <user name> <domain>
```

This command joins the specified user to the domain.

```
join -w workgroup
```

This command joins the specified user to the work group.

```
list * . - +
```

This command displays information for the specified domain:

`*` is the primary domain

`.` is the local domain

`-` is other domains

`+` is the selected domain controller

`remove-member -m <user name> [[-m user name]...] <group name>`

This command removes one or more users from the specified group.

`rename <group name> <new group name>`

This command specifies a new name for the group.

The 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 name cannot consist solely of periods (.) and spaces. Be consistent in the way you enter names because when Nexsan Unity™ presents lists of user and group accounts, they are displayed in alphabetic order.

`set -p <property value> [[-p <property value>]...] <group name>`

This command sets properties for the specified group.

`show -m|-p|<group name>`

This command displays information for member names, member privileges, and security identifier (SID) number. When creating users and groups, SID numbers are automatically assigned by Windows.

2

Example 1 — We create the `Finance2013` group with a description describing the location, `Montreal`.

```
smbadm create -d Montreal Finance2013
Finance2013 created
```

Example 2 — We delete group `Finance2010`.

```
smbadm delete Finance2010
```

Example 3 — We disable user `Bob`.

```
smbadm disable-user bob
```

Example 4 — We enable user `John`.

```
smbadm enable-user john
```

Example 5 — We join user `Bob` to domain `qadomain.net`.

```
smbadm join -u bob qadomain.net
```

Example 6 — We display information for the primary domain.

```
smbadm list *
[*] [QADOMAIN]
[*] [qadomain.net]
 [+qa-ad.qadomain.net] [172.21.14.30]
[.] [ES260786-176-01] [S-1-5-21-3198797834-3143126336-
2597567724]
[*] [QADOMAIN] [S-1-5-21-971380349-303191883-3091725001]
```

```
[-] [AD] [S-1-5-21-2350514478-2414906159-379160445]
```

Example 7 We remove users `Bob` and `Alex` from group `FinanceMTL`.

```
smbadm remove-member -m bob -m alex financemtl
```

Example 8 We rename group `FinanceMTL` to `FinanceQC`.

```
smbadm rename FinanceMTL FinanceQC
```

Example 9 We display member information.

```
smbadm show -m
administrators (Members can fully administer the
computer/domain)
SID: S-1-5-32-544
No members
backup operators (Members can bypass file security to back up
files)
SID: S-1-5-32-551
No members
power users (Members can share directories)
SID: S-1-5-32-547
No members
```

Example 10 We display information on member privileges.

```
smbadm show -p
administrators (Members can fully administer the
computer/domain)
SID: S-1-5-32-544
Privileges:
SeTakeOwnershipPrivilege: On
SeBackupPrivilege: Off
SeRestorePrivilege: Off
backup operators (Members can bypass file security to back up
files)
SID: S-1-5-32-551
Privileges:
SeTakeOwnershipPrivilege: Off
SeBackupPrivilege: On
SeRestorePrivilege: On
power users (Members can share directories)
SID: S-1-5-32-547
Privileges:
SeTakeOwnershipPrivilege: Off
```

```
SeBackupPrivilege: Off
SeRestorePrivilege: Off
```

Example 11 We display the SID number for group `Finance2013` that we created in `smbadm create -d <description> <group name>`.

```
smbadm show Finance2013
Finance2013 (Montreal)
SID: S-1-5-21-1038995503-2884952912-4047149105-2147583648
```

smbrestart

To run this command:

1. Access the CLI command shell—see Accessing the nxadmin and nxcmd CLIs on page 13.
2. Type the command using the syntax provided in this topic.
3. Press Enter.

Description This command restarts the CIFS server on the Unity Storage System. Use this command if any Windows client on your network is unable to access a CIFS file system on the Unity Storage System but—only after you verify that the network connection between the Windows client and the Unity Storage System is functional.

Note: No output is displayed during this process. If an error appears, please contact Nexsan Technical Support.

Controller You must run this command on both controllers.

Syntax `smbrestart`

Options None

smbserver

To run this command:

1. Access the CLI command shell—see Accessing the nxadmin and nxcmd CLIs on page 13.
2. Type the command using the syntax provided in this topic.
3. Press Enter.

Description This command manages the CIFS server version on the Unity Storage System. It displays the current CIFS server version and enables you to update to a newer version if you have upgraded.

Controller You must run this command on both controllers.

Syntax

```
smbserver
[-c setv12]
[-c setv21] if you hsv
[-c extended_requests=on|off]
```

```
[-c krb5=on|off]
[-c idmap_mapping_mode=idmu]
[-c show]
[-x]
[-h]
```

Options

`-c setv12`

This command updates the controller to CIFS server version 1.2. It will require you to confirm the update and will reboot the controller.

`-c setv21`

This command updates the controller to CIFS server version 2.1. It will require you to confirm the update and will reboot the controller.

`-c extended_requests=on|off`

This command enables or disables extended requests. It is set to `OFF` by default after performing a fresh installation of the Nexsan operating system, or after performing an upgrade of a the Unity Storage System that did not have this option.

`-c krb5=on|off`

This command enables or disables Kerberos version 5 for CIFS version 2.1. Kerberos is a network authentication protocol. It is designed to provide strong authentication for client/server applications by using secret-key cryptography.

`-c idmap_mapping_mode=idmu`

This command enables Identity Mapping for UNIX (IDMU). In previous releases, if you joined an Active Directory domain and then unjoined the domain, IDMU was always enabled.

In version 3.2, unjoining an Active Directory domain disables IDMU. If you rejoin the Active Directory domain, you need to manually enable IDMU to access your NFS file systems.

After running the command, you can run `smbserver -c show` to verify the setting was applied properly.

`-c show`

This command will display the current version of CIFS server.

`-x`

This command copies a specific CIFS server version when used with the `-c set` command.

`-h`

This command provides online help for the command usage.

Example

We display the CIFS server settings on the Unity Storage System.

```
smbserver -c show
CIFS Protocol Unity version: 2.1h2
```

```
Extended Requests: off
Krb5 nstcifs Support: off
nstusermaps mapping mode: none
```

snmpadm

To run this command:

1. Access the CLI command shell—see Accessing the nxadmin and nxcmd CLIs on page 13.
2. Type the command using the syntax provided in this topic.
3. Press Enter.

Description

This command gives you access to the SNMP (Simple Network Management Protocol) menu. The Nexsan Unity SNMP module allows existing SNMP monitoring environments to view, query, and monitor Nexsan the Unity Storage Systems and Nexsan E-Series storage units using the Simple Network Management Protocol. The Unity Storage System acts as a gateway, allowing the SNMP monitoring system to pass commands to, and receive data from, any and all Nexsan storage units that are visible to the gateway unit.

When the gateway unit is set up in NeST mode, the SNMP monitoring system is able to view, query, and monitor any storage on the gateway unit itself and on any Nexsan storage units that are directly attached to the gateway via SAS.

You can connect to the agent using a commercially available SNMP management application. Connect to the Nexsan Unity SNMP module using the unit's management IP address. The Nexsan Unity SNMP module is compliant with SNMPv1 and SNMPv2c.

Note: Make sure to allow outbound traffic on UDP port **161** on your firewall before starting the SNMP server.

Controller

Run this command on the active controller.

Syntax

```
snmpadm
```

Options

The NestOS SNMP menu offers these options:

```
1 - Display current SNMP settings
2 - Restart the SNMP server
3 - Stop the SNMP server
4 - Start the SNMP server
5 - Show the SNMP server status
6 - Display managed devices and community strings
q - Exit
```

Management Information Bases

The Nexsan Unity SNMP module requires Management Information Bases (MIBs) for it to work with Nexsan storage units. The MIBs that are included with the module are listed below. For complete information, refer to the SNMP Management Information Bases appendix.

- Host resources

- Interface
- LM sensor
- RFC1213
- SNMP framework
- SNMPv2 framework
- UCD disk I/O
- UCD SNMP

Example 1

We start or restart the Nexsan Unity SNMP module. The SNMP module needs to be restarted whenever a new Nexsan storage unit is attached to the Unity Storage System. The startup/restart process may take up to a minute.

- To start the SNMP module: type **4** and press Enter.
- To restart the SNMP module: type **2** and press Enter.

When the message *Done* appears, the SNMP module has been started/restarted and is running.

Example 2

We view current SNMP settings.

Type **1** and press Enter. The system displays the current SNMP settings: Build, Agent Mode, and Listening Address.

```
Build: 3.1.3.56630_r_Release-3-3.1-3.1.3 Agent Mode: NeST
Listening Address: agentaddress udp:161,tcp:161
```

Example 3

We display current SNMP server status.

Type **5** and press Enter. The system displays the status, as follows:

- If the server is online, the status says *enabled* and the current day is displayed.

  ```
  enabled May_16 system.nest-nxsnmp
  ```

- If the server is offline, the status says *disabled* and the day at which it was stopped is displayed

  ```
  disabled Jun_28 system.nest-nxsnmp
  ```

Example 4

We view Managed Devices and Community Strings. Community strings are used by SNMP management systems to connect to and retrieve data from managed devices.

Type **6** and press Enter.

The managed devices are displayed in the following format:

```
Server Instance 1
+ Nexsan Storage : IP 192.168.3.1, System ID 28643d0 [public_
028643d0]
```

The text between the square brackets is the community string. The part before the underscore is the community string of the main Unity Storage System itself, which is almost always `public`. The part after the underscore is the Nexsan storage unit's system ID preceded by a zero (`0`). The entire string (`agentname_systemID`) must be used by the SNMP management application to send data to or retrieve data from that Unity Storage System.

snmpproperty

To run this command:

1. Access the CLI command shell—see Accessing the nxadmin and nxcmd CLIs on page 13.
2. Type the command using the syntax provided in this topic.
3. Press Enter.

Description

This command configures SNMP (Simple Network Management Protocol) properties. The Unity Storage System includes an SNMP agent that allows existing SNMP monitoring environments to view, query, and monitor Nexsan the Unity Storage Systems and Nexsan E-Series storage units using the Simple Network Management Protocol.

Use the snmpadm command at the NestOS command prompt to access the SNMP menu for additional SNMP commands.

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.

Controller

Run this command on either controller.

Syntax

```
snmpproperty
[-c <list | get | set>]
[-p <property>]
[-v <value>]
```

Options

`-c list`

This option displays the properties that can be configured. When used with the `-p` argument, the possible values are displayed.

`-c get`

This option gets the value of a property. It must be used with the `-p` argument.

`-c set`

This option sets the value for the specified property. It must be used with the `-p` and `-v` arguments.

Examples

We display available properties.

```
snmpproperty -c list
SNMP-PublicROCommunity Sets the read-only community name.
Default is public.
```

snmptosyslog

To run this command:

1. Access the CLI command shell—see Accessing the nxadmin and nxcmd CLIs on page 13.
2. Type the command using the syntax provided in this topic.
3. Press Enter.

Prerequisite

- In the Unity Web interface, set an SNMP trap destination of 127.0.0.1. In Unity 2.0, click System Tools & Settings > Notifications. In Unity 5, click System > Notifications.

Description — This command forwards local SNMP traps to a remote syslog server, version 2.

The logs will be sent with the syslog facility local5.

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.

Controller — Run this command on either controller; it will be applied to both.

Syntax

```
snmptosyslog forward <remote syslog server IP address>
```

Options

```
forward <remote syslog server IP address>
```

Requires an IP to forward syslog messages to.

```
disable
```

Stops the forwarding of SNMP messages to the remote syslog server.

Examples

```
snmptosyslog forward 127.0.0.1
Running on ES156190-001-01
Running on ES156190-001-02
snmptosyslog disable
Running on ES156190-001-01
Running on ES156190-001-02
```

SVC

To run this command:

1. Access the CLI command shell—see Accessing the nxadmin and nxcmd CLIs on page 13.
2. Type the command using the syntax provided in this topic.
3. Press Enter.

Description — This command displays all active services on the Unity Storage System.

Controller — You must run this command on both controllers.

Syntax

```
svc [show <service name> (default)]
svc [enable <service name>]
svc [disable <service name>]
svc [restart <service name>]
```

Options

```
show <service name> or (default)
```

This option displays the current status of the specified service. If you just type `show`, all services are displayed, including legacy, disabled, and enabled services.

`enable <service name>`

This option enables the specified service.

`disable <service name>`

This option disables the specified service.

CAUTION: Some services are dependent on other services to function properly. Only run this command if requested by Nexsan Technical Support. To view service dependency, use the services command.

`restart <service name>`

This option restarts the specified service.

CAUTION: Some services are dependent on other services to function properly. Restarting a service may affect other services. To view service dependency, use the services command.

Example

▶ **svc output excerpt:**

svc

```
legacy_run May_16 rc2_d/S05checkmem
legacy_run May_16 rc2_d/S12rebootnxrequired
legacy_run May_16 rc2_d/S13upgradenxversion
legacy_run May_16 rc2_d/S98nest
legacy_run May_16 rc2_d/S99rsf
legacy_run May_16 rc3_d/S98refreshidmapcache
legacy_run May_16 rc3_d/S99nest
disabled May_16 network/physical:nwam
disabled May_16 network/install:default
disabled May_16 system/install/config:default
disabled May_16 network/location:default
disabled May_16 network/ipsec/manual-key:default
online May_16 system/nxglassfishservice:default
online May_16 network/nfs/rquota:default
online May_16 network/nfs/server:default
online May_16 network/updateports-rpc:default
online 16:39:51 system/nest-discovery-server:default
online 10:55:30 network/ldap/client:default
online 10:55:30 milestone/name-services:default
online 10:55:30 system/filesystem/reparse:default
online 10:55:30 network/nfs/mapid:default
online 10:55:30 network/nfs/client:default
online 10:55:30 system/filesystem/autofs:default
online 10:55:32 network/nstcifs/client:default
```

```
online 14:38:00 network/nstcifs/server:default
```

term

To run this command:

1. Access the CLI command shell—see Accessing the nxadmin and nxcmd CLIs on page 13.
2. Type the command using the syntax provided in this topic.
3. Press Enter.

Description: This command enables you to set the type of terminal connection to use for the current connection to the Unity Storage System.

Controller: Run this command on the current controller.

Syntax: `term [show|ansi|vt102|xterm-color|putty|console6]`

Options:

`show`

This option displays the type of connection of your current terminal.

`ansi|vt102|xterm-color|putty|console6`

Specifies the supported connection types with an the Unity Storage System terminal.

Example:

1. Type **`term`**.
2. A menu appears, similar to this output:

```
1: ansi
2: vt102
3: xterm-color
4: putty
5: console6
```

3. Enter the number corresponding to the terminal type you want.
4. Press Enter.

top

To run this command:

1. Access the CLI command shell—see Accessing the nxadmin and nxcmd CLIs on page 13.
2. Type the command using the syntax provided in this topic.
3. Press Enter.

Description: This command displays the top 30 processes currently being managed by the Unity Storage System operating system. Raw CPU percentage is used to rank the processes. If you provide the `number` parameter, the top number processes are displayed instead of the default.

Controller: Run this command on the controller where you want to see the processes.

Syntax

```
top [-C|-I|-S|-T|-a|-b|-c|-i|-n|-q|-t|-u|-v]
[-d <count number>]
[-m <mode number>]
[-o <field name>]
 [-s <time delay>]
[-U <user name>]
[number]
```

Options

`-C`

This option turns off the use of color in the display.

`-I`

This option does not display idle processes. By default, the `top` command displays both active and idle processes.

`-S`

This option shows system processes in the display. By default, system processes are not shown.

`-T`

This option lists all available color tags and the current set of tests used for color highlighting, and then it exits.

`-a`

This option shows all processes for as long as possible. This is shorthand for `-d all all`. This option is useful in batch mode.

`-b, -n`

This option sets the batch mode. In this mode, all input from the terminal is ignored, except for interruption characters (such as ^C).

`-c`

This option shows the full command line for each process. By default, only the command name is displayed.

`-i`

This option sets the interactive mode. In this mode, any input is immediately read for processing. When the command is processed, the screen gets updated. This mode is the default when the output is an intelligent terminal.

`-q`

This option displays the top 20 processes so that the command runs faster. You can use this option to improve the possibility of discovering a problem. You must be logged in as a root user to use this option.

`-t`

This option displays individual threads on separate lines. By default, each process is

displayed with a count of the number of threads.

`-u`

This option prevents the system from mapping UID numbers to user names, in order to save time. The UID numbers are displayed instead of user names.

`-v`

This option writes the version number information and exits immediately. To see current version information while `top` is running, use the help command "`?`".

`-d <count number>`

This option shows only `count` displays then exits. A display is considered to be one update of the screen. You can select the number of displays you want to see before `top` automatically exits. To indicate an infinite number of displays, use the words `infinitiy`, `maximum`, or `all`. The default for intelligent terminals is `infinity` and for dumb terminals, it is `1`.

`-m <mode number>`

This option starts the display in an alternate mode, by indicating the number for the mode to display. The default is `0`. On platforms that do not have multiple display modes, this option has no effect.

`-o <field name>`

This option sorts the process display area on the specified field. The field is the column name as seen in the output, in lower case. For example, you can use `cpu`, `size`, `res`, or `time`.

`-s <time delay>`

This option sets the delay between screen updates to the specified number of seconds. You must use user names with this option, not UID numbers.

`-U <user name>`

This option only displays processes owned by the specified user name. You must use user names with this option, not UID numbers.

`number`

The number can be a digit or the words `infinitiy`, `maximum`, or `all` to indicate all processes.

Example

We display the top 10 processes.

```
top -q 10
last pid: 13366; load avg: 0.45, 0.53, 0.50; up 6+01:13:19
15:16:50
87 processes: 86 sleeping, 1 on cpu
CPU states: 97.3% idle, 1.2% user, 1.5% kernel, 0.0% iowait,
0.0% swap
Kernel: 1077 ctxsw, 27 trap, 1260 intr, 1203 syscall, 23 flt
Memory: 4096M phys mem, 1276M free mem, 2048M total swap, 2048M
```

```
free swap
PID   USERNAME NLWP PRI NICE SIZE  RES   STATE TIME CPU   COMMAND
22684 root     1    28  0    2832k 1508k cpu/0 0:00 3.83% prtconf
2449  root     34   59  0    155M  149M  sleep 2:12 3.08% java
2381  root     16   59  0    129M  55M   sleep 0:59 0.27% java
2511  root     93   59  0    522M  510M  sleep 2:42 0.17% java
22653 root     1    52  0    3928k 2268k cpu/3 0:00 0.09% top
51    root     12   59  0    3168k 2132k sleep 0:01 0.09% dlmgmtd
21897 root     1    158 -20  4220k 2428k sleep 0:01 0.06% rsfmon
2360  root     59   59  0    149M  97M   sleep 0:07 0.05% java
29118 daemon   6    60  -20  2924k 1972k sleep 0:17 0.05% nfsd
648   root     17   59  0    19M   11M   sleep 1:06 0.03% smbd
```

trace

To run this command:

1. Access the CLI command shell—see Accessing the nxadmin and nxcmd CLIs on page 13.
2. Type the command using the syntax provided in this topic.
3. Press Enter.

Description

This command enables you to run Nexsan trace scripts in order to examine system performance. You can view which traces are available, which arguments you can use for each trace, and then view the trace results.

Controller

Run this command on the controller where you want to run the trace.

Syntax

```
trace
[-c show|help|run]
[-t arcstat|cifssvrtop|iscsiop|nfssvrtop]
[-a <trace arguments>]
```

Options

`-c show`

This option displays which traces are available.

`-c help [-t arcstat | cifssvrtop | iscsiop | nfssvrtop]`

This option displays the help for the specified trace and lists the arguments available for that trace.

`-c run [-t arcstat | cifssvrtop | iscsiop | nfssvrtop] [-a trace arguments]`

This option runs a trace with the specified arguments.

These traces are available:

- `arcstat`

  The `arcstat` trace reports metrics on the file system main memory cache.

- `cifssvrtop`

  The `cifssvrtop`trace reports IOPS metrics per client and per file system, such as which CIFS file system is mounted on which computer, and various statistics on Read/Write. This trace enables you to view computers actively performing work on the Unity Storage System.

- `iscsiop`

  The `iscsiop`trace reports IOPS metrics per iSCSI initiator, per iSCSI target, and per LUN.

- `nfssvrtop`

  The `nfssvrtop`trace reports metrics for the NFS server running on the Unity Storage System.

`-a <trace arguments>`

This option is used to send one or more arguments to the specified trace. For this reason, `-a` must be placed after `-c` and `-t`. Each trace has it own arguments.

arcstat arguments

`[-h|-v|-x|-r] [-f] [-s] [interval [count]]`

- `-h` displays help content.
- `-v` lists all possible field headers and definitions.
- `-x` displays extended statistics. This option is useful to verify cache performance. For example, high readings in the `mfug` and `mrug` fields (see `-v`) indicate that you may have to add more FASTier™ cache devices.
- `-r` displays values in raw output mode (values are not scaled).
- `-f` specifies which fields to display (see `-v`). Use a comma to separate the fields.
- `-s` overrides the default field separator with the specified custom character or string.
- `interval [count]` specifies a digit number for the interval and optionally count. For example, you can specify `5 12` for twelve five-second samples.

arcstat field definitions

These fields are displayed when running the `arcstat` trace without arguments:

- `time`: Current time
- `read`: Total ARC accesses per second
- `miss`: ARC misses per second
- `miss%`: ARC miss percentage
- `dmis`: Demand Data misses per second
- `dm%`: Demand Data miss percentage
- `pmis`: Prefetch misses per second
- `pm%`: Prefetch miss percentage
- `mmis`: Metadata misses per second
- `mm%`: Metadata miss percentage
- `arcsz`: ARC Size

- `c`: ARC Target Size

These fields are displayed when running the `arcstat` trace with the `-x` argument:

- `mfu`: MFU List hits per second
- `mru`: MRU List hits per second
- `mfug`: MFU Ghost List hits per second
- `mrug`: MRU Ghost List hits per second
- `eskip`: evict_skip per second
- `mtxmis`: mutex_miss per second
- `rmis`: recycle_miss per second
- `dread`: Demand data accesses per second
- `pread`: Prefetch accesses per second
- `read`: Total ARC accesses per second

These fields can be displayed if running the `arcstat` trace with the `-f` argument:

- `l2hit%`: L2ARC access hit percentage
- `mh%`: Metadata hit percentage
- `l2miss%`: L2ARC access miss percentage
- `dhit`: Demand Data hits per second
- `l2miss`: L2ARC misses per second
- `l2bytes`: bytes read per second from the L2ARC
- `hits`: ARC reads per second
- `l2read`: Total L2ARC accesses per second
- `mhit`: Metadata hits per second
- `ph%`: Prefetch hits percentage
- `l2size`: Size of the L2ARC
- `l2hits`: L2ARC hits per second
- `hit%`: ARC Hit percentage
- `dh%`: Demand Data hit percentage
- `mread`: Metadata accesses per second
- `phit`: Prefetch hits per second

cifssvrtop arguments

`[-c <client workstation>] [-t] [-b] [-w] [interval [count]]`

When no arguments are specified, the default output is displayed in 10-second samples.

- `-c <client workstation>` displays trace information for the current workstation. Enter the workstation name.
- `-t` displays the top number of entries only. It must be used with a count argument to specify the number of lines; for example, `-a -t 20` will display the top 20 lines only.

- `-b` specifies the block size. It must be used with a count argument to specify the number of bytes; for example, `-a - b 1024` will check the alignment on a 1 KB boundary.
- `-w` displays the workstation name instead of the IP address (IPv4).
- `interval [count]` specifies a digit number for the interval and optionally count. For example, you can specify 5 12 for twelve five-second samples.

cifssvrtop field definitions

These fields are displayed when running the `cifssvrtop` trace:

- `Client` : Client IPv4 address or workstation name
- `ver`: Version of the client (1 or 2 for cifsvrtop, and 2,3 or 4 for nfssvrtop)
- `r/s`: Read operations per second
- `w/s`: Write operations per second
- `kr/s`: Reads amount per second shown in br/s(bytes), kr/s(kilobytes) or mr/s (megabytes)
- `kw/s`: Writes amount per second shown in bw/s(bytes), kw/s(kilobytes) or mw/s (megabytes)
- `iops/s`: IO Operations per second
- `artm(us)`: Average Read Time in microseconds
- `awtm(us)`: Average Write Time in microseconds
- `Share`: Name of the File System/Share

iscsiop arguments

`[-m] [-s]`

When no arguments are specified, the default output is displayed in 10-second samples.

- `-m` displays the management targets.
- `-s` displays the system pool targets.

iscsiop field definitions

These fields are displayed when running the `iscsiop` trace:

- `client`: IP addresses of the clients present on the site
- `target`: Unique qualifier names (IQN) of the ISCSI targets, including the management targets and system pool targets, if you specified the `-m` and `-s` arguments
- `initiator`: Unique qualifier names (IQN) of the iSCSI initiators
- `lun`: Logical unit number
- `OPS`: iSCSI operations per interval

nfssvrtop arguments

`[-s]`

Specifies the file system mountpoint; for example,

```
trace -c run -t nfssvrtop -a -s /pools/Pool1/FileSystem2
```

The default output is displayed in 10-second samples.

nfssvrtop field descriptions

These fields are displayed when running the `nfssvrtop` trace:

- `Client` :Client IPv4 address or workstation name
- `ver`: Version of the client (1 or 2 for cifsvrtop, and 2,3 or 4 for nfssvrtop)
- `r/s`: Read operations per second
- `w/s`: Write operations per second
- `kr/s`: Reads amount per second shown in br/s(bytes), kr/s(kilobytes) or mr/s (megabytes)
- `kw/s`: Writes amount per second shown in bw/s(bytes), kw/s(kilobytes) or mw/s (megabytes)
- `iops/s`: IO Operations per second
- `artm(us)`: Average Read Time in microseconds
- `awtm(us)`: Average Write Time in microseconds
- `Share`: Name of the File System/Share

Example 1

We list the available the Unity Storage System traces.

```
trace -c show
arcstat - Reports metrics on the file system memory usage
cifssvrtop - Reports metrics on the CIFS server
iscsiop - Reports IOPS metrics
nfssvrtop - Reports metrics on the NFS server
```

Example 2

We display help content for the `arcstat` trace.

```
trace -c help -t arcstat
arcstat - Reports metrics on the file system memory usage
Usage: arcstat [-hvxr] [-f fields] [-s string] [interval
[count]]
-h : Displays this help message
-v : Lists all possible field headers and definitions
-x : Displays extended statistics
-r : Displays raw output mode (values are not scaled)
-f : Displays specific fields (see -v)
-s : Overrides the default field separator with custom
characters or strings
Examples:
arcstat -v
arcstat -f time,hit%,dh%,ph%,mh% 1
```

Example 3

We run the `arcstat` trace to view extended statistics.

```
trace -c run -t arcstat -a -x
Running: arcstat -x
```

```
time      mfu  mru  mfug  mrug  eskip  mtxmis  rmis  dread  pread  read
15:35:43  0    0    0     0     0      0       0     0      0      0
```

Example 4

We run the `nfssvrtop` trace. The path is "unknown" because I/O operations hit cache before being written to disk. Therefore, the device path is not traced.

```
trace -c run -t nfssvrtop
```

```
Client          ver r/s w/s kr/s kw/s ops/s artm   awtm   Path
                                             (us)   (us)
10.170.128.40 3   0   0   0    0    0     0      0      <unknown>
10.170.128.41 3   0   0   0    0    0     0      0      <unknown>
```

traceroute

To run this command:

1. Access the CLI command shell—see Accessing the nxadmin and nxcmd CLIs on page 13.
2. Type the command using the syntax provided in this topic.
3. Press Enter.

Description

This command displays the route (path) that an IP packet follows to another Internet host. It also measures transit delays of data packets on the network.

Controller

Run this command on the controller where you want to see routes.

Syntax

```
traceroute
[-a|-d|-F|-I|-l|-n|-S|-v|-x]
[-A <address family>]
[-c <traffic class>]
[-f <first hop>]
[-g gateway [-g gateway...]|-r]
[host [packet length]]
[-i <network interface>]
[-L <flow label>]
[-m <maximum hop>]
[-P <pause>]
[-p <port number>]
[-Q <maximum timeout>]
[-q <number of queries>]
[-s <source address]
[-t <type of service>]
[-w <wait time>]
```

Options

`-a`

The `-a` option probes all of the addresses of a multi-homed destination. The output

looks like traceroute has been run once for each IP address of the destination.

If this option is used together with `-A`, `traceroute` probes only the addresses that are of the specified address family.

`-d`

The `-d` option sets the `SO_DEBUG` socket option.

`-F`

The `-F` option turns off fragmentation. For IPv4 and IPv6, fragmentation will not be allowed when datagrams are sent. If the `packetlen` exceeds the MTU, traceroute may report that sending failed due to the message being too long.

`-I`

The `-I` option uses ICMP (ICMP6) `ECHO` instead of UDP datagrams.

`-l`

The `-l` option displays the value of the hop limit field in each packet received.

`-n`

The `-n` option displays hop addresses numerically rather than symbolically and numerically. This saves a `nameserver` address-to-name lookup for each gateway found on the path.

`-S`

The `-S` option displays a summary of how many probes were not answered for each hop.

`-V`

The `-V` option displays verbose output. For each hop, the size and the destination of the response packets is displayed. Also ICMP (ICMP6) packets received other than TIME_EXCEEDED and UNREACHABLE are listed as well.

`-x`

The `-x` option prevents `traceroute` from calculating checksums. Checksums are usually required for the last hop when using ICMP ECHO probes. This option is valid only on IPv4. See the `-I` option.

`-A <address family>`

The `-A` option specifies the address family of the target host; can be either `inet` or `inet6`. Address family determines which protocol to use. For an argument of inet, IPv4 is used. For inet6, IPv6 is used.

`-c <traffic class>`

The `-c` option specifies the traffic class of probe packets. The value must be an integer in the range from 0 to 255. Gateways along the path may route the probe packet differently depending upon the value of `traffic_class` set in the probe packet. This option is valid only on IPv6.

`-f <first hop>`

The -f option sets the starting hop limit value to first_hop, to override the default value of 1. traceroute skips processing for those intermediate gateways which are less than first_hop hops away.

-g gateway [-g gateway...]

The -g option specifies a loose source route gateway. The user can specify more than one gateway by using -g for each gateway. The maximum number of gateways is 8 for IPv4 and 127 for IPv6. Note that some factors such as the link MTU can further limit the number of gateways for IPv6. This option cannot be used with the -r option.

-r

The -r option bypasses the normal routing tables and sends directly to a host on an attached network. If the host is not on a directly-attached network, an error is returned. This option can be used to send probes to a local host through an interface that has been dropped by the router daemon. You cannot use this option if the -g option is used.

host [packet length]

The host option specifies the network host.

-i <network interface>

For IPv4, the -i option specifies a network interface to obtain the source IP address. This is normally only useful on a multi-homed host. The -s option is also another way to do this. For IPv6, the -i option specifies the network interface on which probe packets are transmitted. The argument can be either an interface index, for example, 1, 2, or an interface name, for example, eri0, hme0.

-L <flow label>

The -L option specifies the flow label of probe packets. The value must be an integer in the range from 0 to 1048575. This option is valid only on IPv6.

-m <maximum hop>

The -m option sets the maximum hop limit used in outgoing probe packets. The default is 30 hops, which is the same default used for TCP connections.

-P <pause>

The -P option specifies a delay, in seconds, to pause between probe packets. This may be necessary if the final destination does not accept undeliverable packets in bursts. By default, traceroute sends the next probe as soon as it has received a reply.

-p <port number>

The -p option sets the base UDP port number used in probes. The default is 33434. traceroute hopes that nothing is listening on UDP ports (base+(nhops-1)*nqueries) to (base+(nhops*nqueries)-1) at the destination host, so that an ICMP (ICMP6) PORT_UNREACHABLE message will be returned to terminate the route tracing. If something is listening on a port in the default range, this option can be used to select an unused port range. nhops is defined as the number of hops between the source and the destination.

-Q <maximum timeout>

The `-Q` option stops probing this hop after `max_timeout` consecutive timeouts are detected. The default value is 5. Useful in combination with the `-q` option if you have specified a large number of probe queries.

`-q <number of queries>`

The `-q` option sets the desired number of probe queries. The default is `3`.

`-s <source address>`

The `-s` option specifies the source IP address in outgoing probe packets. On multi-homed hosts, having with more than one IP address, this option can be used to force the source address to be something other than the IP address traceroute picks by default.

For IPv4, when used together with the `-i` option, the given IP address should be configured on the specified interface. For IPv6, the interface name and the source address do not have to match.

`-t <type of service>`

The `-t` option sets the type-of-service in probe packets to the specified value. The default is 0. The value must be an integer in the range from 0 to 255. Gateways along the path may route the probe packet differently depending upon the `-t` value set in the probe packet. This option is valid only on IPv4.

`-w <wait time>`

The `-w` option sets the time, in seconds, to wait for a response to a probe. The default is `5` seconds.

Example

We trace the route using an IP address.

```
traceroute 172.21.156.192
traceroute: Warning: Multiple interfaces found; using 172.21.156.192 @ nx0:1
traceroute to 172.21.156.192 (172.21.156.192), 30 hops max, 40 byte packets
1 ES156190-001-mgmt-vip (172.21.156.192) 0.069 ms 0.037 ms 0.026 ms
```

ui

To run this command:

1. Access the CLI command shell—see Accessing the nxadmin and nxcmd CLIs on page 13.
2. Type the command using the syntax provided in this topic.
3. Press Enter.

Description

Use this procedure if you have upgraded to Unity [[[Undefined variable Unity.Firmware Version]]], and you want to set Unity to the HTML5 interface.

The Unity Classic and HTML5 graphical user interfaces can operate concurrently in separate browser windows or tabs.

Controller

Run this command on either controller.

Syntax `ui -c <set_new | set_legacy>`

Options `-c <set_new | set_legacy>`

The `-c` option specifies the user interface to apply. The value must be either `set_new` or `set_legacy`.

Example Apply the new interface.

```
ui -c set_new
HOST: ES156190-001-01
Setting system to the new UI...
Running on the peer...
HOST: ES156190-001-02
Setting system to the new UI...
```

uptime

To run this command:

1. Access the CLI command shell—see Accessing the nxadmin and nxcmd CLIs on page 13.
2. Type the command using the syntax provided in this topic.
3. Press Enter.

Description This command displays the number of days that the system has been running since the last reboot/shutdown sequence. It also displays the numbers of active users and the average number of jobs in the run queue over the last 1, 5, and 15 minutes.

Controller Run this command on the controller for which you want to see the information.

Syntax `uptime`

Options None

Example

Output example of a system updated today:

```
4:03pm up 2:25, 2 users, load average: 0.33, 0.35, 0.34
```

Output example of a system running for several days:

```
3:01pm up 10 day(s), 1:23, 8 users, load average: 0.36, 0.37,
0.38
```

useradd

To run this command:

1. Access the CLI command shell—see Accessing the nxadmin and nxcmd CLIs on page 13.
2. Type the command using the syntax provided in this topic.
3. Press Enter.

Description This command enables you to add local user accounts on the Unity Storage System that

file systems.

You must perform additional steps depending on whether you are using a NFSv3 or NFSv4 client to access file systems; refer to the *Managing File Systems* chapter of the *Nexsan Unity Software User Guide*.

You can also use this command to add local user accounts if you are using Nexsan Unity™ authentication.

Note: No output gets displayed, except in the case of error.

Controller — You can run this command on any controller.

Syntax — `useradd -u <UID> <name>`

Options — `UID`

This parameter specifies the user identification.

You cannot use these UID numbers because they are reserved:

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

If there are conflicting IDs, please contact Nexsan Technical Support.

`name`

This parameter specifies the user name.

Example — We add user `Bob` as local account with a UID of `300`.

```
useradd -u 300 Bob
```

userdel

To run this command:

1. Access the CLI command shell—see Accessing the nxadmin and nxcmd CLIs on page 13.
2. Type the command using the syntax provided in this topic.
3. Press Enter.

Description — This command enables you to delete local user accounts on the Unity Storage System that correspond to UNIX/Linux Microsoft Active Directory domain accounts.

Note: No output gets displayed, except in the case of error.

Controller — You can run this command on any controller.

Syntax — `userdel <name>`

Options — `<name>`

This option specifies the name of user to delete.

Example We delete user `Alex` from local accounts.

```
userdel Alex
```

userquota

To run this command:

1. Access the CLI command shell—see Accessing the nxadmin and nxcmd CLIs on page 13.
2. Type the command using the syntax provided in this topic.
3. Press Enter.

Description This command enables you to display and set user quotas on file systems.

Controller Run this command on the controller hosting the pool or file system.

Syntax

```
userquota
[-c set|get]
[-t user|group]
[-u user name]
[-s M|G|T|none]
[-h]
```

Options

`-c set`

This command sets the space usage quota for the specified user or group and specified file system.

`-c get]`

This command displays the space usage quota defined for the specified user or group.

`[-t user|group]`

The `-t` option specifies the type: `user` or `group`. This option is always required.

`[-u user name]`

The `-u` option specifies the name of the user or group, in this format: `user@domain.lan`.

For example, `bob@qadomain.net` or `Tat Yi Ci@qadomain.net`.

This option is required with the `-c set` command, and optional with the `-c get` command.

Note: If you enter only the user name instead of the fully qualified domain name, the Unity Storage System will treat this user as a new user.

The `-s` option specifies the size of the space usage quota:

- `M` for megabytes,
- `G` for gigabytes, or
- `T` for Terabytes; for example, `5T` for five terabytes.
- `None` if you do not want to specify a size.

The `-s` parameter is optional when using the `-c get` command.

`-h`

This option specifies the file system name. This parameter is optional if you specify a user when using the `-c get` command.

Example 1 — We set a user quota for a user named `Bob` and we set his usage quota to 2 terabytes on a file system called `FinanceFileSystem`.

```
userquota -c set -t user -u bob@domain.com -s 2T -h
FinanceFileSystem
```

Example 2 — We display the quota for user `Bob` for all file systems.

```
userquota -c get -u bob@domain.com -t user
```

vmstat

To run this command:

1. Access the CLI command shell—see Accessing the nxadmin and nxcmd CLIs on page 13.
2. Type the command using the syntax provided in this topic.
3. Press Enter.

Description — This command displays summary information and statistics for system virtual memory.

Controller — Run this command on the controller where you want to see the information.

Syntax

```
vmstat [-i|-p|-q|-s|-S]
[-T d|u]
[disk ...]
[interval [count]]
```

Options

`-i`

This option displays the number of interruptions per device. You do not need to specify `count` and `interval` for this option.

`-p`

This option displays paging activity in detail.

`-q`

This option suppresses messages related to state changes.

`-s`

This option displays the total number of system events since it was booted. You do not need to specify `count` and `interval` for this option.

`-S`

This option displays information on swapping only.

`-T d|u`

This option changes the way time information is displayed:

- specify `u` for a printed representation of the internal representation of time.
- specify `d` for the standard time format.

Example **`vmstat`**

```
kthr memory        page                disk      faults       cpu
r b w swap   free   re  mf  p p f d s f s s s in   sy   cs  u s i
                       i o r e r 0 1 2 3             s y d
0 0 0 13053  28649  35  414 0 0 0 0 0 - 8 1 1 164  431  192 3 4 9
      48     92     2   3               0   0 0 5    3    2       3
```

vssadm

To run this command:

1. Access the CLI command shell—see Accessing the nxadmin and nxcmd CLIs on page 13.
2. Type the command using the syntax provided in this topic.
3. Press Enter.

Description This command enables you to display status information on the All Ports / All LUNs feature on the Nexsan NST6000™.

Controller Run this command on the controller where you want to see the information.

Syntax `vssadm <show-apal>`

Options `<show-apal>`

This option displays information on APAL status, node, channel, and I/O statistics. This option must be used with the command.

Example **`vssadm show-apal`**

```
APAL Status : enabled
APAL Node : 0
APAL Channel : IP
APAL Read I/O : 28
APAL Write I/O : 0
APAL Other I/O : 6929
```

whoami

To run this command:

1. Access the CLI command shell—see Accessing the nxadmin and nxcmd CLIs on page 13.
2. Type the command using the syntax provided in this topic.
3. Press Enter.

Description This command displays the user currently logged in to the The Unity Storage System.

Controller	You can run this command on any controller.
Syntax	`whoami`
Options	None
Example	► **Output example:** `nxadmin`

wwn

► **To run this command:**

1. Access the CLI command shell—see Accessing the nxadmin and nxcmd CLIs on page 13.
2. Type the command using the syntax provided in this topic.
3. Press Enter.

Description	This command displays World Wide Names (WWNs) for iSCSI or Fibre Channel IDs, along with their status, protocol, and number of active sessions. WWNs are unique 8 byte (64-bit) identifiers in SCSI or Fibre Channel similar to that of MAC Addresses on a Network Interface Card (NIC).
Controller	Run this command on either controller.
Syntax	`wwn`
Options	None

Example	**`wwn`**
	`Node 1 Target: iqn.1999-02.com.nexsan:site1:lin2:0`
	`Operational Status : Online`
	`Protocol : iSCSI`
	`Sessions : 0`
	`Node 1 Target: iqn.1999-02.com.nexsan:es200070-001:lin2:mgmt`
	`Operational Status : Online`
	`Protocol : iSCSI`
	`Sessions : 0`
	`Node 1 Target: wwn.50003A400000241C`
	`Operational Status : Online`
	`Protocol : Fibre Channel`
	`Sessions : 0`
	`Node 1 Target: wwn.50003A400000241D`
	`Operational Status : Online`
	`Protocol : Fibre Channel`
	`Sessions : 1`
	`Initiator: wwn.21000024FF67617A`

```
Logged in since: Mon Sep 30 16:02:08 2013
Node 1 Target: wwn.50003A400000241A
Operational Status : Online
Protocol : Fibre Channel
Sessions : 1
Initiator: wwn.2101001B32BAE462
Logged in since: Mon Sep 30 16:02:52 2013
Node 2 Target: iqn.1999-02.com.nexsan:site1:lin2:0
Operational Status : Online
Protocol : iSCSI
Sessions : 0
Node 2 Target: iqn.1999-02.com.nexsan:es200070-001:lin2:mgmt
Operational Status : Online
Protocol : iSCSI
Sessions : 0
Node 2 Target: wwn.50003A400000241C
Operational Status : Online
Protocol : Fibre Channel
Sessions : 0
Node 2 Target: wwn.50003A4000002402
Operational Status : Online
Protocol : Fibre Channel
Sessions : 0
Node 2 Target: wwn.50003A4000002404
Operational Status : Online
Protocol : Fibre Channel
Sessions : 0
```


ypcat

To run this command:

1. Access the CLI command shell—see Accessing the nxadmin and nxcmd CLIs on page 13.
2. Type the command using the syntax provided in this topic.
3. Press Enter.

Description	This command displays values from a NIS database in an NIS integration. Since `ypcat` uses the NIS network, you do not need to specify a NIS server. For steps to integrate NIS, see Integrating with Network Information Service (NIS).
Controller	Run this command on the active controller. (The active controller has the System Management component running on it.)

Syntax `ypcat [-k <key>] [-d <domain name>] [-t <map name>] [-x]`

Options `-k <key>`

This option displays the database values for the specified key.

`-d <domain name>`

This option specifies the domain name of the NIS server.

`-t <map name>`

This option inhibits the translation of database map nick names for the specified name. The name can be a map name or map nickname.

`-x`

This option displays the translation table for map nick names.

Example We display the list of NIS users.

`ypcat -k passwd`

ypinit

To run this command:

1. Access the CLI command shell—see Accessing the nxadmin and nxcmd CLIs on page 13.
2. Type the command using the syntax provided in this topic.
3. Press Enter.

Description This command initializes the NIS client, including building a master NIS server database and a slave database on the NIS server. For steps to integrate NIS, see Integrating with Network Information Service (NIS).

Controller Run this command on the active controller. (The active controller has the System Management component running on it.)

Syntax `ypinit [-c] [-m] [-s <master server>]`

Options `-c`

This command sets an NIS client. You must run the `ypinit -c` command whenever a new NIS server is added to the network or when an existing one is decommissioned.

Note: The `ypinit -c` command must be run on both controllers. This is required if you are integrating NIS with the Unity Storage System.

`ypinit -m`

This command builds a master server NIS database.

`ypinit -s <master server>`

This command builds a slave database on the NIS server. The Master Server must be the same server map name (or map nick name) returned by the `ipwhich` command.

Example We create a slave database on the NIS master server.

`ypinit - s nis.nisdomain2.lan`

ypwhich

To run this command:

1. Access the CLI command shell—see Accessing the nxadmin and nxcmd CLIs on page 13.
2. Type the command using the syntax provided in this topic.
3. Press Enter.

Description

This command displays the name of the NIS server that provides the NIS name services to a NIS client on the Unity Storage System, or which is the master for a map . If you run this command without arguments, it displays the NIS server for the local system. For steps to integrate NIS, see Integrating with Network Information Service (NIS).

Controller

Run this command on the active controller. (The active controller has the System Management component running on it.)

Syntax

```
ypwhich [-d <domain name>] [[-t] -m <map name>|[-Vn] <host>]
ypwhich -x
```

Options

`-d <domain name>`

This option specifies the domain name of the NIS server.

`-t`

This option inhibits the translation of map nick names.

`-m <map name>`

This option specifies the map name or the nick name of a map.

`-Vn`

This option specifies the version of ypbind; version 3 is the default.

`host`

This option specifies the host name.

`-x`

This option displays the translation table for map nick names.

Example

We display the translation table.

```
ES156190-001-01:P:/> ypwhich -x
Use "passwd"      for map "passwd.byname"
Use "group"       for map "group.byname"
Use "project"     for map "project.byname"
Use "networks"    for map "networks.byname"
Use "hosts"       for map "hosts.byname"
Use "ipnodes"     for map "ipnodes.byname"
Use "protocols"   for map "protocols.byname"
Use "services"    for map "services.byname"
```

```
Use "mail"          for map "mail.byname"
Use "ehters"        for map "ethers.byname"
```

Chapter 3

Using the menu-driven nxadmin CLI

The nxadmin CLI's main menu—or, the NestOS Admin Menu—includes several main menu options that give you access to sub-menus containing commands and functions that you can perform on the Unity Storage System. Depending on the option you select in the NestOS Admin Menu, there can be multiple levels of sub-menus corresponding to the selected function.

Each submenu provides the `q` (Exit) option that exits the current submenu and returns you to the previous, or root, submenu in the structure. When you type `q` in the NestOS Admin Menu, the system logs you off the system.

To access the menu-driven CLI:

- Type `menu` at the nxadmin CLI prompt.

The NestOS Admin Menu includes these main options:

Network menu 202
Shut down and Reboot menu 216
Restart the Web service 221
Run a command 221
Fault Repair menu 247
Configure file systems and Active Directory 248
Reset the Unity Storage System 267
System menu 268

Network menu

You configure network settings on the Unity Storage System using the **Network Menu** option from the NestOS Admin Menu.

```
NestOS Network Menu

1 - Network Configuration Menu
2 - Network Adapter Aggregation Menu
3 - Replication Settings
4 - Configure the IPMI Network Settings
5 - Configure the update server
6 - Configure iSCSI targets

q - Exit

Select an option:
```

This section includes these topics:

- Setting or modifying network settings below
- Displaying aggregation information for network interfaces on the facing page
- Configuring data replication settings on page 204
- Modifying IPMI settings on page 210
- Setting an IP address for the Update Server on page 212
- Configuring iSCSI targets on page 213

Setting or modifying network settings

This section explains how to set or modify IP configuration settings on the Unity Storage System.



CAUTION: Modifying network settings affects user access to data. If you modify network settings on the Unity Storage System, any clients or applications that access the data on the system will be disconnected.

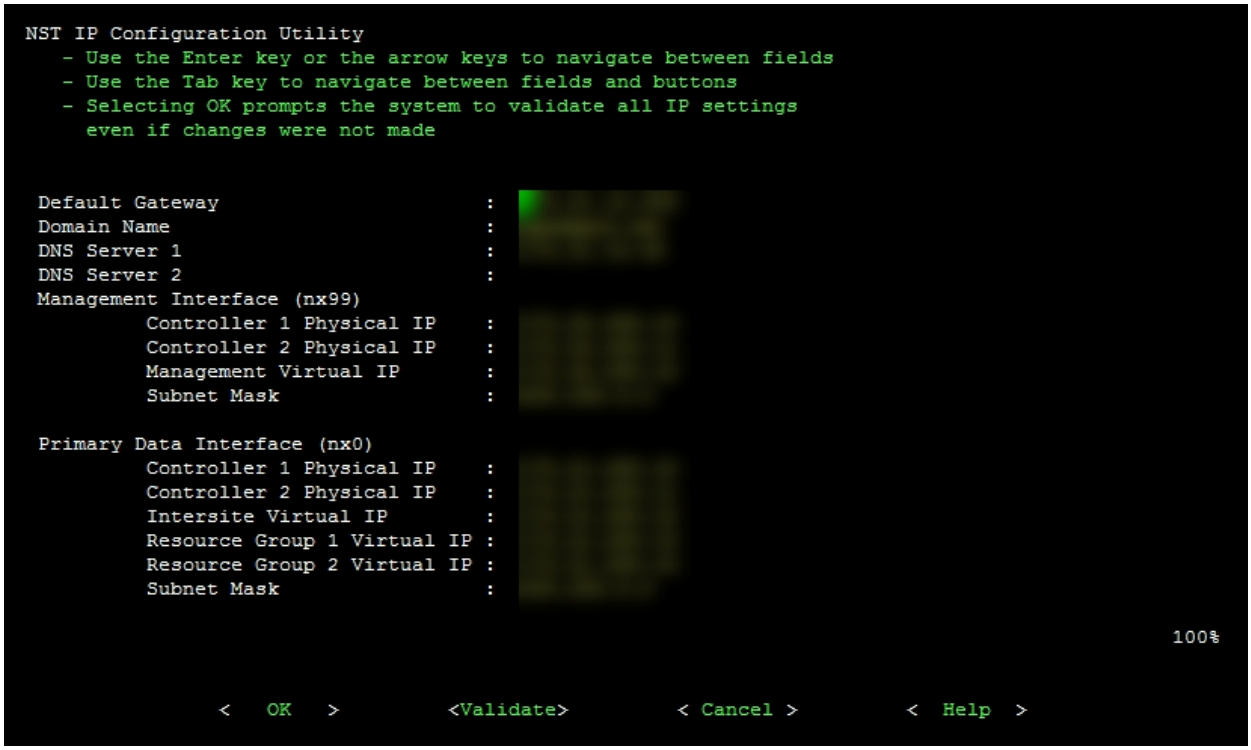
This can also be performed using the `setip` command in the command shell; see setip on page 159.

To modify network settings on the Unity Storage System:

1. In the NestOS Admin Menu, type **1** (**Network Menu**) and then press Enter. This displays the NestOS Network Menu.

2. Type **1** (**Network Configuration Menu**) and then press Enter.

   This displays the IP configuration screen where you set or modify the network settings for the Unity Storage System's management interface (nx99) and primary data network interface (nx0).



3. Type the network settings in each of the corresponding fields; use the Tab key to navigate between fields.
4. When you finish setting or modifying network settings for the Unity Storage System's management interface (nx99) and primary data network interface (nx0), tab to the **<Test>** option and press Enter; the Unity Storage System validates the new or updated network settings.
5. Once the validation process completes, tab to the **<OK>** option and press Enter to apply the network settings to the system.

Displaying aggregation information for network interfaces

On a Unity Storage System with both the (onboard) 1Gb and (optional) 10Gb network interfaces, the system uses the 10Gb interface as the primary data network interface. All ports on any (optional) 10Gb network interface are aggregated, by default, to provide redundancy and fault tolerance in the event that one of the connections goes down. The nxadmin CLI enables you to de-aggregate ports, if needed. You use the nic command to configure aggregation and other advanced network settings.

The management interface on the Unity Storage System is referred to as `nx99`, the primary data network interface as `nx0`, and the secondary as `nx1` (if it exists).

To show aggregation information for network interfaces:

1. In the NestOS Admin Menu, type **1** (**Network Menu**) and then press Enter. This displays the **NestOS Network Menu**.
2. Type **2** (**Network Adapter Aggregation Menu**) and press Enter. This displays the **NestOS Network**

Adapter Aggregation Menu.

3. Type **1** (**Show Aggregation Information**) and press Enter.

Configuring data replication settings

The nxadmin CLI enables you to modify data replication settings using NestOS Replication Bandwidth Menu.

```
NestOS Replication Bandwidth Menu

1 - Show Default Replication Bandwidth Limit
2 - Change Default Bandwidth Limit
3 - Show Current Replication Compression Setting
4 - Change Replication Compression Setting
5 - Show Replication Interface Setting
6 - Change Replication Interface Setting
7 - Show Current Replication Network Type Setting
8 - Change Replication Network Type Setting
9 - Show Current Replication Encryption Setting
10 - Change Replication Encryption Setting
11 - Show Current Replication HPNBufferSize
12 - Change Replication HPNBufferSize
 13 - Show Maximum Number of Concurrent Replications per Controller
 14 - Change Maximum Number of Concurrent Replications per Controller
15 - Show Replication Priority Adjustment
16 - Change Replication Priority Adjustment
17 - Perform a Network Performance Test
18 - Perform a Network Connectivity Test

q - Exit

Select an option:
```

This section covers these topics:

- Configuring the network bandwidth for data replication on the facing page
- Configuring compression settings for data replication on the facing page
- Configuring the network interface for data replication on the facing page
- Configuring the network type for data replication on page 206
- Configuring encryption settings for data replication on page 207
- Configuring the buffer size for High Performance Networks (HPN) on page 207
- Setting the maximum number of concurrent replications per controller on page 208
- Changing the replication priority adjustment on page 208
- Running a network performance test on page 209
- Running a network connectivity test on page 209

Configuring the network bandwidth for data replication

The nxadmin CLI enables you to configure the network bandwidth for data replication on the Unity Storage System.

By default, the Unity Storage System uses all the available bandwidth on the primary network interface for data replication. You can restrict the bandwidth, if needed.

To configure the network bandwidth for data replication:

1. In the NestOS Admin Menu, type **1** (**Network Menu**) and then press Enter. This displays the **NestOS Network Menu**.
2. Type **3** (**Replication Settings**) and press Enter; this displays the **NestOS Replication Bandwidth Menu**.
3. Type **2** (**Change Replication Bandwidth Limit**), and press Enter.
4. Enter a value for the bandwidth limit in kilobytes per second (Kb/s), and then press Enter.

The Unity Storage System restricts the replication bandwidth according to the limit you specify.

Note On a the Unity Storage System with both the (onboard) 1Gb and (optional) 10Gb network interfaces, where the 1Gb interface is NOT being used as the primary interface, you can configure data replication to be routed through the 1Gb interface by adding a host entry for the remote Unity Storage System to the routing table on the primary Unity Storage System; for more information, see Run a command on page 221.

Configuring compression settings for data replication

The nxadmin CLI enables you to turn on or off replication compression for data replication on the Unity Storage System. By default, the Unity Storage System does not compress replication data. If you need to turn this feature on, you can use the NestOS Replication Bandwidth Menu.

Note The compression setting can also be set from Unity, as described in the *Nexsan Unity Software User Guide*.

To configure compression settings for data replication on the Unity Storage System:

1. In the NestOS Admin Menu, type **1** (**Network Menu**) and then press Enter. This displays the **NestOS Network Menu**.
2. Type **3** (**Replication Settings**) and press Enter; this displays the **NestOS Replication Bandwidth Menu**.
3. Type **4** (**Change Replication Compression Setting**), and press Enter.
4. You will be prompted to confirm the action, type **yes** and press Enter.

Configuring the network interface for data replication

The nxadmin CLI enables you to choose the network interface for data replication on the Unity Storage System.

By default, the Unity Storage System uses the primary data network interface (nx0) to access and replicate data. If other data network interfaces (nx1, nx2, nx99, etc.) are configured on the Unity Storage System, you can change the default network interface to another one for data replication with the NestOS Replication Bandwidth Menu.

The network interface that you set on the primary system (for the outgoing replication stream) can be different from the one on the remote system (for the incoming stream).

To set up additional network interfaces, refer to the `nic create-aggr` command; see nic on page 103. To view aggregation information, see Displaying aggregation information for network interfaces on page 203.

Note The nx0 and nx99 network interfaces can also be selected from Unity, as described in the *Nexsan Unity Software User Guide*. For other network interfaces, you must use the Network Menu.

To change the network interface for data replication:

1. In the NestOS Admin Menu, type **1** (**Network Menu**) and then press Enter. This displays the **NestOS Network Menu**.
2. Type **3** (**Replication Settings**) and press Enter. This displays the **NestOS Replication Bandwidth Menu**.
3. Type **5** (**Show Replication Interface Setting**), and press Enter.

   The command returns a blank field:

   ```
   Current Replication interface setting is:
   ```

   This means that nx0 is being used.
4. Type **6** (**Change Replication Interface Setting**), and press Enter.
5. At the prompt, enter the network interface name and press Enter.
6. Verify that the new setting was applied. Type **5** (**Show Replication Interface Setting**), and press Enter.

   The command should return:

   ```
   Current Replication interface setting is: nx1
   ```

Note If an error occurs, the command defaults back to nx0.

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). Setting the network type to **WAN** also increases the HPNBuffersize from the default to 4 MB.

Note The network type can also be set from Unity, as described in Configuring network settings for Asynchronous Replication on page 1 of the the *Nexsan Unity Software User Guide*.

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.

Configuring encryption settings for data replication

The Unity Storage System enables you to encrypt data that is replicated for added security. Encryption is enabled by default. If you replicate data on a secure network and do not require to encrypt data, you can disable encryption.

▶ **To change the encryption setting:**

1. In the NestOS Admin Menu, type **1** (**Network Menu**) and then press Enter. This displays the **NestOS Network Menu**.
2. Type **3** (**Replication Settings**) and press Enter. This displays the **NestOS Replication Bandwidth Menu**.
3. Type **10** (**Change Replication Encryption Setting**), and press Enter.
4. Perform one of these actions, and press Enter:
   - To enable encryption, type **1**.
   - To disable encryption, type **2**.
5. When `Press Any Key` appears, press Enter. The Unity Storage System changes to the encryption setting according to your selection.
6. (Optionally) To view the updated setting, type **9**.

Tip To exit the `command:` prompt and return to the NestOS Admin Menu, type **`Exit`**, and then press Enter.

Configuring the buffer size for High Performance Networks (HPN)

The Unity Storage System uses the open source SSH protocol (OpenSSH) for network connectivity. OpenSSH relies on the TCP/IP protocol, which is used to replicate data. High Performance Networks (HPN) over SSH improve network performance, and thus the speed of data replication. It implements a flow control mechanism to make sure that the network connection is not overwhelmed.

HPN-SSH uses a receive buffer to indicate how much data the sender should be sending at any one point. The default buffer size to 64 KB, which may be too small for very high speed connections over long

distances. The Unity Storage System enables you to set this buffer much higher to allow transfers at very high rates.

To configure the HPN buffer size:

1. In the NestOS Admin Menu, type **1** (**Network Menu**) and then press Enter. This displays the **NestOS Network Menu**.
2. Type **3** (**Replication Settings**) and press Enter. This displays the **NestOS Replication Bandwidth Menu**.
3. Type **12** (**Set the HPNBufferSize**), and press Enter.
4. Select **1** to set the HPN buffer size and press Enter.
5. Enter a number between **2048** and **8192**, or type **default**, and press Enter.
6. (Optional) To verify the new value, select **11** (**Show Current Replication HPNBufferSize**).

Tip To exit the `command:` prompt and return to the NestOS Admin Menu, type **`Exit`**, and then press Enter.

Setting the maximum number of concurrent replications per controller

The Unity Storage System enables you to specify the maximum number of concurrent replications per controller for better performance. The default is 6

To configure the HPN buffer size:

1. In the NestOS Admin Menu, type **1** (**Network Menu**) and then press Enter. This displays the **NestOS Network Menu**.
2. Type **3** (**Replication Settings**) and press Enter. This displays the **NestOS Replication Bandwidth Menu**.
3. Type **14** (**Change Maximum Number of Concurrent Replications per Controller**), and press Enter.
4. Enter a number between **1** and **100**, and press Enter.

Tip To exit the `command:` prompt and return to the NestOS Admin Menu, type **`Exit`**, and then press Enter.

Changing the replication priority adjustment

The Unity Storage System enables you to adjust the replication priority. Replication priority is a priority requested and set by the operating system. The replication process cannot exceed a certain amount of CPU time and this is controlled by its priority. If the replication process runs for longer than expected, the operating system will decrease its priority. This type of priority is called *dynamic*.

If you want the replication process to continue running over the expected CPU time, you need to set the replication priority to *fixed*. This is done by disabling the replication priority adjustment. By default, the replication priority adjustment is enabled.

To disable replication priority:

1. In the NestOS Admin Menu, type **1** (**Network Menu**) and then press Enter. This displays the **NestOS Network Menu**.
2. Type **3** (**Replication Settings**) and press Enter. This displays the **NestOS Replication Bandwidth Menu**.
3. Type **16** (**Change Replication Priority Adjustment**), and press Enter.
4. Enter **y** to confirm and press Enter.

Tip To exit the `command:` prompt and return to the NestOS Admin Menu, type **`Exit`**, and then press Enter.

Running a network performance test

The nxadmin CLI enables you to run a bandwidth performance test for data replication on Unity Storage System. You can run this test using a storage pool or the IP addresses of the controller nodes. To change the default replication bandwidth limit, see Configuring the network bandwidth for data replication on page 205.

▶ **To test the replication bandwidth:**

1. In the NestOS Admin Menu, type **1** (**Network Menu**) and then press Enter. This displays the **NestOS Network Menu**.
2. Type **3** (**Replication Settings**) and press Enter. This displays the **NestOS Replication Bandwidth Menu**.
3. Type **17** (**Perform a Network Performance Test**), and press Enter. This displays the **NestOS Replication Bandwidth Test Menu**, with the list of storage pools created on the Unity Storage System.
4. Type **1** (**From IP**) and press Enter.
5. Enter the IP address of the peer node and press Enter.
6. Enter the IP address of the local node or press Enter to skip IP banding.
7. Enter the size for transmission (in megabytes) and press Enter. The default is 100. The Unity Storage System runs the test and returns the number of gigabits per second.

Figure 3-1: Example of NestOS Replication Bandwidth Test Menu

```
1 - From IP
q - Exit
Select an option: 1
Enter the IP of the peer [or just hit enter to cancel]:
172.21.156.191
Using IP 172.21.156.191 to perform the test.
Enter the local IP [or just hit enter to skip IP banding]:
Local IP not defined
Enter transmit size in MBytes (default 100):90
Bandwidth test from local to 172.21.156.191(nx0) starts...
[ ID] Interval Transfer Bandwidth
[ 3] 0.0- 0.5 sec 90.0 MBytes 1.55 Gbits/sec
Test completed.
```

Tip To exit the `command:` prompt and return to the NestOS Admin Menu, type **`Exit`**, and then press Enter.

Running a network connectivity test

The nxadmin CLI enables you to run a network connectivity test for data replication. The Unity Storage System will test the local replicated storage pools and the peer replicated storage pools on the selected network. This process tests the connection to the peer Unity Storage System (site) and the peer storage pool using `ping` and then `SSH`. The result gets displayed after each test.

If there is no replication set up for the Unity Storage System, the command does not display any result.

To verify network connectivity:

1. In the NestOS Admin Menu, type **1** (**Network Menu**) and then press Enter. This displays the **NestOS Network Menu**.
2. Type **3** (**Replication Settings**) and press Enter. This displays the **NestOS Replication Bandwidth Menu**.
3. Type **18** (**Perform a Network Connectivity Test**), and press Enter.

Figure 3-2: Output example

```
Select an option: 18
Test local replicated pools through specified interfaces
Pool: p6, local interface: nx0, peer interface: nx0
Ping peer site 172.21.200.112 ... PASS
Ping peer pool 172.21.200.113 (-i nx0) ... PASS
SSH to peer site 172.21.200.112 port 22 ... PASS
SSH to peer pool 172.21.200.113 port 18000 encryption on (-b
172.21.202.31)... PASS
Test peer replicated pools through specified interfaces
```

Tip To exit the `command:` prompt and return to the NestOS Admin Menu, type **`Exit`**, and then press Enter.

Modifying IPMI settings

The Unity Storage System supports IPMI over LAN and includes the Intelligent Platform Management Interface (IPMI) to manage the Unity Storage System. The IPMI interface enables you to perform administrative tasks to remotely manage the Unity Storage System in the event that you are unable to connect to the system using a conventional method (through Nexsan Unity or from the nxadmin CLI); administrative tasks that you can perform through the IPMI interface include: setting network settings for the Unity Storage System, viewing hardware-related error conditions, launching a remote console session to the Unity Storage System, and performing other maintenance tasks on the system.

The Unity Storage System's IPMI interface is provided as a Web-used utility that you can access from a browser using the Unity Storage System's IPMI IP address. Before you can access the Unity Storage System's Web-based IPMI interface, you must first set an IPMI IP address, subnet mask, and a default gateway IP address for the Unity Storage System. On a clustered system, you must set a separate IPMI IP address for each controller node.

Note To enable IPMI for the Unity Storage System, 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's chassis; this second LAN port is located at the bottom of each controller node, closest to the bottom-edge of the controller box.

```
NestOS IPMI Menu

1 - Show information
2 - Change Network Settings to static
3 - Change Network Settings to dhcp
4 - Set the IPMI login password
5 - Set the IPMI login password to default
6 - Unset network settings for IPMI access
```

```
q - Exit

Select an option:
```

This section includes these topics:

- Switching between DHCP and Static IP addressing for the IPMI interface below
- Setting the IPMI password below
- Resetting the IPMI password to default on the next page
- Clearing IPMI network settings on the next page

Switching between DHCP and Static IP addressing for the IPMI interface

By default, the IPMI interface on the Unity Storage System uses static IP addressing. You can change to DHCP (dynamic) IP addressing for the IPMI interface if your network has a DHCP server.

To switch between DHCP and Static IP addressing:

1. In the NestOS Admin Menu, type **1** (**Network Menu**) and then press Enter. This displays the **NestOS Network Menu**.
2. Type **4** (**Configure the IPMI Network Settings**) and press Enter. This displays the **NestOS IPMI Menu**.
3. Perform one of these actions:

To...	Do this
switch from Static IP addressing to DHCP	a. Type **3** (**Change Network Settings to dhcp**). b. Press Enter. c. A prompt displays asking if you want to continue; type **yes**. d. Press Enter.
switch from DHCP IP addressing to Static	a. Type **2** (**Change Network Settings to static**). b. Press Enter. c. A prompt displays asking if you want to continue; type **yes**. d. Press Enter. e. You are then prompted to enter the IPMI IP addresses for each controller node on the system, as well as the subnet mask and gateway IP address for the IPMI interface.

Setting the IPMI password

The IPMI interface provides the default ADMIN account, with its default password set to ADMIN.

To change the IPMI password of the ADMIN account:

1. In the NestOS Admin Menu, type **1** (**Network Menu**) and then press Enter. This displays the **NestOS Network Menu**.

2. Type **4** (**Configure the IPMI Network Settings**) and press Enter. This displays the **NestOS IMPI Menu**.
3. Type **4** (**Set the IPMI login password**) and press Enter.
4. When prompted, type a new password for the IPMI interface's ADMIN account, and press Enter to save the password.

Resetting the IPMI password to default

The IPMI interface provides the default ADMIN account, with its default password set to ADMIN. If you changed this password using option 4, you have the possibility to reset it to ADMIN.

▶ **To reset the IPMI password to default:**

1. In the NestOS Admin Menu, type **1** (**Network Menu**) and then press Enter. This displays the **NestOS Network Menu**.
2. Type **4** (**Configure the IPMI Network Settings**) and press Enter This displays the **NestOS IMPI Menu**.
3. Type **5** (**Set the IPMI login password to default**) and press Enter.

Clearing IPMI network settings

If needed, you can clear the network settings for the IMPI interface on the Unity Storage System. This process removes the IPMI IP addresses for each controller node on the system, as well as the subnet mask and gateway IP address for the IPMI interface. It also resets the password for the ADMIN account to the default password (ADMIN).

▶ **To clear IMPI network settings on the Unity Storage System:**

1. In the NestOS Admin Men, type **1** (**Network Menu**) and then press Enter. This displays the **NestOS Network Menu**.
2. Type **4** (**Configure the IPMI Network Settings**) and press Enter. This displays the **NestOS IMPI Menu**.
3. Type **6** (**Unset network settings for IPMI access**) and press Enter.
4. A prompt displays asking if you want to continue; type **yes** and press Enter.

Setting an IP address for the Update Server

The Update Server enables you to automatically update the software components on the Unity Storage System by downloading the latest software from the server. By default, the Unity Storage System is configured with the URL of the Update Server. If your DNS server is unable to resolve the URL for the Update Server, or if your network infrastructure does not include a DNS server, you can set an IP address for the Update Server on the Unity Storage System to configure a direct connection to the Update Server. You must request an IP address for Update Server from Nexsan Technical Support.

▶ **To set an IP address for the Update Server:**

1. In the NestOS Admin Menu, type **1** (**Network Menu**) and then press Enter. This displays the **NestOS Network Menu**.

2. Type **5** (**Configure the update server**) and press Enter. This displays the **NestOS Update Server Menu**.

```
NestOS Update Server Menu

1 - Show Update Server Name Resolution Configuration
2 - Set an IP for the Update Server
3 - Remove an IP for the Update Server and use DNS resolution

q - Exit

Select an option:
```

3. Type **2** (**Set an IP for the Update Server**), and press Enter.
4. Enter the IP address for the Update Server provided to you by Nexsan Technical Support, and press Enter.

Configuring iSCSI targets

When you add a LUN to a storage pool on the Unity Storage System, you 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.

Each storage pool on the Unity Storage System can have one or multiple iSCSI targets, with a maximum of 255 targets per storage pool (0 to 254).

The nxadmin CLI enables you to configure the network interfaces for iSCSI targets on the Unity Storage System.

```
NestOS iSCSI Network Adapter Allocation Menu

1 - Show Allocation Information
2 - Recalculate Allocations To Detect IP Address Changes
3 - Change the network interface that an iSCSI target is presented on

q - Exit

Select an option:
```

This section covers these topics:

- Displaying iSCSI target allocations below
- Recalculating iSCSI target allocations on the next page
- Changing the network interface for iSCSI targets on page 215

Displaying iSCSI target allocations

The nxadmin CLI enables you to display the virtual IP addresses for the primary data network interface on the Unity Storage System, as well as the current iSCSI targets allocated.

To set or modify IP addresses, see Setting or modifying network settings on page 202.

To display iSCSI target allocation information:

1. In the NestOS Admin Menu, type **1** (**Network Menu**) and then press Enter. This displays the **NestOS Network Menu**.
2. Type **6** (**Configure iSCSI targets**) and press Enter. This displays the **NestOS iSCSI Network Adapter Allocation Menu**.
3. Type **1** (**Show Allocation Information**), and press Enter.

   the Unity Storage System returns output similar to this.

```
Loading Network Configuration...
Interfaces on this system
-------------------------
 name: nx0     type: mgmt     IP: 172.21.14.176
 name: nx0     type: rg1      IP: 172.21.10.30
 name: nx0     type: rg2      IP: 172.21.10.31
Targets on this system
----------------------
name: iqn.1999-02.com.nexsan:financesite176:financepool1:0
IPs: 172.21.10.30
name: iqn.1999-02.com.nexsan:es260786-176:financepool1:mgmt
IPs: 172.21.10.30
Press enter to continue...
```


Recalculating iSCSI target allocations

The nxadmin CLI enables you to recalculate iSCSI target allocations. This is useful if IP addresses were modified on the Unity Storage System (see Setting or modifying network settings on page 202.) Before starting (or restarting) a replication process, it is recommended to recalculate target allocations so that all network settings get updated on both controllers.

To recalculate iSCSI target allocations on the Unity Storage System:

1. In the NestOS Admin Menu, type **1** (**Network Menu**) and then press Enter. This displays the **NestOS Network Menu**.
2. Type **6** (**Configure iSCSI targets**) and press Enter. This displays the **NestOS iSCSI Network Adapter Allocation Menu**.

3. Type **2** (**Recalculate Allocations to Detect IP Address Changes**), and press Enter.

   The Unity Storage System returns output similar to this:

```
RECALCULATING...
Executing on peer...
RECALCULATING...
Loading Network Configuration...
Checking if any upgrades configuration are required
Making sure targets were not moved from one service to another...
Moving Targets from default...
Making sure IPs are correct...
Checking if any upgrades configuration are required
Making sure targets were not moved from one service to another...
Cleaning unused Target Port Groups...
done
Moving Targets from default...
Making sure IPs are correct...
Cleaning unused Target Port Groups...
done
```


Changing the network interface for iSCSI targets

The nxadmin CLI enables you to change the network interface for iSCSI targets on the Unity Storage System.

By default, the Unity Storage System uses the IP addresses configured on the primary data network interface (nx0) for iSCSI targets. The NestOS iSCSI Network Adapter Allocation Menu enables you to add and remove network interfaces for the specified target.

To change the network interface for an iSCSI target:

1. In the NestOS Admin Menu, type **1** (**Network Menu**) and then press Enter. This displays the **NestOS Network Menu**.
2. Type **6** (**Configure iSCSI targets**) and press Enter. This displays the **NestOS iSCSI Network Adapter Allocation Menu**.
3. Type **3** (**Change the network interface that an iSCSI target is presented on**), and press Enter.
4. The Unity Storage System automatically recalculates the iSCSI target allocations, then displays the available targets that this change applies to. Choose an iSCSI target and press Enter.

   Output example:

```
List of Targets to make modifications to:
1: iqn.1999-02.com.nexsan:financesite176:financepool1:0 - 172.21.10.30
```

```
2: iqn.1999-02.com.nexsan:es260786-176:financepool1:mgmt - 172.21.10.30
```

5. The Unity Storage System prompts you to choose one of these options:

To...	Do this
add an interface for the target to listen to	a. Choose **1** and press Enter. b. Choose an IP address from the list of IPs and press Enter.
remove an interface that the target is listening to	a. Choose **2** and press Enter. b. Choose an IP address from the list of IPs and press Enter. **Note** If there is only one IP address, you will not be allowed to remove it since it is currently used by the iSCSI target.

Shut down and Reboot menu

The nxadmin CLI provides command functions for shutting down and restarting the Unity Storage System, including performing either a graceful or forceful/aggressive restart or shutdown of the system; on a clustered system, you can restart or shutdown each controller node individually, as well as obtain the status and chassis location of each node.

You shut down or restart the Unity Storage System, and/or individual controller nodes on the system by accessing the **Shutdown and Reboot Menu**.

This section explains the process for shutting down and restarting the Unity Storage System, and/or individual controller nodes on the system; it includes these topics:

- Restarting the Unity Storage System or one of its controller nodes below
- Shutting down the Unity Storage System or one of its controller nodes on the facing page
- Obtaining the status and location of a controller node on page 218
- Powering down or powering up the peer node on page 220

Restarting the Unity Storage System or one of its controller nodes

The nxadmin CLI provides three different options for restarting, or rebooting, the Unity Storage System, or one of its controller nodes:

- **Graceful reboot**: this option quiesces (or stops), in sequential order, all services on the Unity Storage System before restarting the system (or one of its controller nodes).
- **Aggressive reboot**: this option forcefully quiesces system services on the Unity Storage System before restarting the system, or one of its controller nodes. It should only be used if a graceful reboot does not restart the system (or one of its controller nodes).
- **Power reset**: this option does not automatically quiesce system services on the Unity Storage System; it forces a reboot of the system, or one of its controller nodes. This option should only be used if both the graceful reboot and aggressive reboot options do not restart the system (or one of its controller nodes).

Note In a clustered system, you can only perform a graceful reboot of the peer node. The Aggressive reboot and Power reset options are not available for the peer node. To perform an Aggressive reboot and/or Power reset of the peer node, access the corresponding node via SSH or remote console.

To restart the Unity Storage System or one of its controller nodes:

1. In the NestOS Admin Menu, type **2** (**Shutdown and Reboot Menu**) and then press Enter. This displays shutdown and restart options for the Unity Storage System.

```
1 - Graceful Reboot of this node
2 - Aggressive Reboot (more aggressive about killing processes)
3 - Power Reset this node (non graceful reboot)
4 - Graceful Shutdown this node
5 - Force power off this node (non graceful power off)

6 - Graceful Reboot of the Peer Controller
7 - Graceful Shutdown of the Peer Controller
8 - Power Control Menu for the Peer Controller (status/poweroff/poweron)
9 - Graceful Shutdown both nodes of the cluster

q - exit
Enter a selection:
```

2. Perform one of these actions:

To restart the...	Do this
current node	Type either **1**, **2**, or **3**.
peer node	Type **6**.

3. Press Enter.

Shutting down the Unity Storage System or one of its controller nodes

The nxadmin CLI provides these options for shutting down the Unity Storage System, or one of its controller nodes:

- **Graceful shut down**: this option quiesces (or stops), in sequential order, all services on the Unity Storage System before shutting down the system (or one of its controller nodes).
- **Force power off**: this option does not automatically quiesce system services on the Unity Storage System; it forces a shutdown of the system, or one of its controller nodes. This option should only be used if the graceful shut down option does not shut down the system (or one of its controller nodes).

Note In a clustered system, you can power down or power up the peer node by accessing the corresponding options from the **Controller Menu**; see Obtaining the status and location of a controller node on the next page.

CAUTION: When you shut down the Unity Storage System, or one of its cluster nodes, the controller node does NOT physically power down. You must press and hold the power button of the Unity Storage System's chassis to power off the system. If you shut down only a controller node on the Unity Storage System, you must remove the node's corresponding power cable from the back of the Unity Storage System's chassis before attempting to physically access the controller node.

To shut down the Unity Storage System or one of its controller nodes:

1. In the NestOS Admin Menu, type **2** (**Shutdown and Reboot Menu**) and then press Enter. This displays shutdown and restart options for the Unity Storage System.

```
1 - Graceful Reboot of this node
2 - Aggressive Reboot (more aggressive about killing processes)
3 - Power Reset this node (non graceful reboot)
4 - Graceful Shutdown this node
5 - Force power off this node (non graceful power off)

6 - Graceful Reboot of the Peer Controller
7 - Graceful Shutdown of the Peer Controller
8 - Power Control Menu for the Peer Controller (status/poweroff/poweron)
9 - Graceful Shutdown both nodes of the cluster

q - exit
Enter a selection:
```

2. Perform one of these actions:

To...	Do this
shut down the current node	Type either **4** or **5**.
(gracefully) shut down the peer node	Type **7**.
(gracefully) shut down both nodes on a clustered system	Type **9**.

3. Press Enter.

Obtaining the status and location of a controller node

On a clustered system, the nxadmin CLI provides the status of each node—**up** or **down**, and whether the controller node is **active** or **passive** in the cluster—as well as the location of the node in the Unity Storage System's chassis—left or right of the chassis (when facing the front of the Unity Storage System).

▶ To obtain the status and/or location of a controller node on the Unity Storage System:

1. In the NestOS Admin Menu, type **2** (**Shutdown and Reboot Menu**) and then press Enter. This displays shutdown and restart options for the Unity Storage System.

```
1 - Graceful Reboot of this node
2 - Aggressive Reboot (more aggressive about killing processes)
3 - Power Reset this node (non graceful reboot)
4 - Graceful Shutdown this node
5 - Force power off this node (non graceful power off)

6 - Graceful Reboot of the Peer Controller
7 - Graceful Shutdown of the Peer Controller
8 - Power Control Menu for the Peer Controller (status/poweroff/poweron)
9 - Graceful Shutdown both nodes of the cluster

q - exit
Enter a selection:
```

2. Type **8**, and then press Enter. This displays the **Controller Menu**.

```
Controller Menu

1 - Show Location
2 - Show Status
3 - Show Peer Location
4 - Show Peer Status
5 - Show Peer Power Off
6 - Show Peer Power On

q - Exit

Select an option:
```

3. To show the location of a controller node on the Unity Storage System:
   - Type **1** to show the location of the node where you are currently accessing the nxadmin CLI from.
   - Type **3** to show the location of the second controller node.
4. Press Enter. The Unity Storage System displays the chassis location of the specified node; for example: `Right side of chassis from front, slot 00.`
5. To show the status of a controller node on the Unity Storage System:
   - Type **2** to show the status of the node where you are currently accessing the nxadmin CLI from.
   - Type **4** to show the status of the second controller node
6. Press Enter. The Unity Storage System displays the status of the specified node; for example: `Up and passive.`

Powering down or powering up the peer node

On a clustered system, you can power down or power up the peer node from the **Controller Menu**.



CAUTION: When you power down the peer node on the Unity Storage System, the system does NOT physically power down the peer node. To power off the peer node, you must remove the node's corresponding power cable from the back of the Unity Storage System's chassis before attempting to physically access the controller node.

▶ **To power down or power up the peer node:**

1. In the NestOS Admin Menu, type **2** (**Shutdown and Reboot Menu**) and then press Enter. This displays shutdown and restart options for the Unity Storage System.

```
1 - Graceful Reboot of this node
2 - Aggressive Reboot (more aggressive about killing processes)
3 - Power Reset this node (non graceful reboot)
4 - Graceful Shutdown this node
5 - Force power off this node (non graceful power off)

6 - Graceful Reboot of the Peer Controller
7 - Graceful Shutdown of the Peer Controller
8 - Power Control Menu for the Peer Controller (status/poweroff/poweron)
9 - Graceful Shutdown both nodes of the cluster

q - exit
Enter a selection:
```

2. Type **8**, and then press Enter. This displays the **Controller Menu**.

```
Controller Menu

1 - Show Location
2 - Show Status
3 - Show Peer Location
4 - Show Peer Status
5 - Show Peer Power Off
6 - Show Peer Power On

q - Exit

Select an option:
```

3. Perform one of these actions:

To...	Do this
power down to peer node	Type **5**.
power up the peer node	Type **6**.

4. Press Enter.

To verify whether the peer node has been powered on or off, verify its status; see Obtaining the status and location of a controller node on page 218.

Restart the Web service

The nxadmin CLI enables you to restart the Web service on the Unity Storage System in the event that you are unable to access the system from Nexsan Unity (Nexsan Unity does not load, or you are unable to log on to the Unity Storage System).

▶ **To restart the Web service on the Unity Storage System:**

1. In the NestOS Admin Menu, type **3** (**Restart Web Service**).
2. Press Enter.

The Unity Storage System attempts to disable the Web service on the system (if it is not already disabled); it then attempts to reenable the Web service.

Once the Web service is enabled and online, the Unity Storage System displays this information:

```
The service has reached state online.
```

You should now be able to access the system from Nexsan Unity. If you are still unable to connect to the Unity Storage System, or log on to the system, please contact Nexsan Technical Support.

Run a command

the Unity Storage System's operating system (NestOS) command shell provides a set of commands that allow you to perform advanced management functions related to network configuration, user authentication, and so on, on the Unity Storage System.

▶ **To list all commands available in the NestOS command shell:**

1. In the NestOS Admin Menu, type **4** (**Run a command**) and press Enter.
2. Type **`help`** at the `command:` prompt and press Enter.

Table 3-1: Menu-driven nxadmin CLI commands

Command	Description
`chown`	This command enables you to change the owner—the user and/or the group—of one or more files or directories within a file system on the Unity Storage System.
`createlogpackage`	This command collects all system log files on the Unity Storage System and creates an encrypted package that you download from the system, using a specific URL provided during command execution.

Command	Description
date	This command writes the date and time to standard output or attempts to set the system date and time. With no arguments, the current date and time is written.
fcinfo	This command displays administrative information for the fibre channel host bus adapter (HBA) ports on the Unity Storage System. It also displays information for any fibre channel targets that might be connected to the ports.
firewall	The firewall command enables you to enable, disable, and configure the firewall on the Unity Storage System.
groupadd	This command enables you to add a local group account on the Unity Storage System that corresponds to a UNIX/Linux Microsoft Active Directory domain account. This allows members of the group account that you add to the Unity Storage System to access NFS file systems in a Microsoft Active Directory environment.
ifconfig	This command displays the current configuration for the primary (nx0) network interface on the Unity Storage System.
iostat	This command displays input/output statistics for the Unity Storage System, including terminal and disk I/O activity and CPU utilization.
ipmitool	This command displays Intelligent Platform Management Interface (IPMI) configuration information for the Unity Storage System.
listug	This command displays local user and group accounts configured on the Unity Storage System.
modgid	This command enables you to modify the GID of a local user account that you added to the Unity Storage System using the useradd command.
moduid	This command enables you to modify the UID of a local user account that you added to the Unity Storage System using the useradd command.
nestpool clear	This command clears the error counters for a storage pool, or for a device associated with a storage pool. You should use this command only if you deem any device errors as transient, in that they are unlikely to effect the future health of the device, or the associated storage pool.
nestpool iostat	This command displays the accumulated statistics since boot for all storage pools on the system, including the storage pool (rpool) in which the Unity Storage System's operating system (NestOS) and system configuration reside.

Command	Description
nestpool status	This command displays the physical state of the storage pools on the Unity Storage System, as well as of the storage pool (rpool) in which the Unity Storage System's operating system (NestOS) and system configuration reside.
nfs	This command enables you to change or set the NFS version (NFSv4) domain on the Unity Storage System, and also set the maximum version for NFS—version 3 or 4.
nic	This command enables you to display and configure advanced network settings on the system, such as, link aggregation, including creating, adding, modifying, and removing aggregations.
nscacherestart	This command clears the DNS client cache on the Unity Storage System.
nstfcdata	This command displays administrative information for the Fibre Channel host bus adapter (HBA) ports on the Unity Storage System
nstsasdata	This command displays administrative information for the Serial Attached SCSI-2 (SAS-2) host bus adapter (HBA) on the Unity Storage System.
nstusermaps	This command enables you to map a user or group account that you add to the Unity Storage System, using the useradd or groupadd commands, to a corresponding user or group account in the Microsoft Active Directory domain.
resetcache	This command resets the system cache.
restartldapclient	This command resets NFS user identity mapping on the Unity Storage System.
route	This command enables you to add TCP/IP routing entries to the routing table on the Unity Storage System.
sasinfo	This command displays administrative information for the Serial Attached SCSI-2 (SAS-2) host bus adapter (HBA) on the Unity Storage System. More specifically, the sasinfo command displays attributes of HBA ports and of storage devices and SCSI target devices that might be connected to the HBA ports.
showmount	This command lists the UNIX/Linux clients that have remotely mounted an NFS share on the Unity Storage System.
showroutes	This command displays the routing table on the Unity Storage System.

Command	Description
smbrestart	This command restarts the CIFS server on the Unity Storage System.
useradd	This command enables you to add a local user account on the Unity Storage System that corresponds to a UNIX/Linux Microsoft Active Directory domain account; this allows the user account that you add to the Unity Storage System to access NFS file systems in a Microsoft Active Directory environment.

chown

The chown command enables you to change the owner—the user and/or the group—of a folder within a file systemon the Unity Storage System, as well as the files within that folder (if the recursive, `-R`, option is specified).

▶ **To use the chown command:**

1. In the NestOS Admin Menu, type **4** (**Run a Command**) and press Enter.
2. At the `command:` prompt, type the chown command using one of these command variations and arguments:

   `chown [-R] [<user name>[:<group name>]] <file name>`
3. Press Enter.

Tip If you only want to change the user and/or group ownership of a folder, and not have the change recursively applied to all files and subfolders within that folder, simply omit the `-R` option when using the chown command.

Note To exit the `command:` prompt and return to the NestOS Admin Menu, type **`Exit`**, and then press Enter.

▶ **Example: changing user ownership in a file system**

For example, if you want to change ownership of the `Data1` folder in the `PayRollData2` file system, under the `FinancePool` storage pool to the user `Bob`, type:

`chown -R bob /pools/FinancePool/PayRollData2/Data1`

▶ **Example: changing folder ownership in a file system**

For example, if you want to change ownership of the `Data1` folder in the `PayRollData2` file system, under the `FinancePool` storage pool to the user `Bob` in the `Finance` group, type:

`chown -R bob:finance /pools/FinancePool/PayRollData2/Data1`

createlogpackage

This command collects all system log files on the Unity Storage System and creates an encrypted package that you download from the Unity Storage System, using a specific URL provided during command execution.

This command must be run on the controller where the logs you wish to package are located.

▶ **To create log packages:**

1. In the NestOS Admin Menu, type **4** (**Run a Command**).
2. Press Enter.

3. At the `command:` prompt, type **`createlogpackage`**.
4. Press Enter.

▶ **Sample output:**

```
Generating local logs...
.....................................................................
Finished local logs.
About to request the logs from the cluster peer...
Generating remote logs...
.....................................................................
Finished remote logs.
Retrieving remote logs...
Cleaning up remote logs...
Archiving...
done.
Preparing the cluster peer to have the logs...
Copying the logs to the cluster peer...
Finished copying the log package to the peer node web folder.
Main URL(s) to retrieve the log package(note that most likely any of the IPs
can be used):
http://172.21.156.180/Help/ecentrelogs_ES156180-001_2015-08-07_12-47-36.zip
or
http://172.21.156.181/Help/ecentrelogs_ES156180-001_2015-08-07_12-47-36.zip
```

date

This command writes the date and time to standard output or attempts to set the system date and time. With no arguments, the current date and time is written.

You can run this command on either controller.

▶ **To run the date command:**

1. In the NestOS Admin Menu, type **4** (**Run a Command**).
2. Press Enter.
3. At the `command:` prompt, type:

   `date`

   `[-u [-R] [+format]]`

   `[-a [-]<sss.fff>]`

   `[-u][<mm>][<dd>]<HHMM>[<.SS>] | <mmddHHMM>[<cc>][<yy>][<.SS>]]`
4. Press Enter.

Where:

- `-u` displays (or sets) the date in Greenwich Mean Time (GMT—universal time), bypassing the normal conversion to (or from) local time.

- `-R` displays the time in RFS 2822 format; for example: `Wed, 19 Jun 2015, 19:13:20 -0400`.
- `-a [-]<sss.fff>` slowly adjusts the time by `sss.fff` seconds (where `fff` represents fractions of a second). This adjustment can be positive (no notation) or negative (adding - before `sss.fff`). The system's clock is sped up or slowed down until it has drifted by the number of seconds specified.
- `[[<mm>][<dd>]<HHMM>[<.SS>] | <mmddHHMM>[<cc>][<yy>][<.SS>]]` allow you to set the time and/or date.
  - Used without `-u`, it sets the time/date in local time.
  - Used with `-u`, it sets the time/date in GMT.

  The individual operands are:
  - `<mm>`: The month
  - `<dd>`: The date of the month
  - `<HH>`: The hour, in 24-hour time format
  - `<MM>`: The minute
  - `<.SS>`: The second
  - `<cc>`: The century (a year divided by 100 and truncated to an integer) as a decimal number (`00-99`). For example, `<cc>` is `19` for the year 1988 and `20` for the year 2007.
  - `<yy>`: The last two digits of the year number. If century (`<cc>`) is not specified, then values in the range `69-99` shall refer to years 1969 to 1999 inclusive, and values in the range `00-68` shall refer to years 2000 to 2068, inclusive.

  The month, day, year number, and century may be omitted; the current values are applied as defaults.

3

fcinfo

The fcinfo command displays administrative information for the Fibre Channel host bus adapter (HBA) ports on the Unity Storage System. It also displays information for any Fibre Channel targets that might be connected to the ports. World Wide Name (WWN) are unique 8 byte (64-bit) identifiers in SCSI or Fibre Channel similar to that of MAC Addresses on a Network Interface Card (NIC).

The command syntax is identical to that of the `nstfcdata` command in the CLI command shell; for details on the syntax, see nstfcdata on page 116.

▶ To run the fcinfo command:

1. In the NestOS Admin Menu, type **4** (**Run a Command**) and press Enter.
2. At the `command:` prompt, type the command:

   ```
   fcinfo
   [hba-port <port WWN>]
   [remote-port <port WWN>]
   [logical-unit | lu <device path>]
   [-?] [-V] [--help]
   ```

3. Press Enter.

Tip To exit the `command:` prompt and return to the NestOS Admin Menu, type **`Exit`**, and then press Enter.

▶ Example:

We display version information for the Fibre Channel driver.

fcinfo -v

firewall

The firewall command enables you to enable, disable, and configure the firewall on the Unity Storage System. The Unity Storage System's firewall service prevents both inbound and outbound traffic on specific ports. You can use the firewall command to open a specific UDP or TCP port.

You can also use this command to open all dynamic ports on the Unity Storage System for specific IP addresses; this is particularly useful for NDMP-based backups where you may want to grant an NDMP server access to the Unity Storage System through the firewall.

Note You need to run this command on both controllers.

To run the firewall command:

1. In the NestOS Admin Menu, type **4** (**Run a Command**).
2. Press Enter.
3. At the `command:` prompt, type:

   firewall

   [startservice]

   [stopservice]

   [status]

   [reloadconfig]

   [custom add <port number> <udp | tcp> <description>]

   [custom remove <port number | all> <udp | tcp>]

   [custom show]

   [dynamic add <IP> <udp | tcp> <description>]

   [dynamic remove <IP | all> <udp | tcp>]

   [dynamic show]

4. Press Enter.

Where:

- `startservice` starts the firewall service.

  Note: When you start the firewall service, anything that uses a dynamic port may be disconnected.
- `stopservice` stops the firewall service.
- `status` shows the current status of the firewall service, including port routing.
- `reloadconfig` reloads the firewall configuration file.
- `custom add <port number> <udp | tcp> <description>` adds a custom port with the specified port number, type, and description. The description must NOT contain quotes or spaces. Underscores are permitted.
- `custom remove <port number | all> <udp | tcp>` removes one or all custom ports. To remove a specific port, specify its port number and protocol. To remove all custom ports, type **all** and the protocol.
- `custom show` displays all custom ports, their port numbers, and their descriptions.

- `dynamic add <IP> <udp | tcp> <description>` adds a dynamic port with the specified IP address, type, and description. The description must NOT contain quotes or spaces. Underscores are permitted.
- `dynamic remove <IP | all> <udp | tcp>` removes one or all dynamic ports. To remove a specific port, specify its IP address and protocol. To remove all custom ports, type **`all`** and the protocol.
- `dynamic show` displays all dynamic ports, their IP addresses, and their descriptions.

groupadd

This command enables you to add local group accounts on the Unity Storage System that correspond to Microsoft Active Directory domain accounts in an environment with both Linux/UNIX and Windows client. The group accounts can then access NFS file systems. You must perform additional steps depending on whether you are using a NFSv3 or NFSv4 client to access file systems; refer to the *Managing file systems* chapter of the *Nexsan Unity Software User Guide*.

This command must be run on the active controller node. (The active controller has the System Management component running on it.)

The command syntax is identical to that of the `groupadd` command in the CLI command shell; see groupadd on page 59.

Obtain this information about the Microsoft Active Directory group account that you want to add:

- groupname
- UNIX GID

Note You can find this information in the `/etc/passwd` and `/etc/group` files on a UNIX/Linux client machine on the network.

To run the groupadd command:

1. In the NestOS Admin Menu, type **4** (**Run a Command**).
2. Press Enter.
3. At the `command:` prompt, type the **groupadd** command using this syntax:

   `groupadd -g <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.
4. Press Enter.

Tip To exit the `command:` prompt and return to the NestOS Admin Menu, type **`Exit`**, and then press Enter.

What's next:

For NFSv3 support, you must map the local group accounts to UNIX accounts using the `nstusermaps` command; see nstusermaps on page 130.

ifconfig

The `ifconfig` command displays the current configuration for the primary (nx0) network interface on the Unity Storage System. You can also use this command to display the configuration for the virtual network interface on the Unity Storage System.

The command syntax is the same as that of the `ifconfig` command in the command shell; see ifconfig on page 61.



CAUTION: The `ifconfig` command provides several administrative commands and options—which are not described in this section—for configuring network interface parameters on the Unity Storage System. These commands are intended for advanced users and/or for Nexsan Technical Support personnel; some options should only be performed with the assistance of an Nexsan Support Engineer, or with explicit instructions provided by an Nexsan Support Engineer.

To run the ifconfig command:

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 display the configuration for the primary (nx0) network interface, type: **`ifconfig nx0`**
   - To display the configuration for the virtual network interface, type: **`ifconfig nx0:1`**
4. Press Enter.

Tip To exit the `command:` prompt and return to the NestOS Admin Menu, type **`Exit`**, and then press Enter.

Output example from the `ifconfig nx0` command:

```
nx0: flags=1000843<UP,BROADCAST,RUNNING,MULTICAST,IPv4> mtu 1500 index 2
 inet 172.21.12.101 netmask fffffc00 broadcast 17.2.21.15.255
 ether 0:25:90:23:b7:4a
```

Output example from the `ifconfig nx0:1` command:

```
nx0:1: flags=1000843<UP,BROADCAST,RUNNING,MULTICAST,IPv4> mtu 1500 index 2
inet 172.21.14.176 netmask fffffc00 broadcast 17.2.21.15.255
```

iostat

The `iostat` command displays input/output statistics for the Unity Storage System, including terminal and disk I/O activity and CPU utilization. The command syntax is identical to that of the `iostat` command in the command shell; see iostat on page 65.

To run the iostat command:

1. In the NestOS Admin Menu, type **4** (**Run a Command**).
2. Press Enter.
3. At the `command:` prompt, type **`iostat`**.
4. Press Enter.

Tip To exit the `command:` prompt and return to the NestOS Admin Menu, type **`Exit`**, and then press Enter.

See also:

- nestpool iostat on page 233
- nestpool status on page 234

ipmitool

The `ipmitool` command displays Intelligent Platform Management Interface (IPMI) configuration information for the Unity Storage System, such as IPMI network settings (for example, the IPMI IP address (es), subnet mask, and gateway). This command is identical to `ipmitool` in the command shell; see ipmi on page 69.



CAUTION: The `ipmitool` command provides several administrative commands and options—which are not described in this section—for configuring the IPMI interface on the Unity Storage System. These commands are intended for advanced users and/or for Nexsan Technical Support personnel; some options should only be performed with the assistance of an Nexsan Support Engineer, or with explicit instructions provided by a Nexsan Support Engineer.

To run the ipmitool command:

1. In the NestOS Admin Menu, type **4** (**Run a Command**).
2. Press Enter.
3. At the `command:` prompt, type: **`ipmitool lan print 1`**
4. Press Enter.

Tip To exit the `command:` prompt and return to the NestOS Admin Menu, type **`Exit`**, and then press Enter.

Output example: ipmitool lan print 1

```
Set in Progress         : Set Complete
Auth Type Support       : NONE MD2 MD5 OEM
Auth Type Enable        : Callback : NONE MD2 MD5 OEM
                        : User     : NONE MD2 MD5 OEM
                        : Operator : NONE MD2 MD5 OEM
                        : Admin    : NONE MD2 MD5 OEM
                        : OEM      :
IP Address Source       : Static Address
IP Address              : 172.21.12.172
Subnet Mask             : 255.255.252.0
MAC Address             : 00:25:90:23:b7:4e
SNMP Community String   : AMI
IP Header               : TTL=0x00 Flags=0x00 Precedence=0x00 TOS=0x00
BMC ARP Control         : ARP Responses Disabled, Gratuitous ARP Disabled
Gratituous ARP Intrvl   : 0.0 seconds
Default Gateway IP      : 172.21.12.254
Default Gateway MAC     : 00:00:00:00:00:00
Backup Gateway IP       : 0.0.0.0
Backup Gateway MAC      : 00:00:00:00:00:00
802.1q VLAN ID          : Disabled
802.1q VLAN Priority    : 0
RMCP+ Cipher Suites     : 1,2,3,6,7,8,11,12,0
Cipher Suite Priv Max   : aaaaXXaaaXXaaXX
                        :     X=Cipher Suite Unused
                        :     c=CALLBACK
                        :     u=USER
                        :     o=OPERATOR
                        :     a=ADMIN
                        :     O=OEM
```

listug

This command displays local user and group accounts configured on the Unity Storage System.

Note You need to run this command on the active controller.

To view local users and groups:

1. In the NestOS Admin Menu, type **4** (**Run a Command**).
2. Press Enter.
3. At the `command:` prompt, type:

   `listug [users | groups]`
4. Press Enter.

Where:

- `users` displays local user accounts configured on the Unity Storage System.
- `groups` displays local group accounts configured on the Unity Storage System.

modgid

The `modgid` command enables you to modify the GIDs of local user accounts that you added to the Unity Storage System using the `useradd` command; for more information, see useradd on page 246.

You can modify the GIDs of local user accounts to correspond to the GIDs of the user accounts on NFS client computers, where you intend to mount NFS file systems.

To modify the GID of a local user account:

1. In the NestOS Admin Menu, type **4** (**Run a Command**).
2. Press Enter.
3. At the `command:` prompt, type this command:

   `modgid <user name> <GID>`

   Where `<username>` represents the local user you added to the system and `<GID>` corresponds to the GID of a group that you added to the system using the `groupadd`command; see groupadd on page 228.

   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.
4. Press Enter.

Tip To exit the `command:` prompt and return to the NestOS Admin Menu, type **`Exit`**, and then press Enter.

moduid

The `moduid` command enables you to modify the UIDs of local user accounts that you added to the Unity Storage System using the `useradd` command; for more information, see useradd on page 246.

You can modify the UIDs of local user accounts to correspond to the UIDs of the users accounts on NFS client computers, where you intend to mount NFS file systems.

To modify the UID of a local user account:

1. In the NestOS Admin Menu, type **4** (**Run a Command**).
2. Press Enter.

3. At the `command:` prompt, type this command:

   `moduid <user name> <UID>`

   Where `<username>` represents the local user you added to the system and `<UID>` corresponds to the relevant user's UID on the NFS client computer.

   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.

4. Press Enter.

Tip To exit the `command:` prompt and return to the NestOS Admin Menu, type **`Exit`**, and then press Enter.

nestpool clear

The `nestpool clear` command enables you to clear the error counters for a storage pool, or for a device associated with a storage pool. You should use this command only if you deem any device errors as transient, in that they are unlikely to effect the future health of the device(s), or the associated storage pool.

▶ **To run the nestpool clear command:**

1. In the NestOS Admin Menu, type **4** (**Run a Command**)
2. Press Enter.
3. At the `command:` prompt, type this command, referencing the storage pool, and, if needed, the device (s) that you want to clear error counters for.

   `nestpool clear [-nF] <pool name> [device name]`

4. Press Enter.

Tip To exit the `command:` prompt and return to the NestOS Admin Menu, type **`Exit`**, and then press Enter.

▶ **Example 1:**

We clear all device errors within a storage pool.

`nestpool clear FinancePool1-86f059b6-9707-45a0-b4d8-7c2daf8f9f16`

▶ **Example 2:**

We clear device errors for one or more devices within a storage pool.

`nestpool clear FinancePool1-86f059b6-9707-45a0-b4d8-7c2daf8f9f16 c1t5000C50025DE68D7d0`

nestpool iostat

This section explains how to run the `nestpool iostat` command. This command displays the accumulated statistics since boot for all storage pools on the system, including the storage pool (rpool) in which the Unity Storage System's operating system (NestOS) and system configuration reside.

The command syntax is identical to that of the `nstpool iostat` command in the command shell; see nstpool on page 123.

To run the nestpool iostat command:

1. In the NestOS Admin Menu, type **4** (**Run a Command**).
2. Press Enter.
3. Type **`nestpool iostat`**.
4. Press Enter.

Tip To exit the `command:` prompt and return to the NestOS Admin Menu, type **`Exit`**, and then press Enter.

Example:

```
                                          capacity   operations   bandwidth
pool                                    alloc free   read  write read  write
LAB-090d9cc5-2379-4a89-8738-9ba1fbeef57f  2.78M 1.56G 0     0     142   2.51K
nstbootpool                               4.14g 11.7g 5     15    207k  114k
```

Related commands:

- iostat on page 229
- nestpool status below

nestpool status

This section explains how to run the `nestpool status` command. This command displays the physical state of the storage pools on the Unity Storage System, as well as of the storage pool (`rpool`) in which the Unity Storage System's operating system (NestOS) and system configuration reside.

The status of a storage pool can be one of these:

- ONLINE: Normal
- FAULTED: Missing, damaged, or mis-seated device
- DEGRADED: Device being resilvered
- UNAVAILABLE: Device cannot be opened
- OFFLINE: Administrative action

The command syntax is identical to that of the `nstpool status` command in the command shell; see nstpool on page 123.

To run the nestpool status command:

1. In the NestOS Admin Menu, type **4** (**Run a Command**),
2. Press Enter.
3. At the `command:` prompt, type **`nestpool status`**.
4. Press Enter.

Tip To exit the `command:` prompt and return to the NestOS Admin Menu, type **`Exit`**, and then press Enter.

See also:

- nestpool iostat on the previous page
- iostat on page 229

nfs

The `nfs` command enables you to change or set the NFS version (NFSv4) domain on the Unity Storage System, and also set the maximum version for NFS—version 3 or 4. The command syntax for this command is identical to that of the nfs command in the command shell; see nfs on page 101.

By default, the Unity Storage System uses the domain that you configure in Nexsan Unity for NFSv4 support (see *Accessing file systems* in the *Nexsan Unity Software User Guide*. This domain is used for identifying user and group attribute strings in the NFSv4 protocol. NFSv4 UNIX/Linux clients that access NFS file systems on the Unity Storage System must match with this domain for operation to proceed normally. You can use the `nfs` command to override the default domain setting, or to configure a domain if none exists.

The NFS command also enables you to prevent, or allow, NFSv4 clients from accessing NFS file systems on the Unity Storage System, by changing the maximum version for NFS. By default, the maximum version is set to 4.

To run the nfs command:

1. In the NestOS Admin Menu, type **4** (**Run a Command**).
2. Press Enter.
3. At the `command:` prompt, type this command:

   `nfs [domain [show] [set <domain name>] [unset]]`

   `[maxversion [show] [set 3|4]]`
4. Press Enter.

Tip To exit the `command:` prompt and return to the NestOS Admin Menu, type **`Exit`**, and then press Enter.

Example: nfs domain show

We display the current NFSv4 domain configured on the Unity Storage System.

`nfs domain show`

Example: nfs domain set

We configure or set a new NFSv4 domain.

`nfs domain set <domain.name>`

Example: nfs domain unset

We remove the current NFSv4 domain. The domain name we specify must contain a period (.); for example: **Unity.domain**.

`nfs domain unset`

Example: maxversion show

We display the current maximum version for NFS.

`nfs maxversion show`

Example: maxversion set

We set the maximum version for NFS to version 3.

`nfs maxversion set 3`

nic

This command enables you to display and configure advanced network settings on the system, such as, link aggregation, including creating, adding, modifying, and removing aggregations. The command syntax for this command is identical to that of the `nic` command in the command shell; for complete details on the syntax, see nic on page 103.

CAUTION: The `nic` command provides several administrative commands and options for configuring data-link interfaces on the Unity Storage System. These commands are intended for advanced users and/or for Nexsan Technical Support personnel. Some options available with this command should only be performed with the assistance of a Support Engineer, or with explicit instructions provided by a Support Engineer.

▶ To run the nic command:

1. In the NestOS Admin Menu, type **4** (**Run a Command**).
2. Press Enter.
3. At the `command:` prompt, type:

   `nic`
4. Press Enter. The nxadmin CLI displays syntax and options for the `nic` command; the only options you should use are listed here:

```
[rename-link <oldlink> <newlink>]
[show-link [-pP] [-o <field>,..] [-s [-i <interval>]] [<link>]]
[create-aggr [-t] [-P <policy>] [-L <mode>] [-T <time>] [-u <address>]]
[-l <link> [-l <link>...] <link>]
[delete-aggr [-t] <link>]
[add-aggr [-t] -l <link> [-l <link>...] <link>]
[remove-aggr [-t] -l <link> [-l <link>...] <link>]
[modify-aggr [-t] [-P <policy>] [-L <mode>] [-T <time>] [-u <address>]
<link>]
[show-aggr [-pPLx] [-o <field>,..] [-s [-i <interval>]] [<link>]]
[set-linkprop [-t] -p <prop>=<value>[,...] <name>]
[reset-linkprop [-t] [-p <prop>,...] <name>]
[show-linkprop [-cP] [-o <field>,...] [-p <prop>,...] <name>]
[delete-phys <link>]
[show-phys [-pP] [-o <field>,..] [-H] [<link>]]
[show-usage [-a] [-d | -F <format>] [-s <DD/MM/YYYY,HH:MM:SS>]]
[-e <DD/MM/YYYY,HH:MM:SS>] -f <logfile> [<link>]
```

Tip To exit the `command:` prompt and return to the NestOS Admin Menu, type **`Exit`**, and then press Enter.

▶ Example: nic show-link

We display link aggregation information for the network interfaces on the system.

`nic show-link`

```
LINK            CLASS          MTU     STATE    BRIDE          OVER
```

```
ixgbe0          phys            1500    up      --              --
igb0            phys            1500    up      --              --
ixgbe1          phys            1500    up      --              --
igb1            phys            1500    down    --              --
ixgbe4          phys            1500    down    --              --
ixgbe5          phys            1500    down    --              --
ixgbe2          phys            1500    down    --              --
ixgbe3          phys            1500    down    --              --
nx0             aggr            1500    up      --              igb0 igb1
private0        aggr            1500    up      --              ixgbe0 ixgbe1
```

nscacherestart

The `nscachrestart` command clears the DNS client cache on the Unity Storage System. Use this command if you want to reset, or flush, cached DNS entries on the Unity Storage System after you make changes to the DNS server on your network.

This command is identical to the `nscacherestart` command in the command shell; see nscacherestart on page 115.

To run the nscachrestart command:

1. In the NestOS Admin Menu, type **4**(**Run a Command**).
2. Press Enter.
3. At the `command:` prompt, type:

   `nscachrestart`
4. Press Enter. No output is displayed during this process. If an error appears, please contact Nexsan Technical Support.

Tip To exit the `command:` prompt and return to the NestOS Admin Menu, type **`Exit`**, and then press Enter.

nstfcdata

This command displays administrative information for the Fibre Channel host bus adapter (HBA) ports on the Unity Storage System. It also displays information for any Fibre Channel targets that might be connected to the ports.

Note You need to run this command on the controller where you want to see Fibre Channel information.

To view FC HBA ports:

1. In the NestOS Admin Menu, type **4** (**Run a Command**).
2. Press Enter.

3. At the `command:` prompt, type:

   `nstfcdata`

   `[hba-port <port WWN>]`

   `[remote-port <port WWN>]`

   `[logical-unit | lu <device path>]`

   `[-?]`

   `[-V]`

   `[--help]`

4. Press Enter.

Where:

- `hba-port <arguments> <port WWN>` displays information for all initiator mode and target mode fibre channel HBA ports on the Unity Storage System. If you don't specify a port WWN, all initiator mode and target mode fibre channel HBA ports on the host are displayed.

  Note: World Wide Name (WWN) are unique 8 byte (64-bit) identifiers in SCSI or fibre channel similar to that of MAC Addresses on a Network Interface Card (NIC).

  You can use these optional arguments with `hba-port`:

  - `-i` displays all initiator mode fibre channel HBA ports.
  - `-t` displays all target mode fibre channel HBA ports.
  - `-e` displays information for all FCoE ports.
  - `-l` displays the link error statistics information for the HBA ports.

- `remote-port <arguments> <port WWN>` displays information for HBA ports on a remote the Unity Storage System. If you don't specify a port, all initiator mode and target mode Fibre Channel HBA ports on the remote host are displayed.

  You can use these optional arguments with `remote-port`:

  - `-s` displays SCSI target information for the remote ports.
  - `-l` displays the link error statistics information for the remote ports.

- `logical-unit | lu <device path>` displays the logical unit referenced by the specified device path. If you don't specify a device path, all Fibre Channel logical units are listed. This option applies only to the initiator mode.
- `-V` displays version information for the fibre channel driver.
- `--help` displays help content for the `nstfcdata` command.

nstsasdata

This command displays administrative information for the Serial Attached SCSI-2 (SAS-2) host bus adapter (HBA) on the Unity Storage System.

Run this command on the controller where you want to see SAS information.

► To display SAS information:

1. In the NestOS Admin Menu, type **4** (**Run a Command**).
2. Press Enter.

3. At the `command:` prompt, type:

   `nstsasdata`

   `[hba <hba name>]`

   `[hba-port <hba port name>]`

   `[expander <expander device sas address>]`

   `[target-port <target port SAS address>]`

   `[logical-unit|lu <operating system device>]`

   `[-V]`

   `[--help]`

4. Press Enter.

Where:

- `hba <hba_name> [-v]` displays information for a specific HBA, by its HBA name. You can use the `-v` option to display additional information.
- `hba-port <hba_port_name> [-y] [-v] [-a] [-l]`

  This option displays information for the specified HBA port name.

  Note: If you do not specify a name, the `nstsasdata hba-port` command lists all HBA ports.

  You can use these arguments with the `nstsasdata hba-port` command:

  - `-y` displays the physical information on the HBA port.
  - `-v` displays details on hardware information, such as SAS address, topology device, and so on.
  - `-a` displays the HBA port information from the HBA name of an HBA.
  - `-l` displays the link error statistics information for the HBA port.
- `expander <expander device sas address> [-v] [-t] [-p <hba port name>]` displays the hierarchical view of the expander, referenced by the specified Expander Device SAS address.

  Note: If you do not specify an Expander Device SAS address, the `sasinfo expander` command displays all expanders that are visible across all HBA ports.

  You can use these arguments with the `nstsasdata expander` command:

  - `-v` displays detailed information for all expanders that are visible through the specified HBA port.
  - `-t` displays all target ports that are attached to expanders connected to the specified HBA port.
  - `-p` displays expander information for a specific port; you must specify the HBA port name.
- `target-port [-v] [-s] <target port SAS address>` Displays information for a specific target port, by its Target Port SAS Address.

  Note: If you do not specify a Target Port SAS Address, the `sasinfo target-port` command displays all discovered target ports.

  You can use these arguments with the `nstsasdata target-port` command:

  - `-v` displays target ports with the HBA port and expander that they are connected to.
  - `-s` displays the SCSI attributes for target ports.

- `logical-unit | lu [-v] <operating system device>` displays the logical unit information for a device.

  Note: If you do not specify a device, the `sasinfo logical-unit` or `lu` command displays all SAS logical units, including the SAS Management Protocol (SMP) target port.

  You can use the `-v` option to display additional information about the logical unit.

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; see nstusermaps on page 130.

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>`

resetcache

The Unity Storage System caches system-level configuration settings at the server-level, and then delivers cached information on demand at the management level through Nexsan Unity. This ensures that the system performs optimally.

You may be required, under certain circumstances, to manually refresh the system cache; for example, if Nexsan Unity appears to be out of sync with configuration settings on the Unity Storage System. This command is equivalent to the **Refresh System Cache** option available from Nexsan Unity's global toolbar.

Run this command on the active controller. (The active controller has the System Management component running on it.)

To reset the cache:

1. In the NestOS Admin Menu, type **4** (**Run a Command**).
2. Press Enter.
3. At the `command:` prompt, type **`resetcache`**.
4. Press Enter.

restartldapclient

The `restartldapclient` command resets NFS user identity mapping on the Unity Storage System. Use this command if you experience permission and/or identity mapping issues while accessing NFS file systems on the Unity Storage System from a UNIX/Linux client system on the network.

To run the restartldapclient command:

1. In the NestOS Admin Menu, type **4** (**Run a Command**).
2. Press Enter.
3. At the `command:` prompt, type:

   `restartldapclient`
4. Press Enter. No output is displayed during this process. If an error appears, please contact Nexsan Technical Support.

Tip To exit the `command:` prompt and return to the NestOS Admin Menu, type **`Exit`**, and then press Enter.

route

On an the Unity Storage System with both the (onboard) 1Gb network interface and the (optional) 10Gb interface, if you configured the 1Gb interface as a secondary network connection, you can use the `route` command to add a routing entry to the routing table on the Unity Storage System, in order for the system to route data requests to the subnet that you configured for the secondary 1Gb interface.

The command syntax is identical to that of the `route` command in the command shell; for the complete syntax explanation, see route on page 153.

When adding a routing entry to the routing table using the route command, you need the:

- The destination host IP or destination network Subnet/Mask
- The IP address of the router (on the same subnet as the 1Gb interface) that will route to the destination host/subnet

▶ To add a routing entry to the routing table:

1. In the NestOS Admin Menu, type **4** (**Run a Command**).
2. Press Enter.
3. At the `command:` prompt, type the route command using one of these command variations and arguments.

   `route [-f|-n|-p|-q|-v] [[-sub-commands] arguments]`
4. Press Enter.

Tip To exit the `command:` prompt and return to the NestOS Admin Menu, type **`Exit`**, and then press Enter.

▶ Example: adding a route to a subnet

If the IP address for the 1Gb interface is set to 10.1.1.100, the router is 10.1.1.1, and the destination subnet is 30.40.20.0 255.255.255.0, type:

```
route -p add -net 30.40.20.0 -netmask 255.255.255.0 10.1.1.1
```

▶ Example: adding a route to a specific host

If the IP address for the 1Gb interface is set to 10.1.1.100, the router is 10.1.1.1, and the destination host is 30.40.20.15, type:

```
route -p add -host 30.40.20.15 10.1.1.1
```

▶ Example: displaying all configured routes

To display all currently configured routes on the Unity Storage System, type:

```
route -p show
```

▶ Example: removing a subnet

After displaying all configured routes on the Unity Storage System (using the `route -p show` command), you want to disable a specific routing entry; for example, persistent: route add -net 30.40.20.0 -netmask 255.255.255.0 10.1.1.1, type:

```
route -p delete -net 30.40.20.0 -netmask 255.255.255.0 10.1.1.1
```

▶ Example: removing a host

After displaying all configured routes on the Unity Storage System (using the `route -p show` command), you want to remove a specific host entry; for example, persistent: route add -host 30.40.20.15 10.1.1.1, type:

```
route -p delete -host 30.40.20.15 10.1.1.1
```

sasinfo

The `sasinfo` command displays administrative information for the Serial Attached SCSI-2 (SAS-2) host bus adapter (HBA) on the Unity Storage System. More specifically, it displays attributes of HBA ports and of storage devices and SCSI target devices that might be connected to the HBA ports.

The command syntax is identical to that of the `nstsasdata` command in the command shell; for complete details on the syntax, see nstsasdata on page 125.

▶ To run the sasinfo command:

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
display version information for the SAS host bus adapter driver	`sasinfo -v`
display information for a specific HBA, by its HBA name	`sasinfo hba [-v] <hba name>`
display information for a specific HBA port, by its HBA port name	`sasinfo hba-port [option] <hba port name>`
display the hierarchical view of the storage referenced by the specified Expander Device SAS address	`sasinfo expander <device sas address>` `sasinfo expander [option] -p <hba port name>`
display information for specific target ports, by their target port SAS address	`sasinfo target-port [option] <target port SAS address>`
display the logical unit information for a device	`sasinfo logical-unit | lu [-v] <operating system device>`

4. Press Enter.

Tip To exit the `command:` prompt and return to the NestOS Admin Menu, type **`Exit`**, and then press Enter.

showmount

The `showmount` command lists the UNIX/Linux clients that have remotely mounted an NFS file systems on the Unity Storage System. It is important to note that the `showmount` command caches mount information, and as such, it may not immediately display information for file systems that were recently mounted, or it may continue to display information for file systems that are no longer remotely mounted. In addition, the `showmount` command does not return information about NFS version 4 (NFSv4) clients.

The command syntax is identical to the `showmount` command in the command shell; see showmount on page 164.

► To run the showmount command:

1. In the NestOS Admin Menu, type **4** (**Run a Command**) and press Enter.
2. At the `command:` prompt, type:

   `showmount`
3. Press Enter.

Tip To exit the `command:` prompt and return to the NestOS Admin Menu, type **`Exit`**, and then press Enter.

► Output example:

```
ES260786-176-001-01
ES260786-176-001-02-rmi
qa-ad.qadomain.net
```

showroutes

The `showroutes` command displays the routing table on the Unity Storage System. More specifically, this command shows the routes currently configured on all (active) network interfaces on the system.

This command is identical to the `showroutes` command in the command shell; see showroutes on page 165.

▶ **To run the showroutes command:**

1. In the NestOS Admin Menu, type **4** (**Run a Command**).
2. Press Enter.
3. At the `command:` prompt, type **`showroutes`**.
4. Press Enter.

Tip To exit the `command:` prompt and return to the NestOS Admin Menu, type **`Exit`**, and then press Enter.

▶ **Output example:**

```
Routing Table: IPv4
 Destination        Gateway            Flags    Ref         Use     Interface
default             172.21.12.254      UG             3      397660
127.0.0.1           127.0.0.1          UH            28   685271097 lo0
172.21.12.0         172.21.14.176      U             11     1135049 nx0
172.21.12.0         172.21.12.101      U             61    48482243 nx0
200.200.200.0       200.200.200.3      U              3  1292470976 private0
200.200.200.0       200.200.200.2      U              3  1659118791 private0


Routing Table: IPv6
 Destination/Mask          Gateway                 Flags    Ref   Use   If
---------------------     ---------------------- -------  --- ------- ------
::1                        ::1                    UG         2   19970 lo0
```

smbrestart

The `smbrestart` command restarts the CIFS server on the Unity Storage System. Use this command if any Windows client on your network is unable to access a CIFS file systems on the Unity Storage System—but only after you verify that the network connection between the Windows client and the Unity Storage System is functional.

This command is identical to the `smbrestart` command in the command shell; see smbrestart on page 171.

▶ **To run the smbrestart command:**

1. In the NestOS Admin Menu, type **4** (**Run a Command**).
2. Press Enter.
3. At the `command:` prompt, type:

   `smbrestart`
4. Press Enter. No output is displayed during this process. If an error appears, please contact Nexsan Technical Support.

Tip To exit the `command:` prompt and return to the NestOS Admin Menu, type **`Exit`**, and then press Enter.

useradd

This command enables you to add local user accounts on the Unity Storage System that correspond to Microsoft Active Directory domain accounts in an environment with both Linux/UNIX and Windows client. The user accounts can then access NFS file systems. You must perform additional steps depending on whether you are using a NFSv3 or NFSv4 client to access file systems; refer to the *File Systems* chapter of the *Nexsan Unity Software User Guide*.

The `useradd` command must be run on the active controller node. (The active controller has the System Management component running on it.)

The command syntax is identical to that of the `useradd` command in the command shell; see useradd on page 190.

Before you begin:

Obtain this information about the Microsoft Active Directory user account that you want to add:

- username
- UNIX UID

Note You can find this information in the `/etc/passwd` and `/etc/group` files on a UNIX/Linux client machine on the network.

To run the useradd command:

1. In the NestOS Admin Menu, type **4** (**Run a Command**).
2. Press Enter.
3. At the `command:` prompt, type: **`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.
4. Press Enter.

Tip To exit the `command:` prompt and return to the NestOS Admin Menu, type **`Exit`**, and then press Enter.

Example:

We add the user `Bob Summers`.

```
useradd -u 200 bsummers
```

What's next:

You can add the user to a group account; see modgid on page 92. By default, new users are added to the Unity group.

For NFSv3 support, you must map the local user accounts to UNIX accounts using the `nstusermaps` command; see nstusermaps on page 130.

Fault Repair menu

The Unity Storage System provides a fault management mechanism that tracks and reacts to system faults. The Unity Storage System's fault management mechanism provides fault monitoring for several pieces of hardware on the Unity Storage System, including CPU, memory, and I/O bus events.

The Unity Storage System's fault management mechanism reports error messages in a well-defined and explicit format. Each error code is uniquely identified by a resource identifier. Each Field Replaceable Unit (FRU) has its own resource identifier. Resource identifiers are associated with one of the following conditions:

- **ok**: present and available for use.
- **unknown**: not present or not usable, perhaps because it is offline or not configured.
- **degraded**: present and usable, but one or more problems have been identified.
- **faulted**: present but not usable; unrecoverable problems have been diagnosed and the resource has been disabled to prevent damage to the system.

```
NestOS Fault Management Menu

1 - Show Faults Information
2 - Repair Fault
3 - Restore Retired Devices

q - Exit

Select an option:
```


▶ **To view system faults:**

1. In the NestOS Admin Menu, type **5** (**Fault Repair Menu**) and press Enter. This displays the **NestOS Fault Management Menu**.
2. Type **1** (**Show Faults Information**) and press Enter. The Unity Storage System's fault management mechanism displays any faults on the system.
3. Type **q** to exit the list of faults and return to the **NestOS Fault Management Menu**.

▶ **To clear system faults:**



CAUTION: Before attempting to clear system faults, please contact Nexsan Technical Support for guidance regarding a fault, and whether or not it is safe to clear a specific fault.

1. In the NestOS Admin Menu, type **5** (**Fault Repair Menu**) and press Enter. This displays the **NestOS Fault Management Menu**.
2. Type **2** (**Repair Fault**) and press Enter. The Unity Storage System's fault management mechanism displays the faults on the system, and prompts you to type the FRU code corresponding to the fault that you want to clear.
3. Type the relevant FRU code, and press Enter.

The Unity Storage System's fault management mechanism attempts to clear the specified fault. The mechanism notifies you as to whether or not it successfully cleared the fault from the system.

To restore retired devices:

1. In the NestOS Admin Menu, type **5** (**Fault Repair Menu**) and press Enter. This displays the **NestOS Fault Management Menu**.
2. Type **3** (**Restore Retired Devices**) and press Enter.
3. A prompt displays to ask you to confirm the action; type **yes** and press Enter.

What's next:

Reboot the controller on which you are restoring the retired devices.

Configure file systems and Active Directory

The **Configure File Systems and Active Directory** menu enables you to restrict access to CIFS and NFS file systems based on a client system's IP address; set space usage quotas on file systems for individual user and/or group accounts in your Microsoft Active Directory or LDAP Directory domain (or, if the Unity Storage System is configured to use Nexsan Unity authentication, for individual user and group accounts that you create on the system); enable/disable the offline files functionality (also know an Client Side Caching or CSC); set the blocksize for file systems and pool; and configure advanced settings for the Active Directory client on the Unity Storage System.

```
NestOS File Systems menu

1 - Configure File System Access Lists
2 - Configure File System User/Group Quotas
3 - Configure File System Offline Files
4 - Configure the Active Directory client
5 - Configure the blocksize of file systems or pools
6 - Configure File System Access Based Enumeration
7 - Configure the LDAP Client in AD mode

q - Exit

Select an option:
```

This section includes these topics:

- Setting IP-based access restrictions on a file system on the facing page
- Setting a space usage quota on a file system on page 257
- Displaying space usage quotas on file systems on page 258
- Disabling the Offline Files function for a file system on page 260
- Enabling the Offline Files function for a file system on page 260
- Configuring the Active Directory client on page 261
- Modifying the block size of a file system or a storage pool on page 261
- Enabling access-based enumeration of folders and files in a CIFS file system on page 262
- Configuring the LDAP Client in AD mode on page 263

Setting IP-based access restrictions on a file system

The nxadmin CLI enables you to restrict access to CIFS and NFS file systems based on a client system's IP address.

With this mechanism, you can give a client system, or a group of client systems on a specific subnet, one of these access levels to a file system:

- **Read-write access (rw)**: when you configure Read-write access for a file system, 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)**: when you configure Read-only access for a file system, 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 systemis 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)**: when you configure No access for a file system, 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 systemis prevented from accessing the file system.

You can configure separate access restrictions for each file systemon the Unity Storage System. In addition, you can configure one, or more, access levels—`rw` (Read-write), `ro` (Read-only), or `none` (No access) for each file system—as needed. For example, a file systemcan have Read-write and Read-only IP-based accessed restrictions configured for it.

Note **IP-based restrictions on a file system are additive to file system-level user access permissions**:When you enable IP-based `rw` (Read-write) or `ro` (Read-only) access for a file system to specific client systems on the network, this does NOT grant user access to the file system; 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 file system. Once the Unity Storage System validates and authorizes a client system's IP address, it then determines user access to the corresponding file system, based on permission settings you configure for the file systemin Nexsan Unity.

You can also set the *no_root_squash* property on an NFS file system to allow NFS clients on the network to connect to and mount an NFS file system on the Unity Storage System as `root`; see Enabling the no_root_squash property on an NFS file system on page 254.

In addition, all NFS file systems, by default, have their Read-write flag set to `enabled`. You can clear this flag, or set it to `enabled` again, if needed; you can also set or clear the Read-only or No access list flags for NFS file systems.

This section includes these topics:

- Setting IP-based restrictions on a CIFS file system below
- Setting IP-based restrictions on an NFS file system on page 252
- Enabling the no_root_squash property on an NFS file system on page 254

Setting IP-based restrictions on a CIFS file system

This section explains how to restrict access to a CIFS file system based on a client machine's IP address. You must run these commands on the controller hosting the CIFS file system.

To set IP-based restrictions on a CIFS file system:

1. In the NestOS Admin Menu, type **6** (**Configure File Systems and Active Directory**).
2. Press Enter. This displays the **File Systems** submenu.
3. Type **1** (**Configure File System Access Lists**).
4. Press Enter. This displays all the file systems configured on the Unity Storage System.

```
SHARE LIST

   0 - SMS share      :PayRollData1
     rw access-list    :@172.21.12.232
   1 - SMB share      :PayRollData2
   2 - SMB share      :PayRollData3
   3 - NFS share      :PayRollData_NFS
         rw flag       :enabled

Please select the share number, h for info, s to see secondary modes or q
to exit:
```

The file system list displays all the file systems that you configured on the Unity Storage System, as well as any Read-only, Read-write, or No access IP-based restrictions currently set for each file system. If a file system has both CIFS and NFS sharing enabled for it, the file system list displays 2 separate entries for it: an SMB (CIFS) entry and an NFS entry.

Note CIFS file systems in the file system list are identified as `SMB file system`.

5. In the file systemlist, locate the CIFS file system that you want to set IP-based restrictions on, and type its file systemnumber; then, press Enter. For example, to set IP-based access restrictions on SMB (CIFS) file system `PayRollData2`, type **1**, and press Enter. This displays the Restrictions Options screen for `PayRollData2`.

```
SELECTED SHARE:

      SMB share      :PayRollData2

INFORMATION:

When the share is primary at this site, the settings will be as shown.

When the share is secondary at this site, the rw and no_root_squash access
lists will be added to the ro lists.

When just a flag is set, it defaults to all.

When the share is secondary, if rw exists with no value, and ro has a
value then a * will appended to the ro access-list.


OPTIONS:

rw             - configure the rw access-list (or just the flag).
ro             - configure the ro access-list (or just the flag).
none           - configure the none access-list (or just the flag).
no_root_squash - configure the no_root_squash access-list (or just the
                 flag).


(please note that with NFS, the default is to have only the rw flag)


Please select an option or q to cancel:
```

6. Type the access level—`rw` (Read-write), `ro` (Read-only), or `none` (No access)—that you want to configure for the file system, and press Enter.

   For example, if you want only a specific group of client systems on the network to have Read-write access to the file system, type **rw** and press Enter. This displays the Access Lists screen:

```
SELECTED SHARE:
                SMB file     :PayRollData2
                system
SELECTED TYPE: rw
OPTIONS:
          a - add an entry to the (rw) access list.
          r - remove an entry from the (rw) access list.
          c - clear all entries in the (rw) access list.
Please select an option or q to cancel:
```

7. Type **a**, **add an entry to the [rw] access list**, and press Enter; you are prompted to enter the IP addresses, prefix, or subnet mask, corresponding to the client systems that you want to give Read-write access to the CIFS file system.

```
Please type in the new entry.

The entry should start with the @ symbol.

The entry can be and IP address      (ex: @10.11.1.1)
The entry can be and IP prefix       (ex: @10.11)
The entry can be and IP with mask    (ex: @10.11/16)
```

8. Type the corresponding IP addresses, prefix, or subnet mask, preceded by the commercial at symbol (@), and then press Enter.
   - For example, if you want to give a specific client system Read-write access to the CIFS file system, type the client system's corresponding IP address: `@172.21.12.189`
   - If you want to give two or more client systems with specific IP addresses Read-write access to the CIFS file system, type the corresponding IP addresses in this format: `@172.21.12.189:@172.21.12.190`
   - If you want to give client systems on a specific subnet Read-write access to the CIFS file system, type the corresponding IP address range and subnet mask in this format: `@172.21/16`
   - If you want to give all client systems on the network Read-write access to the CIFS file system, type the asterisk symbol (*): `*`
9. If needed, repeat the last two steps to configure IP-based access restrictions for the file system's Read-only or No access levels.

Setting IP-based restrictions on an NFS file system

This section explains how to restrict access to a NFS file system based on a client machine's IP address. You must run these commands on the controller hosting the NFS file system.

► **To set IP-based restrictions on an NFS file system:**

1. In the NestOS Admin Menu, type **6** (**Configure File Systems and Active Directory**).
2. Press Enter. This displays the **File Systems** sub-menu.
3. Type **1** (**Configure File System Access Lists**).

4. Press Enter. This displays all the file systems configured on the Unity Storage System.

```
SHARE LIST

   0 - SMS share      :PayRollData1
     rw access-list    :@172.21.12.232
   1 - SMB share      :PayRollData2
   2 - SMB share      :PayRollData3
   3 - NFS share      :PayRollData_NFS
        rw flag        :enabled

Please select the share number, h for info, s to see secondary modes or q
to exit:
```

   The file system list displays all the file systems that you configured on the Unity Storage System, as well as any Read-only, Read-write, or No access IP-based restrictions currently set for each file system. If a file system has both CIFS and NFS sharing enabled for it, the file system list displays 2 separate entries for it: an SMB (CIFS) entry and an NFS entry.

5. In the file system list, locate the NFS file system that you want to set IP-based restrictions on, and type its file system number; then, press Enter. For example, to set IP-based access restrictions on NFS file system `PayRollData_NFS`, type **3**, and press Enter. This displays the Restrictions Options screen for `PayRollData_NFS`.

```
SELECTED SHARE:

      NFS share      :PayRollData_NFS
        rw flag              :enabled

INFORMATION:

When the share is primary at this site, the settings will be as shown.

When the share is secondary at this site, the rw and no_root_squash access
lists will be added to the ro lists.

When just a flag is set, it defaults to all.

When the share is secondary, if rw exists with no value, and ro has a
value then a * will appended to the ro access-list.


OPTIONS:

rw             - configure the rw access-list (or just the flag).
ro             - configure the ro access-list (or just the flag).
none           - configure the none access-list (or just the flag).
no_root_squash - configure the no_root_squash access-list (or just the
                 flag).


(please note that with NFS, the default is to have only the rw flag)


Please select an option or q to cancel:
```

6. Type the access level—`rw` (Read-write), `ro` (Read-only), or `none` (No access)—that you want to configure for the file system, and press Enter.

   For example, if you want only a specific group of client systems on the network to have Read-write access to the file system, type **rw** and press Enter. This displays the Access Lists screen.

```
SELECTED SHARE:
     NFS share          :PayRollData_NFS
SELECTED TYPE: rw
       rw flag            :enabled

OPTIONS:
a - add an entry to the (rw) access list.
r - remove an entry from the (rw) access list.
cr - clear all the entries and clear the (rw) flag.
ck - clear all the entries (if there are any) and keep the (rw) flag (or
add it if is not currently set).
Please select an option or q to cancel:
```

7. Type **a**, **add an entry to the [rw] access list**, and press Enter; you are prompted to enter the IP addresses, prefix, or subnet mask, corresponding to the client systems that you want to give Read-write access to the NFS share.

```
Please type in the new entry.

The entry should start with the @ symbol.

The entry can be and IP address      (ex: @10.11.1.1)
The entry can be and IP prefix       (ex: @10.11)
The entry can be and IP with mask    (ex: @10.11/16)
```

8. Type the corresponding IP addresses, prefix, or subnet mask, preceded by the commercial at symbol (@), and then press Enter.
   - For example, if you want to give a specific client system Read-write access to the NFS share, type the client system's corresponding IP address: `@172.21.12.189`
   - If you want to give two or more client systems with specific IP addresses Read-write access to the NFS share, type the corresponding IP addresses in this format: `@172.21.12.189:@172.21.12.190`
   - If you want to give client systems on a specific subnet Read-write access to the NFS share, type the corresponding IP address range and subnet mask in this format: `@172.21/16`
   - If you want to give all client systems on the network Read-write access to the NFS share, type the asterisk symbol (*): `*`
9. If needed, repeat the last two steps to configure IP-based access restrictions for the file system's Read-only or No access levels.

Enabling the no_root_squash property on an NFS file system

The nxadmin CLI enables you to enable the no_root_squash (`root`) property on NFS file system. You must run these commands on the controller hosting the NFS file system.

The `no_root_squash` property is a setting that allows NFS clients on the network to connect to and mount an NFS file system on the Unity Storage System as `root`.

To enable the no_root_squash property for an NFS file system:

1. In the NestOS Admin Menu, type **6** (**Configure File Systems and Active Directory**).
2. Press Enter. This displays the **File Systems** sub-menu.
3. Type **1** (**Configure File System Access Lists**).
4. Press Enter. This displays all the file systems configured on the Unity Storage System.

```
SHARE LIST

   0 - SMS share      :PayRollData1
     rw access-list    :@172.21.12.232
   1 - SMB share      :PayRollData2
   2 - SMB share      :PayRollData3
   3 - NFS share      :PayRollData_NFS
         rw flag       :enabled

Please select the share number, h for info, s to see secondary modes or q
to exit:
```

The file system list displays all the file systems that you configured on the Unity Storage System, as well as any Read-only, Read-write, or No access IP-based restrictions currently set for each file system. If a file system has both CIFS and NFS sharing enabled for it, the file system list displays 2 separate entries for it: an SMB (CIFS) entry and an NFS entry.

5. In the file systems list, locate the NFS file system that you want to enable the no_root_squash property for, and type its file system number; then, press Enter. For example, to enable the no_root_squash flag for `PayRollData_NFS`, type **3**, and press Enter. This displays the Restrictions Options screen for `PayRollData_NFS`.

```
SELECTED SHARE:

NFS file system      :PayRollData_NFS
        rw flag              :enabled

INFORMATION:

When the share is primary at this site, the settings will be as shown.

When the share is secondary at this site, the rw and no_root_squash access
lists will be added to the ro lists.

When just a flag is set, it defaults to all.

When the share is secondary, if rw exists with no value, and ro has a
value then a * will appended to the ro access-list.


OPTIONS:

rw             - configure the rw access-list (or just the flag).
ro             - configure the ro access-list (or just the flag).
none           - configure the none access-list (or just the flag).
no_root_squash - configure the no_root_squash access-list (or just the
                 flag).


(please note that with NFS, the default is to have only the rw flag)


Please select an option or q to cancel:
```

6. Type **no_root_squash** and press Enter. This displays the Root Access Lists screen.

```
SELECTED SHARE:
     NFS share          :PayRollData_NFS
SELECTED TYPE: rw
       rw flag            :enabled

OPTIONS:

a - add an entry to the (rw) access list.

r - remove an entry from the (rw) access list.

cr - clear all the entries and clear the (rw) flag.

ck - clear all the entries (if there are any) and keep the (rw) flag (or
add it if is not currently set).

Please select an option or q to cancel:
```

7. Type **a**, **add an entry to the [root] access list**, and press Enter; you are prompted to enter the IP addresses, prefix, or subnet mask, corresponding to the client systems that you want to give root access to the NFS file system.

```
Please type in the new entry.

The entry should start with the @ symbol.

 The entry can be an IP address    (ex: @10.11.1.1)
 The entry can be an IP prefix     (ex: @10.11)
 The entry can be an IP with mask  (ex: @10.11/16
```

8. Type the corresponding IP addresses, prefix, or subnet mask, preceded by the commercial at symbol (@), and then press Enter.
   - For example, if you want to give a specific client system root access to the NFS file system, type the client system's corresponding IP address: `@172.21.12.189`
   - If you want to give two or more client systems with specific IP addresses root access to the NFS file system, type the corresponding IP addresses in this format: `@172.21.12.189:@172.21.12.190`
   - If you want to give client systems on a specific subnet root access to the NFS file system, type the corresponding IP address range and subnet mask in this format: `@172.21/16`
   - If you want to give all client systems on the network root access to the NFS file system, type: `@0/0`

Note To enable root access to the NFS file system for all client systems on the network using the `0/0` option, you must also enable the `rw` flag for the File System; see Setting IP-based restrictions on an NFS file system on page 252.

Setting a space usage quota on a file system

The nxadmin CLI provides a mechanism that enables you to allocate space usage quotas on file systems to individual user and/or group accounts in your Microsoft Active Directory or LDAP Directory domain, or to local user and group accounts (if you are using Nexsan Unity authentication). This function enables you to set the amount of disk space consumed by files that are owned by a particular user or group.

This command is also available in the nxadmin command-shell; see userquota on page 192.

Note You can only set space usage quotas on file systems; this mechanism is not supported for shares. However, if you set a space usage quota for a particular user or group on a file system, the quota is automatically applied to any shares that the user or group has access to. For example, if you set a `5G` quota for the user, `Bob`, on the `PayRollData2` file system, and then, you add a share to `PayRollData2` and give `Bob` access permissions to the share, the Unity Storage System sets a 5 GB disk space restriction for `Bob` on both `PayRollData2` and the share that `Bob's` user account has access to.

▶ **To set a space usage quota on a file system for a user and/or group:**

1. In the NestOS Admin Menu, type **6** (**Configure File Systems and Active Directory**) and press Enter. This displays the **File Systems** sub-menu.
2. Type **2** (**Configure File System Quotas**) and press Enter.

3. The nxadmin CLI prompts you to select either the **Get** or **Set** command:
   - **Get**: displays the space usage quota setting for a user and/or group on a specific file system, or on all file systems, if applicable.
   - **Set**: sets a space usage quota for a specific user and/or group on a specific file system.

   Type **2** (**Set**) and press Enter.
4. The nxadmin CLI prompts you to select either the **User** or **Group** option.
   a. Type either **1** or **2**, depending on whether you want to set a space usage quota on a file system for a user account or a group account, respectively.
   b. Press Enter.
5. The nxadmin CLI prompts you to enter the user or group name of the user or group account that you want to set a space usage quota for.
6. Type the user or group name. You can use the user's or group's friendly domain name; for example, to allocate a space usage quota to the user `Bob` in the domain `qadomain.net`, type: `bob@qadomain.net`

   You can also use the fully qualified domain name; for example, user `Bob` in this case can be entered as `Bob Smith`.
7. The nxadmin CLI prompts you to enter the quota limit that you want to allocate to the specified user or group account.

   Enter a quota limit value, followed by a capacity unit: `M` (for Megabytes), `G` (for Gigabytes), `T` (for Terabytes), and so on. For example, to allocate a 5 Gigabyte quota, type **5G**.
8. Press Enter. The nxadmin CLI displays all the file systems on the Unity Storage System, and prompts you to select the file system that you want to set the specified space usage quota on, for the specified user or group account.

```
Please select a file system...
1 - PayRollData1
2 - PayRollData2
3 - PayRollData3
4 - PayRollData4
Please select an option or q to quit:
```

9. Type the numerical value corresponding to the file system that you want to set the specified space usage quota on. For example, to set the space usage quota on `PayRollData2`, type **1**.
10. Press Enter to continue.
11. The nxadmin CLI prompts you to press Enter again to confirm the configuration. Press Enter.

Once this process completes, the nxadmin CLI returns you to the **File Systems** sub-menu.

Displaying space usage quotas on file systems

The nxadmin CLI provides a mechanism that enables you to display space usage quotas on file systems currently allocated to individual user and/or group accounts in your Microsoft Active Directory or LDAP Directory domain; or to local user and/or group accounts that you create on the system (if you are using Nexsan Unity authentication).

To display space usage quotas on file systems:

1. In the NestOS Admin Menu, type **6** (**Configure File Systems and Active Directory**) and press Enter. This displays the **File Systems** submenu.
2. Type **2** (**Configure File System Quotas**) and press Enter.
3. The nxadmin CLI prompts you to select either the **Get** or **Set** command:
   - **Get**: displays the space usage quota setting for a user and/or group on a specifc file system, or on all file systems, if applicable.
   - **Set**: sets a space usage quota for a specific user and/or group on a specific file system.

   Type **1** (**Get**) and press Enter.
4. The nxadmin CLI prompts you to select either the **User** or **Group** option. Type either **1** (user account) or **2** (group account), and press Enter.
5. Enter the user or group name. For example, if you want to display space usage quotas currently allocated to the user `Bob` in the domain `qadomain.net`, type: `bob@qadomain.net` and press Enter.
6. The nxadmin CLI displays all the file systems on the Unity Storage System. Select a specific file system to display the space usage quota currently configured on the file system for the specified user or group account.

   ```
   Please select a file system...
   1 - PayRollData1
   2 - PayRollData2
   3 - PayRollData3
   4 - PayRollData4
   4 - PayRollData5
   5 - all

   Please select an option or q to quit:
   ```
7. Type the numerical value corresponding to the file system. For example:
   - To display the space usage quota on `PayRollData2` for the user `Bob`, type **1**.
   - To display all file systems that you configured space usage quotas on for the user `Bob`, type **5**.
8. Press Enter to continue.

   The nxadmin CLI displays the space usage quota on the selected file system currently allocated to the specified user or group, including the amount of disk space that the specified user or group has already consumed on the file system:

   ```
   Please select an option or q to quit: 5
   User: bob@qadomain.net
   SHARENAME - USED QUOTA
   PayRollData2 - 5G
   Press enter to continue...
   ```

   If you specified **all** file systems, the nxadmin CLI displays all the file systems on the Unity Storage System that you allocated a space usage quota on for the specified user or group, including the amount of disk space that the specified user or group has already consumed on each file system.

Disabling the Offline Files function for a file system

Offline Files (also known as Client Side Caching or CSC) is a feature available in Windows that makes network files available to an end user when a network connection to the server, where the files are located, is unavailable, or when the connection to the server is slow.

If you disable the Offline Files function for a CIFS file system, the files and folders in the file system will not be available to CIFS clients (in offline mode) when the file system becomes inaccessible (to the client systems) over the network. By default, all CIFS file systems on the Unity Storage System have the Offline Files function enabled.

To disable the Offline Files function for a file systems:

1. In the NestOS Admin Menu, type **6** (**Configure File Systems and Active Directory**), and press Enter. This displays the **File Systems** submenu.
2. Type **3** (**Configure File System Offline Files**), and press Enter. The nxadmin CLI displays all CIFS file systemson the system.

   ```
   Please select a file system...
   1 - PayRollData1
   2 - PayRollData2
   ```
3. Type the numerical value corresponding to the file systems that you want to disable the Offline Files function for. For example, to disable the Offline Files function for `PayRollData1`, type **1**.
4. Press Enter to continue. The nxadmin CLI prompts you to type `e`, to enable the Offline Files function for the file system, or `d` to disable it:
5. Type **d**, then press Enter.

The nxadmin CLI sets the Offline Files function for the selected file system to disabled; once this process completes, the nxadmin CLI returns you to the **File Systems** submenu.

Enabling the Offline Files function for a file system

This section explains how to re-enable the Offline Files function for a CIFS file system.

To enable the Offline Files function for a file system:

1. In the NestOS Admin Menu, type **6** (**Configure File Systems and Active Directory**).
2. Press Enter. This displays the **File Systems** sub-menu.
3. Type **3** (**Configure File System Offline Files**).
4. Press Enter. The nxadmin CLI displays all CIFS file systems on the system.

   ```
   Please select a file system...
   1 - PayRollData1
   2 - PayRollData2


   Please select an option or q to quit:
   ```
5. Type the numerical value corresponding to the file system that you want to enable the Offline Files function for. For example, to enable the Offline Files function for `PayRollData1`, type **1**.
6. Press Enter to continue.

7. The nxadmin CLI prompts you to type **e**, to enable the Offline Files function for the file system, or **d** to disable it. Type **e**.
8. Press Enter.

The nxadmin CLI sets the Offline Files function for the selected file system to enabled; once this process completes, the nxadmin CLI returns you to the **File Systems** sub-menu.

Configuring the Active Directory client

With authentication through a Microsoft Windows Active Directory domain or an LDAP Directory service, a user enters a user name and password and Nexsan Unity checks the Microsoft Windows Active Directory server or LDAP Directory server for a matching user record.

If you are integrating the Unity Storage System 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.

Option 4 in the Shares menu enables you to configure the password used for authentication with the Active Directory server. By default, the password is encrypted. You can change the configuration settings so that the password is sent in clear text instead. This is useful for Active Directory environments where passwords are not encrypted.

► **To configure the Unity Storage System to authenticate with a specific domain controller:**

1. In the NestOS Admin Menu, type **6** (**Configure Shares and Active Directory**).
2. Press Enter. This displays the **Shares** sub-menu.
3. Type **4** (**Configure the Active Directory client**) and press Enter. This displays the AD Client sub-menu.
4. Type **1** (**Configure the Active Directory client to authenticate with a specific domain controller**) and press Enter.
5. Type the name of a domain user and press Enter.
6. Type the password of the domain user and press Enter.
7. Type the IP address of the Active Directory server or LDAP Directory server and press Enter.

► **To configure the Unity Storage System to send passwords in clear text:**

1. In the NestOS Admin Menu, type **6** (**Configure Shares and Active Directory**).
2. Press Enter. This displays the **Shares** sub-menu.
3. Type **4** (**Configure the Active Directory client**) and press Enter. This displays the AD Client sub-menu.
4. Type **2** (**Configure the Active Directory client to use clear text authentication**) and press Enter.
5. Type the name of a domain user and press Enter.

Modifying the block size of a file system or a storage pool

The nxadmin CLI provides a mechanism that enables you to modify the default block/record size of file systems and/or storage pools on the Unity Storage System. By default, the block size for both file systems and storage pools is set to 128 KB.

To modify the block size of a file system:

1. In the NestOS Admin Menu, type **6** (**Configure File Systems and Active Directory**).
2. Press Enter. This displays the **File Systems** submenu.
3. Type **5** (**Configure the blocksize of file systems or pools**).
4. Press Enter. The nxadmin CLI displays the Blocksize menu.
5. Type **4** (**Change File System blocksize**).
6. Press Enter. The nxadmin CLI displays a list of file systems on the system.
7. Type the numerical value corresponding to the file system that you want to modify the block size for, and then press Enter.
8. Type a block size to set for the file system. The block size can be any power of 2 from 512 bytes to 128 KB.
9. Press Enter.

To modify the block size of a a storage pool:



CAUTION: Modifying the block size of a storage pool also changes the block size of all file systems in the storage pool.

1. In the NestOS Admin Menu, type **6** (**Configure File Systems and Active Directory**).
2. Press Enter. This displays the **File Systems** submenu.
3. Type **5** (**Configure the blocksize of file systems or pools**).
4. Press Enter. The nxadmin CLI displays the Blocksize menu.
5. Type **3** (**Change Pool blocksize**).
6. Press Enter. The nxadmin CLI displays a list of storage pools on the system.
7. Type the numerical value corresponding to the storage pool that you want to modify the block size for, and then press Enter.
8. Type a block size to set for the file system. The block size can be any power of 2 from 512 bytes to 128 KB.
9. Press Enter.

Enabling access-based enumeration of folders and files in a CIFS file system

The nxadmin CLI provides a mechanism that enables administrators to restrict display of folders and file entries 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.

To enable access-based enumeration of folders and files in a CIFS file system:

1. In the NestOS Admin Menu, type **6** (**Configure File Systems and Active Directory**) and press Enter. This displays the **File Systems** submenu.
2. Type **6** (**Configure File System Access Based Enumeration**) and press Enter. The nxadmin CLI displays a list of CIFS file systems on the system.

3. Type the numerical value corresponding to the file system for which you want to enable access-based enumeration of folders and files and press Enter.
4. Type **e** to enable this setting and press Enter.

Configuring the LDAP Client in AD mode

A UNIX environment can use either a Local directory service or the NIS or LDAP protocol to access the directory service and the data stored on any UNIX server on the network. If the UNIX environment also communicates with a Windows environment, other directory services must be taken into account for proper access to directory services. For example, if Active Directory is used as the main directory service in your environment, you must join the Active Directory domain in addition to using your current UNIX directory service.

This section covers these topics:

- Showing current LDAP client information below
- Initializing LDAP to Active Directory mapping below
- Uploading a Certification Authority (CA) certificate on the next page
- Removing a Certification Authority (CA) certificate on page 265
- Setting the LDAP Client configuration on page 265
- Configuring the file system group lookup on page 265
- Resetting the LDAP Client configuration on page 265
- Clearing the nstusermaps cache on page 266
- Viewing instructions on using nstusermaps for LDAP to AD mapping on page 266
- Showing ACLs on file systems on page 266
- Setting ACLs on file systems on page 266
- Restarting the LDAP Client service on page 267

Showing current LDAP client information

▶ **To display LDAP client information:**

1. In the NestOS Admin Menu, type **6** (**Configure Shares and Active Directory**) and press Enter.
2. This displays the `Shares` sub-menu. Type **7** (**Configure the LDAP Client in AD Mode**) and press Enter.
3. This displays the `LDAP Client in AD Mode` menu. Type **1** (**Show current information**) and press Enter.

Initializing LDAP to Active Directory mapping

▶ **To initialize LDAP:**

1. In the NestOS Admin Menu, type **6** (**Configure Shares and Active Directory**) and press Enter.
2. This displays the `Shares` submenu. Type **7** (**Configure the LDAP Client in AD Mode**) and press Enter.
3. This displays the `LDAP Client in AD Mode` menu. Type **2** (**Initialize LDAP to Active Directory mapping**) and press Enter.

Figure 3-3: NestOS LDAP Client in AD Mode menu

```
1 - Show current information
2 - Initialize LDAP to Active Directory mapping
3 - Upload a CA Certificate
4 - Remove a CA Certificate
5 - Set LDAP Client configuration
6 - Configure file systems group lookup
7 - Reset the LDAP Client configuration
8 - Clear the nstusermaps cache
9 - View instructions on using nstusermaps for LDAP to AD mapping
10 - Show ACLs on file systems
11 - Set ACLs on file systems
 12 - Restart the LDAP Client Service

q - Exit

Select an option:
```


The Unity Storage System initializes the mapping on both the current cluster node and the other cluster node.

Uploading a Certification Authority (CA) certificate

By default, LDAP communications between client and server applications are not encrypted. This means that it would be possible to use a network monitoring device or software and view the communications traveling between LDAP client and server computers. This includes credentials (user name and password) passed over the network unencrypted. This could lead to the compromise of credentials.

By uploading a certificate, you allow a secure LDAP authentication on the domain controller.

To upload a CA certificate:

1. In the NestOS Admin Menu, type **6** (**Configure Shares and Active Directory**) and press Enter.
2. This displays the `Shares` submenu. Type **7** (**Configure the LDAP Client in AD Mode**) and press Enter.
3. This displays the `LDAP Client in AD Mode` menu. Type **3** (**Upload a CA Certificate**) and press Enter.
4. Enter the certificate nick name and press Enter.
5. Use this command to insert the certificate:

   `edit /etc/ldapcert`
6. When prompted to continue, type **y** and press Enter.
7. Enter the certificate contents.

   Note Make sure to enter the first line as `-----BEGIN CERTIFICATE-----` and the last line as `-----END CERTIFICATE-----`.

Removing a Certification Authority (CA) certificate

▶ **To remove a CA certificate:**

1. In the NestOS Admin Menu, type **6** (**Configure Shares and Active Directory**) and press Enter.
2. This displays the `Shares` submenu. Type **7** (**Configure the LDAP Client in AD Mode**) and press Enter.
3. This displays the `LDAP Client in AD Mode` menu. Type **4** (**Remove a CA Certificate**) and press Enter.
4. Enter the nick name of the certificate to delete and press Enter.

The Unity Storage System looks for the certificate and deletes it on the first controller, then performs the same operation on the peer controller.

Setting the LDAP Client configuration

▶ **To configure the LDAP client:**

1. In the NestOS Admin Menu, type **6** (**Configure Shares and Active Directory**) and press Enter.
2. This displays the `Shares` submenu. Type **7** (**Configure the LDAP Client in AD Mode**) and press Enter.
3. This displays the `LDAP Client in AD Mode` menu. Type **5** (**Set LDAP Client configuration**) and press Enter.
4. Select one of the two options:

   `1 - anonymous`:

   a. Type **1** and press Enter to set the LDAP Client configuration to `anonymous`.

   b. Select one of the two credential options (`tls` or `none`) by typing its number and pressing Enter.

   `2 - simple bind`:

   a. Type **2** and press Enter to set the LDAP Client configuration to `simple bind`.

   b. Enter the proxy DN and press Enter .

Configuring the file system group lookup

▶ **To configure the file system group lookup:**

1. In the NestOS Admin Menu, type **6** (**Configure Shares and Active Directory**) and press Enter.
2. This displays the `Shares` submenu. Type **7** (**Configure the LDAP Client in AD Mode**) and press Enter.
3. This displays the `LDAP Client in AD Mode` menu. Type **6** (**Configure the file system group lookup**) and press Enter.
4. When prompted to select a file system, enter the number corresponding to the desired file system and press Enter.
5. The Unity Storage System displays the current group lookup setting for the file system. Select one of the available options (POSIX or MULTI) and press Enter.

Resetting the LDAP Client configuration

This feature enables you to put the LDAP client configuration back to the default settings.

To reset the LDAP client configuration:

1. In the NestOS Admin Menu, type **6** (**Configure Shares and Active Directory**) and press Enter.
2. This displays the `Shares` submenu. Type **7** (**Configure the LDAP Client in AD Mode**) and press Enter.
3. This displays the `LDAP Client in AD Mode` menu. Type **7** (**Reset the LDAP Client configuration**) and press Enter.

Clearing the nstusermaps cache

To clear the nstusermaps cache:

1. In the NestOS Admin Menu, type **6** (**Configure Shares and Active Directory**) and press Enter.
2. This displays the `Shares` submenu. Type **7** (**Configure the LDAP Client in AD Mode**) and press Enter.
3. This displays the `LDAP Client in AD Mode` menu. Type **8** (**Clear the nstusermaps cache**) and press Enter.

The Unity Storage System clears the LDAP cache on the first controller and then on the peer controller.

Viewing instructions on using nstusermaps for LDAP to AD mapping

For information on the `nstusermaps` menu command, see nstusermaps on page 240.

To view instructions:

1. In the NestOS Admin Menu, type **6** (**Configure Shares and Active Directory**) and press Enter.
2. This displays the **Shares** submenu. Type **7** (**Configure the LDAP Client in AD Mode**) and press Enter.
3. This displays the LDAP Client in AD Mode menu. Type **9** (**View instructions on using nstusermaps for LDAP to AD mapping**) and press Enter.

Showing ACLs on file systems

You can view the Access Control Lists of file systems using CIFS or NFS sharing.

To view ACLs on file systems:

1. In the NestOS Admin Menu, type **6** (**Configure Shares and Active Directory**) and press Enter.
2. This displays the `Shares` submenu. Type **7** (**Configure the LDAP Client in AD Mode**) and press Enter.
3. This displays the `LDAP Client in AD Mode` menu. Type **10** (**Show ACLs on file systems**) and press Enter.
4. When prompted to select a file system, enter the number corresponding to the desired file system and press Enter.

The Unity Storage System provides the user name, the access granted to that user, and the authentication type.

Setting ACLs on file systems

This feature enables you to set Windows or UNIX Access Control Lists (ACLs) to grant access privileges to file systems on the Unity Storage System.

To set ACLs on file systems:

1. In the NestOS Admin Menu, type **6** (**Configure Shares and Active Directory**) and press Enter.
2. This displays the `Shares` submenu. Type **7** (**Configure the LDAP Client in AD Mode**) and press Enter.
3. This displays the `LDAP Client in AD Mode` menu. Type **11** (**Set ACLs on file systems**) and press Enter.
4. When prompted to select a file system, enter the number corresponding to the desired file system and press Enter.
5. The Unity Storage System displays the current users and their access privileges on the selected file system. Enter each ACL entry and separate them with a comma, in this format:
   - For a user entry: `user:(username) : (access)`
   - For a group entry: `group: (groupname) : (access)`

   Where

   `username` and `groupname` can be:
   - for Active Directory users and groups: *name@domain.com*
   - for LDAP users and groups: enter the unique LDAP name

     If users are mapped to both AD and LDAP, you can use either one of them.

   `access` can be:
   - *FullControl*
   - *ReadWrite*
   - *Read*

   For example:

   `user:user1@domain.com:ReadWrite,group:group1:FullControl,user:user2:Read`
6. Press Enter.

Tip Use `REMOVEALL` to remove all ACL entries.

Restarting the LDAP Client service

To restart the LDAP Client service:

1. In the NestOS Admin Menu, type **6** (**Configure Shares and Active Directory**) and press Enter.
2. This displays the `Shares` submenu. Type **7** (**Configure the LDAP Client in AD Mode**) and press Enter.
3. This displays the `LDAP Client in AD Mode` menu. Type **12** (**Restart the LDAP Client Service**) and press Enter.

Reset the Unity Storage System

The reset process deletes all storage pools and file systems from the Unity Storage System; unjoins the Unity Storage System from the Microsoft Active Directory Server or LDAP Directory Service, or if the Unity Storage System is configured with Nexsan Unity Authentication, it deletes all local users and groups on the system.

Optionally, this process removes the Unity Storage System from the list of peer sites on any remote Unity Storage Systems that the system is connected to.

Note The reset process does not remove the network configuration for the Unity Storage System.

To reset the Unity Storage System using the NestOS:

1. In the NestOS Admin Menu, type **7** (**Reset Site**), and press Enter.
2. This displays 2 options for resetting the Unity Storage System:

```
Please select one of the following:
1. Reset this site to factory defaults, and remove this site from any
connected sites.
2. Reset this site to factory defaults, but DO NOT alter any other site.

Enter your selection [1-2]:
```

   - Type **1** if you want to reset the Unity Storage System and also remove the system from the list of peer sites on any remote the Unity Storage Systems that the system is connected to.
   - Type **2** if you do not want to make any changes to any remote Unity Storage System(s).
3. Press Enter.

   If you have any external Unity Storage Systems connected to the Unity Storage System, the nxadmin CLI asks you if you want to reset the RAID configuration on the storage systems.
4. Type **y** to reset the RAID configuration on the storage systems, or **n** to skip this process.
5. Press Enter to continue.
6. The nxadmin CLI prompts you to confirm the process for resetting the Unity Storage System. Type **YES** to continue, and press Enter.

   If the Unity Storage System is connected to a Microsoft Active Directory or LDAP Directory domain, the nxadmin CLI prompts you to enter the domain administrator's user name and password, in order to unjoin, or remove, the system from the domain.
7. Type the domain administrator's user name, and press Enter.
8. When prompted, type the domain administrator's password, and press Enter.

System menu

The System Menu enables you to configure Nexsan Unity SNMP module on the Unity Storage System. The Nexsan Unity SNMP module allows existing SNMP monitoring environments to view, query, and monitor Nexsan the Unity Storage System Storage Systems using the Simple Network Management Protocol. For complete information and usage procedures for the Nexsan Unity SNMP module, refer to the `snmpadm` command in the CLI command shell, as described in snmpadm on page 173.

The System Menu also enables you to configure the NTP (Network Time Protocol) server. the Unity Storage System connects to the primary domain controller, which 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; or, if you configure the Unity Storage System to connect to a specific domain controller in the forest, the specified domain controller 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 NTP source for the Unity Storage System to synchronize its date and time with.

To configure the NTP server on the Unity Storage System:

1. In the NestOS Admin Menu, type **8** (**System Menu**), and press Enter.
2. Type **2** (**Set NTP Server**) and press Enter.
3. When prompted, type **2** to select the server and press Enter.
4. When prompted, type the host name or IP address of the NTP server, and press Enter.

To configure an NTP multicast client on the Unity Storage System:

1. In the NestOS Admin Menu, type **8** (**System Menu**), and press Enter.
2. Type **2** (**Set NTP Server**) and press Enter.
3. When prompted, type **1** to select the multicast client and press Enter.
4. When prompted, type the host name or IP address of the NTP server, and press Enter.

3

Appendix A

Enabling LACP

LACP (Link Aggregation Control Protocol) allows multiple individual Ethernet links to be aggregated to form a single logical channel. LACP enables a network device to negotiate an automatic bundling of links by sending LACP packets to the peer (directly connected device that also implements LACP).

LACP is typically used for two purposes:

1. Load balancing: bundling two or more links together provides increased throughput and a level of load balancing for when the speed of individual Ethernet lines is limited.
2. Redundancy: links in a LACP aggregation provide an automatic fallback should one of the links fail, providing enhanced resilience. All traffic is routed from the failed link to the remaining links.

The Unity Storage System supports both active and passive LACP modes:

- Active mode: places a port into an active negotiating state in which the port initiates negotiations with other ports by sending LACP packets.
- Passive mode: places a port into a passive negotiating state in which the port responds to LACP packets that it receives but does not initiate LACP packet negotiation.

This section explains how to enable and configure LACP on the Unity Storage System.

Understanding link aggregation 272
Requirements and guidelines for implementing LACP 272
Enabling LACP using the nxadmin CLI 272
Troubleshooting LACP 273
Disabling LACP on the Unity Storage System 274

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

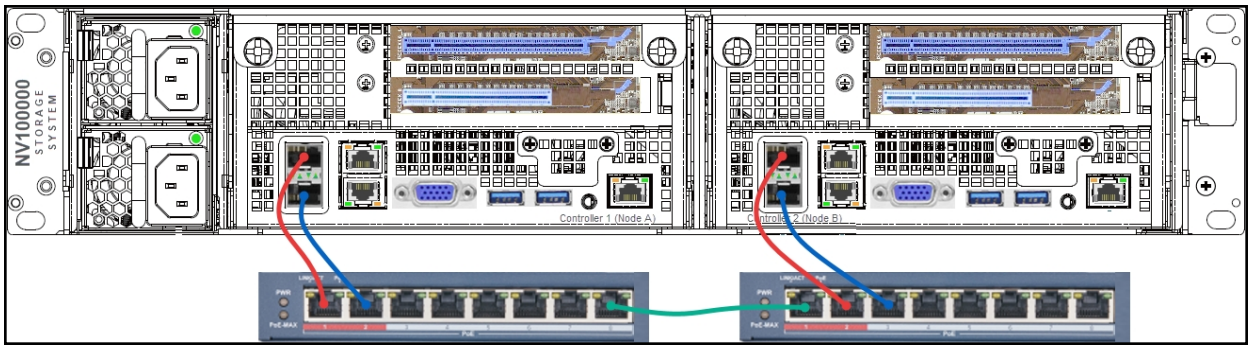
Requirements and guidelines for implementing LACP

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*.

A

Figure A-1: Connecting controllers to Ethernet switches on the NV10000



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.

Troubleshooting LACP

To detect that LACP is enabled on the switches and not on the Unity Storage System:

- Verify that LACP is enabled on the switches as passive or active; see Enabling LACP using the nxadmin CLI on the previous page.
- Verify the Unity Storage System network interface LACP status.

To verify the network interface LACP status:

1. At the command: prompt, type:

   ```
   nic show-aggr -L
   ```
2. Press Enter.

   You will see similar results as displayed below when the protocol is up.

A

```
ES200100-001-02:P:/> nic show-aggr -L
LINK        PORT         AGGREGATABLE SYNC COLL DIST DEFAULTED EXPIRED
nx0         ixgbe2       yes          yes  yes  yes  no        no
--          ixgbe3       yes          yes  yes  yes  no        no
private0    ixgbe0       yes          yes  yes  yes  no        no
--          ixgbe1       yes          yes  yes  yes  no        no
nx99        igb0         yes          no   no   no   no        no
```

Disabling LACP on the Unity Storage System

To disable LACP on the Unity Storage System:

1. At the command: prompt, type:

   `nic modify-aggr -L off nx0`

   Where `nx0` represents the primary interface on the Unity Storage System. To disable LACP on the secondary interface, if applicable, replace `nx0` with `nx1`.

2. Press Enter.
3. Repeat these steps on the second controller node after you transition cluster resources back to the node you finished configuring.

A

Appendix B

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.

B

Appendix C

Integrating with Network Information Service (NIS)

In UNIX environments (for connectivity to NFS file systems), the Unity Storage System supports three UNIX directory services: LDAP (Lightweight Directory Access Protocol), NIS (Network Information Service), and Unity authentication.

If you have UNIX users that authenticate through NIS—regardless of the authentication set up for the Unity Storage System—you must run some nxadmin CLI commands in a specific order to fully integrate the Unity Storage System with NIS.

To integrate the Unity Storage System with NIS:

1. Create the name of the domain. Type this command:

   `domainname <domain>`

   Where **`<domain>`** is the name of the NIS domain used; for further details, see domainname on page 49.

2. Define the domain as the default NIS domain used; for further details, see setdefaultdomain on page 158.

   `setdefaultdomain <domain>`

3. Reconfigure the `etc/nsswitch.conf` file after changing the authentication mode so that the NIS authentication settings are added to password and group files. Type this command:

   `changenameservices -c add -s nis`

   For further details, see changenameservices on page 29.

4. To initialize the NIS server, type this command on the active controller:

   ypinit -c

   For further details, see ypinit on page 197.

   a. You will be prompted to enter the NIS server name:

      "In order for NIS to operate successfully, we have to construct a list of the NIS servers. Please continue to add the names for YP servers in order of preference, one per line. When you are done with the list, type a <control D> or a return on a line by itself."

      next host to add: **nis.nisdomain2.lan**

      next host to add:

   b. When prompted to confirm the NIS server name, type **y** and press Enter:

      The current list of yp servers looks like this: nis.nisdomain2.lan
      Is this correct? [y/n: y] **y**

      If you see `svcadm` messages about services missing, similar to this:

      svcadm: Pattern 'network/nis/server:default' doesn't match any instances

      you may ignore these messages.

5. Add the NIS server host to `/etc/hosts` on both controllers.

   a. Open the `hosts` configuration file, type: **edit /etc/hosts**

   b. Add the NIS server to the list, in this format:

      <server IP address> nis-p-<server name> <domain name>

6. To start active services for the NIS client, type this command on both controllers:

   svc enable nis/client

   For further details, see svc on page 176.

7. To display the list of NIS users, type:

   ypcat -k passwd

   For further details, see ypcat on page 196.

8. To display the list of NIS groups, type:

   ypcat -k group

What's Next:

1. Give the NIS users access to the file using the `chmod` command. For information, see chmod on page 30.
2. Map users using the `nstusermaps` command. For information, see nstusermaps on page 130.

Appendix D

SNMP Management Information Bases

The Nexsan Unity SNMP module requires Management Information Bases (MIBs) for it to work with Nexsan Unity Storage Systems. The MIBs that are included with the module are described in this section, along with their individual objects.

To configure SNMP, see snmpproperty on page 175; to use the SNMP menu, see snmpadm on page 173.

Topics in this section:

Host Resources 280
Interface 286
LM Sensor 294
RFC1213 295
SNMP Framework 295
SNMPv2 Framework 296
UCD Disk I/O 297
UCD SNMP 297

Host Resources

MIB object and OID	Description
hrSystemUptime **1.3.6.1.2.1.25.1.1**	The amount of time since this host was last initialized. This is different from **sysUpTime** in the SNMPv2-MIB [RFC1907] because **sysUpTime** is the uptime of the network management portion of the system.
hrSystemDate **1.3.6.1.2.1.25.1.2**	The host's local date and time.
hrSystemProcesses **1.3.6.1.2.1.25.1.6**	The number of processes currently loaded or running on this system.
hrMemorySize **1.3.6.1.2.1.25.2.2**	The amount of physical read-write main memory, typically RAM, contained in the host.

MIB object and OID	Description
hrStorageTable **1.3.6.1.2.1.25.2.3**	The (conceptual) table of logical storage areas on the host. An entry is placed in the storage table for each logical area of storage that is allocated and has fixed resource limits. The amount of storage represented in an entity is the amount actually usable by the requesting entity. This excludes loss due to formatting or file system reference information. These entries are associated with logical storage areas, such as might be seen by an application, rather than physical storage entities which are typically seen by an operating system. Storage such as tapes and floppy disks without file systems on them are typically not allocated in chunks by the operating system to requesting applications, and therefore shouldn't appear in this table. Examples of valid storage for this table include disk partitions, file systems, RAM (for some architectures this is further segmented into regular memory, extended memory, and so on), and backing storage for virtual memory ('swap space'). This table is intended to be a useful diagnostic for 'out of memory' and 'out of buffers' types of failures. In addition, it can be a useful performance monitoring tool for tracking memory, disk, or buffer usage. A (conceptual) entry for one logical storage area on the host. As an example, an instance of the **hrStorageType** object might be named *hrStorageType.3*. **hrStorageIndex** **1.3.6.1.2.1.25.2.3.1.1** — A unique value for each logical storage area contained in the host. **hrStorageType** **1.3.6.1.2.1.25.2.3.1.2** — The type of storage represented by this entry. **hrStorageDescr** **1.3.6.1.2.1.25.2.3.1.3** — A description of the type and instance of the storage described by this entry. **hrStorageAllocationUnits** **1.3.6.1.2.1.25.2.3.1.4** — The size, in bytes, of the data objects allocated from this pool. If this entry is monitoring sectors, blocks, buffers, or packets, for example, this number is commonly greater than 1. Otherwise this number is typically 1. **hrStorageSize** **1.3.6.1.2.1.25.2.3.1.5** — The size of the storage represented by this entry, in units of **hrStorageAllocationUnits**. This object is writable to allow remote configuration of the size of the storage area in those cases where such an operation makes sense and is possible on the underlying system. For example, the amount of main memory allocated to a buffer pool might be modified, or the amount of disk space allocated to

MIB object and OID	Description
	virtual memory might be modified.
hrStorageUsed **1.3.6.1.2.1.25.2.3.1.6**	The amount of storage represented by this entry that is in use, in units of **hrStorageAllocationUnits**.

MIB object and OID	Description
hrDeviceTable **1.3.6.1.2.1.25.3.2**	The (conceptual) table of devices contained in the host. A (conceptual) entry for one device contained in the host. As an example, an instance of the **hrDeviceType** object might be named *hrDeviceType.3*. **hrDeviceIndex** **1.3.6.1.2.1.25.3.2.1.1** — A unique value for each device contained in the host. The value for each device must remain constant from one re-initialization of the agent to the next re-initialization. **hrDeviceType** **1.3.6.1.2.1.25.3.2.1.2** — An indication of the type of device. If this value is '*hrDeviceProcessor {hrDeviceTypes 3}*', then an entry exists in the **hrProcessorTable** which corresponds to this device. If this value is '*hrDeviceNetwork { hrDeviceTypes 4}*', then an entry exists in the **hrNetworkTable** which corresponds to this device. If this value is '*hrDevicePrinter { hrDeviceTypes 5}*', then an entry exists in the **hrPrinterTable** which corresponds to this device. If this value is '*hrDeviceDiskStorage { hrDeviceTypes 6}*', then an entry exists in the **hrDiskStorageTable** which corresponds to this device. **hrDeviceDescr** **1.3.6.1.2.1.25.3.2.1.3** — A textual description of this device, including the device's manufacturer and revision, and optionally its serial number. **hrDeviceID** **1.3.6.1.2.1.25.3.2.1.4** — The product ID for this device. **hrDeviceStatus** **1.3.6.1.2.1.25.3.2.1.5** — The current operational state of the device described by this row of the table. A value *unknown(1)* indicates that the current state of the device is unknown. The value *running (2)* indicates that the device is up and running and that no unusual error conditions are known. The *warning(3)* state indicates that agent has been informed of an unusual error condition by the operational software (e.g., a disk device driver) but that the device is still 'operational'; for example, a high number of soft errors on a disk. A value of *testing(4)* indicates that the

MIB object and OID	Description	
		device is not available for use because it is in the testing state. The state of *down(5)* is used only when the agent has been informed that the device is not available for any use.
	hrDeviceErrors **1.3.6.1.2.1.25.3.2.1.6**	The number of errors detected on this device. It should be noted that, as this object has a SYNTAX of *Counter32*, it does not have a defined initial value. However, it is recommended that this object be initialized to 0 (zero), even though management stations must not depend on such an initialization.
hrNetworkTable **1.3.6.1.2.1.25.3.4**	The (conceptual) table of long-term storage devices contained in the host. In particular, disk devices accessed remotely over a network are not included here. Note that this table is potentially sparse: a (conceptual) entry exists only if the correspondent value of the **hrDeviceType** object is '*hrDeviceDiskStorage*'. A (conceptual) entry for one long-term storage device contained in the host. The hrDeviceIndex in the index represents the entry in the **hrDeviceTable** that corresponds to the **hrDiskStorageEntry**. As an example, an instance of the **hrDiskStorageCapacity** object might be named *hrDiskStorageCapacity.3*.	
	hrNetworkIfIndex **1.3.6.1.2.1.25.3.4.1.1**	The value of **ifIndex** which corresponds to this network device. If this device is not represented in the **ifTable**, then this value is 0 (zero).

D

MIB object and OID	Description
hrDiskStorageTable **1.3.6.1.2.1.25.3.6**	The (conceptual) table of long-term storage devices contained in the host. In particular, disk devices accessed remotely over a network are not included here. Note that this table is potentially sparse: a (conceptual) entry exists only if the correspondent value of the **hrDeviceType** object is '*hrDeviceDiskStorage*'. A (conceptual) entry for one long-term storage device contained in the host. The **hrDeviceIndex** in the index represents the entry in the hrDeviceTable that corresponds to the **hrDiskStorageEntry**. As an example, an instance of the **hrDiskStorageCapacity** object might be named *hrDiskStorageCapacity.3*. **hrDiskStorageAccess** **1.3.6.1.2.1.25.3.6.1.1** — An indication of whether this long-term storage device is readable and writable or only readable. This reflects the media type, any write-protect mechanism, and any device configuration that affects the entire device. **hrDiskStorageMedia** **1.3.6.1.2.1.25.3.6.1.2** — An indication of the type of media used in this long- term storage device. **hrDiskStorageRemovable** **1.3.6.1.2.1.25.3.6.1.3** — Denotes whether or not the disk media may be removed from the drive. **hrDiskStorageCapacity** **1.3.6.1.2.1.25.3.6.1.4** — The total size for this long-term storage device. If the media is removable and is currently removed, this value is 0 (zero).
hrSWRunPerfTable **1.3.6.1.2.1.25.5.1**	The (conceptual) table of running software performance metrics. A (conceptual) entry containing software performance metrics. As an example, an instance of the **hrSWRunPerfCPU** object might be named *hrSWRunPerfCPU.1287*. **hrSWRunPerfCPU** **1.3.6.1.2.1.25.5.1.1.1** — The number of centi-seconds of the total system's CPU resources consumed by this process. On a multi-processor system, this value may increment by more than one centi- second in one centi-second of real time. **hrSWRunPerfMem** **1.3.6.1.2.1.25.5.1.1.2** — The total amount of real system memory allocated to this process.

D

Interface

D

MIB object and OID	Description
ifNumber **1.3.6.1.2.1.2.1**	The number of network interfaces (regardless of their current state) present on this system.

MIB object and OID	Description
ifTable **1.3.6.1.2.1.2.2**	A list of interface entries. The number of entries is given by the value of **ifNumber**. An entry containing management information applicable to a particular interface.
ifIndex **1.3.6.1.2.1.2.2.1.1**	A unique value, greater than zero, for each interface. It is recommended that values are assigned contiguously, starting from **1**. The value for each interface sub-layer must remain constant from one re-initialization of the entity's network management system to the next re- initialization.
ifDescr **1.3.6.1.2.1.2.2.1.2**	A textual string containing information about the interface. This string should include the name of the manufacturer, the product name, and the version of the interface hardware/software.
ifType **1.3.6.1.2.1.2.2.1.3**	The type of interface. Additional values for **ifType** are assigned by the Internet Assigned Numbers Authority (IANA) through updating the syntax of the **IANAifType** textual convention.
ifSpeed **1.3.6.1.2.1.2.2.1.5**	An estimate of the interface's current bandwidth in bits per second. For interfaces which do not vary in bandwidth or for those where no accurate estimation can be made, this object contains the nominal bandwidth. If the bandwidth of the interface is greater than the maximum value reportable by this object, then this object reports its maximum value (4,294,967,295), and **ifHighSpeed** must be used to report the interace's speed. For a sub- layer which has no concept of bandwidth, this object is **0** (zero).
ifPhysAddress **1.3.6.1.2.1.2.2.1.6**	The interface's address at its protocol sub-layer. For example, for an 802.x interface, this object contains a MAC address. The interface's media- specific MIB must define the bit and byte ordering and the format of the value of this object. For interfaces which do not have such an address (e.g., a serial line), this object contains an octet string of zero length.
ifAdminStatus **1.3.6.1.2.1.2.2.1.7**	The desired state of the interface. The *testing (3)* state indicates that no operational packets

MIB object and OID	Description
	can be passed. When a managed system initializes, all interfaces start with **ifAdminStatus** in the *down(2)* state. As a result of either explicit management action or per configuration information retained by the managed system, **ifAdminStatus** is then changed to either the *up(1)* or *testing(3)* states (or remains in the *down(2)* state).
ifOperStatus **1.3.6.1.2.1.2.2.1.8**	The current operational state of the interface. The *testing(3)* state indicates that no operational packets can be passed. If **ifAdminStatus** is *down(2)*, then **ifOperStatus** is also *down(2)*. If **ifAdminStatus** is changed to *up(1)*, then **ifOperStatus** also changes to *up(1)* if the interface is ready to transmit and receive network traffic; it changes to *dormant(5)* if the interface is waiting for external actions (such as a serial line waiting for an incoming connection); it remains in the *down(2)* state if and only if there is a fault that prevents it from going to the *up(1)* state; it remains in the *notPresent(6)* state if the interface has missing (typically, hardware) components.
ifLastChange **1.3.6.1.2.1.2.2.1.9**	The value of **sysUpTime** at the time the interface entered its current operational state. If the current state was entered prior to the last re- initialization of the local network management subsystem, then this object contains a zero value.
ifInOctets **1.3.6.1.2.1.2.2.1.10**	The total number of octets received by the interface, including framing characters. Discontinuities in the value of this counter can occur at re-initialization of the management system and at other times as indicated by the value of **ifCounterDiscontinuityTime**.
ifInUcastPkts **1.3.6.1.2.1.2.2.1.11**	The number of packets, delivered by this sub-layer to a higher (sub-)layer, which were not addressed to a multicast or broadcast address at this sub-layer. Discontinuities in the value of this counter can occur at re-initialization of the management system and at other times as indicated by the

D

MIB object and OID	Description
	value of **ifCounterDiscontinuityTime**.
ifInErrors **1.3.6.1.2.1.2.2.1.14**	For packet-oriented interfaces, the number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol. For character-oriented or fixed-length interfaces, the number of inbound transmission units that contained errors preventing them from being deliverable to a higher-layer protocol. Discontinuities in the value of this counter can occur at re-initialization of the management system and at other times as indicated by the value of **ifCounterDiscontinuityTime**.
ifOutOctets **1.3.6.1.2.1.2.2.1.16**	The total number of octets transmitted from the interface, including framing characters. Discontinuities in the value of this counter can occur at re-initialization of the management system and at other times as indicated by the value of **ifCounterDiscontinuityTime**.
ifOutUcastPkts **1.3.6.1.2.1.2.2.1.17**	The total number of packets that higher-level protocols requested be transmitted, and which were not addressed to a multicast or broadcast address at this sub-layer, including those that were discarded or not sent. Discontinuities in the value of this counter can occur at re-initialization of the management system and at other times as indicated by the value of **ifCounterDiscontinuityTime**.
ifOutErrors **1.3.6.1.2.1.2.2.1.20**	For packet-oriented interfaces, the number of outbound packets that could not be transmitted because of errors. For character-oriented or fixed-length interfaces, the number of outbound transmission units that could not be transmitted because of errors. Discontinuities in the value of this counter can occur at re-initialization of the management system and at other times as indicated by the value of **ifCounterDiscontinuityTime**.
ifSpecific **1.3.6.1.2.1.2.2.1.22**	A reference to MIB definitions specific to the particular media being used to realize the interface. It is recommended that this value point to an instance of an MIB object in the media-specific MIB; i.e., that this object have the semantics associated with the

MIB object and OID	Description
	InstancePointer textual convention defined in RFC 2579. In fact, it is recommended that the media-specific MIB specify what value **ifSpecific** should/can take for values of **ifType**. If no MIB definitions specific to the particular media are available, the value should be set to *OBJECT IDENTIFIER { 0 0 }*.

MIB object and OID	Description
ifXTable **1.3.6.1.2.1.31.1.1**	A list of interface entries. The number of entries is given by the value of **ifNumber**. This table contains additional objects for the interface table. An entry containing additional management information applicable to a particular interface. **ifName** **1.3.6.1.2.1.31.1.1.1.1** — The textual name of the interface. The value of this object is the name of the interface as assigned by the local device and is suitable for use in commands entered at the device's 'console'. This might be a text name, such as 'le0' or a simple port number, such as '1', depending on the interface naming syntax of the device. If several entries in the **ifTable** together represent a single interface as named by the device, then each will have the same value of **ifName**. For an agent which responds to SNMP queries concerning an interface on some other (proxied) device, then the value of **ifName** for such an interface is the proxied device's local name for it. If there is no local name, or this object is otherwise not applicable, then this object contains a zero-length string. **ifHCInOctets** **1.3.6.1.2.1.31.1.1.1.6** — The total number of octets received by the interface, including framing characters. This object is a 64-bit version of **ifInOctets**. Discontinuities in the value of this counter can occur at re-initialization of the management system and at other times as indicated by the value of **ifCounterDiscontinuityTime**. **ifHCInUcastPkts** **1.3.6.1.2.1.31.1.1.1.7** — The number of packets, delivered by this sub-layer to a higher (sub-)layer, which were not addressed to a multicast or broadcast address at this sub-layer. This object is a 64-bit version of **ifInUcastPkts**. Discontinuities in the value of this counter can occur at re-initialization of the management system and at other times as indicated by the value of **ifCounterDiscontinuityTime**. **ifHCOutOctets** **1.3.6.1.2.1.31.1.1.1.10** — The total number of octets transmitted from the interface, including framing characters. This object is a 64-bit version of **ifOutOctets**. Discontinuities in the value of this counter can occur at re-initialization of the management

MIB object and OID	Description
	system and at other times as indicated by the value of **ifCounterDiscontinuityTime**.
ifHCOutUcastPkts **1.3.6.1.2.1.31.1.1.1.11**	The total number of packets that higher-level protocols requested be transmitted, but which were not addressed to a multicast or broadcast address at this sub-layer, including those that were discarded or not sent. This object is a 64- bit version of **ifOutUcastPkts**. Discontinuities in the value of this counter can occur at re-initialization of the management system and at other times as indicated by the value of **ifCounterDiscontinuityTime**.
ifHighSpeed **1.3.6.1.2.1.31.1.1.1.15**	An estimate of the interface's current bandwidth in units of 1,000,000 bits per second. If this object reports a value of 'n', then the speed of the interface is somewhere in the range of 'n-500,000' to 'n+499,999'. For interfaces which do not vary in bandwidth or for those where no accurate estimation can be made, this object contains the nominal bandwidth. For a sub-layer which has no concept of bandwidth, this object is **0** (zero).

LM Sensor

MIB object and OID	Description
lmTempSensorsTable **1.3.6.1.4.1.2021.13.16.2**	Table of temperature sensors and their values. An entry containing a device and its statistics. **lmTempSensorsIndex** Reference index for each observed device. **1.3.6.1.4.1.2021.13.16.2.1.1** **lmTempSensorsDevice** The name of the temperature sensor being read. **1.3.6.1.4.1.2021.13.16.2.1.2** **lmTempSensorsValue** The temperature of this sensor in mC. **1.3.6.1.4.1.2021.13.16.2.1.3**
lmFanSensorsTable **1.3.6.1.4.1.2021.13.16.3**	Table of fan sensors and their values. An entry containing a device and its statistics. **lmFanSensorsIndex** Reference index for each observed device. **1.3.6.1.4.1.2021.13.16.3.1.1** **lmFanSensorsDevice** The name of the fan sensor being read. **1.3.6.1.4.1.2021.13.16.3.1.2** **lmFanSensorsValue** The rotation speed of the fan in RPM. **1.3.6.1.4.1.2021.13.16.3.1.3**
lmVoltSensorsTable **1.3.6.1.4.1.2021.13.16.4**	Table of voltage sensors and their values. An entry containing a device and its statistics. **lmVoltSensorsIndex** Reference index for each observed device. **1.3.6.1.4.1.2021.13.16.4.1.1** **lmVoltSensorsDevice** The name of the device being read. **1.3.6.1.4.1.2021.13.16.4.1.2** **lmVoltSensorsValue** The voltage in mV. **1.3.6.1.4.1.2021.13.16.4.1.3**

RFC1213

MIB object and OID	Description	
ipAddrTable **1.3.6.1.2.1.4.20**	The table of addressing information relevant to this entity's IP addresses. The addressing information for one of this entity's IP addresses.	
	ipAdEntAddr **1.3.6.1.2.1.4.20.1.1**	The IP address to which this entry's addressing information pertains.
	ipAdEntIfIndex **1.3.6.1.2.1.4.20.1.2**	The index value which uniquely identifies the interface to which this entry is applicable. The interface identified by a particular value of this index is the same interface as identified by the same value of **ifIndex**.
	ipAdEntNetMask **1.3.6.1.2.1.4.20.1.3**	The subnet mask associated with the IP address of this entry. The value of the mask is an IP address with all the network bits set to **1** and all the hosts bits set to **0**.
	ipAdEntBcastAddr **1.3.6.1.2.1.4.20.1.4**	The value of the least-significant bit in the IP broadcast address used for sending datagrams on the (logical) interface associated with the IP address of this entry. For example, when the Internet standard all-ones broadcast address is used, the value will be **1**. This value applies to both the subnet and network broadcasts addresses used by the entity on this (logical) interface.
	ipAdEntReasmMaxSize **1.3.6.1.2.1.4.20.1.5**	The size of the largest IP datagram which this entity can re-assemble from incoming IP fragmented datagrams received on this interface.

SNMP Framework

MIB object and OID	Description
snmpEngineID **1.3.6.1.6.3.10.2.1.1**	An SNMP engine's administratively-unique identifier. This information should be stored in non-volatile storage so that it remains constant across re-initializations of the SNMP engine.
snmpEngineBoots **1.3.6.1.6.3.10.2.1.2**	The number of times that the SNMP engine has (re-)initialized itself since **snmpEngineID** was last configured.

MIB object and OID	Description
snmpEngineTime **1.3.6.1.6.3.10.2.1.3**	The number of seconds since the value of the **snmpEngineBoots** object last changed. When incrementing this object's value would cause it to exceed its maximum, **snmpEngineBoots** is incremented as if a re-initialization had occurred, and this object's value consequently reverts to **0** (zero).
snmpEngineMaxMessageSize **1.3.6.1.6.3.10.2.1.4**	The maximum length in octets of an SNMP message which this SNMP engine can send or receive and process, determined as the minimum of the maximum message size values supported among all of the transports available to and supported by the engine.

SNMPv2 Framework

MIB object and OID	Description
sysDescr **1.3.6.1.2.1.1.1**	A textual description of the entity. This value includes the full name and version identification of the system's hardware type, software operating system, and networking software.
sysObjectID **1.3.6.1.2.1.1.2**	The vendor's authoritative identification of the network management subsystem contained in the entity. This value is allocated within the SMI enterprises subtree (**1.3.6.1.4.1**) and provides an easy and unambiguous means for determining 'what kind of box' is being managed. For example, if vendor '*Flintstones, Inc.*' is assigned the subtree *1.3.6.1.4.1.424242*, it could assign the identifier *1.3.6.1.4.1.424242.1.1* to its '*Fred Router*'.
sysUpTime **1.3.6.1.2.1.1.3**	The time (in hundredths of a second) since the network management portion of the system was last re-initialized.
sysContact **1.3.6.1.2.1.1.4**	The textual identification of the contact person for this managed node, together with information on how to contact this person. If no contact information is known, the value is a zero-length string.
sysName **1.3.6.1.2.1.1.5**	An administratively-assigned name for this managed node. By convention, this is the node's fully-qualified domain name. If the name is unknown, the value is a zero-length string.

MIB object and OID	Description
sysORLastChange **1.3.6.1.2.1.1.8**	The value of **sysUpTime** at the time of the most recent change in state or value of any instance of **sysORID**.
sysORTable **1.3.6.1.2.1.1.9**	The (conceptual) table listing the capabilities of the local SNMP application acting as a command responder with respect to various MIB modules. SNMP entities having dynamically-configurable support of MIB modules will have a dynamically-varying number of conceptual rows. An entry (conceptual row) in the **sysORTable**. **sysORIndex** **1.3.6.1.2.1.1.9.1.1** — The auxiliary variable used for identifying instances of the columnar objects in the **sysORTable**. **sysORID** **1.3.6.1.2.1.1.9.1.2** — An authoritative identification of a capabilities statement with respect to various MIB modules supported by the local SNMP application acting as a command responder. **sysORDescr** **1.3.6.1.2.1.1.9.1.3** — A textual description of the capabilities identified by the corresponding instance of **sysORID**. **sysORUpTime** **1.3.6.1.2.1.1.9.1.4** — The value of **sysUpTime** at the time this conceptual row was last instantiated.

UCD Disk I/O

MIB object and OID	Description
diskIOTable **1.3.6.1.4.1.2021.13.15.1**	Table of I/O devices and how much data they have read/written. An entry containing a device and its statistics. **diskIOIndex** **1.3.6.1.4.1.2021.13.15.1.1.1** — Reference index for each observed device. **diskIODevice** **1.3.6.1.4.1.2021.13.15.1.1.2** — The name of the device being counted/ checked. **diskIOReads** **1.3.6.1.4.1.2021.13.15.1.1.5** — The number of read accesses from this device since boot. **diskIOWrites** **1.3.6.1.4.1.2021.13.15.1.1.6** — The number of write accesses to this device since boot.

UCD SNMP

MIB object and OID	Description
memTotalReal **1.3.6.1.4.1.2021.4.5**	The total amount of real/physical memory installed on this host.

Glossary

#

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 Key
: An access 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 can be compared to concept of a username/password pair.

Active Directory
: Microsoft Active Directory® is a directory service that stores directory information on a network and makes this information available to network users and administrators. AD stores information about user accounts, such as names, passwords, phone numbers, and so on, and enables other authorized users on the same network to access this information.

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.

Asynchronous data replication
: Asynchronous data replication replicates data between two Unity Storage Systems—a primary and a remote (or secondary) system—over a LAN or WAN connection. See the Terminology section for details

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 the Unity Storage System.

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.

Bucket
: A bucket is a basic container that holds data. It can be used to organize and control access to the data.

C

CHAP authentication
: 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 the Unity Storage System to servers (initiators) that provide the correct user name and password (or secret) combination. The Unity System's iSCSI implementation provides several layers of CHAP authentication.

CIFS
: (Common Internet File System) The protocol used in Windows environments for shared folders.

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 System offers a command-line interface. Abbreviated "CLI".

Clustering
: Provides both high-availability and load balancing, using the Unity Storage System's redundancy features, including dual controllers and RAIDs. See also Active/Active Clustering

Committed space
: The final HDD location of data. In Unity, write operations are collected into transaction groups on SSD FASTier drives, and later written sequentially to their final location in the storage pool, typically on spinning media.

Controller
: The controller in a Unity Storage System acts as the interface between Unity and network clients. The Unity Storage System has two controller nodes, represented by the Clusters node in Unity™, for which you can configure both cluster and network settings. Can also be referred to as Controller Node or Node.

D

Dataset
: A dataset is any file system, iSCSI LUN, or CIFS share.

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 System 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.

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).

E

Electrostatic discharge (ESD)
: The sudden and momentary electric current that flows between two objects at different electrical potentials caused by direct contact or induced by an electrostatic field. Potentially harmful to electronic components.

Ethernet
: A local area network (LAN) architecture using a bus or star topology and supporting data transfer rates of 10, 100, and 1000 Mbps. It is one of the most widely implemented LAN standards. The 802.11 protocols are often referred to as “wireless Ethernet.”

Event log
: A record of system events that tracks informational, warning, and error events, such as when significant milestones are reached or when errors occur during activity.

Expansion Controller
: A module of Unity Storage Expansions that connects via SAS to a Unity Storage Expansion 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. In Nexsan Unity systems, failover describes one Controller Node taking over the host connections and storage pool control of the other Controller Node when that controller fails.

FASTier™
: Nexsan’s proprietary cache system that uses SSD or NVDIMM technology to increase random I/O performance of SATA and SAS disk drives.

FCC
: The Federal Communications Commission; the federal agency that regulates electromagnetic emissions.

Fibre Channel
: A gigabit (Gb) speed network technology primarily used for storage networking and the current standard connection type for storage area networks (SANs). Despite its name, Fibre Channel signaling can run on both twisted-pair copper wire and fiber-optic cables.

Fibre Channel port
: Any entity that actively communicates over a Fibre Channel network. Usually implemented in a device such as disk storage or a Fibre Channel switch. Depending on the system, the Fibre Channel ports on Nexsan Unity Storage Expansions can support 2Gb/s, 4Gb/s, or 8Gb/s connections.

Fibre Channel switch
: A network switch compatible with the Fibre Channel protocol. Allows the creation of a Fibre Channel network, which is currently the core component of most storage area networks (SANs).

Fibre Channel target
: A storage system end-point on the Unity Storage System that uses Fibre Channel connectivity. Each storage pool can have one or multiple Fibre Channel targets. Fibre Channel targets can be seen by all ports on the Unity Storage System.

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 System to the remote Unity System. Only the initial replication, when you first set up asynchronous data replication between two systems, is a full replication. All successive replications are incremental.

G

Gateway
: An internetworking 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.

Graphical user interface (GUI)
: 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

Home directory
: A dedicated folder where users store their files. In Unity, home directories can be created using a file system configured to use Microsoft Active Directory for the user authentication method. Set up the feature from the Storage > Home Directories panel.

Host
: A computer, server, or other device which accesses the shares in a Nexsan Unity System storage system. The host can be connected to the storage system with a Fibre Channel connection, an iSCSI connection, or a 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 immutable snapshot 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 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).

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.

IP

(Internet Protocol) The network layer for the TCP/IP protocol suite widely used on Ethernet networks.

IP address

(Internet Protocol address) A numerical label assigned to each device (such as a computer, printer, or Nexsan Unity Storage Expansion) on a computer network that uses TCP/IP for communication.

IPMI

(Intelligent Platform Management Interface) The IPMI interface enables you to perform administrative tasks to remotely manage the Unity Storage System in the event that you are unable to connect to the Unity Storage System using a conventional method: through Unity™ or from the nxadmin CLI.

IQN

(iSCSI qualified name) Unique identifier of a device in an iSCSI network. iSCSI uses the form iqn.date.authority:uniqueid for IQNs. For example, iqn.1999-02.com.nexsan:Unity_system_name:pool_name:unique_ID. This name indicates that this is an iSCSI device from Nexsan, which was registered as a company in February of 1999. The naming authority is simply the DNS name of the company reversed; in this case, com.nexsan. Following this is the site name, the storage pool name where the target exists, and a user-defined unique ID to identify the target.

iSCSI

(Internet Small Computer System Interface) A transport protocol that provides for the SCSI protocol to be carried over a TCP/IP network.

iSCSI Target
: A storage system end-point on the Unity Storage System that processes iSCSI commands and I/O requests from an initiator. Each storage pool on the Unity Storage System 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 the Unity Storage System is identified by a unique addressing method (IQN).

iSCSI Target public alias
: This is a symbolic name that you can assign to a target on the Unity Storage System. 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 the Unity Storage System 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
: (Internet Storage Name Service) Protocol designed to facilitate the automated discovery, management, and configuration of iSCSI devices on a TCP/IP network. You can configure iSCSI targets to use an iSNS server.

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).

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 (Logical Unit Number) refers to a block of storage with a unique number on the Unity Storage System, that can be expanded using virtual disk space. LUNs can be exposed over iSCSI and Fibre Channel. When associated with an iSCSI target, a LUN forms a unique iSCSI block device that can be accessed by one or more iSCSI initiators. When exposed to the common Fibre Channel target on the Unity Storage System, a LUN forms a block device identified by a unique HBA port WWN that can be accessed by one or more FC initiators.

LUN mask
: A LUN mask uses authentication to make a Logical Unit Number accessible to selected storage targets.

M

Management target
: Each storage pool on the Unity Storage System 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 the Unity Storage System. The VSS host connects to a storage pool's Management target via iSCSI to view, create, and manage snapshots of the LUNs in the storage pool. You can assign a CHAP (Challenge Handshake Authentication Protocol) user to the Management target to restrict access to LUN snapshots in a storage pool, to specific VSS hosts.

Manual replication
: In asynchronous replication, an offline, or manual, replication is a replication process that you start manually on a storage pool. With offline replication, you can replicate the data in the storage pool to the remote Unity System, or to a USB storage device attached to the primary Unity System.

Mb
: Megabit. Approximately one million (1,000,000) bits.

Mb/s
: (Megabits (Mb) per second) Used to describe the speed of network data transmission.

MPIO (Multipathing I/O)
: MPIO 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.

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.

NDMP
: (Network Data Management Protocol) 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.

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). and Session service (TCP port 139).

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.

NIS
: (Network Information Service) One of the three UNIX directory services supported by the Unity Storage System. 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.

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.

NTP
: (Network Time Protocol) A protocol designed to synchronize the clocks of devices over a network.

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.

Offline replication
: In asynchronous replication, an offline, or manual, replication is a replication process that you start manually on a storage pool. With offline replication, you can replicate the data in the storage pool to the remote Unity System, or to a USB storage device attached to the primary Unity System.

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.

Pool
: see Storage Pool

Pool Resource Groups
: Pool Resource Groups act as the virtual access point for the data (file system and/or LUNs) in storage pools. Specifically, end users and client systems on the network access their data in the storage pools using the corresponding Pool Resource Group's virtual IP address. Each Pool Resource Group is hosted on one of the two controller nodes in the cluster.

Power supply unit (PSU)
: A module that regulates electrical power to the components of Nexsan Unity Storage Expansions.

Primary
: In asynchronous replication, a primary site refers to a Unity System that contains the data to be replicated (to a remote, or secondary, Unity System). a Unity System can be the primary site in a replicated environment and also perform double-duty as the remote data replication site for another Unity System.

Public alias
: This is a symbolic name that you can assign to a target on the Unity Storage System. 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.

Q

Quiesce
: To gracefully shut down or disconnect a Unity Storage System, pending a maintenance or administrative operation.

R

RAID 10
: RAID 10 provides very high performance and redundancy. In a RAID 10 implementation, data is simultaneously mirrored and striped. 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, and please refer to "Understanding storage pools, volumes, and storage enclosures".

RAID 5
: RAID 5 provides redundancy by writing data and parity information across three or more drives, thereby increasing performance. You need at least 3 disk drives for a RAID 5 implementation. RAID 5 can withstand a single disk failure without losing data or access to data. It is ideally suited for transaction processing, database applications, file and print servers.

RAID 6
: RAID 6 is similar to RAID 5, but with better fault tolerance. RAID 6 stripes blocks of data and parity across an array of drives like RAID 5, except that it calculates two sets of parity information for each parcel of data. This significantly improves fault tolerance: RAID 6 can withstand the failure of any two drives in the array without losing data or access to data. 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.

Random-access memory (RAM)
: 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.

Read-only memory (ROM)
: 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.

Remote
: In asynchronous replication, a remote or secondary site represents the system to which data from the primary Unity System is replicated. In a deployment where asynchronous replication is not implemented, a remote Unity System represents a site that is being managed remotely from another Unity System or site.

Replica
: A duplicate of a file system on a Nexsan Unity System copied onto another Nexsan Unity System. At the time of replication, replicas contain all of the data on the original volume. Replicas can be promoted to full file systems, after which replication between the two file systems is no longer possible.

Replication
: A function of Nexsan Unity Systems that allows the user to make replicas of a volume onto another Nexsan Unity System to protect data in

the event of a disaster, or as part of a backup and restore architecture.

Reserved space
: You can reserve a set amount of disk space in the storage pool for the exclusive use of file systems, LUNs, or CIFs shares (data sets). Unity then automatically allocates the specified amount of disk space in the storage pool to the data set. If you add another data set to the storage pool, the space available to the new one is the difference of the total disk space in the storage pool minus any reservations that you set for other data sets on the system.

S

SAN
: (Storage area network) An architecture that provides for attachment of remote computer storage devices to servers in such a way that the devices appear as locally attached to the operating system.

SAS
: (Serial Attached SCSI) A serial version of the SCSI interface. A point-to-point architecture that uses a disk controller with four or more channels that operate simultaneously. Each full-duplex channel, known as a SAS port, transfers data at 1.5Gb/s, 3Gb/s, or 6Gb/s in each direction. SAS also supports Serial ATA (SATA) drives, which can be mixed with SAS drives in a variety of configurations.

SATA
: (Serial Advanced Technology Attachment) A connection standard for fixed and removable hard disk drives.

Scheduled replication
: In asynchronous replication, a scheduled replication refers to an automatic replication that occurs according to a schedule you define. You can configure a separate replication schedule for each storage pool on the Unity Storage System.

Scrubbing
: A mechanism provided in Unity that checks for and repairs read and write errors to the meta data that comprise storage pools and volumes.

SCSI
: (Small Computer System Interface) A collection of standards and proposed standards for input/output (I/O) communication, primarily intended for connecting storage subsystems or devices to hosts.

Secondary
: In asynchronous replication, a remote or secondary site represents the system to which data from the primary Unity System is replicated. In a deployment where asynchronous replication is not implemented, a remote Unity System represents a site that is being managed remotely from another Unity System 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.

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.

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.

SNMP
: (Simple Network Management Protocol) The SNMP agent included in the Unity Storage System 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 the Unity Storage System.

SSD
(Solid State Disk) A high-performance storage device that contains no moving parts.

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.

Storage Pool
A storage pool (also referred to as a "pool") groups disks into volumes, to which you can add file systems and LUNs. Pools allow you to expose file systems and shares to CIFS clients (Windows-based systems) and NFS clients (UNIX/Linux-based and Macintosh 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 devices in the 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.

Subnet mask
A means of restricting IP addresses on a subnet to a specific range.

Synchronous data replication
Use the synchronous data replication feature to synchronously replicate a storage pool between two Unity Storage Systems connected to Unity via SAS (or Fibre Channel). The synchronous data replication feature essentially mirrors all the data contained in a storage pool between a source Unity Storage System and a target Unity Storage System—both of which are connected to the same Unity System via SAS (or Fibre Channel). You designate the storage system to use as the source (the system on which you create the storage pool and store your data) and the target, where the source data is mirrored. Synchronous replication ensures that a copy of the data, which is identical to the source copy, is created at the time the source copy is updated. In synchronous replication, an I/O-update operation is not considered done until completion is confirmed on both the source and target. An incomplete operation is rolled back on both the source and target, ensuring that the target is always an exact mirror image of the source.

T

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.

Thin Provisioning
Thin Provisioning enables you to dynamically allocate disk space to a client system (initiator) connected to a LUN on the Unity Storage System. With Thin Provisioning, you can flexibly allocate disk space (on a LUN) to the client system (initiator), to expand the storage capacity available to the client system at any time. 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.

U

Unity
: A Web-based interface for managing Unity Storage Systems, providing a hierarchical view of all system components. Includes wizard-based and CLI-based configuration tools for creating storage pools, file systems, shares, replication sites, and for performing other storage management tasks on the system.

V

VAAI
: The VMware vStorage APIs for Array Integration plugin provides hardware acceleration on Unity when integrated into a VMware ESX/ESXi environment. See Terminology

Volume
: A volume represents a storage-area network, block-type subset of the aggregated disk space available on Unity. The total number of volumes available on Unity internal disk storage, as well as on storage systems attached externally to Unity, depends on the RAID level (5, 6, or 10) and RAID sets that you specify during initial setup. For example, on a Unity system with 15 disk drives installed in the front bay of the system, a RAID 5 configuration with 2 RAID sets results in 2 volumes with 7 disks drives in each volume, and 1 hot spare assignment for the array.

VSS
: (Volume Shadow Service) The Unity Storage System's VSS Hardware Provider enables a VSS host to create and manipulate shadow copies (point-in-time snapshots) of the data in LUNs on the Unity System. 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 the Unity Storage System.

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).

Index

A

About this document ix
Access to the CallHome service 24
Accessing file systems using FTP 57
Accessing the nxadmin CLI
    from the IPMI Web-based interface 14
    Using an SSH client 13
    Using KVM ports 13, 16
Accessing the SNMP menu 173
ACL permissions 17
aclpropagate 17
ACLs 18, 33, 45, 86, 119, 162, 264, 266
Activating maintenance mode 90
Active mode 271
Adding local group accounts that correspond
        to UNIX/Linux Microsoft Active
        Directory domain accounts 59
Adding local user accounts 190
Adding one or more links to an existing
        aggregation 105
Adding TCP/IP routing entries to the routing
        table 153
Address Resolution Protocol 19
Adjusting replication priority 208
Aggregation information 203
Aggressive reboot 216
ansi 178
APAL status 194
arcstat 181
arp 19
    <hostname> 19
    -a 19
    -d 20
    -f 20
    -s 20
Assigning access permissions to NFS
        shares 160
audit 21
    -c 21
    -n 21
    -u 21
autolog 22
    disable 22
    enable 22
    status 22
    time 22
    update 22
Available commands in the nxadmin CLI's
        command-based shell 60
Aysnchronous replication
    configuration settings 151
    progress 151

B

bedit 23
Buffer size for High Performance
        Networks 207
Building a master NIS server database 197

C

callhome 24
    hosts 25
    monitor 25
    sendlogs 25
    start 24
    status 24
    stop 24
    test 25
    version 25
cap 26
cat 27
    <filename> 27
cd 28
    .. 28
    <directory> 28
changeenclosureid 28

changenameservices 29
-c 29, 277
-s 30
Changing a storage enclosure ID 28
Changing a user password 139
Changing directories in Unity's operating system command shell 27
Changing the network interface for iSCSI targets 215
Changing the NFS version 4 (NFSv4) domain 101
Changing the password of the nxadmin account 139
Changing the replication priority adjustment 208
Changing the stored intersite virtual IP, name, or site serial 166
Changing the system prompt 145
chassis (ipmitool) 71
Chassis LED configuration 75
Chassis sensor information 155
Checking system performance 181
Checksums 91
chown 224
CIFS 249
CIFS file systems 249
CIFS server restart 171
CIFS server setup 171
CIFS shares 160
CIFS sharing 129, 160, 167, 171, 182, 224, 245, 248-249, 253, 255, 260, 262, 266
cifssvrtop 182
cleandev 36
-c 36
-C 36
-i 36
-n 36
-r 36
-s 37
-t 37
-v 37
clear
devices errors in a pool 123
Clear event flags 53
Clearing IPMI network settings 212
Clearing the DNS client cache 115
Clearing the nstusermaps cache 266
clearjbodflags 37
Closing the SSH session 53
cloudconnector 38
cloudcron 41
Cluster Resources tab 16
clustering 42
config 42
mgmt 43
rg1 43
rg2 43
show 42
Collecting all system log files on Unity 43, 224
Concurrent replications per controller 208
config
clustering 42
Configuring advanced network settings 103
Configuring CIFS local groups and users 167
Configuring compression settings for data replication 205
Configuring data replication settings 204
Configuring disk heartbeats 48
Configuring iSCSI targets 213
Configuring LACP 272
Configuring LEDs for chassis and drives 75
Configuring shares and Active Directory 248
Configuring the Active Directory client 261
Configuring the buffer size for High Performance Networks 207
Configuring the file system group lookup 265
Configuring the firewall 54, 227
Configuring the LDAP Client in AD mode 263
Configuring the network bandwidth for data replication 205
Configuring the network interface for data replication 205
Configuring the network type for data replication 206
Connecting to a Nexsan storage system using the Nexsan Management Protocol 115
Connecting to the peer controller node 140
Connecting to Unity via remote console using KVM ports 13
Connecting via console using KVM ports 16
console6 178
Controler node shutdown 166
Controller node reboot 151
CPU utilization 65
createlogpackage 43
custom add (firewall) 55
custom remove (firewall) 55
custom show (firewall) 55

D

DAR 119
dataproperty 44
-c 44
-n 45
-p 45
-t 46
-v 45
date 46
<mm><dd><HHMM><.SS> 47
<mmddHHMM><cc><yy><.SS> 47
-a 47
-R 47
-u 47
DDAR 119
Deactivating maintenance mode 90

Defining network settings 159, 202
Defining the default domain 158
Defining the properties of naming services 29
Deleting a link aggregration 105
Deleting local group accounts 60
Deleting local user accounts 191
disable
autolog 22
Disable write protection 89
Disabling a service 158
Disabling extended requests 172
Disabling LACP 274
Disabling the firewall 54, 227
Disabling the Offline Files function for a file system 260
Disk hearbeats 48
Disk I/O activity 65
diskhbcfg 48
check 48
get 48
set 48
update 48
Displaying a list of all available commands in the nxadmin CLI's command-based shell 60
Displaying a list of all disk drives 49
Displaying aggregation information for network interfaces 203
Displaying all active services 176
Displaying APAL status 194
Displaying available disk drives on the system 56
Displaying aysnchronous replication progress 151
Displaying chassis/system sensor information 155
Displaying connected Nexsan storage systems 49
Displaying help information for nxadmin CLI commands 17
Displaying historical network usage 110
Displaying information about the device and attributes of a physical link 109
Displaying information for the Fibre Channel host bus adapter (HBA) ports 116, 237
Displaying information for the Serial Attached SCSI-2 (SAS-2) host bus adapter 125, 238
Displaying input/output statistics for Unity 65
Displaying iSCSI target allocations 213
Displaying link aggregation information 105
Displaying link configuration or statistics 107
Displaying link status information for each network interface 100
Displaying local user and group accounts 78, 231
Displaying NFS statistics 102
Displaying property values for a file sharing protocol 128
Displaying replication settings 151
Displaying resilvering status 152
Displaying shares 164
Displaying space usage quotas on file systems for a user and/or group 258
Displaying storage pool status 123
Displaying summary information and statistics for system virtual memory 193
Displaying the configuration for network interfaces 61
Displaying the contents of a file in the terminal window 27
Displaying the contents of certain network-related data structures 95
Displaying the current or persistent values of one or more link properties 109
Displaying the current version of CIFS server 172
Displaying the domain name used for NIS integration 49
Displaying the full path of the current, working directory 150
Displaying the host name 61
Displaying the menu-driven nxadmin CLI 92
Displaying the most recent error logs 52
Displaying the name of NIS server 198
Displaying the names of native instruction sets for applications 73
Displaying the number of active users 190
Displaying the number of days that the system has been running 190
Displaying the numeric exit code for the last operation that was run 51
Displaying the physical locations of the network ports on the current Controller node 113
Displaying the process tree 149
Displaying the route (path) that an IP packet follows to another Internet host 186
Displaying the routing table 165
Displaying the Secure Hash Algorithm (SHA-256) hash of a file 160
Displaying the status of cluster resources 42
Displaying the status of Vault Protection Modules 133
Displaying the top 30 processes being managed by NestOS 178
Displaying the user currently logged in to Unity 194
Displaying Unity network configuration utility 159
Displaying user quotas on shares 192
Displaying values from a NIS database 196
Displaying various properties of the pool or file system data 44
Displaying version information for the

software components 64
Displayings all running processes on Unity 147
domain name 49
domainname 49
<domain> 49, 277
-s 49
Drive LED configuration 75
drives 49
paths 49
dynamic add (firewall) 55
dynamic remove (firewall) 56
dynamic show (firewall) 56

E

echo 50
$? 51
<text> 51
edit 51
<file name> 51
enable
autolog 22
Enable write protection 89
Enabling a service 158
Enabling access-based enumeration of folders and files in a CIFS share 262
Enabling extended requests 172
Enabling jumbo frames 275
Enabling jumbo frames for iSCSI interfaces 100
Enabling LACP 273
Enabling LACP on Unity 271
Enabling link aggregation 100
Enabling the firewall 54, 227
Enabling the no_root_squash property on an NFS file system 254
Enabling the Offline Files function for a share 260
enforcessl 51
Environment with both Linux/UNIX and Windows clients 190
errorlog 52
<number of lines> 52
E-Series storage 115
etc/logadm.conf 78
etc/nsswitch.conf 29
Ethernet switches for LACP 272-273
eventflag 53
clear 53
show 53
exit 53

F

fcinfo 226
fcstat 54
Fibre Channel clients 77
Fibre Channel statistics 54
firewall 54
custom add 55
custom remove 55
custom show 55
dynamic add 55
dynamic remove 56
dynamic show 56
reloadconfig 55
startservice 55
status 55
stopservice 55
format 56
FRU information 70
ftpconfig 57
fullcheck (ipmi) 69
Full-Duplex 272

G

GID 59, 232
modgid 92
Giving access permissions to NFS shares 160
Graceful reboot 216
groupadd 59, 228
<group name> 59
-g 59
-o 59
groupdel 60
<group name> 60
groups (listug) 78

H

HBA ports 116, 237
Hearbeats 48
help 60
High Performance Networks (HPN) 207
hostname 61
hosts
callhome 25
HTTP hosts 25

I

Identifying hardware or component faults 155
Identifying various attributes of the CPU 73
ifconfig 61, 229
<netname> 62
-a 62
immutablecron 62
-c add 62

-c clear 62
-c remove 62
-c test 62
Improving resilvering performance 152
info 64
Initializing LDAP to Active Directory mapping 263
Initializing the NIS client 197
Input statistics 65
Integrating with Network Information Service (NIS) 277
interval rate (iostat) 67
intmonitoring 64
-c 65
-s 65
iostat 65, 229
interval rate 67
nstpool 123
update count 67
IP-based restrictions 249
ipgroups 67
IPMI
Web-based interface 14
ipmi 69
fullcheck 69
updatesettings 69
IPMI console 273, 275
IPMI settings 210
ipmitool 70, 230
-c 70
chassis 71
-f 71
-H 71
-I 71
lan 72
-p 71
-U 71
-v 71
-V 71
isainfo 73
-b 73
-k 73
-n 74
-v 73
-x 74
iscsiop 182

J

Java™ viewer 15
Jumbo frames 275

K

kill 74
<process ID> 74
KVM console 273
KVM ports 16

L

LACP 271
configuring 272
disabling 274
monitoring 273
Requirements and guidelines 272
Understanding link aggregation 272
lan (ipmitool) 72
Launch Console 15
LDAP 132, 134, 138, 248, 257-258, 261, 263-267, 277
Clearing the nstusermaps cache 266
Configuring the file system group lookup 265
Initializing LDAP to Active Directory mapping 263
Removing a Certification Authority (CA) certificate 265
Resetting the LDAP Client configuration 265
Restarting the LDAP Client service 267
Setting ACLs on file systems 266
Setting the Client configuration 265
Showing ACLs on file systems 266
Showing current client information 263
Uploading a Certification Authority (CA) certificate 264
Viewing instructions on using nstusermaps for LDAP to AD mapping 266
Leaving the nxadmin CLI 53
led 75
Link aggregation 103, 272
list
nstpool 123
listfcclients 77
Listing Fibre Channel clients 77
Listing storage pools on Unity 123
Listing the contents of the current working folder 83, 99
Listing UNIX/Linux clients that have remotely mounted an NFS share 164
listug 78
groups 78
users 78
Load balancing 271
Local user and group accounts 78, 231
log file 79
logrotate 78
<log file> 79
-a 81
-A 82
-b 81

-c 81
-C 82
-e 79
-E 82
-F 79
-f 79
-g 81
-h 79
-l 81
-m 81
-M 81
-N 79
-n 79
-o 81
-p 80
-P 80
-r 79
-R 81
-s 80
-S 83
-t 82
-T 83
-V 79
-v 80
-w 80
-z 82
ls 83
lun 89

M

maintenance 90
off 90
on 90
show 90
man 91
<command name> 91
Managing the CIFS server 171
Manually refreshing the system cache 152, 242
Mapping local users to Microsoft Active Directory users 131
Maximum number of concurrent replications per controller 208
Maximum number of targets per pool 213
MD5 (128-bit) checksums 91
md5sum 91
<file name> 91
Measuring transit delays of data packets on the network 186
menu 92
Menu-driven nxadmin CLI 201
Change network interface setting 205
Change network type setting 206
Change Replication Bandwidth Limit 205
Change Replication Compression Setting 205
Change the network interface that an iSCSI target is presented on 215
Configure iSCSI targets 213
Configure Share Access Based Enumeration 262
Configure Share Access Lists 249, 252, 254
Configure Share Offline Files 260
Configure Share Quotas 257-258
Configure the Active Directory client 261
Configure the blocksize of shares or pools 261
Configure the IPMI Network Settings 211
Configure the LDAP Client in AD mode 263
Configuring shares and Active Directory 248
NestOS Update Server Menu 212
Network Adapter Allocation Menu 213
Network Configuration menu 202
Recalculate Allocations to Detect IP Address Changes 214
Repair Fault 247
Reset Unity Storage System 267
Restart Web service 221
Restarting Unity or one of its controller nodes 216
Restore Retired Devices 248
Run a command 221
chown 224
moduid 232
Set the IPMI login password 211
Set the IPMI login password to default 212
Show Aggregation Information 203
Show Allocation Information 213
Show Faults Information 247
Shutdown and Reboot Menu 216
Shutting down Unity or one of its controller nodes 217
System Menu 268
Unset network settings for IPMI access 212
menu-driven nxadmin CLI
Controller Menu 218, 220
mgmt
clustering 43
Microsoft Active Directory 59-60, 131, 138, 190-191, 222, 228, 240, 246, 248, 257-258, 261, 267-268
modgid 92, 232
<new GID> 92
<UID> 92
Modifying a link aggregration 105
Modifying a storage enclosre ID 28
Modifying IPMI settings 210
Modifying network settings 159, 202
Modifying the block size 261

Modifying the group ID (GID) of a local user account 92
Modifying the Internet-to-MAC address translation table 19
Modifying the user ID (UID) of a local user account 93
moduid 93, 232
<new UID> 93
UID 93
monitor
callhome 25
Monitoring LACP 273
Monitoring system performance 140
Monitoring Unity appliances and Nexsan E-Series™ storage units using SNMP 173
Moving cluster resources from one cluster to the other 42
mpstat 93
<count> 95
<interval> 95
-a 94
-p 94
-P 94
-q 94
-T 94

N

nameservices 30
NDMP sessions 119
NestOS Admin Menu 201
Configure shares and Active Directory 248
Fault Repair Menu 247
Network Menu 202
Reset Unity Storage System 267
Restart Web Service 221
Run a command 221
chown 224
moduid 232
Shutdown and Reboot Menu 216
Shutdown and Reboot menu 275
System Menu 268
NestOS IPMI Menu 210
Configure the IPMI Network Settings 211
Set the IPMI login password 211
Set the IPMI login password to default 212
Unset network settings for IPMI access 212
NestOS LDAP Client in AD Mode menu 264
NestOS Network Adapter Allocation Menu 213
Change the network interface that an iSCSI target is presented on 215
Recalculate Allocations to Detect IP Address Changes 214
Show Allocation Information 213
NestOS Network menu 202
NestOS IPMI Menu 210
Network Configuration menu 202
Replication Bandwidth menu 204
Show Aggregation Information 203
NestOS Replication Bandwidth menu 204
Change network onterface setting 205
Change network type setting 206
Change Replication Bandwidth Limit 205
Change Replication Compression Setting 205
NestOS Shares Menu 248
Configure Share Access Based Enumeration 262
Configure Share Access Lists 249, 252, 254
Configure Share Offline Files 260
Configure Share Quotas 257-258
Configure the Active Directory client 261
Configure the blocksize of shares or pools 261
Configure the LDAP Client in AD mode 263
NestOS Shutdown and Reboot Menu 216
Controller Menu 218, 220
restarting Unity 216
shutting down Unity 217
NestOS SNMP menu 173
NestOS Update Server Menu 212
nestpool clear 233
nestpool iostat 233
nestpool status 234
netstat
<count> 98
<interval> 98
-a 96
-D 97
-f 96
-g 97
-i 97
-I 98
-m 97
-M 97
-n 96
-P 97
-p 97
-R 96
-r 97
-s 97
-T 98
-v 96
network 100
get link 100
get|set lacp 100
get|set mtu 101

get|set sbr 100
Network interfaces
route command 153
statistics 113
nfs 101, 235
domain 101
maxversion 102
NFS 249
NFS file systems 252
NFS shares 160, 190
NFS sharing x, 59, 102, 128, 160, 164, 172, 182, 190, 222, 228, 232, 240, 242, 244, 246, 248, 250, 252, 254, 266, 277
NFS statistics 102
nfsstat 102
<count> 103
<interval> 103
-a 103
-c 102
-m 103
-n 102
-r 102
-s 102
-T 103
-v 103
nfssvrtop 182
NFSv3 229
nic 103, 236
add-aggr 105
create-aggr 104
delete-aggr 105
modify-aggr 105, 273-274
remove-aggr 105
rename-link 107
reset-linkprop 108
set-linkprop 108, 275
show-aggr 105, 273
show-link 107
show-linkprop 109
show-phys 109
show-usage 110
nics 113
nicstat 113
-a 114
-h 114
-i interface 114
interval [count] 114
-l 114
-n 114
-p 114
-s 114
-t 114
-u 114
-v 114
-x 114
-z 114
NIS integration 277
changenameservices 29
domainename 49
setdefaultdomain 158
ypcat 196
ypinit 197
ypwhich 198
nmp 115
<host name> 115
<IP address> 115
No access 249
no_root_squash property 254
Node reboot 151
Node shutdown 166
nscacherestart 115, 237
nstfcdata 116
hba-port 117
logical-unit|lu 117
remote-port 117
-V 117
nstls 118
nstndmp 118
disable -a 122
enable -a 122
get -p 119
kill-sessions 122
set -p 122
show-devices 122
show-sessions 122
nstpool 123
<device> 124
<pool> 124
clear 123
iostat 123
list 123
online 123
status 123
nstsasdata 125
expander 125
hba 125
hba-port 125, 239
logical-unit|lu 126
target-port 126
nstsharectl 128
get 128
set 128
status 128
nstusermaps 130, 240, 278
add 131
dump 131
export 131
-f 131
flush 131
get-namemap 132
help 132
import 132
list 132
remove 132
set-namemap 132
show 132
unset-namemap 132
nstvault 134
nvram 135

nx0 159, 206, 229, 273-274
nx1 206, 273-274
nx99 13, 159
nxadmin CLI's command-based shell 17
nxcmd 136

O

Obtaining the status and location of a controller node 218
Opening a remote session from the IPMI Web-based interface 14
Opening all dynamic ports on Unity for specific IP addresses 55, 227
Opening an SSH session to using an SSH client 13
Output statistics 65

P

Passive mode 271
passwd 139
  <user> 139
PASSWORD 14, 16
Password change 139
paths
  drives 49
peer 139
perfmon 140
performance 142
Performing advanced administrative functions on share protocols 128
Permissions 18, 32, 86
Permissions for file systems 17
ping 142
  -a 143
  -A 144
  -b 143
  -c 144
  -d 143
  -D 143
  -F 144
  -g 144
  host 145
  -I 144
  -i 145
  -L 143
  -n 144
  -N 144
  -P 145
  -p 145
  -R 144
  -r 144
  -s 143
  -t 145
  -v 144
Power reset 216
Powering down or powering up the peer node 220
Printing entered text to the output 51
process ID (kill) 74
Processor statistics 93
Progress of aysnchronous replication 151
prompt 145
  ${active} 146
  ${hostname} 146
  ${node} 146
  ${path} 146
  ${site} 146
ps 146
  -a 147
  -A 147
  -c 147
  -d 147
  -e 147
  -f 147
  -g 148
  -G 149
  -H 147
  -h 148
  -j 147
  -l 148
  -L 148
  -n 148
  -o 148
  -P 148
  -p 148
  -s 148
  -t 148
  -u 148
  -U 149
  -y 148
  -Z 148
ptree 149
  -a 149
  -c 149
  PID | <user> 149
  -z 149
Putting the startup mode for the cluster resource groups in Manual 90
Putty 13
putty 178
pwd 150

Q

Querying the NDMP (Network Data Management Protocol) service 119
Querying Unity appliances and Nexsan E-Series™ storage units using SNMP 173

R

Raw CPU percentage 178
Read-only access 249
Read-write access 249
reboot 151
Recalculating iSCSI target allocations 214
Rediscovering Nexsan storage systems connected to Unity 36
Redundancy 271
Refreshing the system cache 152, 242
reloadconfig (firewall) 55
Remote chassis power 70
Remote Control 15
Removing a Certification Authority (CA) certificate 265
Removing one or more links from an existing aggregation 105
Renaming a link 107
replication 151
Replication priority adjustment 208
Replication settings 151
Reporting IOPS metrics per client and per share 182
Reporting IOPS metrics per iSCSI initiator 182
Reporting metrics for the NFS server 182
Reporting metrics on the file system main memory cache 181
Reporting processor statistics in tabular form 93
Requirements and guidelines for implementing LACP 272
resetcache 152
Resetting failure and predicted failure flags on external JBODs 37
Resetting IPMI settings for Unity 69
Resetting one or more properties on a specified link 108
Resetting the IPMI password to default 212
Resetting the LDAP Client configuration 265
Resetting the Unity Storage System 267
resilver 152
Restarting specific services 157
Restarting the CIFS server 171
Restarting the LDAP Client service 267
Restarting the Web service 221
Restarting Unity or one of its controller nodes 216
restartldapclient 242
rg1
  clustering 43
rg2
  clustering 43
Rotating log entries 78
route 153, 242
  add 154
  change 154
  delete 154
  -f 153
  flush 154
  get 154
  monitor 154
  -n 154
  -p 154
  -q 154
  show 154
  -v 154
Routing table 153, 165
Run a command
  fcinfo 226
  groupadd 228
  ifconfig 229
  iostat 229
  ipmitool 230
  modgid 232
  nestpool clear 233
  nestpool iostat 233
  nestpool status 234
  nfs 235
  nic 236
  nscacherestart 237
  nstusermaps 240
  restartldapclient 242
  route 242
  sasinfo 243
  showmount 244
  showroutes 245
  smbrestart 245
  useradd 246
Running NST trace scripts 181
Running system commands 221

S

sasinfo 243
Scripts for traces 181
Secondary network connection 153
Secure Hash Algorithm 160
Secure Shell connection 13
sendlogs
  callhome 25
Sensor readings 70
sensors 155
services 157
setdefaultdomain 158
  <domain name> 159
  <domain> 277
  -d 158
  -s 158
setip 159
Setting a space usage quota on a share for a user and/or group 257
Setting ACLs on file systems 266
Setting an IP address for the Update

Server 212
Setting disk heartbeats 48
Setting IP-based access restrictions on a share 249
Setting IP-based restrictions on a CIFS file systems 249
Setting IP-based restrictions on an NFS file systems 252
Setting one or more properties on the specified link 108
Setting property values for a file sharing protocol 128
Setting source-based routing rules 100
Setting the Controller resource nodes to maintenance mode 90
Setting the current NDMP service variables and properties 119
Setting the domain name used for NIS integration 49
Setting the host name 61
Setting the IPMI password 211
Setting the LDAP Client configuration 265
Setting the maximum number of concurrent replications per controller 208
Setting the maximum version for NFS 101
Setting the NFS version 4 (NFSv4) domain 101
Setting the system date and time 46, 225
Setting the type of terminal connection 178
Setting user quotas on shares 192
Setting various properties of the pool or file system data 44
sha256sum 160
<file name> 160
Share access using FTP 57
Share permissions 17
shareacl 160, 278
-a 162
-c append 161
-c deleteindex 161
-c get 161
-c help 162
-c insert 161
-c replaceall 161
-c resetall 161
-c shares 161
-d 163
-f 163
-g 162
-i 162
-p 162
-s 162
-u 162
shares 164
SHH hosts 25
show
clustering 42
maintenance 90
Show event flags 53
Showing ACLs on file systems 266
Showing APAL status 194
Showing current LDAP client information 263
Showing information for Fibre Channel targets connected to HBA ports 116, 237
showmount 164, 244
<host name> 165
-a 164
-d 164
-e 165
showroutes 165, 245
shutdown 166
Shutting down the controller node 166
Shutting down Unity or one of its controller nodes 217
siteinfo 166
-c change 167
-c show 167
smbadm 167
add-member 168
create 168
delete 168
disable-user 168
enable-user 168
get 168
-h 168
join -u 168
join -w 168
list 168
remove-member 169
rename 169
set 169
show 169
smbrestart 171, 245
smbserver 171
-c extended_requests 172
-c setv12 172
-c setv21 172
-c show 172
-h 172
idmap_mapping_mode 172
krb5 172
-x 172
SMTP 137
SNMP 173, 175-176, 268, 279, 292, 295, 297
SNMP menu 173
snmpadm 173
snmpproperty 175
-c get 175
-c list 175
-c set 175
snmptosyslog 175
SSH client 13
start
callhome 24
Starting the nxcmd ommand line interface 136
Starting Unity network configuration

utility 159
startservice (firewall) 55
Statistics for network interfaces 113
status
autolog 22
callhome 24
firewall 55
nstpool 123
nstsharectl 128
Steps to integrate NIS 277
stop
callhome 24
Stopping a running process 74
Stopping specific services 157
stopservice (firewall) 55
Storage enclosure ID 28
svc 176
disable 177
enable 177, 278
restart 177
show 176
Switching between DHCP and Static IP addressing for the IPMI interface 211
Syntax for nxadmin CLI commands 17
System performance 140, 142
System prompt change 145
system sensor information 155

T

TCP port 55, 227
term 178
show 178
Terminating a running process 74
test
callhome 25
Testing the reachability of a host on the network 142
time
autolog 22
top 178
<number> 180
-a 179
-b, -n 179
-C 179
-c 179
-d 180
-I 179
-i 179
-m 180
-o 180
-q 179
-S 179
-s 180
-T 179
-t 179
-u 180
-U 180
-v 180
trace 181
-a 182
arcstat arguments 182
arcstat field definitions 182
-c help 181
-c run 181
-c show 181
cifssvrtop arguments 183
cifssvrtop field definitions 184
iscsiop arguments 184
iscsiop field definitions 184
nfssvrtop arguments 184
nfssvrtop field descriptions 185
traceroute 186
-a 186
-A 187
-c 187
-d 187
-F 187
-f 187
-g 188
host 188
-I 187
-i 188
-l 187
-L 188
-m 188
-n 187
-P 188
-p 188
-Q 188
-q 189
-r 188
-S 187
-s 189
-t 189
-V 187
-w 189
-x 187
Troubleshooting LACP issues 273

U

UDP port 54, 227
ui
-c 190
ui, reverting to legacy 189
ui, switching to new 189
UID 232, 246
modgid 92
moduid 93
useradd 191
Unable to access a CIFS share 171
Understanding link aggregation 272
UNIX users that authenticate through NIS 277

update
autolog 22
update count (iostat) 67
updatesettings (ipmi) 69
Updating stored configuration settings for remote the Unity Storage Systems 166
Updating the CIFS server to version 1.2 172
Updating the CIFS server to version 2.1 172
Uploading a Certification Authority (CA) certificate 264
uptime 190
User access permissions 249
useradd 190, 246
<name> 191
UID 191
userdel 191
<name> 191
userquota 192
-c get 192
-c set 192
-h 193
users (listug) 78
Using the Fault Repair menu 247
Using the nxadmin CLI's command-based shell 17
Using the Shut down and Reboot menu 216
Using the System menu 268

V

Viewing all active services 176
Viewing aysnchronous replication progress 151
Viewing chassis/system sensor information 155
Viewing Fibre Channel clients 77
Viewing Fibre Channel statistics 54
Viewing I/O statistics for a specific storage pool 123
Viewing instructions on using nstusermaps for LDAP to AD mapping 266
Viewing LEDS for chassis and drives 75
Viewing replication settings 151
Viewing running processes 147
Viewing service dependencies 157
Viewing service status 157
Viewing shares 164
Viewing status of file-sharing protocols 128
Viewing summary information and statistics for system virtual memory 193
Viewing the name of NIS server 198
Viewing the number of active users 190
Viewing the route (path) that an IP packet follows to another Internet host 186
Viewing the routes currently configured on all (active) network interfaces 165
Viewing the system performance 142
Viewing the system uptime 190
Viewing the top 30 processes being managed by NestOS 178
Viewing the user currently logged in to Unity 194
Viewing Unity appliances and Nexsan E-Series™ storage units using SNMP 173
Viewing UNIX/Linux clients that have remotely mounted an NFS share 164
Viewing user quotas on shares 192
Virtual memory 193
vmstat 193
-i 193
-p 193
-q 193
-s 193
-S 193
-T 193
vssadm 194
show-apal 194
vt102 178

W

whoami 194
World Wide Name (WWN) 117, 195, 238
Write protection 89
Writing the date and time to standard output 46, 225

X

xterm-color 178

Y

ypcat 196
-d 197
-k 197, 278
-t 197
-x 197
ypinit 197
-c 197
–c 278
-m 197
-s 197
ypwhich 198
<host> 198
-d 198
-m 198
-t 198
-Vn 198

-x 198



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: 20260323AM103833

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