i series manager
CLI User Manual

Table of Contents

Chapter 1 Introduction

Chapter 2 i series Operations

Chapter 3 Volume Operations

Chapter 4 Monitoring & Statistics

Chapter 5 Command Line Interface Reference

Index

List of Figures

List of Tables

Chapter 1
Introduction

This chapter provides an overview of the i series.

iSCSI Overview

iSCSI transmits native SCSI commands and data over the TCP/IP protocol stack. iSCSI transfers and stores SCSI commands and data at any iSCSI enabled storage location with access to a LAN, MAN, WAN or the Internet. iSCSI enables the creation of high performance IP-SANs.

iSCSI has many benefits including:

- Can use existing Ethernet cabling and existing network elements.
- Uses common TCP/IP for global connectivity.
- Leverages the existing expertise of network administrators, integrators and support services.

iSCSI Initiator and Targets

iSCSI initiators establish TCP connections with iSCSI targets. Data can be transferred via iSCSI when an iSCSI initiator establishes a TCP connection with an iSCSI target.

- The iSCSI initiator resides in the host computer.
- The iSCSI target resides in the i series.
- iSCSI initiators and targets have a *World Wide Unique Identifier* (WWUI) of up to 223 free form characters, e.g. www.nexsan.switch1.target1.

Portals

To enable iSCSI communications over TCP, the system administrator must configure portals during the initial i series configuration. A portal is comprised of both an IP address and its assigned TCP port. Each configured portal automatically becomes an iSCSI access point to each target that exists in the i series. Typically, there are few portals and many targets.

Targets and LUNs

An iSCSI initiator can access, read and write to a disk only after the disk is “exposed”. An exposed disk is a disk that has been attached to a target and assigned a LUN (*Logical Unit Number)*. An exposed disk can be accessed by any iSCSI initiator unless ACL restrictions are configured.

When creating iSCSI targets, the user administrator assigns an alias and name for each one. The alias is an internal identifier for the system administrator. The name is the WWUI used to connect initiators to the target.

Note:
When creating targets, keep in mind that:

- ✓ *Each target can have multiple LUNs.*
- ✓ *Each target should be exposed by only one i series in a cluster.*
- ✓ *Each target can be accessed by multiple hosts*

There are two ways to expose a disk:

1. Create a new target and assign a LUN in the same process. For more information see ***Exposing Disks and Creating a New Target in Chapter 4.***
2. Assign LUNs to previously created targets. For more information, see ***Creating a New Stand-Alone Target in Chapter 4.***

Example:

In Figure 1-1 Vol 1 is exposed via Target 1 and is accessible to any iSCSI initiator via either portal (IP1, 3260) or (IP2, 3260). Likewise, Vol 2 is exposed via Target 2, Vol 3 and Vol 4 are exposed via Target 3.

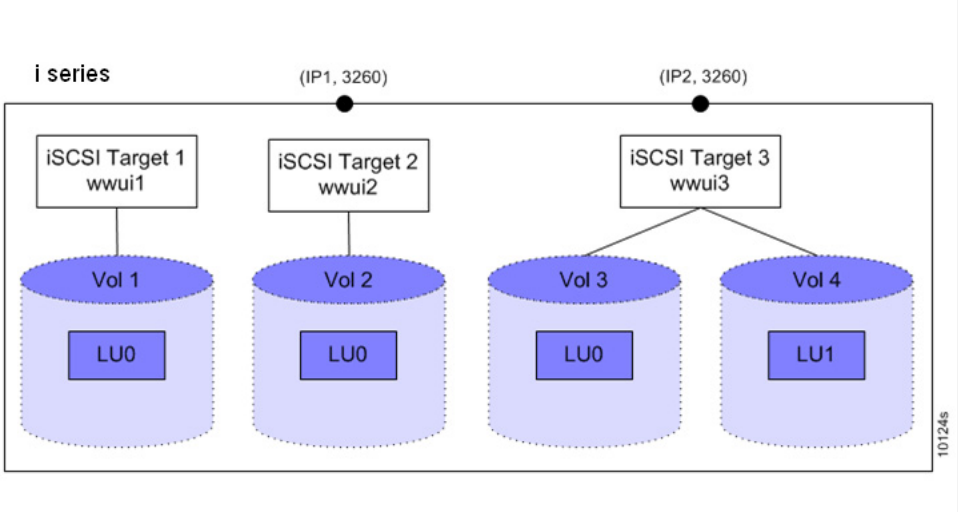


Figure 1-1. iSCSI Target Access

Discovery Methods

The i series supports three types of discovery: iSCSI Discovery, SLP and iSNS.

iSCSI Discovery

In an iSCSI discovery session the user administrator configures an IP and port of the iSCSI target in the initiator. The initiator discovers all applicable targets and LUNs.

SLP

SLP (Service Location Protocol) is a common broadcast-based discovery mechanism that uses agents. The i series acts as an SLP Service Agent (SA) and advertises its iSCSI service. The initiator identifies the i series and discovers the i series's targets.

iSNS

iSNS is a client/server protocol designed for compatibility with FC's Simple Name Server (SNS). Once an iSNS server is located (either through DHCP or SLP), discovery can take place without the need for broadcasts. iSNS enables iSCSI initiators in the IP-SAN to locate the i series targets automatically.

iSCSI Security

No matter what discovery method is used, ACL (Access Control List) allows only those targets that are defined as available to be accessed. To allow selective iSCSI initiator access to iSCSI target disks, the i series uses *identities* to define pools of initiators. An identity is a user-defined list of iSCSI initiators. Attaching an identity to a target restricts its access to the list of initiators defined by that identity.

Note:
When planning and creating identities, keep in mind that:

- ✓ *Each identity can contain one or more iSCSI initiators.*
- ✓ *Each identity can be assigned one or both login authentication methods (CHAP, SRP).*
- ✓ *Each identity can be attached to more than one target.*
- ✓ *Each target is first automatically coupled to a default read-write un-authenticated access identity and therefore can be accessed by everyone.*

Each target can have more than one identity. The order of the identities is important. The first match is used, not the best match.

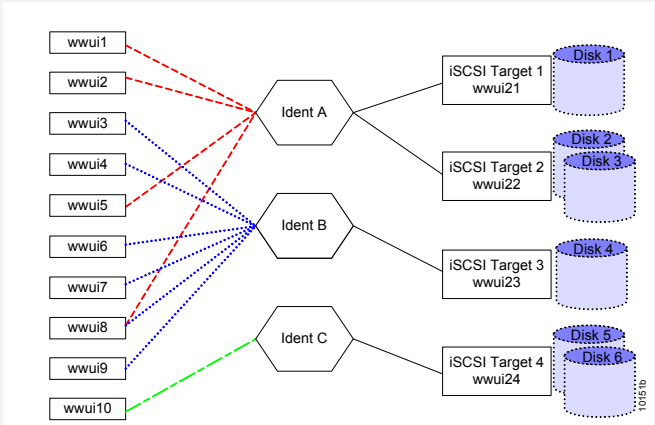
Note:
If you are working with an iSNS server, all hosts are able to see all targets but only those hosts with access rights are able to connect to the authorized targets.

Example:

In Figure 1-2 identities are coupled with iSCSI targets to limit iSCSI initiator access to a target's underlying disks. An identity can be used with more than one target and each target can have more than one identity.

- Identity A is coupled with both Targets 1 and 2.
- Identity B is coupled with Target 3.
- Identity C is coupled with Target 4.

As a result, each iSCSI initiator has access to the following disks:



iSCSI Initiator	Accessible Volumes					
	Disk 1	Disk 2	Disk 3	Disk 4	Disk 5	Disk 6
WWUI1	√	√	√			
WWUI2	√	√	√			
WWUI3				√		
WWUI4				√		
WWUI5	√	√	√			
WWUI6				√		
WWUI7						
WWUI8	√	√	√	√		
WWUI9				√		
WWUI10					√	√

Figure 1-2. Identities Coupled with Targets

When you assign an identity to a target, you give the identity a *position.* A position is an identity's rank in the i series scan for an "*iSCSI initiator – identity match*". When the i series scans the list of identities coupled with a target, it starts with the highest position and stops with the first match. After matching, the initiator is granted the identity's access rights.

An identity can be connected to more than one target to provide the same pre-defined list of initiators for each target.

Example:

In Figure 1-3, the default identities for Target 1 and Target 2 have been modified to not accessible (NA) for all initiators.

- Target 1 is coupled with Identity A with read-write (RW) access to Identity A's list of iSCSI initiators (WWUI1).
- Target 2 is coupled with Identity B with read-write (RW) access to Identity B's list of iSCSI initiators (WWUI2).

When iSCSI initiator WWUI1 logs in to Target 1, the i series first scans Identity A and finds the initiator listed there. The scan stops and the initiator is granted read-write access to Target 1's underlying disk, Disk 1.

If iSCSI initiator WWUI1 tries to login to Target 2, the i series first scans Identity B. It does not find the initiator listed so it continues to scan the next identity, the default identity. The default identity implicitly lists all iSCSI initiators, including WWUI1. However, the scan stops and the initiator is denied access to Target 2's underlying disks (Vol 2 and Vol 3), since the default identity is configured as not accessible.

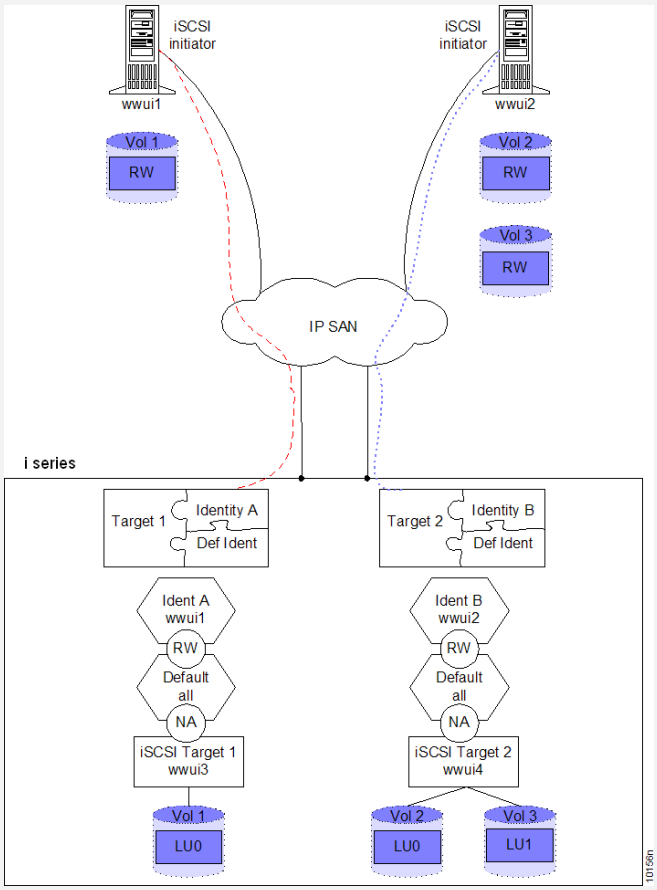


Figure 1-3. Default Identities

Access Rights

When you couple an identity and a target, you assign access rights: read-write (RW), read-only (RO) or not accessible (NA). The access rights are per identity-target pair.

- An identity can be coupled with multiple targets, each time with different access rights.
- A target can have multiple identities, each with different access rights.

Note:
If you add or modify Identities on a target after its disks have been exposed, the access rights will take effect only at the next login for each iSCSI initiator.

Example:

In Figure 1-4 Identity A is coupled with both Target 1 and Target 2.

- The pair Identity A – Target 1 is assigned iSCSI initiator read-write access to Target 1 disks.
- However, the pair Identity A – Target 2, is assigned iSCSI initiator read-only access to Target 2 disks.

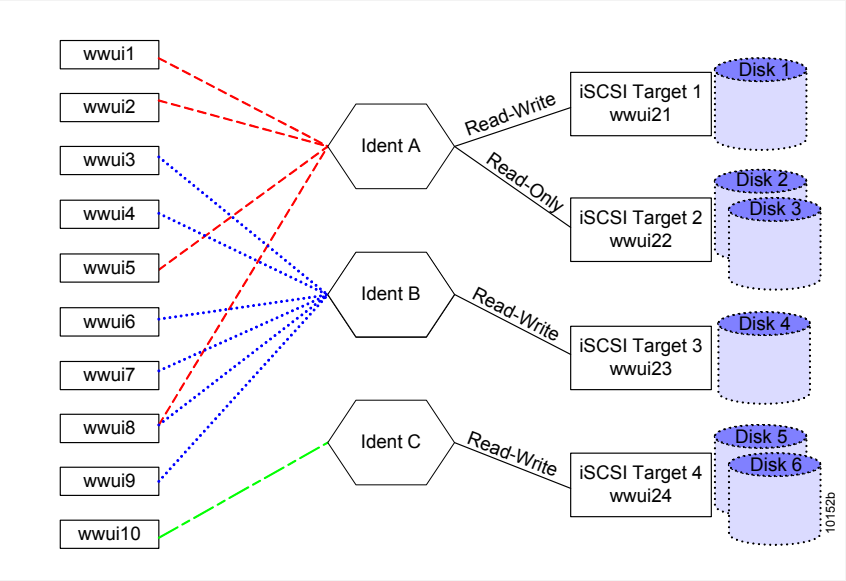


Figure 1-4. Access Rights per Identity-Target Pair

Target and Initiator Authentication

The i series supports the authentication methods CHAP and SRP for the iSCSI initiator. The credentials for CHAP and SRP are the combination of user name + password.

CHAP

CHAP is a protocol that is used to authenticate the peer of a connection and is based upon the peers sharing a secret (a security key that is similar to a password). The target and the initiator authenticate each other.

The i series supports two way CHAP authentication. The target authenticates the initiator and the initiator can authenticate the target (it is up to the initiator to request target authentication). A separate secret can be set for each target and for each initiator in the storage area network (SAN).

Note:
An authentication method is assigned per identity and not per iSCSI initiator.

- ✓ *An identity can be assigned an additional authentication method.*
- ✓ *If no authentication method is assigned, all listed iSCSI initiators in an identity will have un-authenticated login access rights.*

When an iSCSI initiator logs in to a target, its WWUI is checked against the identity initiator list. After the iSCSI initiator passes the identity stage, if credentials are configured, the iSCSI initiator must authenticate itself. The credentials list is checked for the iSCSI initiator's user name + password. The list can contain:

- A separate user name + password for each initiator.

Note:
There is no strict link between an initiator from the initiator names in the identity and a specific username + password from the credentials of the identity

- A few user name + password pairs common to a few initiators
- A single user name + password for all initiators in the identity.

Example:

In Figure 1-5 there are:

- Six iSCSI initiators in Identity B
- Only four user name + password credentials. Certain initiators have the same user name + password configured on them.

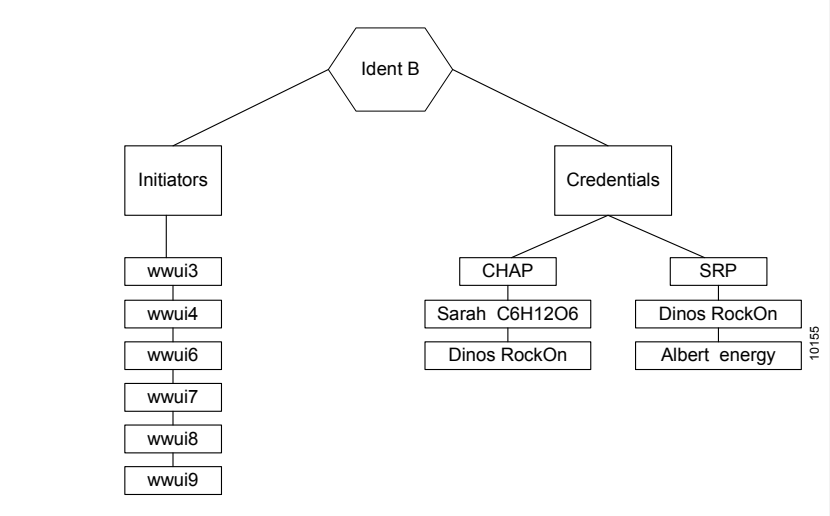


Figure 1-5. Identity with iSCSI Initiators and Credentials

Configuring a RADIUS Server

When a RADIUS Server exists in the network, you can use it to manage the i series. When CHAP user names and passwords are configured on the network in a RADIUS server, the RADIUS server can be configured on the i series to direct a CHAP challenge to the RADIUS server and eliminate the need to configure all user name + password pairs on the i series. This decreases configuration time and increase overall network security.

Example:

In Figure 1-6, a CHAP authentication challenge is sent to the i series.
The i series first checks if the user name is set for RADIUS authentication.

- If it is, the CHAP challenge is passed on to the RADIUS server.
- If it is not, the user name and password are compared against the pairs configured in the i series.

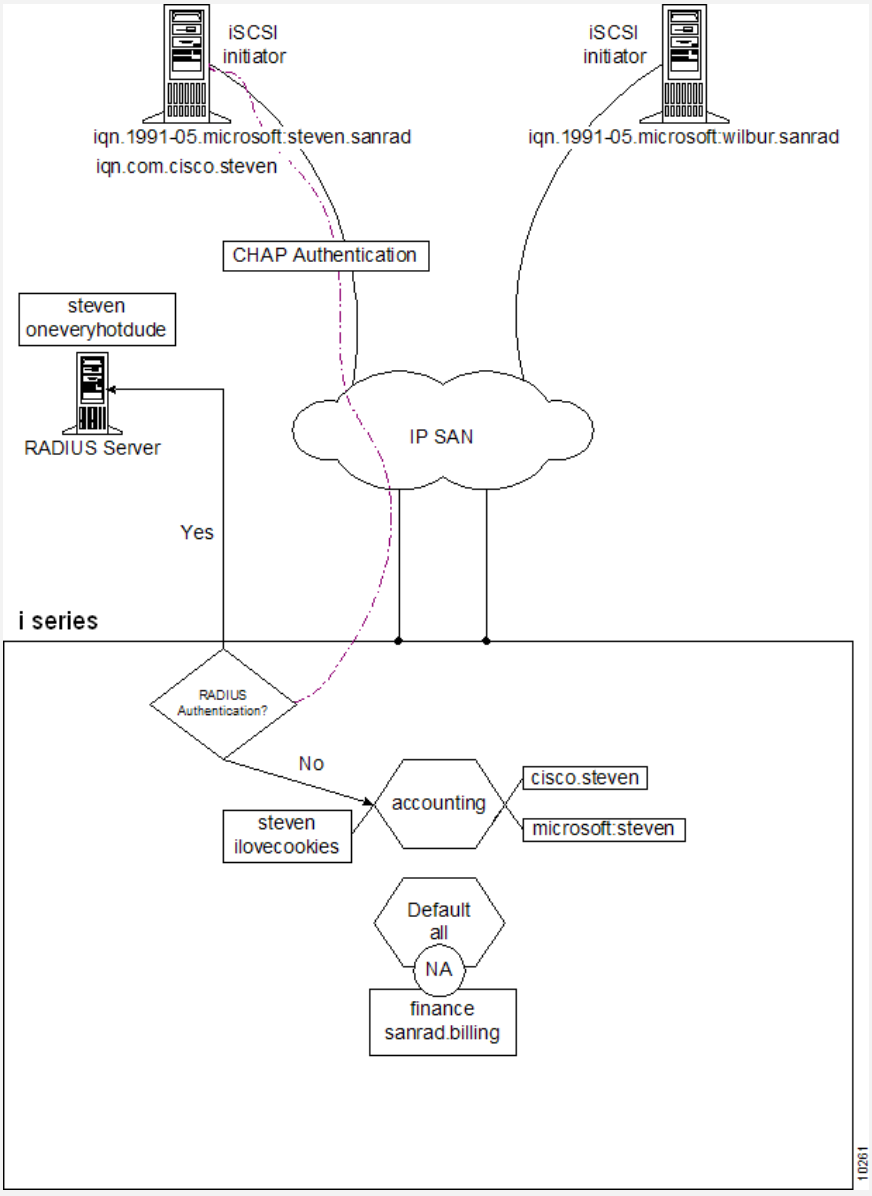


Figure 1-6. Sending a CHAP Authentication Challenge

i series Cluster

A cluster is made from two i series that are attached to the same storage element(s). In a cluster, the i series interact in a peer-to-peer fashion with the other *neighbor* i series. In this active-active configuration, neither i series is configured to act as the master i series. All disks are accessible to each i series and can be exposed on either i series. This allows you to split the load between the two i series. Clusters provide high availability in the event of i series failover.

Each network port on the i series is configured with its own:

- active, or functioning, IP addresses
- inactive, or dormant, neighbor IP addresses.

When one i series goes off-line, the remaining i series activates its neighbor's IP addresses. The hosts continue to access disk targets through the same IP address without sensing that their 'regular' i series has gone offline or noticing any impact on storage performance.

Note:
All LUNs in a RAID controller must be simultaneously exposed through all ports connected to both i series.

Example

In Figure 1-7, two i series are connected to one FC JBOD. From the four physical disks, two virtual disks have been created, both equally accessible to both i series.

i series are both fully operational in a cluster. No i series must sit in stand-by mode.

Both i series are also connected to two hosts via the IP SAN. The disk exposure of the two virtual disks is balanced equally between the two i series for best resource utilization. Vol 1 is exposed via i series 1 to Host 1, represented by the orange dashed line. Vol 2 is exposed via i series 2 to Host 2, represented by the purple dotted line.

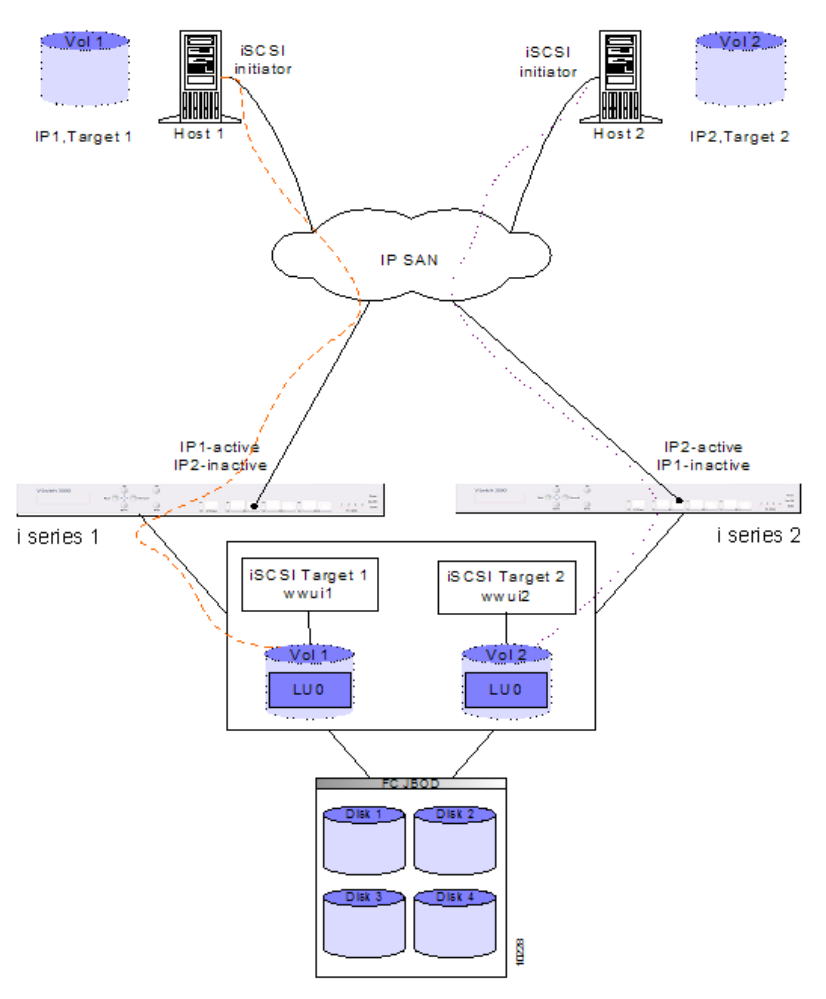


Figure 1-7. i series Cluster Configuration

Example

In Figure 1-8, i series 1 has gone off-line. i series 2 activates i series 1's IP address and takes over exposure of Disk 1 to Host 1, represented by the orange dashed line.

Host 1 continues to access Disk 1 through the same IP address as it did before its i series went off-line. Host 1 has no way of knowing that its regular i series is off-line.

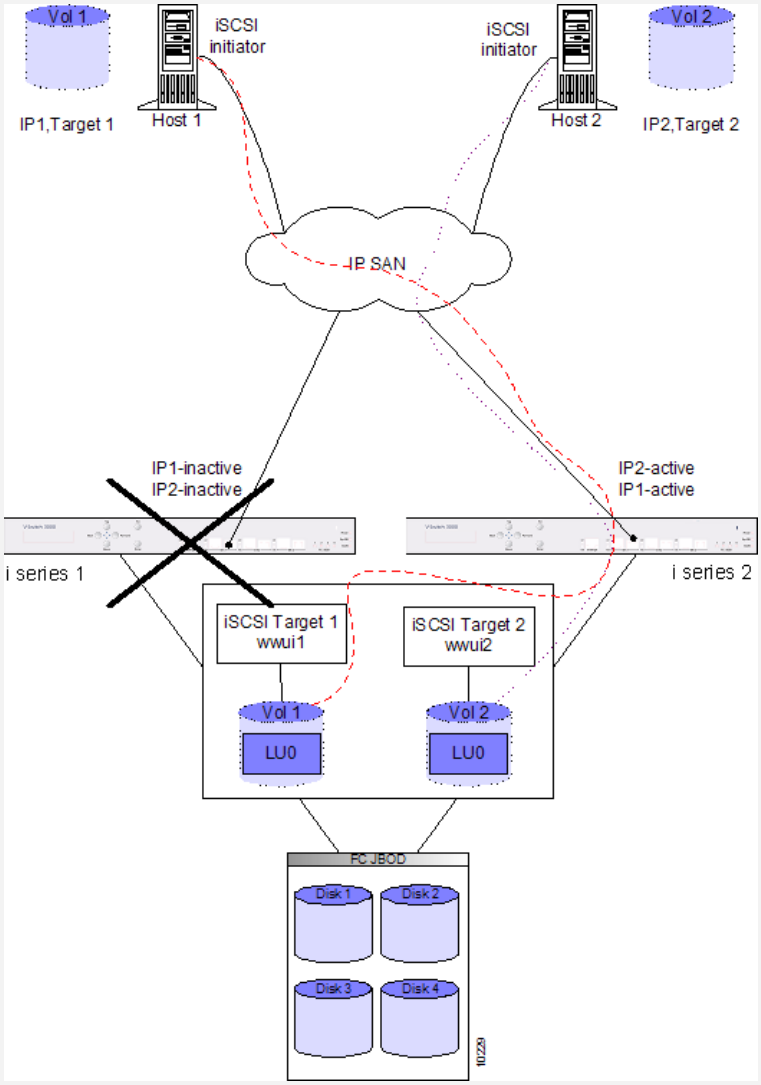


Figure 1-8. Re-Routing Storage Access with Off-line i series

Maintaining Cluster Communications

Once a i series is configured as a cluster, it begins sending out a regular *keep alive* signal to its neighbor. The i series also begins listening for the keep alive signal from its neighbor. The keep alive signal is transmitted through all connecting paths between each neighbor. Thus, if one path fails, the remaining path(s) will still carry the keep alive signal.

If a specified time period passes without a keep alive signal from the neighbor, a *suspicious interval*, measured in seconds, is entered. The i series suspects that its neighbor has gone off-line and begins preparing to activate the neighbor IP addresses to take over disk exposure.

If a keep alive signal is received during the suspicious interval, the timer is reset and the i series continues to function as usual. If a keep alive signal is not received by the end of the suspicious interval, a *faulty interval* is entered. At the end of the faulty interval, the neighboring i series is considered off-line, the failover process is initiated and the on-line i series actives the neighbor IP addresses and takes over disk exposure.

Virtualization

The i series allows you to perform volume virtualization. The i series "*sees*" a collection of storage devices. Each device can be either a physical disk (part of a JBOD) or a LUN (part of RAID).

With the i series, you can:

- Take a resource and attach it via the iSCSI network to the host.
- Build virtual volumes at the network layer.

Volumes Types

i series manager enables you to configure physical volumes into the following types of virtual volumes:

- Transparent
- Concatenated
- Mirrored
- Striped
- Mirrored over Concatenated
- Mirrored over Striped (RAID 0 +1)
- Striped over Mirrored (RAID 10)

There are several ways to create volumes:

1. Take a full disk and expose it as one volume.
2. Create volumes by partitioning disk into subdisks.
3. Create a volume by spanning multiple physical disks or subdisks (e.g. take two disks/subdisks and create mirror).

Transparent Volumes

The primary use for transparent volumes is for attaching tape devices directly to the i series. You can take a physical disk/tape and convert it to a transparent volume ready for direct host exposure.

Note:
Transparent volumes cannot be used in further volume hierarchies

Subdisks (LUN Carving)

You can partition a disk to create a subdisk that can be accessed as a separate virtual volume. You can create one or more subdisks on a physical disk. The subdisks can be used for creating concatenated, striped and mirrored virtual volumes. A subdisk has a start block and end block address within the disk in hexadecimal form.

Example:

In Figure 1-9, the disk is partitioned into subdisks.

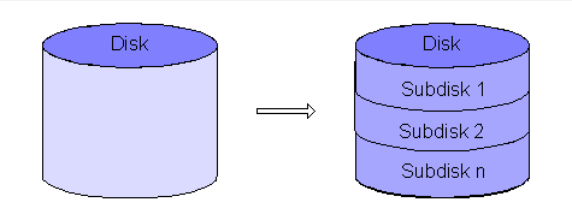


Figure 1-9. Concatenated Volume Block Distribution

Concatenated Volumes

To accommodate large volumes of data or to best utilize small volumes spread over several disks, you can concatenate physical volumes or subdisks across storage devices to create a larger virtual volume. Concatenated volumes can also be created on virtual volumes as part of a volume hierarchy.

Example:

In Figure 1-10, the volume is divided into two equitable chunks to be mapped across two disks.
Data blocks 1 – 4 are mapped to Disk 1, sectors 13 – 16.
Data blocks 5 – 8 are mapped to Disk 2, sectors 13 – 16.

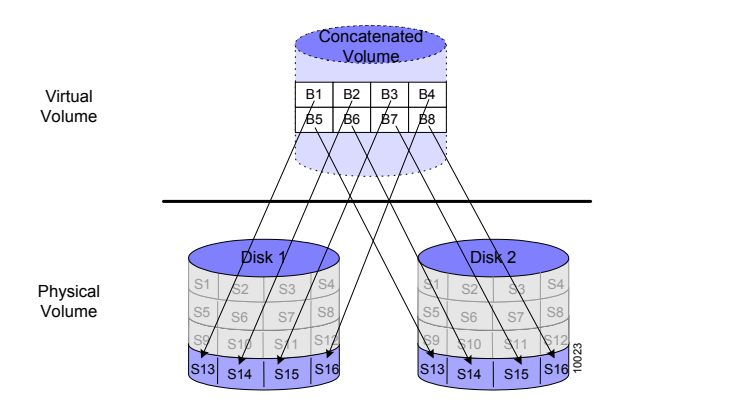


Figure 1-10. Concatenated Volume Block Distribution

Striped Volumes

A striped volume has data written equitably across two or more identical size disks, subdisks or virtual volumes to provide higher read/write rates.

Subdisks within a striped volume need to be on different disks to realize the benefits of striping.

Example

In Figure 1-11, data block 1 is mapped to sector 1 of Disk 1; data block 2 is mapped to sector 1 of Disk 2. Each subsequent data block is then written alternately between sectors on Disks 1 and 2. The striped unit size in this example is one block.

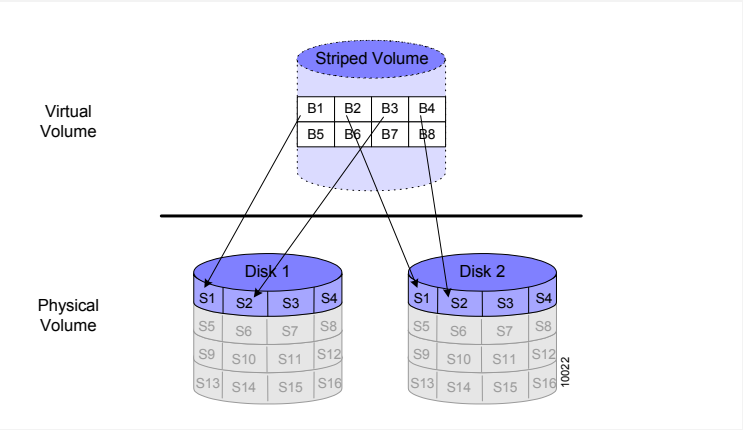


Figure 1-11. Striped Volume Block Distribution

Mirrored Volumes

A mirrored volume is synchronously written into multiple identical size volumes. The read load is balanced between each copy. Mirrored volumes can be created from two to four disks, subdisks or virtual volumes of equal block size. The size of the mirror is determined by its smallest child volume.

Note:

- ✓ *Mirrored volumes must be located on different physical disks.*
- ✓ *To achieve higher availability, NEXSAN recommends configuring mirrored volumes onto different storage systems.*

Example

In Figure 1-12, data block 1 is mapped to both sector 5 on Disk 1 and sector 9 on Disk 2. Data block 2 is mapped to both sectors 6 on Disk 1 and sectors 10 on Disk 2.

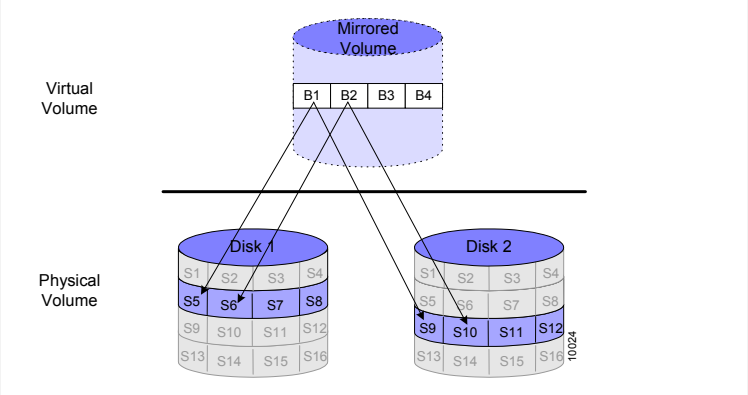


Figure 1-12. Mirrored Volume Block Distribution

RAID 10 & RAID 0+1

You can combine different volume types to create hierarchies. Combining stripe and mirror volumes gives the advantage of both high performance and data redundancy.

- **RAID 10 is striped over mirror**
  Create mirrored volumes and then create striped volumes of the mirrored volumes.
- **RAID 0+1 is mirror over striped**
  Create striped volumes and then create mirrored volumes of the striped volumes.

Example

In Figure 1-13, in the first mirrored volume, data block 1 is mapped to both block 1 on Disk 1 and block 1 on Disk 2. Data blocks 3, 5 and 7 are mapped to blocks 2, 3 and 4 on both Disks 1 and 2.

In the second mirrored volume, data block 2 is mapped to both block 1 on Disk 3 and block 1 on Disk 4. Data blocks 4, 6 and 8 are mapped to blocks 2, 3 and 4 on Disks 3 and 4.

Data blocks 1 and 2 are then compiled in a striped pattern, along with blocks 3 – 8.

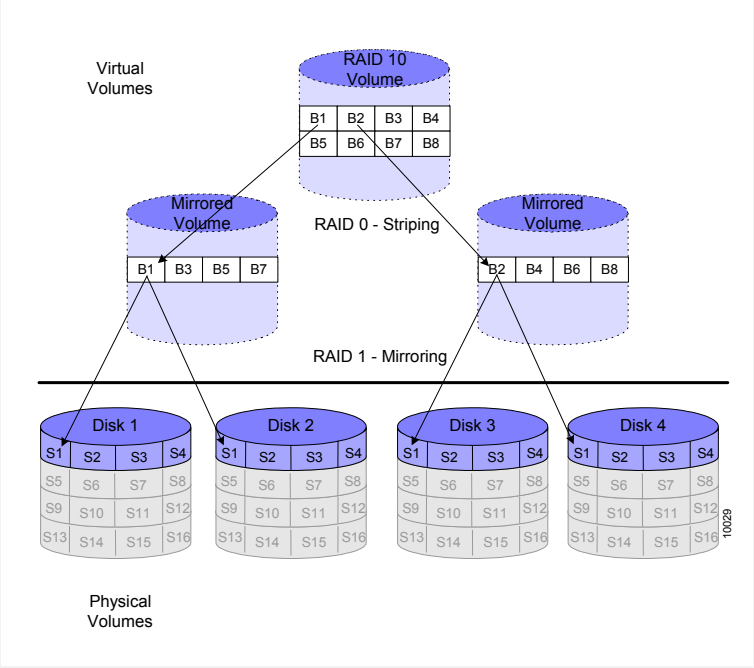


Figure 1-13. RAID 10 Volume Block Distribution

Advanced Volume Configurations

The i series supports several advanced volume operations. Each has its own advantages so it is important to understand their differences to best choose the function most appropriate for your SAN.

Copy Operations

Data can be replicated both offline and online. Offline replication is faster than online replication but both the source and destination volumes must be taken off-line which can create an interruption of service to the volume host(s).

Offline Copy

Offline copy is used to copy any source volume to any destination volume. This is done offline while both the source and destination volumes are unexposed.

Online Copy

Online data replication allows the source volume to remain online with no interruption of service to the volume host(s). Online copy is performed by adding a child to a mirror and breaking it:

Adding a Child to a Mirror

You can perform online data copy, either by increasing the number of children in a mirrored volume (Figure 1-14) or creating a mirrored copy of any other type of volume (Figure 1-15).

Since this is online data copy, the source volume does not need to be taken offline and write operations to the source volume can continue while the mirror is being created. Any data written to the volume will be included in the added child(ren).

Note:
The added child can be any type of volume, except transparent or snapshot, and it must be the same size or greater than the accessible capacity of the source volume.

Example

In Figure 1-14, a mirrored volume with two children has another child added. The mirrored volume stays at the head of the hierarchy.

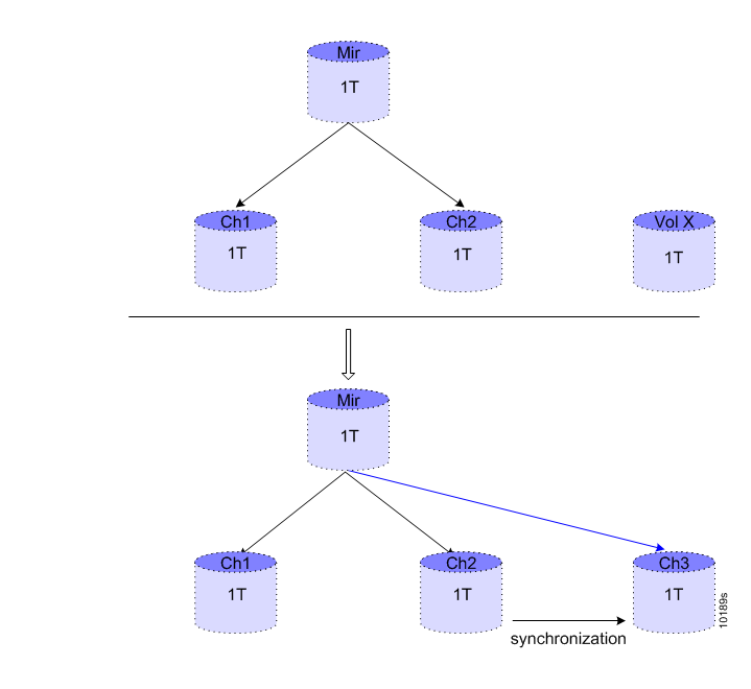


Figure 1-14. Adding Another Child to a Mirror

Example

In Figure 1-15, a concatenated volume becomes one child of a new mirrored volume. This adds a level to the hierarchy. The new mirrored volume becomes the head of the volume hierarchy. The new mirrored volume automatically assumes the LUN from the concatenated volume.

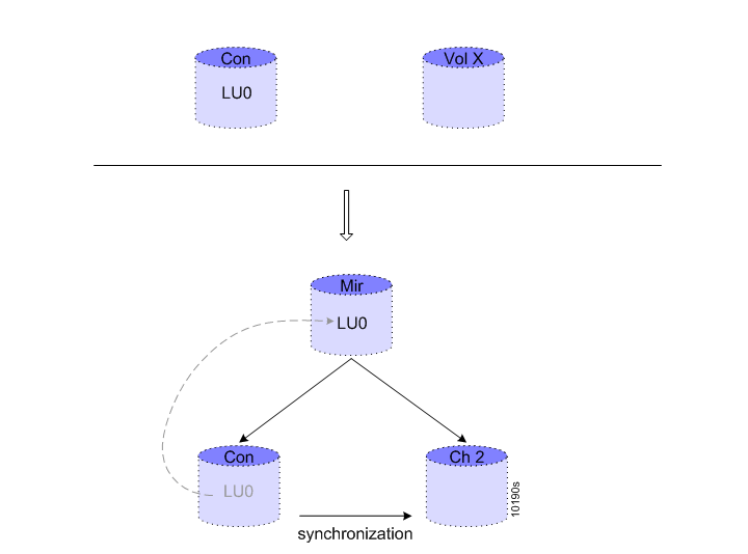


Figure 1-15. Creating a Mirror to Add Data Redundancy

Breaking Mirror Child

Breaking a child from a mirror enables the volume to be used independently. The removed child is a fully functional volume and can be exposed to any host (Figure 1-16).

Note:
The mirror volume cannot be broken while it is in the process of synchronization.

Example

In Figure 1-16, a child is removed from a mirrored volume with two children. This breaks the mirror. If the mirrored volume is exposed or attached to a LUN, the source volume retains the LUN. There is no need to reassign a LUN to the remaining source volume. All read-write operations will be executed without a break in service.

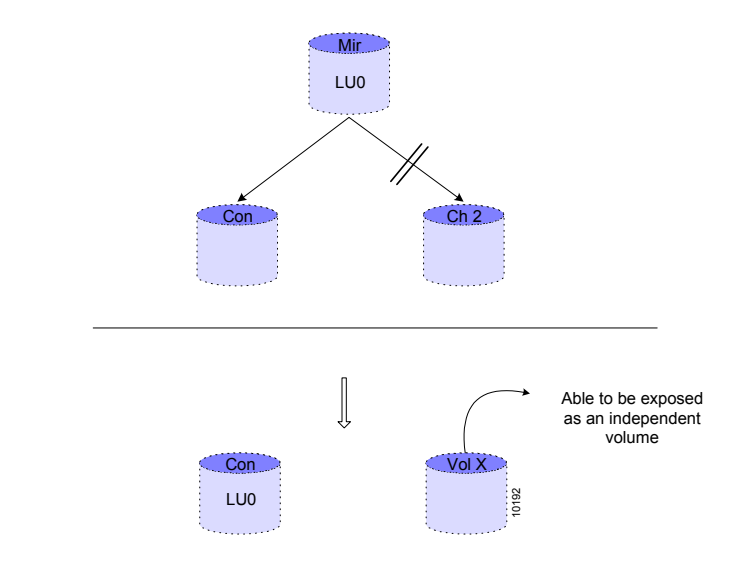


Figure 1-16. Breaking a Mirror

Snapshot Operations

Snapshots can be used for serverless backup, reducing the load on the application server. The backup copy from a snapshot is a full copy of the source volume at the time of the snapshot and adequate size must be allocated for the backup volume.

You can create a *snapshot*, a point-in-time copy, of any volume. A snapshot does not create a full copy of its source volume. It is a dynamic and dependent volume that records only changes to the source volume from the time of the snapshot's creation.

Online Copy versus Snapshot

A mirrored volume copy is a full, complete volume copy. A snapshot is only a record of changes to a volume. Because of this, its capacity can be smaller than a mirrored volume copy. Both a mirrored volume copy and a snapshot can be exposed to a host like any other volume. However, unlike a mirrored copy, a snapshot is nonfunctional if its source volume goes off-line.

Note:
A snapshot volume cannot be used to build virtual volumes.

Example

Figure 1-17, shows a source volume with its snapshot when the snapshot is first created. Initially, a snapshot is empty because there has not yet been a change in its source volume. Only when a write operation is performed on the source volume will the snapshot begin to fill up.

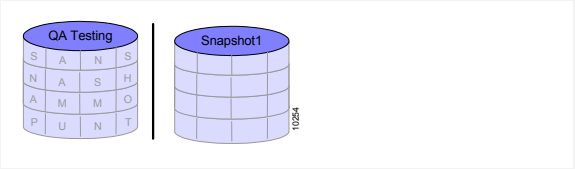


Figure 1-17. 1st Snapshot Created

Example

Figure 1-18 shows the same source and snapshot volume after a write operation to sector 1. The snapshot recorded the original data from sector 1 and then the new data is written to the source volume.

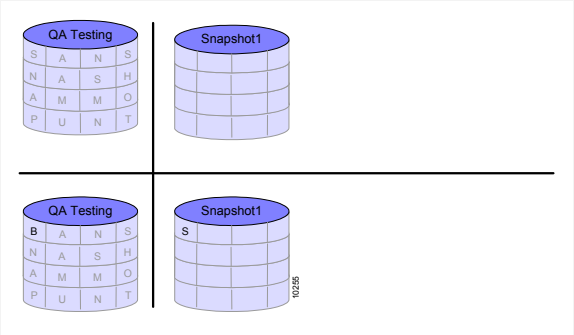


Figure 1-18. 1st Write to Source and Update to 1st Snapshot

Example

Figure 1-19, shows the creation of a second snapshot and a second write operation to the source volume.

Figure 1-19. 2nd Snapshot Created, Write to Source and Update to 1st Snapshot

Example

Figure 1-20, shows the creation of a third snapshot and a third write operation to the source volume. Both Snapshot 1 and Snapshot 2 are updated with the changes to the source volume.

The more active the write operations are to a source volume, the larger its snapshots will need to be. NEXSAN requires a beginning snapshot volume of at least one percent of the size of its source volume. A snapshot volume can be resized to accommodate a growing capacity need. When a snapshot volume's predefined *load threshold* is exceeded, an alert is set to resize the volume. When exposed, a snapshot must be exposed on the same i series as its source volume.

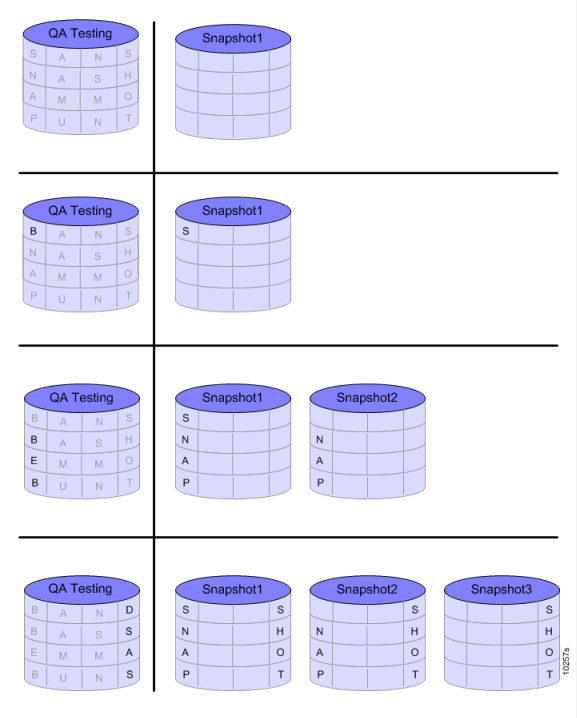


Figure 1-20. 3rd Snapshot Created, Write to Source and Update to 1st & 2nd Snapshot

Volume Resize

You can expand any virtual volume by expanding its child volumes.

Example

In Figure 1-21, Mir is a mirrored volume with an allocated capacity of one terabyte (1T). We want to '*Resize'* the mirror to two terabytes. This is done as follows:

A: A simple volume of 1 terabyte is added to CH2 and the two volumes are concatenated (XSim2).

B: A simple volume of 1 terabyte is added to CH1 and the two volumes are concatenated (XSim1).

C: The original mirror volume is resized to 2 terabytes.

Note:
Until the original mirror volume Mir is 'resized' to two terabytes, the accessible volume remains unchanged (as shown in B).

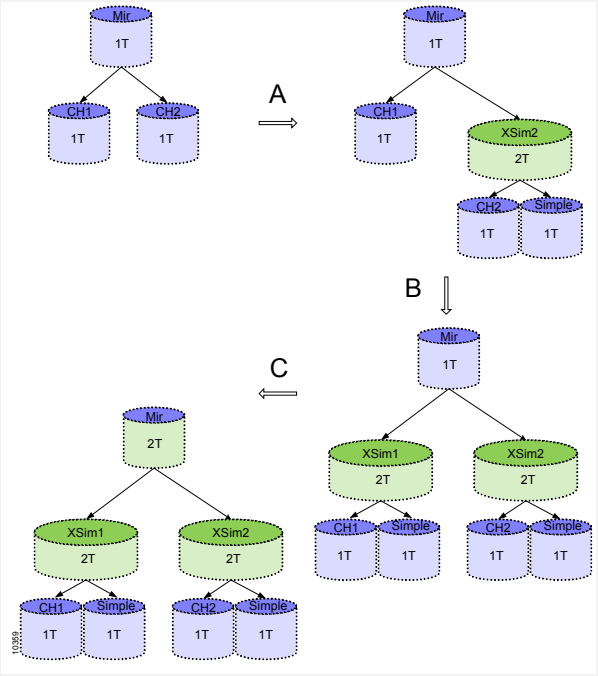


Figure 1-21. Resizing a Volume

Chapter 2
i series Operations

Initial i series Configuration

After powering up the i series, the first thing you must do is to configure its management parameters. This can be done via telnet, SSH, or via a console or dumb terminal to open a direct connection with the i series's RS232 console port.

The i series has a default IP Address of 10.11.12.123. This allows you to set initial startup parameters via a telnet session.

Management IP Address

The management IP address can be set via:

- RS-232 port
- Telnet session

Telnet/SSH Connection

To initialize the i series via telnet/SSH session:

1. Change your computer's IP Address to anything on the same subnet 10.11.12.*
2. Connect to the management port on the i series.
3. Telnet to 10.11.12.123.
4. Enter Username and Password: **admin**.

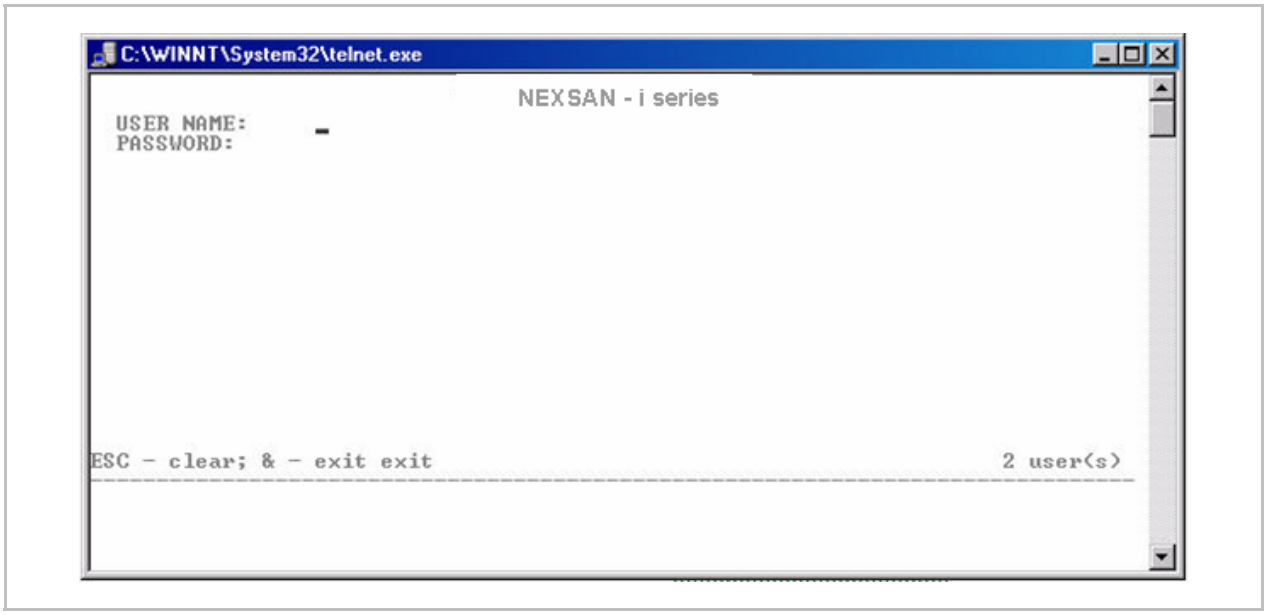


Figure 2-1. T elnet/SSH Session

You will be asked to accept or change the default values for the following:

- Management IP Address
- Management IP Mask
- Device name
- Management port (mgnt or eth1)

RS232 Serial Connection

To initialize the i series via an RS-232 serial connection:

- Connect the cable to the appropriate port on the management server, and open a Terminal session. Set the following parameters in the terminal:

Parameter	System Requirement
CONFIG SERIAL PORT	COMX (ACCORDING TO YOUR PHYSICAL PORT CONNECTION)
BITS PER SECOND	115200
DATA BITS	8
PARITY	NONE
STOP BITS	1
FLOW CONTROL	NONE
EMULATION	AUTO DETECT

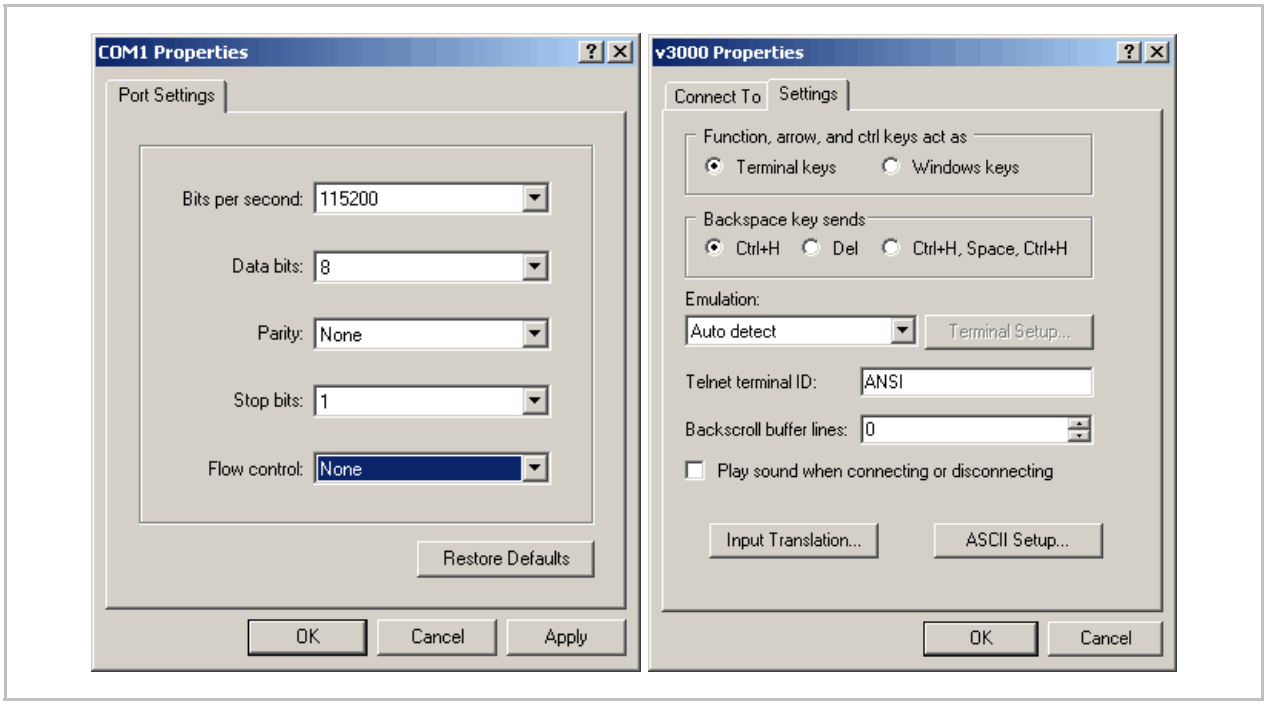


Figure 2-2. Terminal Properties

Configuring Management Parameters

After logging in to the i series, you can change the general management parameters and Telnet communications port as well as add user login profiles and hardware temperature scale.

Set Device Parameters

You can change i series management parameters (IP address and mask) or UDP port number as well as include details of whom to contact in the event of technical difficulties and which read/write communities to send traps to. Use the CLI command **device set** to add or change management parameters. This command will not appear in the CLI menu until the i series is initialized.

Use the CLI command **device set** to add or change management parameters. This command will not appear in the CLI menu until the i series is initialized.

device set

Use the CLI command **device set** to add or change management parameters. This command will not appear in the CLI menu until the i series is initialized.

device set

Switch	Definition	Type	Values/Remarks
-C	CONTACT PERSON IN THE EVENT OF A SYSTEM MALFUNCTION	OPTIONAL[1]	ASCII STRING
-D	LOCAL DATE	OPTIONAL[1]	DD/MM/YYYY
-ID	I SERIES ID IN A CLUSTER	OPTIONAL[1]	0, 1* *EACH I SERIES MUST HAVE A DIFFERENT ID
-IF	MANAGEMENT PORT ALIAS	OPTIONAL[1]	ETH1: (DEFAULT FOR I SERIES 2000) MGNT: (DEFAULT FOR I SERIES 3000, 38000, NOT AVAILABLE FOR I SERIES 2000)
-IM	MANAGEMENT PORT IP MASK	OPTIONAL[1]	IP NETWORK MASK 255.255.255.0
-IP	MANAGEMENT PORT IP ADDRESS	OPTIONAL[1]	IP ADDRESS
-LOC	LOCATION OF THE CONTACT PERSON	OPTIONAL[1]	ASCII STRING
-N	I SERIES NAME	OPTIONAL[1]	ASCII STRING

Switch	Definition	Type	Values/Remarks
-P	PORT THROUGH WHICH ALL SNMP COMMUNICATIONS WILL FLOW	OPTIONAL[1]	INTEGER IN RANGE 0..65535 161
-RCOM	READ COMMUNITY	OPTIONAL[1]	ASCII STRING (MAXIMUM 80 CHARACTERS) PUBLIC
-RLD	REPORT LUN DISCOVERY	OPTIONAL[1]	**Y**(ES), N(O)
-T	LOCAL TIME	OPTIONAL[1]	HH:MM
-TELNET	TELNET PORT FOR I SERIES COMMUNICATIONS	OPTIONAL[1]	23
-TEMPERATURE_UNITS	TEMPERATURE DISPLAY SCALE	OPTIONAL[1]	**C**(ELCIUS), F(AHRENHEIT)
-WCOM	WRITE COMMUNITY	OPTIONAL[1]	ASCII STRING (MAXIMUM 80 CHARACTERS) PRIVATE

Dependencies

optional[1]: at least one of the switches is mandatory

Example:

The i series alias is reset to i series1; the IP address for i series management functions is changed to 212.199.43.47. The date is set to the 21st of July, 2002 and the time to 1:30 p.m. Anna Levin is named as the contact person and she can be reached at the internal office extension 4838.

device set –n i series1 –ip 212.199.43.47 –d 21/07/2002 –t 13:30:00 –c AnnaLevin –loc ext4838

You can now connect to the i series 1 Gb Ethernet port or 10/100Mb management port and begin managing the i series operations and the attached SAN.

Show i series Configuration Information

After setting the general i series Management configurations, you can use the CLI command **info** to access the i series Configuration table and view the current configuration, including whom to contact in the event of technical difficulties.

info

NAME:	172.17.200.159
ID:	-1
DEVICE TYPE:	NEXSAN I SERIES
DESCRIPTION:	SW VERSION: 3.3, BUILD: 0, PATCH: 0
	BOARD VERSION 1, PCB VERSION 2.
	SN: 48523321
CONTACT:	
LOCATION:	
STATUS:	OK
TIME SINCE LAST RESET:	1 DAYS 6H:23M:46 SEC
MANAGEMENT IP ADDRESS:	172.17.200.185
MANAGEMENT NETWORK MASK:	255.255.0.0
SNMP UDP PORT:	161
READ COMMUNITY:	PUBLIC
WRITE COMMUNITY:	PRIVATE
DATE & TIME:	23 FEB 2006. 17:58:26
TELNET PORT:	23
REPORT LUNS DISCOVERY:	TRUE
USERS ONLINE	1

Set Telnet Port

If your Telnet communications connection to the i series traverses a firewall, the standard Telnet communications port 23 may be blocked by the firewall as a security measure. To enable Telnet communications to the i series, you can designate an alternate port using the CLI command **device set -telnet**. This port can be opened in the firewall for dedicated Telnet-i series communications.

device set -telnet

Example:

The port 1597 is programmed as the Telnet communications port.

device set -telnet 1597

Traps and SNMP

The i series supports standard MIB s for monitoring and sends SNMP traps that can be viewed by an SNMP manager/console. Any SNMP manager using the correct default read and write communities can get and set MIB variables. If you are working with i series manager, the i series management system, i series manager will automatically add itself as the SNMP manager. The default SNMP communities are **public** for read and **private** for write. The default communities can be changed by an administrator.

Adding an SNMP Manager

To get trap notifications, an SNMP manager must be registered as a SNMP manager in the database of the SNMP agent. You can add an SNMP manager to the by i series by using the CLI command **snmp manager add**.

Note:
*When adding an SNMP manager, unless the community parameters are specified the community values will be the default community parameters for the i series. Use the VLI command **info** to see the community parameters. Use the VLI command **device set** to change community parameters.*

snmp manager add

This command adds a manager to the i series.

snmp manager add

Switch	Definition	Type	Values/Remarks
-IP	MANAGER IP ADDRESS	MANDATORY	IP ADDRESS
-P	RECEIVE TRAPS THROUGH SPECIFIC PORT	OPTIONAL	INTEGER IN RANGE 0..65535 162
-RCOM	READ COMMUNITY	OPTIONAL	ASCII STRING (MAXIMUM 80 CHARACTERS) USES DEFAULT PARAMETER FOR I SERIES WHEN PARAMETER IS NOT SPECIFIED.
-TRAP	SEND TRAPS TO MANAGER	OPTIONAL	Y (SEND), N (DO NOT SEND)
-WCOM	WRITE COMMUNITY	OPTIONAL	ASCII STRING (MAXIMUM 80 CHARACTERS) USES DEFAULT PARAMETER FOR I SERIES WHEN PARAMETER IS NOT SPECIFIED.

Example:

An SNMP manager is added on IP address 212.199.43.96. It receives traps through port 8162. The manager receives information through the public community and writes information through the private community.

snmp manager add –ip 212.199.43.96 –p 8162 –rcom public –wcom private –trap y

Setting Default SNMP Communities

You can set SNMP read and write communities to regulate SNMP manager access to variables.

- Use the CLI command **device set** to change the default read and write SNMP communities.
- Use the CLI command **info** to check the default communities.

Removing an SNMP Manager

Use the CLI command SNMP manager remove to remove a manager from the i series.

snmp manager remove

This command removes a manager from the i series.

snmp manager remove

Switch	Definition	Type	Values/Remarks
-IP	MANAGER IP ADDRESS	MANDATORY	IP ADDRESS
-P	RECEIVE TRAPS THROUGH SPECIFIED PORT	MANDATORY	INTEGER IN RANGE 0..65535

User Login Profiles

After logging in to a i series, a total of ten user profiles (name plus password) can be configured on a i series using the CLI command **admin add**. The default user name and password admin can be maintained or removed.

The user name can have from one to twenty characters. The user password can have from six to twelve characters. Both fields are case sensitive and accept all characters, including spaces.

admin add

This command adds a user name to the list of valid user login names for the i series. A user name can be from 1 to 19 characters long, including spaces. A password can be from 5 to 11 characters long, including spaces.

admin add

Switch	Definition	Type	Values/Remarks
-PW	USER PASSWORD	MANDATORY	ASCII STRING 5-11 CHARACTERS
-UN	USER NAME	MANDATORY	ASCII STRING 1—19 CHARACTERS

Example:

admin add –un JoeCool –pw 123456

Changing a User Profile

Note:
*If you are working in a i series cluster, a user profile must be changed on both **i** series*

This interactive command enables a user to change their login password for their user name on the i series.

admin password

After entering the command, you are prompted to enter your existing password and the new password.

Removing a User Profile

Note:
*If you are working in a i series cluster, a user profile must be changed on both **i** series.*

You can remove any user profile from the i series database except the profile you are logged in with. This ensures at least one user profile in the database at all times.

admin remove

Switch	Definition	Type	Values/Remarks
-UN	USER NAME	MANDATORY	ASCII STRING 1—19 CHARACTERS

Example:

Remove user profile JoeCool.

admin remove –un JoeCool

Configuring the i series Interfaces

If your i series configuration contains SCSI devices, you can set the storage port bus ID. If your i series configuration contains FC storage ports, you can change the default configuration of each port. Use the CLI command **interface show** to show all storage port connections.

interface show

Table 2-1: iSCSI Gateway Interfaces

Type	Name	Description	Alias	Phys Address
RS232	CONS	RS232 MANAGEMENT CONS INT		000000000000
ETHERNET	ETH1	FAST ETHERNET MANAGE	ETH1	000000000000
FIBRECHANNEL	FC1	FC MMF	FC1	000000000000
FIBRECHANNEL	FC2	FC MMF	FC2	000000000000
ETHERNET	ETH1	GIGABIT ETHERNET NET	ETH1	00081A000110
ETHERNET	ETH2	GIGABIT ETHERNET NET	ETH2	00081A000112

Reset an Interface

Use the CLI command **interface reset** to reset the interface.

interface reset

Switch	Definition	Type	Values/Remarks
-IF	CURRENT INTERFACE ALIAS	MANDATORY	ASCII STRING (MAXIMUM 10 CHARACTERS)

Show SCSI Storage Ports and Bus IDs

Use the CLI command **pscsi show** to view all SCSI storage ports and their corresponding SCSI bus ID.

Note:
This command is available only when a pSCSI interface is present.

pscsi show

Alias	Bus ID
PSCSI3	12
PSCSI4	7

Setting a SCSI Storage Port Bus ID

Each storage port connected to a SCSI device must have a SCSI bus ID. Use the CLI command **pscsi set busid** to set a storage port's SCSI bus ID.

Note:
This command is available only when a pSCSI interface is present.

pscsi set busid

Switch	Definition	Type	Values/Remarks
-IF	INTERFACE ALIAS	MANDATORY	ASCII STRING (MAXIMUM 10 CHARACTERS)
-ID	SCSI BUS IDENTITY	OPTIONAL	0..**7**..15

Example

Storage port 3, pscsi3, is assigned SCSI bus ID 12.

```
pscsi set busid –if pscsi3 –id 12
```

Show FC Interface Information

Use the CLI command **fc interface show** to view all FC ports on the i series; their World Wide Port Names (WWPN) and administrative and operative types.

Note:
This command is available only when an FC interface is present.

fc interface show

Alias	WWPN	Connect Mode	Oper Type	Speed
FC1	20:00:00:20:38:11:34:78	PRIVATE	NLPORT	1GBS
FC2	20:00:00:20:38:00:10:64	PRIVATE	NLPORT	1GBS

Set FC Storage Port

The i series default configuration for FC connections is 1 GB nl port in a public loop. If you want to change the default configuration, each storage port connected to an FC device can be reconfigured to change the connection speed, port type and connection mode. Use the CLI command **fc set** to change the FC storage port communication speed, port type or connection mode.

Note:
This command is available only when an FC interface is present.

fc set

Switch	Definition	Type	Values/Remarks
-IF	STORAGE PORT	MANDATORY	ASCII STRING (MAXIMUM 10 CHARACTERS)
-CM	CONNECTION MODE	OPTIONAL	**AUTO** (AUTO DETECT)* FAB (FABRIC), PUL (PUBLICLOOP), PRL (PRIVATELOOP) PTP (POINT-TO-POINT)
-SP	FC COMMUNICATION SPEED	OPTIONAL	0: AUTO **1**: 1 GB 2: 2 GB

* **Note:** auto detect and ptp are not available for versions prior to 3.3.

Example:

fc set –if fc2 –sp 1 –cm prl

i series World Wide Node Name

Use the CLI command **fc node show** to view the i series World Wide Node Name (WWNN).

Note:
This command is available only when an FC interface is present.

fc node show

Changing a Network Interface Alias

You can change the alias of a i series interface for user convenience. Leaving the new alias field blank will return the alias to its default setting. You can disable the interface.

Note:
*If you are working in a i series cluster, the interface alias must be changed on both **i** series.*

interface set

Switch	Definition	Type	Values/Remarks
-IF	CURRENT INTERFACE ALIAS	MANDATORY	ASCII STRING (MAXIMUM 10 CHARACTERS)
-NA	NEW ALIAS	OPTIONAL	ASCII STRING (MAXIMUM 10 CHARACTERS)
-ENABLE	ENABLES INTERFACE	OPTIONAL	INTERFACE SHOW COMMAND STATUS IS: LINK UP, LINK DOWN
-DISABLE	DISABLES INTERFACE	OPTIONAL	INTERFACE SHOW COMMAND STATUS IS: DISABLED

Example:

Rename storage interface fc1 to Storage 1.

interface set –if fc1 –na Storage1

Adding a Network Interface IP Address

Note:
*If you are working in a i series cluster, the interface IP must be added on both **i** series. Only one i series in a cluster can be active.*

You can assign more than one IP address to each network port.

Note:
Executing this command on the same network port with a different IP address will not reset the network port address. It will add another IP address to the network port

ip config set

Switch	Definition	Type	Values/Remarks
-IP	IP ADDRESS ASSIGNED TO INTERFACE PORT	MANDATORY	IP ADDRESS
-IF	NETWORK INTERFACE PORT	MANDATORY[1]	ETH1, ETH2, ETH3 (FOR NEW CONFIGURATION)
-ACT	ACTIVITY STATUS ONLY ONE I SERIES IN A CLUSTER CAN BE ACTIVE.	OPTIONAL	**1** (ACTIVE), 2 (INACTIVE) RELEVANT ONLY IN CLUSTER
-IM	IP NETWORK MASK	OPTIONAL	IP NETWORK MASK **255.255.255.0**

Dependencies

mandatory[1]: necessary for new configurations

Example:

IP address 212.199.43.57 is added to interface eth1 for a total of two IP addresses assigned to interface eth1.

ip config set –if eth1 –ip 212.199.43.57

Removing a Network Interface IP Address

Note:
If you are working in a i series cluster, the interface IP must be removed on both ***i*** *series.*

You can remove an IP address from the network ports.

ip config remove

Switch	Definition	Type	Values/Remarks
-IP	IP ADDRESS TO REMOVE FROM THE NETWORK INTERFACE PORT	MANDATORY	IP ADDRESS

Example:

The second IP address, 212.199.43.70, on the network interface eth3 is removed.

ip config remove –ip 212.199.12.70

Show IP Configuration

After setting the management and network port IP addresses, you can use the CLI command **ip config show** to access the IP Configuration Table and view all assigned port IP addresses.

ip config show

Table 2-2: i series IP Configuration Table

If Name	IP Address	Net Mask	Activity
MGMT	212.199.43.46	255.255.255.0	ACTIVE
ETH1	212.199.43.56	255.255.255.0	ACTIVE
ETH1	212.199.43.57	255.255.255.0	INACTIVE
ETH2	212.199.75.66	255.255.255.0	ACTIVE
ETH2	212.199.12.70	255.255.255.0	INACTIVE

Configuring IP Routing

To enable communications between the i series and IP networks located outside the i series LAN, you must configure IP routing paths for each external network port. The IP route begins with a specified network port on the i series and ends at the external network IP address. Just as each IP address is unique, each IP routing path is unique. There can be only one IP route to a given external network IP address per i series.

Note:
You can configure only one IP route to a given external network on your i series.

Add an IP Route

You can enable communications to networks outside of your LAN by configuring an IP routing path. This allows volume access to hosts located on external networks. Use the CLI command **ip route add** to add an IP routing path to your i series. If you are working in a i series cluster, you must configure the IP route on both i series in the i series cluster. For more information on i series clusters, see "Configuring a i series Cluster".

ip route add

Switch	Definition	Type	Values/Remarks
-DIP	DESTINATION IP	MANDATORY	IP ADDRESS
-GW	GATEWAY ROUTER IP ADDRESS	MANDATORY	IP ADDRESS
-IF	INTERFACE ALIAS	MANDATORY	ASCII STRING (MAXIMUM 10 CHARACTERS)
-DMASK	HOST DESTINATION IP MASK	OPTIONAL[1]	255.255.255.255

Dependencies

optional[1]: mandatory when '-dip = subnet IP' (network route)

Example:

An IP routing path to Network D, IP 10.10.20.0, and (IP mask 255.255.255.0) is mapped from network port Eth2 through router gateway 30.30.20.20.

```
ip route add –dip 10.10.20.0 –dmask 255.255.255.0 –gw 30.30.20.20 –if eth2
```

Set Default Gateway

You can configure the default gateway for IP routes. This gateway is used for any IP address not specified in the i series routing table. Use the CLI command **ip route default** to set the default gateway IP address. To change the default gateway, repeat the command with the new default gateway IP address.

ip route default

Switch	Definition	Type	Values/Remarks
-GW	IP ADDRESS OF THE DEFAULT GATEWAY ROUTER	MANDATORY	IP ADDRESS
-IF	INTERFACE ALIAS	OPTIONAL	**ETH1**, MGNT

Example:

Set default gateway to 20.20.10.20.

ip route default –gw 20.20.10.20

Check IP Routes

After creating an IP routing path, you can ping any IP-connected device from the i series ETH interface to check that the routing is configured correctly. Use the CLI command **ping** to ping an IP address from the i series. Make sure that the route is defined on the other side as well.

ping

Switch	Definition	Type	Values/Remarks
-IP	IP ADDRESS TO PING	MANDATORY	IP ADDRESS
-IF	INTERFACE ALIAS THAT ISSUES ICMP REQUESTS	OPTIONAL	ASCII STRING (MAXIMUM 10 CHARACTERS)

Example:

Ping ETH1 port on device 172.17.200.69

ping –ip 172.17.200.69 –if ETH1

Show IP Routes

After creating an IP routing path to an external network, you can view it and any other configured IP routing path. Use the CLI command **ip route show** to view a i series's routing table.

ip route show

Table 2-3: i series IP Routing Paths

Dest IP Address	Dest Mask	Interface	Gateway
10.10.20.20	255.255.255.0	ETH2	30.30.20.20
10.12.40.40	255.255.255.0	ETH3	20.22.11.11

Remove an IP Route

You can remove unwanted IP routing paths from your i series. Use the CLI command **ip route remove** to remove an IP routing path. If you are working in a i series cluster, the IP route must be removed from both i series databases. For more information on i series clusters, see "Configuring a i series Cluster".

ip route remove

Switch	Definition	Type	Values/Remarks
-DIP	HOST DESTINATION IP ADDRESS	MANDATORY	IP ADDRESS
-DMASK	HOST DESTINATION IP MASK	OPTIONAL	IP NETWORK MASK **255.555.255.255**
-GW	GATEWAY TO HOST STATION IP ADDRESS	OPTIONAL	IP ADDRESS

Example:

The routing path to destination network IP 10.12.40.0 (IP mask 255.255.255.0) is removed from network port Eth2.

ip route remove –dip 10.12.40.0 –dmask 255.255.255.0

You have now configured all basic i series parameters. If you are creating a i series cluster, continue with "Configuring a i series Cluster".

Configuring iSCSI Portals

Note:

- *Do not create an iSCSI portal on the management IP address.*
- *The i series supports a maximum of 100 portals.*

Create iSCSI Portals

To enable communication between iSCSI initiators and iSCSI targets you need to assign a portal to the iSCSI protocol transport. Use the CLI command **iscsi portal create** to create an iSCSI portal. A portal is the coupling of an IP address and a TCP port. Once created, a portal is opened automatically during a communication session. If you are working in a i series cluster, each portal must be created on both i serieses in the i series cluster. For more information on i series clusters, see "Configuring a i series Cluster".

iscsi portal create

Switch	Definition	Type	Values/Remarks
-IP	NETWORK PORT IP ADDRESS	MANDATORY	IP ADDRESS
-P	TCP PORT FOR iSCSI COMMUNICATION	OPTIONAL	INTEGER IN RANGE 0..65535 **3260**

Example:

An iSCSI portal is created using the default TCP port 3260 for the IP address 212.199.43.66.

```
iscsi portal create –ip 212.199.43.66
```

Show iSCSI Portals

View all created portals using the CLI command **iscsi portal show**.

iscsi portal show

Table 2-4: iSCSI Portals

Protocol	Address Type	Address	Port	Portal Group	Role
6	IPV 4	212.199.43.56	3260		
6	IPV 4	212.199.43.57	3260		
6	IPV 4	212.199.43.66	5003		
6	IPV 4	212.199.43.67	5003		

Protocol 6 is the transport protocol for iSCSI. Address type IPv 4 designates a four byte IP address.

Remove iSCSI Portals

You can remove an iSCSI portal using the CLI command **iscsi portal remove**. Only after all iSCSI portals related to an IP address are removed from a port can the IP address be removed from the port. If you are working in a cluster, the portal must be removed from both i series databases. For more information on i series clusters, see “Configuring a i series Cluster”.

iscsi portal remove

Switch	Definition	Type	Values/Remarks
-IP	NETWORK PORT IP ADDRESS	MANDATORY	IP ADDRESS
-P	TCP PORT FOR ISCSI COMMUNICATION	MANDATORY	INTEGER IN RANGE 0..65535

Discovering iSCSI Targets

iSCSI target discovery is performed across the IP-SAN by the iSCSI initiator located on the server. The i series supports three methods for reporting iSCSI targets in the IP-SAN to iSCSI initiators:

- iSCSI Discovery Session – no configuration is necessary
- SLP– no configuration is necessary
- iSNS– you must add the iSNS server to the i series iSNS client

Add iSNS client

Use the CLI command **ip isns add** to add an iSCSI server to the i series's iSNS client.

ip isns add

Switch	Definition	Type	Values/Remarks
-IP	IP ADDRESS OF ISNS SERVER	MANDATORY	IP ADDRESS UP TO 2 ISNS SERVERS

Example:

Add iSNS server 212.199.43.1 to i series iSNS client.

```
ip isns add –ip 212.199.43.1
```

Show iSNS client

Use the CLI command **ip isns show** to view all added iSCSI server addresses.

ip isns show

Remove iSNS Client

Use the CLI command ip isns remove to remove an iSNS server from the i series iSNS client.

ip isns remove

Switch	Definition	Type	Values/Remarks
-IP	IP ADDRESS OF iSNS SERVER	MANDATORY	IP ADDRESS

Example:

Remove iSNS server 212.199.43.1 from the i series iSNS client.

```
ip isns remove –ip 212.199.43.1
```

Configuring Storage Devices

Discovering Storage Devices

The i series default algorithm for storage devices discovery is using the SCSI command REPORT LUNS. Certain storage devices either do not support this command or do not respond according to the SCSI standard. To discover these devices, the REPORT LUNs command must be disabled. If certain devices in the SAN are not being discovered by the i series, use the CLI command **device set** to disable or re-enable device discovery via REPORT LUNs.

device set

Switch	Definition	Type	Values/Remarks
-RLD	REPORT LUN DISCOVERY	OPTIONAL[1]	Y(ES), N(O)

Example:

Disable device discovery via REPORT LUNs.

```
device set –rld n
```

See "***Device Set***," for the full list of switch parameters for the CLI command **device set**.

storage discovery

This command resets the Fiber Channel loop and reregisters all attached storage devices. In most cases, the i series automatically discovers new storage. Use this command after adding or removing storage devices from the i series topography if it is not automatically discovered. Because this command resets the FC loop, it may cause a failure of any I/O operations being executed when the command is invoked.

storage discovery

Renaming a Storage Device

Note:
If you are working in a i series cluster, the disk must be renamed on both i series.

You can rename a disk.

storage set

Switch	Definition	Type	Values/Remarks
-S	STORAGE ALIAS TO MODIFY	MANDATORY	ASCII STRING (MAXIMUM 10 CHARACTERS)
-INFO	INFORMATION ON STORAGE TO SET	OPTIONAL[1]	ASCII STRING
-NA	NEW ALIAS FOR STORAGE	OPTIONAL[1]	ASCII STRING (MAXIMUM 10 CHARACTERS)

Dependencies

optional[1] : at least one of the switches is mandatory

Example:

The disk, Stor_1, is renamed to RAID1 and a Note: is made for the storage manager that disk was exposed on JAN 12.

storage set –s Stor_1 –na RAID1 –info Exposed_JAN_12

Removing a Storage Device

Note:
If you are working in a i series cluster, the disk must be removed on both i series.

You can remove a disk from the i series database. The disk must be defined as missing to remove it.

storage remove

Switch	Definition	Type	Values/Remarks
-S	STORAGE ALIAS TO REMOVE	MANDATORY	ASCII STRING (MAXIMUM 10 CHARACTERS)

Example:

Disk named Stor_1 is removed from the i series database.

storage remove –s Stor_1

i series Related Commands

Resetting a i series

You can perform a remote soft reset on the i series using the CLI **reset** command. All configuration databases will be maintained on the i series, including user names and passwords; network port aliases; configured disks and iSCSI targets.

system reset

Saving (Uploading) a i series Database File

You can upload a copy of a i series's full database file to the local TFTP server. If the i series fails, its database file can be downloaded to the replacement i series. This eliminates protracted configuration time on the new i series and ensures configuration integrity.

Use the CLI command **ft upload db** to upload a i series's full database file

ft upload <x>

where <x> = config/db/firmware

Switch	Definition	Type	Values/Remarks
-IP	TFTP SERVER IP ADDRESS	MANDATORY	IP ADDRESS
-FN	FILE DIRECTORY AND FILENAME	MANDATORY	ASCII STRING
-PORT	UDP PORT NUMBER	OPTIONAL	INTEGER IN RANGE 0..65535 **69**
-RETRIES	NUMBER OF RETRIES	OPTIONAL	0..**3**..8
-TIMEOUT	TIMEOUT IN SECONDS	OPTIONAL	1..**15**

Example:

Upload the file v1_9dat as a database file to the TFTP server at 212.199.43.70.

ft upload db –ip 212.199.43.70 –fn i series/v1_9/v1_9database

Downloading a i series Configuration File

Note:
Download the database file to the i series before attaching it to the storage devices.

After replacing a failed i series, you can download the replaced i series database file from the TFTP server to the new i series. Unlike a standard i series installation, do not connect the i series to the storage devices before powering up. You first download the database file and then connect the i series to the storage devices. This ensures that autodiscovery will not assign default aliases different from the replaced i series to the discovered disks.

Use the CLI command **ft download db** to download a i series database file from the local TFTP server after you have initialized the replacement i series with an IP management address via LCD or Console.

Note:
The i series must be reset for the downloaded database to become operational.

ft download db

This command downloads the database file.

ft download <x>

where <x> = config/db/firmware

Switch	Definition	Type	Values/Remarks
-IP	IP ADDRESS OF TELNET STATION WHERE TFTP APPLICATION SITS	MANDATORY	IP ADDRESS
-PORT	UDP PORT NUMBER	OPTIONAL	INTEGER IN RANGE 0..65535 **69**
-FN	DIRECTORY TO EXPORT FILES TO	MANDATORY	ASCII STRING MUST END WITH '\' OR '/'
-TIMEOUT	TIMEOUT IN SECONDS	OPTIONAL	1..**15**
-RETRIES	NUMBER OF RETRIES	OPTIONAL	0..**3**..8

Example:

Download the file v1_9database as a database file from the TFTP server at 212.199.43.70.

ft download db –ip 212.199.43.70 –fn i series/v1_9/v1_9database/

Configuring a i series Cluster

You can configure a i series cluster using two i series of the same type. A *cluster* is a group of storage units and switches that function as one unit providing high availability in the event of i series failover.

A cluster can be configured between two i series using CLI or i series manager.

Note:
We recommend using i series manager for cluster configuration. For more information on configuring a cluster using i series manager refer to the i series manager User Manual and on-line help system.

Note:
When configuring a cluster via CLI, you must configure each i series with identical configurations. This requires entering the same CLI commands twice, once for each i series.

Two i series can be concurrently connected to the same storage devices to balance volume exposure thus creating a i series cluster. In a cluster, each i series interacts in an active-active, peer-to-peer fashion with the other i series, or *neighbor*, in the cluster. Neither i series needs special configuration in order for it to act as the master i series in the cluster. This provides higher flexibility in building a cluster.

Note:
Both i series are fully operational in a cluster. No i series must sit in stand-by mode. When working in a cluster, the i series can support a maximum of 100 portals: 50 active and 50 inactive.

Clusters provide high availability in the event of i series failover. Each network port on the i series is configured with its own active, or functioning, IP addresses as well as inactive, or dormant, neighbor IP addresses. If one i series goes off-line, the remaining i series activates its neighbor's IP addresses. The hosts continue to access iSCSI targets through the same IP address without sensing that their 'regular' i series has gone offline or noticing any impact on storage performance.

Note:
When working with RAID controllers, it is imperative that all LUNs in the RAID controller are simultaneously exposed through all ports connected to both i series for the i series to provide high availability during a i series failover.

Set i series ID

When you configure a cluster, you must give each i series a different device ID for proper cluster functioning. Use the CLI command **device set** to configure the i series ID for each i series.

device set

Example:

There are two i series in a cluster. In i series 1 the ID is set to 1.

device set –id 1

In i series 2 the ID is set to 0.

device set –id 0

Add Neighbor

Note:
All CLI names and aliases are case sensitive. When you configure a cluster, you must tell each i series that it has a neighbor and how to contact its neighbor. Use the CLI command ***neighbor add*** *to inform each i series of its neighbor.*

You must tell i series 1 that its neighbor is i series 2 and i series 2 that its neighbor is i series 1.

When creating a cluster, first ensure that you have configured all IP addresses in the correct active/inactive phase as well as portals and IP routes on both **i** series.

neighbor add

Switch	Definition	Type	Values/Remarks
-IP	IP ADDRESS OF MGMT PORT ON NEIGHBOR	MANDATORY	IP ADDRESS
-NB	ALIAS OF NEIGHBOR TO ADD TO CLUSTER	MANDATORY	ASCII STRING (MAXIMUM 10 CHARACTERS)

Example:

i series 1 is informed that it has a neighbor, i series2, and that it can establish communication with i series2 via IP address 212.199.43.75.

neighbor add –nb i series2 –ip 212.199.43.75

Note:
All i series database configurations must be replicated in both i series when creating a i series cluster.

Maintaining Cluster Communications

Once a i series knows that it has a neighbor, it begins sending out a regular *keep alive* signal to its neighbor that it is on-line. The i series also begins listening for the keep alive signal from its neighbor. The keep alive signal is transmitted through all connecting paths between each neighbor. Thus, if one path fails, the remaining path(s) will still carry the keep alive signal.

If a specified time period passes without a keep alive signal from the neighbor, a *suspicious interval*, measured in seconds, is entered. The i series suspects that its neighbor has gone off-line and begins preparing to activate the neighbor IP addresses to take over storage exposure.

If a keep alive signal is received during the suspicious interval, the timer is reset and the i series continues to function as usual. If a keep alive signal is not received by the end of the suspicious interval, a *dead interval* is entered. At the end of the dead interval, the neighboring i series is considered off-line, the failover process is initiated and the on-line i series actives the neighbor IP addresses and takes over volume exposure.

Use the CLI command **cluster show** to view the keep alive parameters of a cluster.

cluster show

KeepAlive Int(s)	Susp Int(s)	Faulty Interval	Failover	State
2	6	10	ENABLED	NOT RELEVANT

Example:

Every 2 seconds i series 1 sends out a keep alive signal. If, after 6 seconds from the last keep alive signal, i series 1 does not receive another keep alive signal from its neighbor, it enters a suspicious interval. If, after 10 seconds from the last keep alive signal, i series 1 enters a dead interval and begins activating the failover process.

Enable/Disable Cluster Failover

Once you have configured your cluster parameters, you need to enable the failover functionality. Use the CLI command **cluster failover enable** to enable this functionality. This command must be executed on both i series in the cluster.

cluster failover enable

If you want to break a cluster or need to take a i series off-line, you must first disable i series failover. Use the CLI command **cluster failover disable** to disable this functionality. This command must be executed on both i series in the cluster.

cluster failover disable

Cluster Failover Force

This command forces the switch to take over. NEXSAN recommends running this on the surviving i series when one of the i series in a cluster fails. This will prevent the surviving i series from waiting for the connection to the second i series to be established.

cluster failover force

Additional i series Cluster Configurations

After configuring neighbor parameters on each i series, you need to configure identical storage configuration and exposure details on each i series in the cluster.

Show Neighbor Details

Use the CLI command **neighbor show -details** to view the neighbor configured on a i series.

neighbor show –details

Switch	Definition	Type	Values/Remarks
-TABLE	DISPLAYS DATA IN TABLE FORMAT	OPTIONAL	DEFAULT DISPLAY
-RECORD	DISPLAYS DATA IN RECORD FORMAT	OPTIONAL	
-DETAILS	DISPLAYS SPECIFIC DETAILS	OPTIONAL[1]	
-NB	ALIAS OF NEIGHBOR IN CLUSTER	OPTIONAL	ASCII STRING (MAXIMUM 10 CHARACTERS)

Dependencies

optional[1]: switch -nd is mandatory for details view

Managing a Cluster

If you modify a i series alias or management IP address, you must implement the updates in the neighboring i series. Use the CLI command **neighbor set** to update a i series regarding changes in its neighbor.

neighbor set

Switch	Definition	Type	Values/Remarks
-IP	IP ADDRESS OF MGMT PORT ON NEIGHBOR	MANDATORY	IP ADDRESS
-NB	ALIAS OF NEIGHBOR TO ADD TO CLUSTER	MANDATORY	ASCII STRING (MAXIMUM 10 CHARACTERS)

Use the CLI command **neighbor remove** to remove a neighbor from a cluster.

neighbor remove

Switch	Definition	Type	Values/Remarks
-NB	ALIAS OF NEIGHBOR TO ADD TO CLUSTER	MANDATORY	ASCII STRING (MAXIMUM 10 CHARACTERS)

Use the CLI command **cluster set** to modify the default keep alive intervals.

cluster set

Switch	Definition	Type	Values/Remarks
-FINT	FAILOVER INTERVAL TIME WHEN SUSPICIOUS INTERVAL IS EXCEEDED	OPTIONAL[1]	
-KAI	KEEP ALIVE INTERVAL TIME BETWEEN KEEP ALIVE SIGNALS FROM NEIGHBORS	OPTIONAL[1]	
-SINT	SUSPICIOUS INTERVAL TIME FROM WHEN A SIGNAL WAS EXPECTED BUT NOT RECEIVED	OPTIONAL[1]	

Dependencies

optional[1]: at least one of the switches is mandatory

Upgrading the i series Firmware

> ***Note:***
> *The i series must be reset for the new firmware to begin functioning.*

You can upgrade the i series firmware via CLI. The firmware upgrade files are first downloaded from the TFTP server. You can then use the CLI command **ft download firmware** to upgrade the i series firmware.

All configured user profiles are unaffected by the firmware upgrade.

ft download firmware

Example:

Update firmware file for version X_Y, patch W, build Z

ft download firmware firmware_file_name_X_Y_W_Z.fw

After upgrading the firmware, the i series must be reset for the new firmware to begin functioning. Use the CLI command **reset** to reset the i series.

System reset

Use the CLI command **info** to view the firmware version to confirm that the firmware has successfully upgraded.

Safe Mode

The i series enters into safe mode automatically when necessary due to boot failures. When the i series boots in safe mode, the i series will be in one of two states:

First State: Current DB

In this state you will see the following screen and you must upload the BD & tech info into files in order to avoid losing important information.

```
************************************************************
*              NEXSAN I series                             *
************************************************************
*  i series is in SAFE MODE, Contact NEXSAN technical support
*
************************************************************
*                                                          *
* I series                                                  *

* Management IP: 172.20.52.1                               *
* Cluster State: Not Relevant                              *
* Description:   SW Version: 3.5 (v3_5_0_391_0_06_02_2008)    *
* Board version 1, PCB version 0. SN: unknown               *
************************************************************
```

```
safemode :>?
debug     : activate debug terminal
ft        : file transfer menu
info      : information about the device
interface : interface menu
ip        : IP configuration menu
ping      : send ICMP ECHO_REQUEST packets to hosts
system    : system menu
traceroute : find all routers on the way to specified IP
safemode :>?
```

1. Reboot the i series using normal boot as follows: **system boot -sm 0**
2. If the i series comes up in safemode again try and reboot the i series using the last good configuration as follows: **system boot -sm 1.**

   Alternatively, you can download another database using the ft commands and try to reboot from using the backup.

Second State: Empty DB/Menu Selection

In this state you will see the following screen. Selecting one of the options from the menu will enable the i series to boot normally (not in safe mode).

```
************************************************************
*             NEXSAN I series                              *
*                                                          *
* I series                                                  *

* Management IP: 0.0.0.0                                   *
* Cluster State: Not Relevant                              *
* Description:   SW Version: 3.5 (v3_5_0_391_0_06_02_2008)    *
* Board version 1, PCB version 0. SN: unknown               *
************************************************************


The i series encountered problem.
Please choose boot type:

(1) Boot with Last Good DB (DB that already boot once)
(2) Boot with initial DB
(3) Format Flash

Please enter your choice [1-3]:
```

Exporting a Corrupted Database

After you reboot the i series from safe mode level 1 or 2, you can use the CLI command **ft upload techinfo** to export the potentially corrupted database to BROCADE technical support for examination.

If you rebooted in safe mode level 1 (last good configuration), the last good database file and the corrupted database file are exported for examination.

If you rebooted in safe mode level 2 (reboot with default factory database), the corrupted database file is exported for examination.

ft upload techinfo

Switch	Definition	Type	Values/Remarks
-IP	TFTP SERVER IP ADDRESS	MANDATORY	IP ADDRESS
-FN	FILE DIRECTORY AND FILENAME	MANDATORY	ASCII STRING
-PORT	UDP PORT NUMBER	OPTIONAL	INTEGER IN RANGE 0..65535 **69**
-RETRIES	NUMBER OF RETRIES	OPTIONAL	0..**3**..8
-TIMEOUT	TIMEOUT IN SECONDS	OPTIONAL	1..**15**

Example

The suspicious database is exported to the directory Corrupted_DB at IP address 212.199.43.70.

```
ft upload techinfo –ip 212.199.43.70 –fn Corrupted_DB
```

Boot Options

You can use the CLI to clear a i series's database to varying degrees. This is useful if you want to change the physical storage pool managed by a i series or make substantial changes to the virtualization configuration.

Safe mode levels 0 and 1 can be executed from any Telnet station but, for extra safety, safe mode levels 2 and 3 can only be executed from a console with a local, direct RS232 connection to the i series.

system boot

Switch	Definition	Type	Values/Remarks
-SM	SAFE MODE LEVEL	MANDATORY	0: NORMAL 1: LAST GOOD CONFIGURATION 2: DEFAULT DATABASE 3: DEFAULT FACTORY SYSTEM

Level optional: Normal Mode

This is the same as resetting the i series. No change is made to the i series configuration.

Level 1: Last Good Configuration

Each time the i series successfully boots up, it saves the database as the last good configuration. If the last time the i series booted was also the first time, the database will be empty. Use this level to erase all configurations executed since the last reboot and return to the previous i series configuration.

For example, if you are modifying or making temporary changes to the i series configuration, first ensure that the current configuration is stored in the i series by resetting the i series then execute the changes. If the changes are no longer desirable, reboot in this level.

Level 2: Default Factory Database

Note:
A direct RS232 connection is necessary.

This clears the database of all configurations except user login profiles. Use this level to erase all virtual configurations except the user profiles.

For example, if you want to transfer the i series to a different physical storage pool within a campus, this level will prepare the i series for its new configuration while maintaining the same user profiles of the same system administrators.

Level 3: Default Factory System

Note:
A direct RS232 connection is necessary.

This clears the database of all configurations executed on the i series, including user login profiles. Use this level if you want to completely clear a i series's database.

For example, if you want to transfer a i series to another branch office or campus department with different system administrators, this level will return the i series to the same state it left the factory for shipping.

Event Log

Displaying System Log Events

Use the CLI command **system log realtime show** to show the events as they occur. Events can be filtered according to severity.

system log realtime show

Switch	Definition	Type	Values/Remarks
-INFO	DISPLAYS EVENTS WITH SEVERITY INFO	OPTIONAL	
-WARN	DISPLAYS EVENTS WITH SEVERITY WARN	OPTIONAL	
-ERROR	DISPLAYS EVENTS WITH SEVERITY ERROR	OPTIONAL	
-FATAL	DISPLAYS EVENTS WITH SEVERITY FATAL	OPTIONAL	

Example:

Show events with severity ERROR and INFO.

system log realtime show -error -info

Use the CLI command **system log show** to show events that were logged. Filters can be used to display events that occurred during a specific time. Events can also be filtered and displayed according to severity.

system log show

Switch	Definition	Type	Values/Remarks
-STARTDATE	DISPLAYS EVENTS STARTING FROM THIS DATE	OPTIONAL	
-STARTTIME	DISPLAYS EVENTS STARTING FROM THIS TIME	OPTIONAL	
-ENDDATE	DISPLAYS EVENTS UP UNTIL THIS DATE	OPTIONAL	
-ENDTIME	DISPLAYS EVENTS UP UNTIL THIS TIME	OPTIONAL	
-SKIP	THE NUMBER OF EVENTS TO SKIP	OPTIONAL	
-EVENTCOUNT	THE NUMBER OF EVENTS TO DISPLAY	OPTIONAL	
-INFO	DISPLAYS EVENTS WITH SEVERITY INFO	OPTIONAL	
-WARN	DISPLAYS EVENTS WITH SEVERITY WARN	OPTIONAL	
-ERROR	DISPLAYS EVENTS WITH SEVERITY ERROR	OPTIONAL	
-FATAL	DISPLAYS EVENTS WITH SEVERITY FATAL	OPTIONAL	

Example:

Show events from period June 27, 2007 to July 3, 2007 with severity fatal.

system log show –startdate 27/06/2007 –enddate 03/07/2007 –fatal

Exporting the System Log

Use the CLI command **ft autoupload enable** to start the automatic export of the system log. Each time the log file is full it is automatically exported to the destination specified.

ft autoupload enable

Switch	Definition	Type	Values/Remarks
-IP	IP ADDRESS OF TELNET STATION WHERE TFTP APPLICATION SITS	MANDATORY	IP ADDRESS
-PORT	UDP PORT NUMBER	OPTIONAL	INTEGER IN RANGE 0..65535 69
-FD	DIRECTORY TO EXPORT FILES TO	OPTIONAL	ASCII STRING (MAXIMUM 10 CHARACTERS)
-TIMEOUT	TIMEOUT IN SECONDS	OPTIONAL	1..**15**
-RETRIES	NUMBER OF RETRIES	OPTIONAL	1..**3**..8

Example:

Export the system logs to directory ‘SystemEventLogs’ at IP 192.1.168.254.

Ft autoupload enable –ip 192.1.168.254 –fd SystemEventLogs

Use the CLI command **ft autoupload disable** to stop the automatic export of the system log.

Use the CLI command **ft autoupload show** to displays the configuration of the autoupload feature.

Chapter 3
Volume Operations

Disk Operations

Identifying and Configuring Storage Devices

All disks are named automatically during the auto-discovery process. For FC, this name includes FC disk's *World Wide Unique Identifier (WWUI)* serial number.

Note:
The i series supports a maximum of 512 disks.

Use the CLI command **storage show** to show the available storage devices and their corresponding aliases needed to configure disks

storage show

Table 3-1: Storage Devices

Alias	Entity Name	LUN	Oper. Status	Type	In Use
STOR_1	500507606058C900	0	ENABLED	DISK	YES
STOR_2	2000002037F88FB8	0	ENABLED	DISK	YES
STOR_3	2000002037C32B1F	0	ENABLED	DISK	NO
STOR_4	2000002037C32450	0	ENABLED	DISK	NO

The storage device operating status has five options.

- Enabled denotes an attached and functioning storage device.
- Storage is missing denotes that a storage device was previously registered and has since lost its connection to the i series.
- Invalid denotes a storage device that was connected, removed and reconnected with a different storage size.
- Unknown denotes that a storage device is connected but is issuing parameters not understandable to the i series.
- Configured denotes the stage when the user has created storage and the i series has not yet connected to it.

Note:
If a tape is attached to the i series the timeout of the FC drivers should be changed using the following command :

device advance set –param StorageDrivers.FC.Tachyon.FCPort.Config.io.TimeoutSec –val 300

The i series automatically generates and assigns storage aliases as each device is discovered. Use the CLI command **storage blink start** to identify the actual physical device for an alias.

storage blink start

Switch	Definition	Type	Values/Remarks
-S	DEVICE ALIAS TO BLINK	MANDATORY	ASCII STRING (MAXIMUM 10 CHARACTERS)
-T	LENGTH OF TIME TO BLINK DEVICE	OPTIONAL	1..3600 SEC **0**: FOREVER

Example:

The storage device, Stor_1, is set to blink for two minutes (one hundred and twenty seconds) to allow it to be identified.

storage blink start –s Stor_1 –t 120

Use the CLI command **storage blink abort** to stop the blinking before the end of the set time.

storage blink abort

Switch	Definition	Type	Values/Remarks
-S	ALIAS OF DEVICE TO BLINK	MANDATORY	ASCII STRING (MAXIMUM 10 CHARACTERS)

Example:

Stop blinking on storage device, Stor_1

storage blink abort –s Stor_1

Once a storage device has been identified, use the CLI command **storage set** to change the device alias or include helpful information on the device.

storage set

Switch	Definition	Type	Values/Remarks
-S	STORAGE ALIAS TO MODIFY	MANDATORY	ASCII STRING (MAXIMUM 10 CHARACTERS)
-INFO	INFORMATION ON STORAGE TO SET	OPTIONAL[1]	ASCII STRING
-NA	NEW ALIAS FOR STORAGE	OPTIONAL[1]	ASCII STRING (MAXIMUM 10 CHARACTERS)

Dependencies

optional[1] : at least one of the switches is mandatory

Example:

The alias of Stor_1 is changed to Disk2JBOD5 for easier identification and it is noted to save the disk for the Exchange Log.

storage set –s Stor_1 –na Disk2JBOD5 –info Exchange_Log

The i series supports write cache enabling for increased performance. Use the CLI command **storage disk set** to enable or disable the write cache.

storage disk set

Switch	Definition	Type	Values/Remarks
-D	DISK DEVICE	MANDATORY	ASCII STRING (MAXIMUM 10 CHARACTERS)
-ALLOC	ALLOCATES STORAGE TO HOST	OPTIONAL	YES, **NO** FOR USE WITH NEXSAN VSS HW PROVIDER
-WCE	WRITE CACHE ENABLED	OPTIONAL	TRUE, FALSE

The i series also recognizes all write-protected storage devices. Use the CLI command **storage show –details -s** to view a device's details, including if it is write-protected.

storage show

Switch	Definition	Type	Values/Remarks
-TABLE	DISPLAYS DATA IN TABLE FORMAT	OPTIONAL	DEFAULT DISPLAY
-RECORD	DISPLAYS DATA IN RECORD FORMAT	OPTIONAL	
-DETAILS	DISPLAYS SPECIFIC DETAILS	OPTIONAL[1]	
-S	STORAGE ALIAS	OPTIONAL	ASCII STRING (MAXIMUM 10 CHARACTERS)
-DISK	DISK DEVICE	OPTIONAL	ASCII STRING (MAXIMUM 10 CHARACTERS)

Dependencies

optional[1]: switch -s is mandatory for details view

Table 3-2: Storage Details

Alias:	Stor_1
Entity Name:	0
LUN (Logical Unit Number)	0000000000000000
Vendor Name	IBM
Additional Info:	
Transport type:	Fibre Channel
Oper. Status:	Storage missing
Time since last Update:	0 days 3h:4m:59 sec 0 (1/100 Sec)
SCSI Version:	3
Revision Level:	F60HDDYF-T18350R
Product Id:	DDYF-T18350R
Serial Number:	TEFB0374
Number Of Blocks:	35843670
Block Size:	512
SubDisks:	Entire
Write Cache Enabled:	true
Write Protected:	false

Creating Volumes

Creating a Transparent Volume

Note:
- *Transparent volumes cannot be used in further volume hierarchies.*
- *Tape devices must be virtualized as transparent volumes.*

You can take a physical disk and its existing configured storage data and convert it to a directly accessible, or transparent, virtual volume using the CLI command **volume create transparent**. A transparent volume is ready for direct host exposure.

Certain vendor storage devices have vendor-specific SCSI commands. To support these SCSI commands, you can convert these storage devices and their contained data to transparent volumes.

This is useful if you have a functioning and fully configured RAID module that you want to use 'as is'. All RAID configurations will be maintained in the transparent volume.

volume create transparent

Switch	Definition	Type	Values/Remarks
-D	DISK ALIAS	MANDATORY	ASCII STRING (MAXIMUM 10 CHARACTERS)
-VOL	ALIAS OF VOLUME TO CREATE	OPTIONAL	ASCII STRING (MAXIMUM 10 CHARACTERS)

Example:

In Figure 3-1, the logical unit, LUN0 on Disk 1, is converted directly to a virtual transparent volume, Transparent 1. This RAID device has only one LUN. For each LUN configured on a RAID device, the i series registers a disk. Therefore, a RAID device with five LUNs will appear to the i series as five disks.

volume create transparent –vol Trans1 –d Disk1

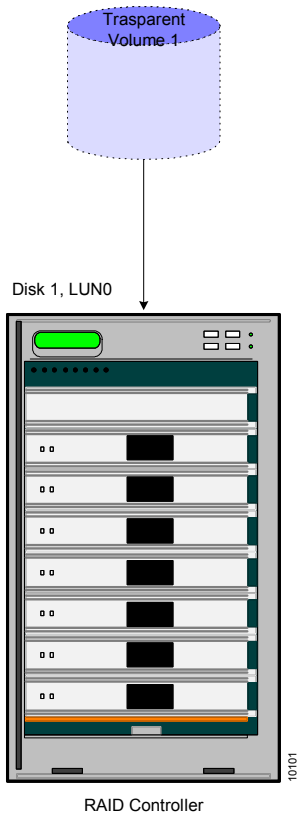


Figure 3-1. Transparent Volume 1

After creating the transparent volume, you can use the CLI command **volume show** to verify the volume creation.

volume show

Table 3-3: Volume Show

Alias	Type	Act # of Blocks	Pot # of Blocks	Block Size	State
TRANS1	TRANSPARENT	N/A	N/A	N/A	INTERNAL

Creating a Subdisk (LUN Carving)

Note:
The i-series supports a maximum of 512 subdisks.

You can create one or more subdisks on a physical disk. The subdisks can then be converted to simple volumes to be used for creating concatenated, striped and mirrored virtual volumes. When you create a subdisk, only the defined area is converted into a subdisk. You must individually convert each disk area into a subdisk for the physical volume to be usable by the Volume Manager.

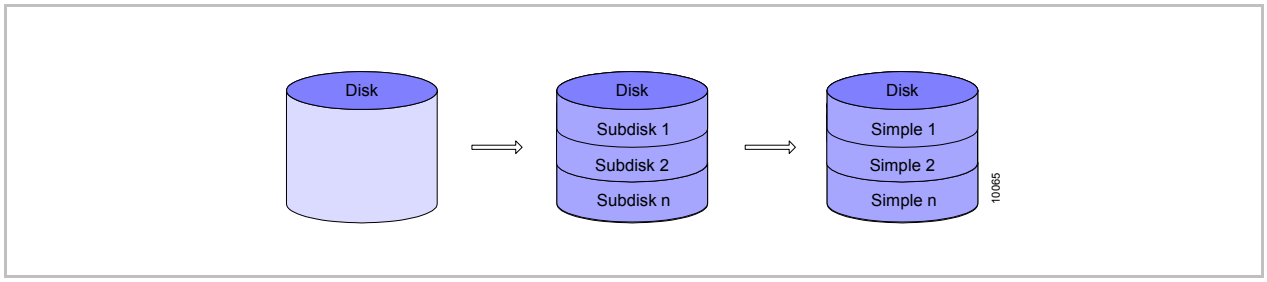


Figure 3-2. Partitioning a Physical Volume

subdisk create

Switch	Definition	Type	Values/Remarks
-D	DISK ALIAS	MANDATORY	ASCII STRING (MAXIMUM 10 CHARACTERS)
-SD	SUBDISK ALIAS	MANDATORY	ASCII STRING (MAXIMUM 10 CHARACTERS)
-SL	LENGTH OF DISK IN BLOCKS	MANDATORY	1 BLOCK = 512 BYTES
-SA	START ADDRESS	OPTIONAL	0

Example:

In Figure 3-3, you see Disk 1 before a subdisk is created on it.

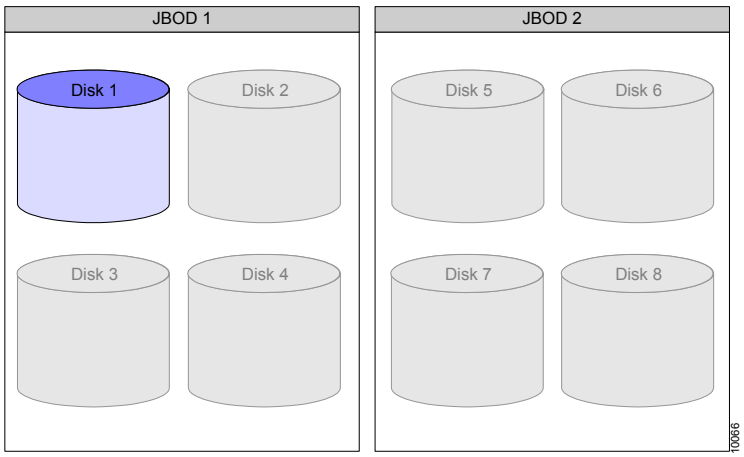


Figure 3-3. Disk 1 before Subdisk

In Figure 3-4, Subdisk 1 has been created on Disk 1. The subdisk is 18,000,000 blocks long (9 GB). The Volume Manager begins counting the 18,000,000 blocks from block 0.

subdisk create –d Disk1 –sl 18000000 –sa 0 –sd Subdisk1

Figure 3-4. Disk 1 with 1 Subdisk

After creating the subdisk, you can use the CLI command **subdisk show** to view it and all configured subdisks. You can use the CLI command **subdisk show –details -sd** to view the details of the created subdisk.

subdisk show

Switch	Definition	Type	Values/Remarks
-TABLE	DISPLAYS DATA IN TABLE FORMAT	OPTIONAL	DEFAULT DISPLAY
-RECORD	DISPLAYS DATA IN RECORD FORMAT	OPTIONAL	
-DETAILS	DISPLAYS SPECIFIC DETAILS	OPTIONAL[1]	
-D	ALIAS OF DISK TO SHOW SUBDISKS ON	OPTIONAL	ASCII STRING (MAXIMUM 10 CHARACTERS)
-SD	ALIAS OF SUBDISK TO SHOW	OPTIONAL	ASCII STRING (MAXIMUM 10 CHARACTERS)

Dependencies

optional[1]: switch -d & -sd are mandatory for details view

This command calls up the following table.

Table 3-4: Details of all Subdisks

Disk	Subdisk	Oper. Status	Start Address	Length	Vol
DISK1	SUBDISK1	ENABLED	0	512	NO

Creating a Simple Volume

Note:
The i series supports a maximum of 512 volumes.

Before you can build concatenated, mirrored and striped volumes, you must create simple volumes from each disk or subdisk in your storage network.

A physical disk or subdisk is converted directly to a virtual simple volume. A simple volume differs from a transparent volume in that virtual volume hierarchies can be built on top of simple volumes but not on transparent volumes.

volume create simple

Switch	Definition	Type	Values/Remarks
-VOL	ALIAS OF VOLUME TO CREATE	OPTIONAL	ASCII STRING (MAXIMUM 10 CHARACTERS)
-SD	SUBDISK ALIAS	OPTIONAL[1]	ASCII STRING (MAXIMUM 10 CHARACTERS)
-D	DISK ALIAS	OPTIONAL[1]	ASCII STRING (MAXIMUM 10 CHARACTERS)

Dependencies

optional[1]: at least one of the switches is mandatory

Assigning a volume alias is optional. If you do not include a volume alias in the command, the volume alias will default to the subdisk alias in which the volume is located. For example, a simple volume created on Subdisk 6 will be named Subdisk 6 by default.

Use the **–sd** switch to assign a subdisk or the **–d** switch to assign a disk.

Example:

In Figure 3-5, Subdisk 1 on Disk 1 is converted to a simple volume, Simple 1.

volume create simple –vol Simple1 –sd Subdisk1

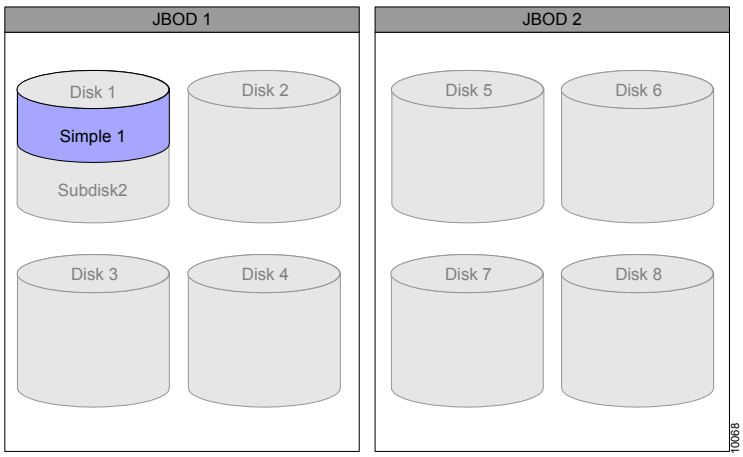


Figure 3-5. Simple Volume 1

Use the CLI command **volume show** to show the created volume:

volume show

Alias	Type	Act # of Bl	Pot # of Bl	Bl Size	State
SIMPLE1	SIMPLE	17999999	17999999	512	INTERNAL

Creating a Concatenated Volume

Note:
The i series supports a maximum of 512 volumes.

To accommodate large volumes of data or to best utilize small volumes spread over several disks, you can concatenate physical volumes across storage devices to create a larger virtual volume.

volume create concatenated

Switch	Definition	Type	Values/Remarks
-VOL	ALIAS OF VOLUME TO CREATE	MANDATORY	ASCII STRING (MAXIMUM 10 CHARACTERS)
-CH	ALIAS OF EACH VOLUME TO INCLUDE IN CONCATENATED VOLUME	MANDATORY[1, 3]	ASCII STRING (MAXIMUM 10 CHARACTERS)
-NBC	NUMBER OF VOLUMES TO CONCATENATE ACROSS	OPTIONAL[1, 2]	**2**..16

Dependencies

[1]: order must be as follows: '-nbc' must be before '-ch'

[2]: mandatory if greater than 2

[3]: can be used up to 16 times

The system default for the number of children being concatenated is two. Therefore, you only need to specify the number of children for numbers greater than two.

Example:

In Figure 3-6, Simple Volume 5 and Simple Volume 12, both built over an entire physical disk, are concatenated to create a concatenated volume, Concat 1. Data is read/written first to Simple 5. When the data chunk gets to the end of Simple 5, it continues with Simple 12 reflecting the volume order as entered in the CLI command.

volume create concatenated –vol Concat1 –ch Simple5 –ch Simple12

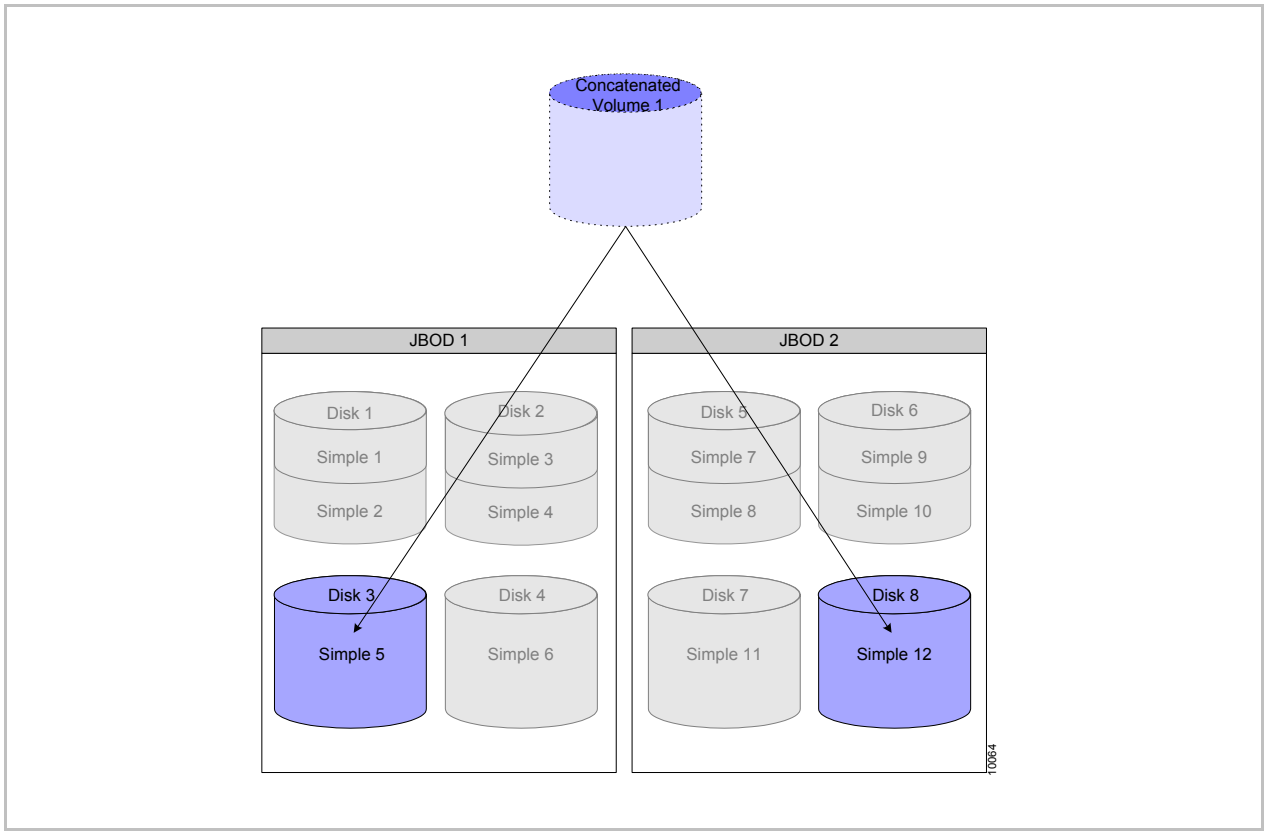


Figure 3-6. Concatenated Volume 1

Creating a Striped Volume

Note:
The i series supports a maximum of 512 volumes.

A striped volume has data written equitably across two or more disks to provide higher read/write rates. Subdisks within a striped volume need to be on different disks to realize the benefits of striping. Throughput increases with the number of disks within a striped volume.

volume create stripe

Switch	Definition	Type	Values/Remarks
-SUS	STRIPE UNIT SIZE	MANDATORY	INTEGER
-VOL	ALIAS OF VOLUME TO CREATE	MANDATORY	ASCII STRING (MAXIMUM 10 CHARACTERS)
-CH	ALIAS OF EACH VOLUME TO INCLUDE IN CONCATENATED VOLUME	MANDATORY[1, 3]	ASCII STRING (MAXIMUM 10 CHARACTERS)
-NBC	NUMBER OF VOLUMES TO CONCATENATE ACROSS	OPTIONAL[1, 2]	**2**..16

Dependencies

[1]: order must be as follows: '-nbc' must be before '-ch'

[2]: mandatory if greater than 2

[3]: can be used up to 16 times

The system default for the number of children data is being striped across is two. Therefore, you only need to specify the number of children for numbers greater than two.

Example:

In Figure 3-7, a striped volume, Stripe 1, is created across four children: Simple 2, Simple 4, Simple 8 and Simple 10. The striped unit size is 100 blocks, meaning that in each read/write function, 100 blocks of data are read/written into Simple 2; then 100 blocks into Simple 4;. then 100 blocks into Simple 8; then 100 blocks into Simple 10 and then back again to 100 blocks in Simple 2 until the end of the data chunk.

volume create stripe –vol Stripe1 –nbc 4 –sus 100 –ch Simple2 –ch Simple4 –ch Simple8 –ch Simple10

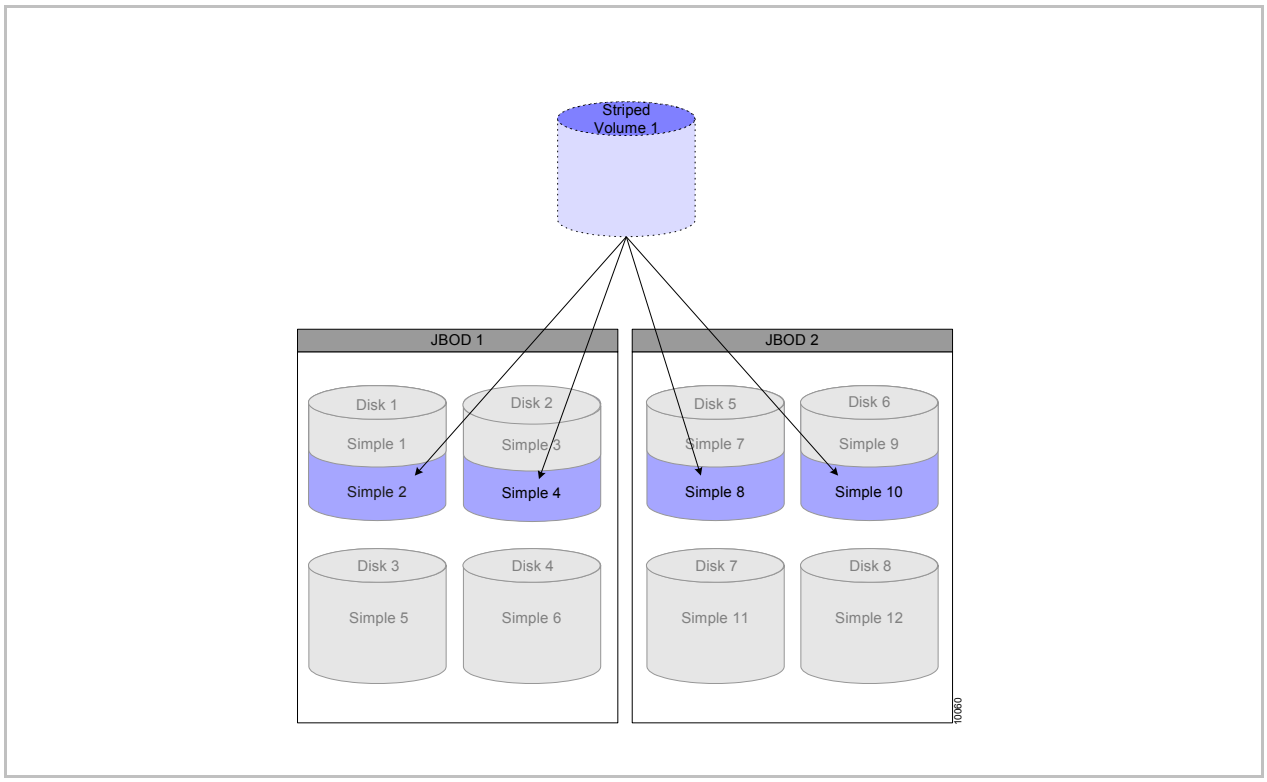


Figure 3-7. Striped Volume 1

Creating a Mirrored Volume

Note:
- *Use mirroring to create data backups.*
- *The i series supports a maximum of 512 volumes.*

A mirrored volume is synchronously written into two or more volumes. Mirrored volumes provide protection against data loss from a physical disk crash. To be a true mirror and realize the full potential of a mirror, the mirrored volumes must be located on different physical disks.

volume create mirror

Switch	Definition	Type	Values/Remarks
-VOL	ALIAS OF VOLUME TO CREATE	MANDATORY	ASCII STRING (MAXIMUM 10 CHARACTERS)
-CH	ALIAS OF EACH VOLUME TO INCLUDE IN CONCATENATED VOLUME	MANDATORY[1, 3]	ASCII STRING (MAXIMUM 10 CHARACTERS)
-NBC	NUMBER OF VOLUMES TO CONCATENATE ACROSS	OPTIONAL[1, 2]	**2**..16

Dependencies

[1]: order must be as follows: '-nbc' must be before '-ch'

[2]: mandatory if greater than 2

[3]: can be used up to 16 times

Example:

In Figure 3-8, a mirrored volume, Mirrored 1, is created using two children, Simple 6 and Simple 11.

volume create mirror –vol Mirrored1 –ch Simple6 –ch Simple11

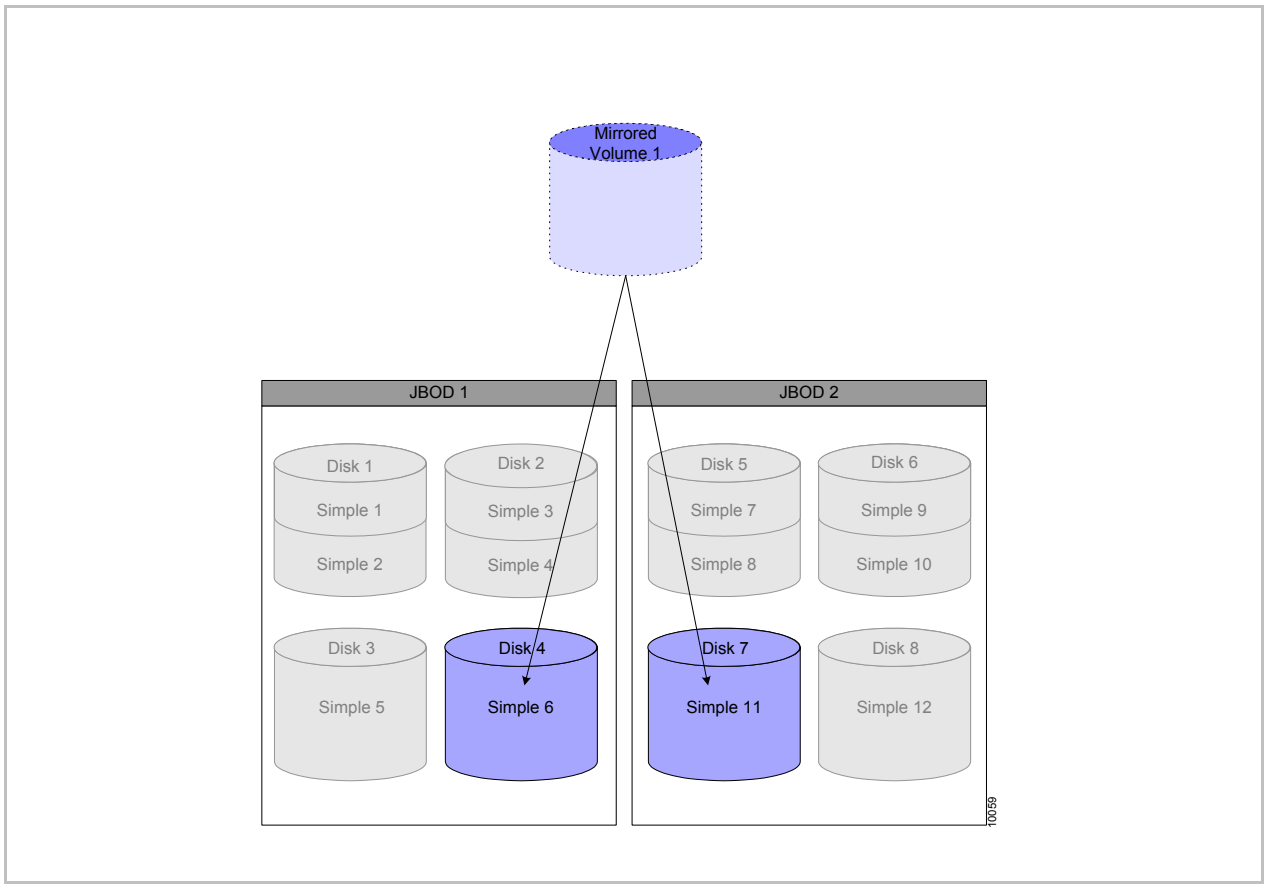


Figure 3-8. Mirrored Volume 1

Creating a RAID 10 and RAID 0+1

You will need two separate commands to create a RAID 10 or 0+1 volume. RAID 10 first creates mirrored volumes and then creates a striped volume of the mirrored volumes. This gives the advantage of both high performance and data redundancy.

RAID 0+1 first creates striped volumes and then creates mirrored volumes of the striped volumes.

Example:

In Figure 3-9, to begin creating a RAID 10 volume, a mirrored volume, Mirror 2, is created using two children: Simple 1 and Simple 7.

volume create mirror –vol Mirror2 –ch Simple1 –ch Simple7

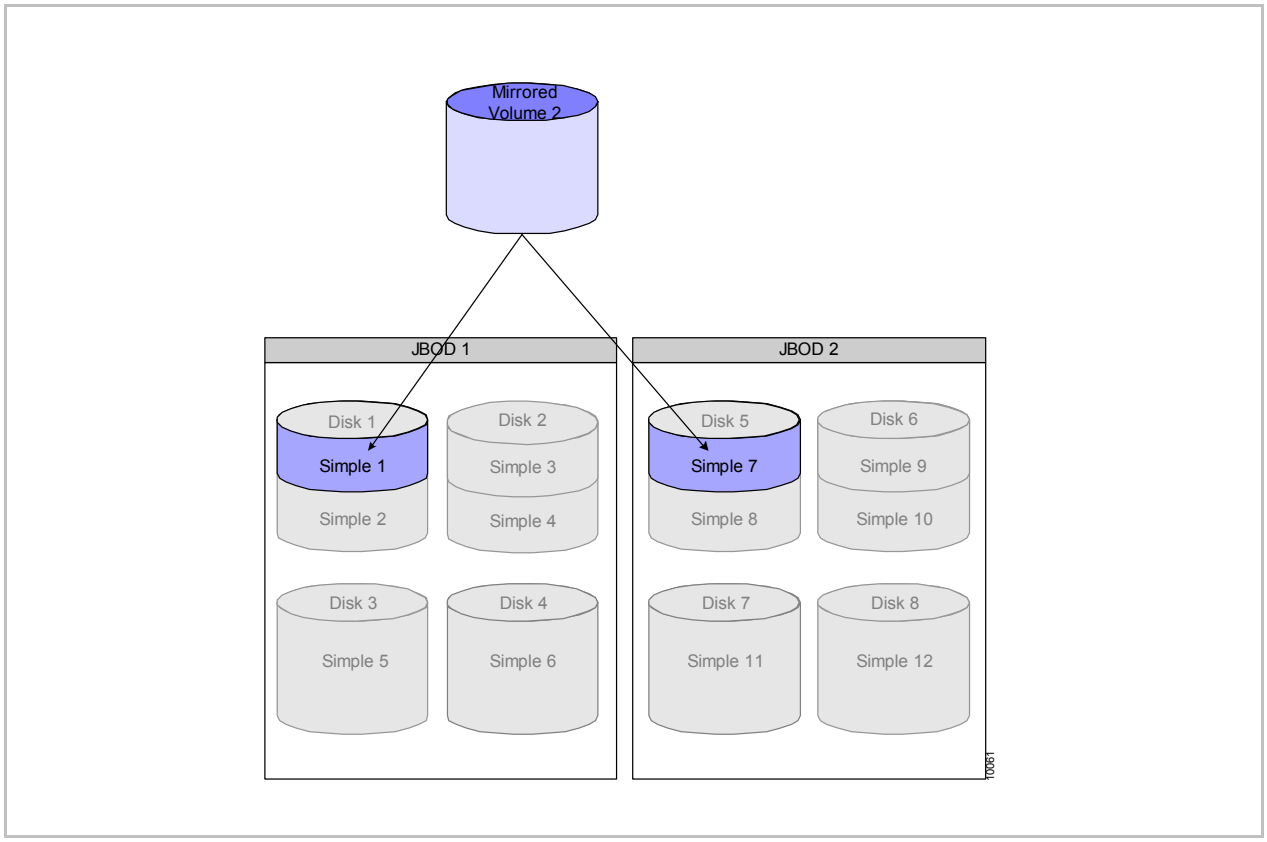


Figure 3-9. First Mirrored Volume of RAID 10

Next, in Figure 3-10, another mirrored volume, Mirror 3, is created using two children: Simple 3 and Simple 9.

volume create mirror –vol Mirror3 –ch Simple3 –ch Simple9

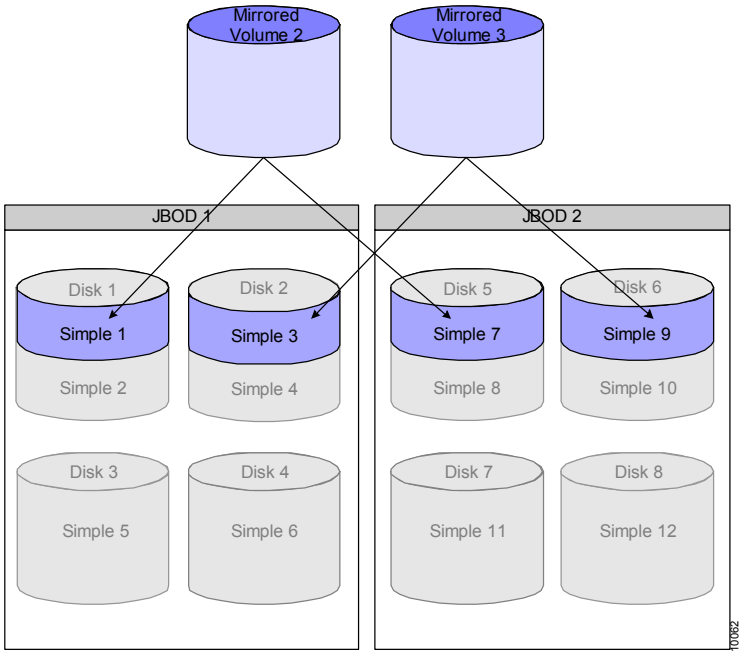


Figure 3-10. Second Mirrored Volume of RAID 10

Finally, in Figure 3-11, a striped volume, Stripe 2, is created using the two mirrored volumes as children: Mirror 2 and Mirror 3. The striped unit size is 100 blocks, meaning that in each read/write function, 100 blocks of data are read/written first into Mirror 2 then Mirror 3 and then back to Mirror 2 until the end of the data chunk.

volume create stripe –vol Stripe2 –sus 100 –ch Mirror2 –ch Mirror3

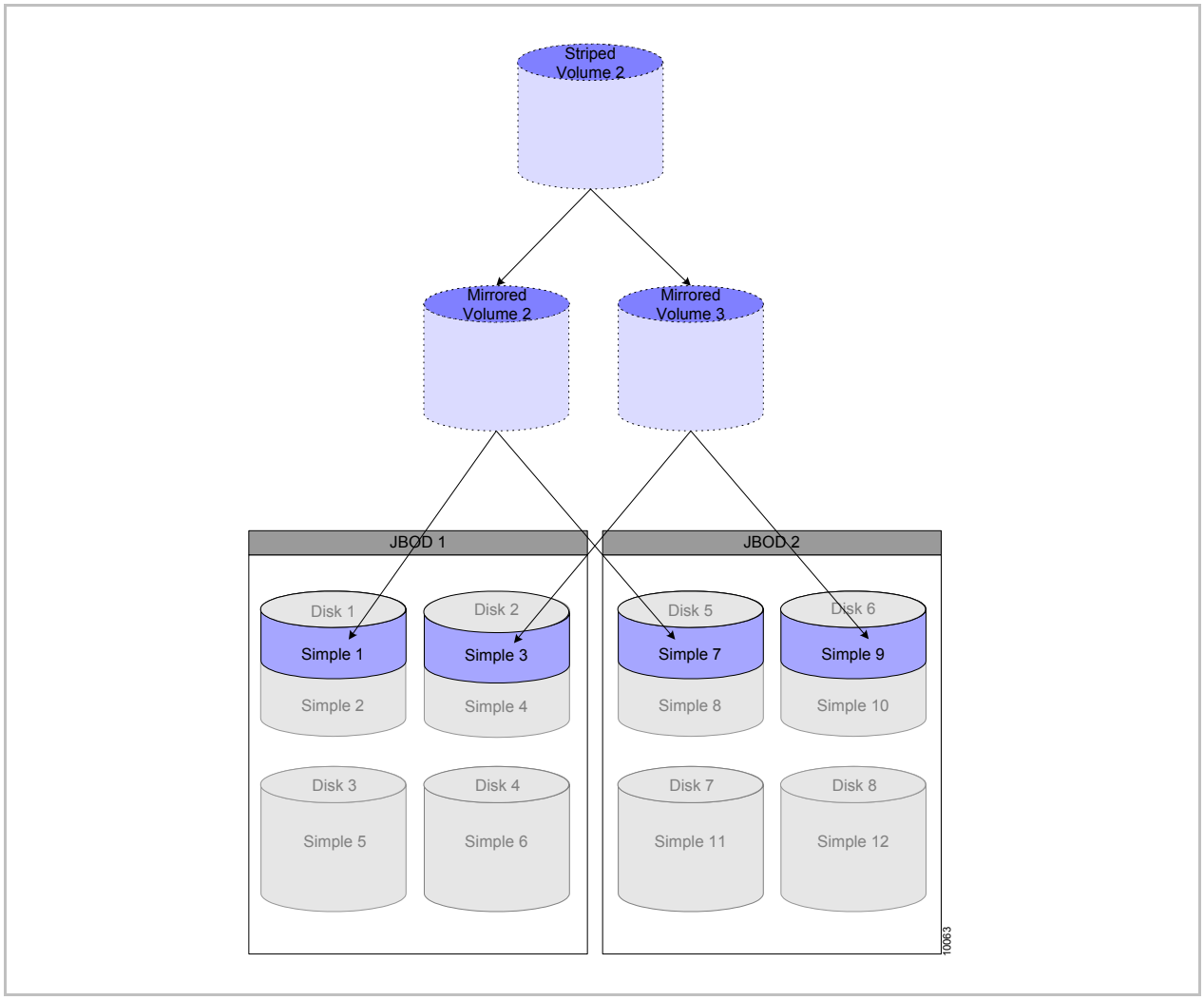


Figure 3-11. Striped Volume of RAID 10

To create a RAID 0+1 volume, invert the commands and first create a striped volume and then mirrored volumes of the stripe.

Volume Exposure & Targets

Exposing an iSCSI Target and LUN

Note:
A LUN value cannot be larger than 255.

To make virtual volume accessible to a host, you need to assign a LUN to it, attach the LUN to an iSCSI target and expose the target. The CLI command **volume expose** is used in two ways:

Create and Expose volume on a new target.

Expose volume on an existing target.

Create and Expose Volume on a New Target.

The CLI command **volume expose -new** creates a new iSCSI target, assigns a LUN and then exposes the new target.

volume expose

Switch	Definition	Type	Values/Remarks
-TA	TARGET ALIAS	MANDATORY	ASCII STRING (MAXIMUM 10 CHARACTERS)
-VOL	ALIAS OF VOLUME	MANDATORY	ASCII STRING (MAXIMUM 10 CHARACTERS)
-NEW	EXPOSE VOLUME ON NEW TARGET	MANDATORY [1]	DO NOT SPECIFY, NO VALUE ALLOWED FOR SWITCH
-TN	USER-ASSIGNED WORLD WIDE UNIQUE IDENTIFIER FOR THE TARGET	MANDATORY [1]	ISCSI WORLD WIDE UNIQUE IDENTIFIER (ASCII STRING OF MAX. 223 CHARACTERS)
-LUN	LUN	MANDATORY[2]	0..255
-DEVICE	I SERIES ALIAS TO EXPOSE TARGET ON	OPTIONAL [1]	ASCII STRING (MAXIMUM 10 CHARACTERS)

Dependencies

mandatory [1] : mandatory on new target

mandatory[2] : mandatory on existing target

optional[1]: optional on new target

Example:

Expose Stor_1 on new target Tar_1 with alias Tar_1, LUN 1 and WWUI www.company.com/SAN/MusicBox

volume expose –vol Stor_1 –new –ta Tar_1 –lun 1 –tn www.company.com/SAN/MusicBox

The command **lu remove** unexposes a disk.

lu remove

Switch	Definition	Type	Values/Remarks
-TA	TARGET ALIAS OF LU	MANDATORY	ASCII STRING (MAXIMUM 10 CHARACTERS)
-LUN	LOGICAL UNIT NUMBER	OPTIONAL	0

Example:

Unexpose stor_1 from target Tar_1

lu remove –ta Stor_1

Note:
*The command **lu remove** does not delete the target. To remove the target, use the command: **iscsi target remove***

Expose Volume on an Existing Target.

After creating a target and LUN, you can add additional LUNs to the target using the CLI command **volume expose** (without the **–new** switch).

volume expose

Example 1:

The target finance already exists. The WWUI of finance has already been assigned to the target. The disk Vol1 is assigned LU0 and attached to the target finance. The exposing device is VSwitch1.

volume expose –device Vol1 –ta finance –lun 0

Viewing LUNs

You can view all created LUNs using the CLI command **`lu show`**.

lu show

Table 3-5: Details of all LUNs

LUN	Tgt Alias	Storage	Oper Status
0	PILOTE	XXX	ACTIVE
0	SPIROU	YYY	ACTIVE
1	PILOTE	MIR1	ACTIVE
0	LUCKY	ZZZ	ACTIVE

Removing an iSCSI Target

The command storage unexposed does not remove targets. Use the CLI command **iscsi target remove** to delete targets.

iscsi target remove

Switch	Definition	Type	Values/Remarks
-TA	ISCSI TARGET ALIAS TO REMOVE	MANDATORY	ASCII STRING (MAXIMUM 10 CHARACTERS)

Example:

iscsi target remove –ta musicbox

Changing iSCSI Target Parameters

This command renames a target alias. Renaming the alias will have no negative effect on the target exposure.

iscsi target set

Switch	Definition	Type	Values/Remarks
-TA	ALIAS OF TARGET TO RENAME	MANDATORY	ASCII STRING (MAXIMUM 10 CHARACTERS)
-DEVICE	ALIAS OF I SERIES TO EXPOSE TARGET ON	OPTIONAL	ASCII STRING
-NA	NEW ALIAS FOR TARGET	OPTIONAL	ASCII STRING (MAXIMUM 10 CHARACTERS)
-CHAPPW	USER PASSWORD FOR CHAP AUTHENTICATION (FOR DUAL AUTHENTICATION)	OPTIONAL[1]	ASCII STRING 12-16 CHARACTERS
-CHAPUN	USER NAME FOR CHAP AUTHENTICATION (FOR DUAL AUTHENTICATION)	OPTIONAL[2]	ASCII STRING

Dependencies

optional[1]: mandatory with CHAP username

optional[2]: mandatory with CHAP password

Example:

The target alias accounting is renamed to finance.

iscsi target set –ta accounting –na finance

Show iSCSI Targets

Use the CLI command **iscsi target show** to view all created iSCSI targets.

iscsi target show

Switch	Definition	Type	Values/Remarks
-TABLE	DISPLAYS DATA IN TABLE FORMAT	OPTIONAL	DEFAULT DISPLAY
-RECORD	DISPLAYS DATA IN RECORD FORMAT	OPTIONAL	
-DETAILS	DISPLAYS SPECIFIC DETAILS	OPTIONAL[1]	
-TA	USER-ASSIGNED ALIAS FOR ISCSI TARGET	OPTIONAL	ASCII STRING (MAXIMUM 10 CHARACTERS)

Dependencies

optional[1]: switch -ta is mandatory for details view

iSCSI Target Details

Use the CLI command **iscsi target show -details –ta** to view the details of an iSCSI target.

Table 3-6: iSCSI Target Details

TARGET ALIAS:	NMS153
TARGET NAME:	EUI.00081AFFFF012345
CHAP USER NAME:	NEXSAN
STATUS:	OK
NUMBER OF PORTS:	1
PORT NAME:	EUI.00081AFFFF012345,T,0
NUMBER OF LUS:	2
# LOGIN FAILURES:	5
LAST FAILURE TIME:	10/12/04 15:30
LAST FAILURE TYPE:	AUTHENTICATION ERROR
LAST INITIATOR NAME:	PLONY
LAST INITIATOR IP:	1.2.3.4

Volume Security

When a target is created, a default access control identity is automatically assigned to its position 0. The default identity allows all hosts read-write access to the target and its underlying disk(s).

Set ACL Parameters

If you want to specify other access rights, you must change the general read-write access. Use the CLI command **acl set** to modify a target's access rights and identity position.

If you add or modify identities on a target after its disks have been exposed, the access rights will take effect only at the next login for each iSCSI initiator. Therefore, it is recommended to modify the default access rights for a target first before creating new identities to insure that it will not inadvertently be exposed to all iSCSI initiators in the beginning.

acl set

Switch	Definition	Type	Values/Remarks
-ID	IDENTITY ALIAS	MANDATORY	ASCII STRING (MAXIMUM 10 CHARACTERS)
-TA	iSCSI TARGET ALIAS	MANDATORY	ASCII STRING (MAXIMUM 10 CHARACTERS)
-ACC	ACCESS RIGHTS TO THE TARGET	OPTIONAL [1]	RW, RO, NA
-POS	ACCESS PRIORITY LEVEL (POSITION)	OPTIONAL [1]	

Dependencies

optional [1]: one of the optional switches is mandatory when changing

Example

The default access rights for the target finance are changed to not accessible meaning a non-specific host is not allowed access to the target finance.

```
acl set –ta finance –id def_all –acc na
```

Create Identity

Note:
If you are working with an iSNS server, all hosts are able to see the target but only those hosts with access rights are able to connect to the target.

If you want to limit host, meaning iSCSI initiator, access to targets, you must create an identity that is more discriminate than the default identity. Use the CLI command **acl identity create** to name and describe an identity.

When creating identities, keep in mind that:

- Each identity can contain one or more iSCSI initiators.
- Each identity can be assigned one or both login authentication methods.
- Each identity can be attached to more than one target.
- Each target is first automatically coupled to a default read-write un-authenticated access identity.
- Each target can have more than one identity.

acl identity create

Switch	Definition	Type	Values/Remarks
-ALIAS	IDENTITY ALIAS	MANDATORY	ASCII STRING (MAXIMUM 10 CHARACTERS)
-INFO	IDENTITY INFORMATION	OPTIONAL	ASCII STRING

Example

An identity, accounting, is created for those accountants allowed read-write access to the accounting records.

acl identity create – alias accounting – info accountants allowed read-write access to accounting records

Show Access Rights

After creating a target, use the CLI command **acl show** to view the target's automatically connected default identity.

acl show

Switch	Definition	Type	Values/Remarks
-TABLE	DISPLAYS DATA IN TABLE FORMAT	OPTIONAL	DEFAULT DISPLAY
-RECORD	DISPLAYS DATA IN RECORD FORMAT	OPTIONAL	
-TA	USER-ASSIGNED ALIAS FOR TARGET	OPTIONAL	ASCII STRING (MAXIMUM 10 CHARACTERS)

Add Initiators to an Identity

After creating an identity, you can begin adding hosts by their iSCSI initiator WWUIs to the identity. The identity is a group of iSCSI initiators. It is not enough for an authorized host to request access to a target. The host must be requesting access from the correct iSCSI initiator. Use the CLI command **acl identity add name** to add iSCSI initiators to an identity. Repeat this command to add all of the desired host initiators to the identity.

acl identity add name

Switch	Definition	Type	Values/Remarks
-ID	IDENTITY ALIAS	MANDATORY	ASCII STRING (MAXIMUM 10 CHARACTERS)
-NAME	WWUI OF INITIATOR	MANDATORY	ISCSI WORLD WIDE UNIQUE IDENTIFIER (ASCII STRING OF MAX. 223 CHARACTERS)

Example

The host, steven, is added to the identity accounting according to his iSCSI initiator wwui, iqn.1991-05.microsoft:steven.NEXSAN.

acl identity add name –id accounting –name iqn. 1991-05.microsoft: steven.NEXSAN

If a host has more than one iSCSI initiator installed, both initiators can be included in the identity.

acl identity add name –id accounting –name iqn.com.NEXSAN.steven

Identity Details

After assigning iSCSI initiators and assigning credentials to an identity, use the CLI command **acl identity show -details** to view the list of iSCSI initiators.

acl identity show -details

Table 3-7: Identity Details

DESCRIPTION:	ACCOUNTS ALLOWED READ-WRITE ACCESS TO ACCOUNTING RECORDS
INITIATORS:	IQN.1991-05.MICROSOFT:STEVEN. NEXSAN IQN.COM.NEXSAN.STEVEN
CREDENTIALS:	CHAP

Add CHAP

You can require initiator authentication before allowing access to a target and its underlying disk(s). The i series supports CHAP and SRP authentication methods. Microsoft initiators support CHAP. Use the CLI command **acl identity add chap/srp** to assign a login authentication method(s) to initiators in an identity.

An assigned authentication method encrypts the host login name and password. The host login and password do not have to relate to the iSCSI initiator WWUI. They can be any selected character strings.

Note:
In the event of a failover, if each identity does not require authentication on both i series, each attached identity will have free access to the target's underlying disks.

If you are working with a Microsoft initiator and configuring target authentication, note that the i series exchanges the final character in the password with a zero. Therefore, do not configure initiator passwords with a zero as the final character. CHAP passwords must be between twelve to sixteen characters in length.

acl identity add chap

Switch	Definition	Type	Values/Remarks
-ID	IDENTITY ALIAS	MANDATORY	ASCII STRING (MAXIMUM 10 CHARACTERS)
-UN	HOST NAME	OPTIONAL [1]	ASCII STRING
-PW	HOST PASSWORD	OPTIONAL[1]	ASCII STRING [6-20 CHARACTERS]
-RADIUS	RADIUS SERVER	OPTIONAL [1]	FLAG

Dependencies

optional[1]:
when using '-radius': -id, -radius are mandatory, -un is optional, -pw is not an option
when not using '-radius': -id, -un, -pw are mandatory, -radius is not an option

Example

The user name, steven, with user password, isatwork, is assigned CHAP credential verification in the identity accounting.

acl identity add chap –id accounting –us steven –pw isatwork

If a host has more than one iSCSI initiator installed, both initiators can be included in the identity and given authentication methods. The user name and password do not need to be the same for different initiators on the same host.

acl identity add chap –id accounting –us steven –pw ilovecookies

Add RADIUS Server

Note:
If you are working in an i series cluster, the RADIUS server must be configured on both i series.

When CHAP user names and passwords are configured on the network in a remote RADIUS server, use the CLI command **acl identity add chap** to direct a CHAP challenge to the RADIUS server and eliminate the need to configure all user name + password pairs on the i series. This decreases configuration time and increase overall network security. Use the CLI command **ip radius add** to add a RADIUS server address to the i series RADIUS client.

ip radius add

Switch	Definition	Type	Values/Remarks
-IP	IP ADDRESS OF RADIUS SERVER	MANDATORY	IP ADDRESS UP TO 2 RADIUS SERVERS
-K	SHARED SECRET BETWEEN I SERIES AND RADIUS SERVER	MANDATORY	ASCII STRING (MAXIMUM 80 CHARACTERS) MIN 16 CHARACTERS
-P	UDP PORT NUMBER TO SEND REQUESTS TO RADIUS SERVER	OPTIONAL	INTEGER IN RANGE 0..65535 **1812**

Example:

The i series is configured to relay CHAP challenges to the identity, accounting, from the user, steven, to the RADIUS server. The i series is configured to communicate with the RADIUS server through port 1812 to IP address 212.199.43.2. The i series – RADIUS key is DataTurnsMeOn.

The user password is not configured on the i series. The RADIUS server authenticates the user password and sends the results back to the i series.

acl identity add chap –id accounting –user steven –radius

ip radius add –ip 212.199.43.2 –p 1812 –k DataTurnsMeOn

Show Configured RADIUS Servers

Use the CLI command **ip radius show** to view all configured RADIUS server IP addresses.

ip radius show

Table 3-8: Configured RADIUS IP Addresses

Address	Port
212.199.43.2	1812
212.199.56.134	1812

Removing a RADIUS Server

Use the CLI command **ip radius remove** to remove a RADIUS server from the i series.

ip radius remove

Switch	Definition	Type	Values/Remarks
-IP	IP ADDRESS OF RADIUS SERVER	MANDATORY	IP ADDRESS
-P	UDP PORT NUMBER TO SEND REQUESTS TO RADIUS SERVER	OPTIONAL	INTEGER IN RANGE 0..65535

Connect an Identity and Target

Note:
If you are working in an i series cluster, each Identity must be connected to the target(s) on both i series.

Once created, an identity must be connected to a target to provide it with access control. An identity specifies which access rights the iSCSI initiators within the Identity have to the target.

When an identity is connected to a target, it is also given a *position*. The position of the identity determines its place in the i series access rights evaluation. An identity with the position 0 (default identity) is the last identity evaluated when an initiator tries to access a disk. If the initiator meets the profile of the identity, it is granted that identity 's access rights. If not, the i series continues to position 1. The i series does not scan all identities to determine which most specifically fits the host. Therefore, identities must be positioned in decreasing specificity to function correctly.

Note:
The i series scans for the first fit and not the best fit.

An identity can be connected to more than one target to provide the same conditions for each target. Use the CLI command **acl add** to connect an identity to a target.

Note:
All CLI names and aliases are case sensitive

acl add

Switch	Definition	Type	Values/Remarks
-ID	IDENTITY ALIAS	MANDATORY	ASCII STRING (MAXIMUM 10 CHARACTERS)
-TA	iSCSI TARGET ALIAS	MANDATORY	ASCII STRING (MAXIMUM 10 CHARACTERS)
-ACC	ACCESS RIGHTS TO THE TARGET	OPTIONAL	**RW**, RO, NA
-POS	ACCESS PRIORITY LEVEL (POSITION) *	OPTIONAL	INTEGER 1-2147482646 * THE NEXT FREE POSITION

Example

The identity, accounting, is connected to the target finance. Accounting is the second identity scanned for an initiator match. Any initiator in the accounting identity is given read-only access. Later, an administrator identity can be created with read-write access and placed in position 0.

acl add –ta finance –id accounting –acc rw –pos 1

Volume Copy Operations

Offline Copy

Data from any volume type can be replicated offline using the CLI command **volume copy create**. Off-line replication is faster than on-line replication but both the source and destination volumes must be off-line which can create an interruption of service to the volume host(s). Because snapshot volumes are internal (off-line) volumes, this is a way of copying a snapshot volume.

volume copy create

Switch	Definition	Type	Values/Remarks
-DST	DESTINATION	MANDATORY	ASCII STRING (MAXIMUM 10 CHARACTERS)
-SRC	SOURCE	MANDATORY	ASCII STRING (MAXIMUM 10 CHARACTERS)

Example

volume copy create –src ScienceLab –dst ScienceLabII

Online Copy

To perform on-line data replication, either by increasing the number of children in a mirrored volume or creating a mirrored copy of any other type of volume, except transparent and snapshot volumes, you can use the CLI commands **volume mirror add** followed by **volume mirror break**.

Note

The added child can be any type of volume, except transparent or snapshot, and it must be the same size or greater than the actual capacity of the mirror volume.

volume mirror add

Switch	Definition	Type	Values/Remarks
-CH	NEW CHILD TO ADD TO MIRROR	MANDATORY	ASCII STRING (MAXIMUM 10 CHARACTERS)
-VOL	ALIAS OF VOLUME	MANDATORY	ASCII STRING (MAXIMUM 10 CHARACTERS)
-NOSYNC	DISABLES AUTOMATIC MIRROR SYNC	OPTIONAL	DO NOT SPECIFY, NO VALUE ALLOWED FOR SWITCH

Example:

The simple volume, Sim6, is added as the third child to mirrored volume Mir4.

volume mirror add –vol Mir4 –ch Sim6

Use the CLI command **volume mirror sync show** to view the status of all mirror synchronizations.

volume mirror sync show

Source	Destination	Oper Status	Admin Status	Progress
SIM4	SIM6	OPERATING	SYNCHRONIZE	60%
CH1	CH3	ENDED OK	DUMMY	100%
SIMLE10	SIMPLE12	ENDED ERROR	ABORT	-

After the volume is 100% synchronized you can break the mirror to finish the online copy operation.

volume mirror break

Switch	Definition	Type	Values/Remarks
-CH	CHILD TO BE REMOVED FROM MIRROR	MANDATORY	ASCII STRING (MAXIMUM 10 CHARACTERS)
-VOL	ALIAS OF VOLUME	MANDATORY	ASCII STRING (MAXIMUM 10 CHARACTERS)

Example:

The simple volume Sim5 is removed from mirrored volume Mir1.

volume mirror break –vol Mir1 –ch Sim5

Snapshot Operations

Creating a Snapshot

You can create a *snapshot*, a point-in-time copy, of any volume using the CLI command **volume create snapshot**.

volume create snapshot

Switch	Definition	Type	Values/Remarks
-CH	ALIAS OF EACH VOLUME TO INCLUDE	MANDATORY	ASCII STRING (MAXIMUM 10 CHARACTERS)
-SRC	SOURCE VOLUME ALIAS	MANDATORY	ASCII STRING (MAXIMUM 10 CHARACTERS)
-VOL	ALIAS OF VOLUME TO CREATE	MANDATORY	ASCII STRING (MAXIMUM 10 CHARACTERS)
-ACTIVATE	ACTIVATION SNAPSHOT VOLUME	OPTIONAL	DO NOT SPECIFY VALUE
-LT	THRESHOLD LOAD %	OPTIONAL	5..**80**..100

Deactivating a Snapshot Volume

An activated snapshot volume can be deactivated. Deactivating a snapshot maintains the snapshot volume associated with its source volume but it deactivates the copy old on write recording to the snapshot volume while it is deactivated. A deactivated snapshot can be reactivated. Reactivating a snapshot erases the content of the snapshot, resetting the baseline to record changes to its source volume.

volume snapshot deactivate

Switch	Definition	Type	Values/Remarks
-VOL	ALIAS OF VOLUME	MANDATORY	ASCII STRING (MAXIMUM 10 CHARACTERS)

Reactivating a Snapshot Volume

volume snapshot activate

Switch	Definition	Type	Values/Remarks
-VOL	ALIAS OF VOLUME	MANDATORY	ASCII STRING (MAXIMUM 10 CHARACTERS)

Viewing Snapshot Volumes

You can view all created snapshot volumes using the CLI command **volume snapshot show**. Use this command to view the source and snapshot volumes, the time the snapshot was created and the percent capacity utilization. At user-defined load threshold utilization, an alert to resize the snapshot is sent.

volume snapshot show

Table 3-9: All Snapshot Volumes

Source	Snapshot	Date & Time	Utilization
MIRROR3	SNP1MIR3	12/12/02 13:00:00	80%
MIRROR3	SNP2MIR3	12/12/02 14:00:00	60%

You can view all snapshots of a single source volume using the CLI command **volume snapshot show -vol**.

volume snapshot show

Switch	Definition	Type	Values/Remarks
-TABLE	DISPLAYS DATA IN TABLE FORMAT	OPTIONAL	DEFAULT DISPLAY
-RECORD	DISPLAYS DATA IN RECORD FORMAT	OPTIONAL	
-VOL	ALIAS OF VOLUME	OPTIONAL	ASCII STRING (MAXIMUM 10 CHARACTERS)

Example:

Table 3-10 lists the only snapshot for Mirror7.

volume snapshot show –vol Mirror7

Table 3-10: All Snapshots of a Specific Volume

Snapshot	Date & Time	Utilization
Snp1Mir1	12/12/02 20:00:00	20%

Snapshot Rollback

Snapshot rollback allows you to rollback to the original state of the volume.

The command **volume snapshot rollback show** shows status of snapshot rollback.

volume snapshot rollback show

The command **volume snapshot rollback start** starts snapshot rollback.

volume snapshot rollback start

Switch	Definition	Type	Values/Remarks
-SNAP	ALIAS OF SNAPSHOT VOLUME	MANDATORY	ASCII STRING (MAXIMUM 10 CHARACTERS)
-FORCE	SKIP CONFIRMATION	OPTIONAL	DO NOT SPECIFY, NO VALUE ALLOWED FOR SWITCH

The command **volume snapshot rollback abort** aborts snapshot rollback.

volume snapshot rollback abort

Switch	Definition	Type	Values/Remarks
-SNAP	ALIAS OF SNAPSHOT VOLUME	MANDATORY	ASCII STRING (MAXIMUM 10 CHARACTERS)

Routine Volume Operations

Resizing a Volumes

volume resize

Switch	Definition	Type	Values/Remarks
-VOL	ALIAS OF VOLUME TO RESIZE	MANDATORY	ASCII STRING (MAXIMUM 10 CHARACTERS)
-WITH	VOLUME TO RESIZE WITH	MANDATORY	ASCII STRING (MAXIMUM 10 CHARACTERS)
-A	NEW ALIAS OF RESIZED VOLUME	OPTIONAL	ASCII STRING (MAXIMUM 10 CHARACTERS)

Example:

In Figure 3-12 the mirrored volume, Mir, is limited in its actual capacity by its smallest child, Sim2. To resize Sim2 to two terabytes, simple volume, Sim3, is concatenated to Sim2 to create the resized cube volume, XSim 2.

volume resize –vol Sim2 –a XSim2 –with Sim3

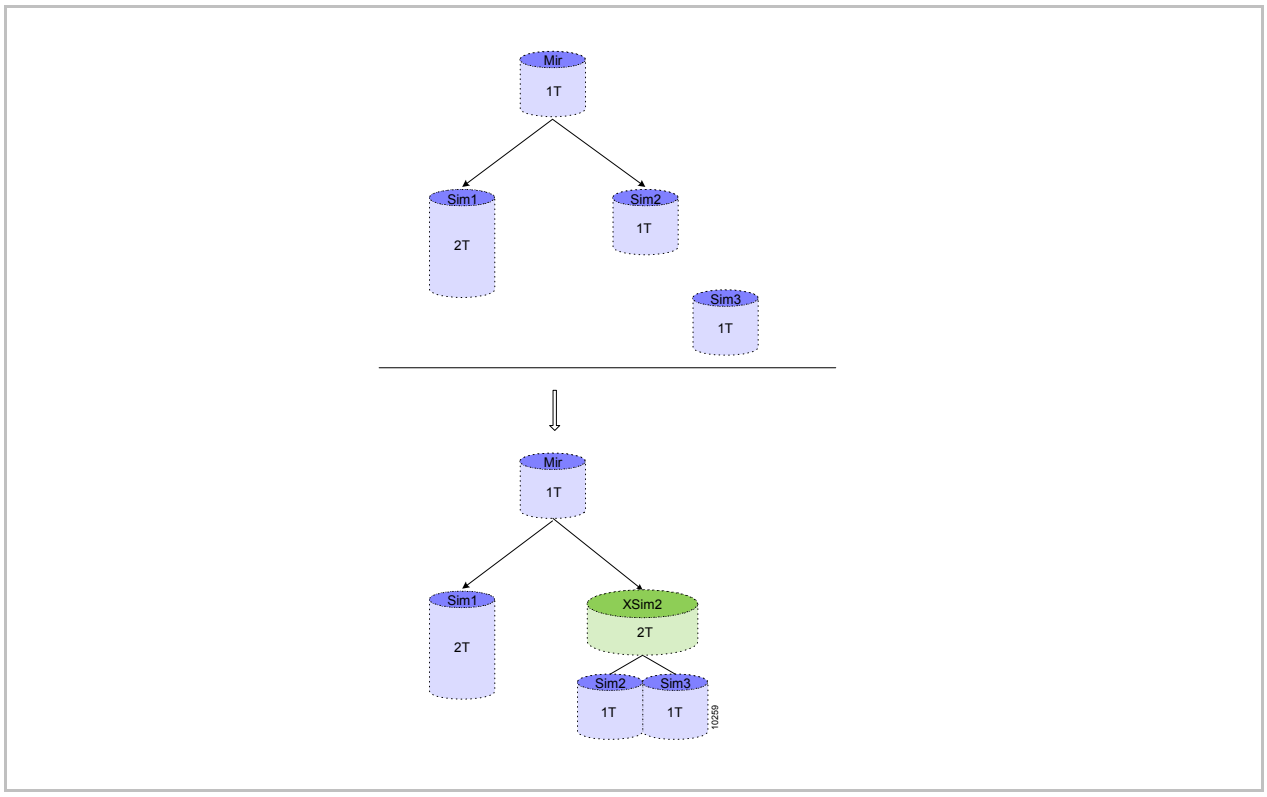


Figure 3-12. Resizing Mirrored Child

After resizing a volume but before expanding its hierarchy, you can use the CLI command **volume retract** to delete the added volume(s) used to resize the original volume. The head of the volume hierarchy is retracted, not the resized volume.

volume retract

Switch	Definition	Type	Values/Remarks
-VOL	ALIAS OF VOLUME	MANDATORY	ASCII STRING (MAXIMUM 10 CHARACTERS)

You must expand a volume's actual capacity, its capacity as identified by the file server, to match its resized potential capacity using the CLI command **volume expand**. If you do not expand the resized volume, its resized capacity will not be available for storage use. After expanding a volume, its host's file server will show its new capacity but the disk partition will not expand automatically. The host must expand the disk partition.

Example:

In Figure 3-13 a mirrored volume is expanded to two terabytes after one of its child volumes was resized and expanded to two terabytes.

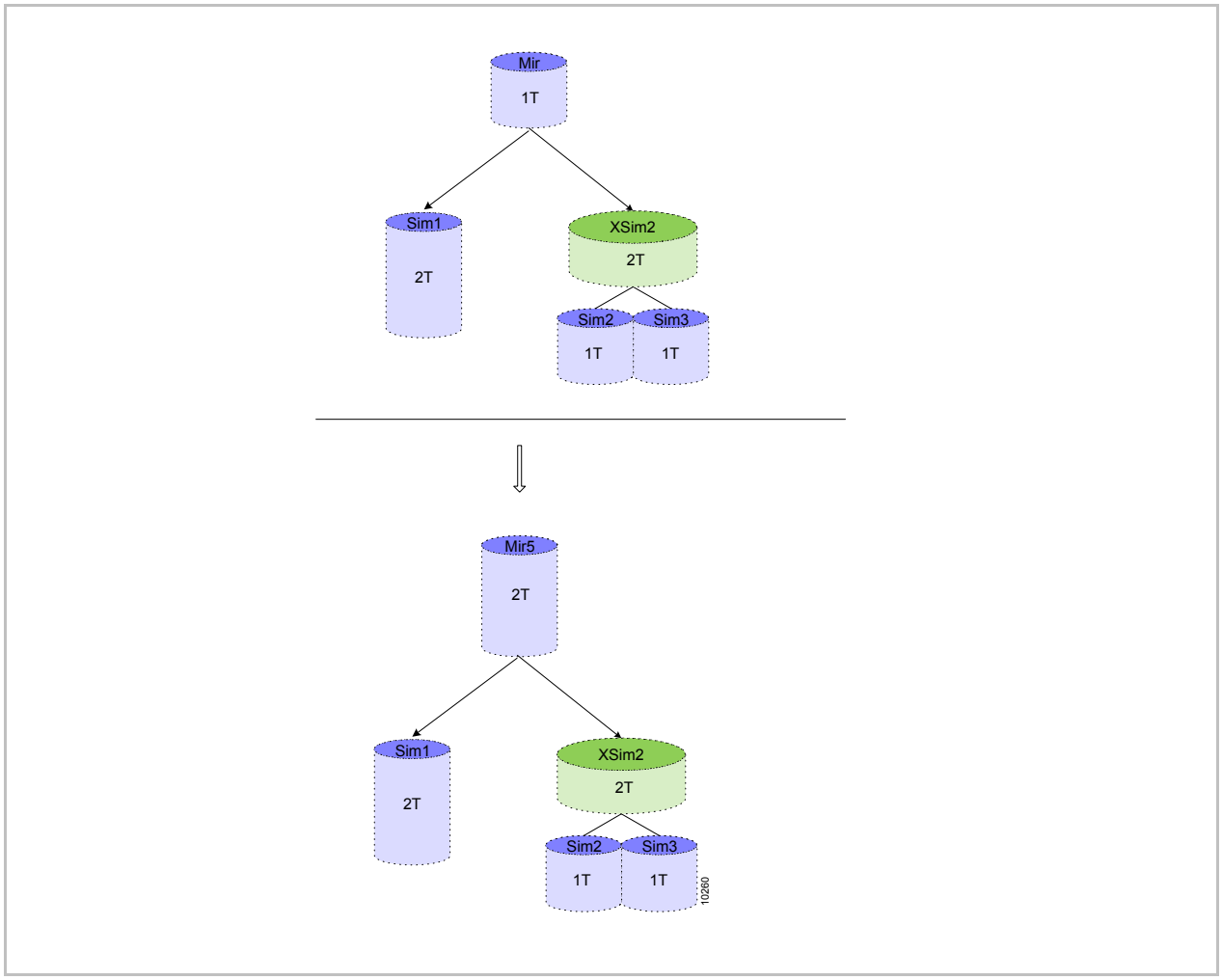


Figure 3-13. Expanding a Mirrored Volume

volume expand

Switch	Definition	Type	Values/Remarks
-VOL	ALIAS OF VOLUME	MANDATORY	ASCII STRING (MAXIMUM 10 CHARACTERS)

Example:

In Figure 3-14 the resized volume, XSim2, is expanded to an actual capacity of two terabytes to match its resized potential capacity. Once XSim2 is expanded, the capacity of Mir5 will automatically adjust itself to two terabytes.

volume expand –vol XSim2

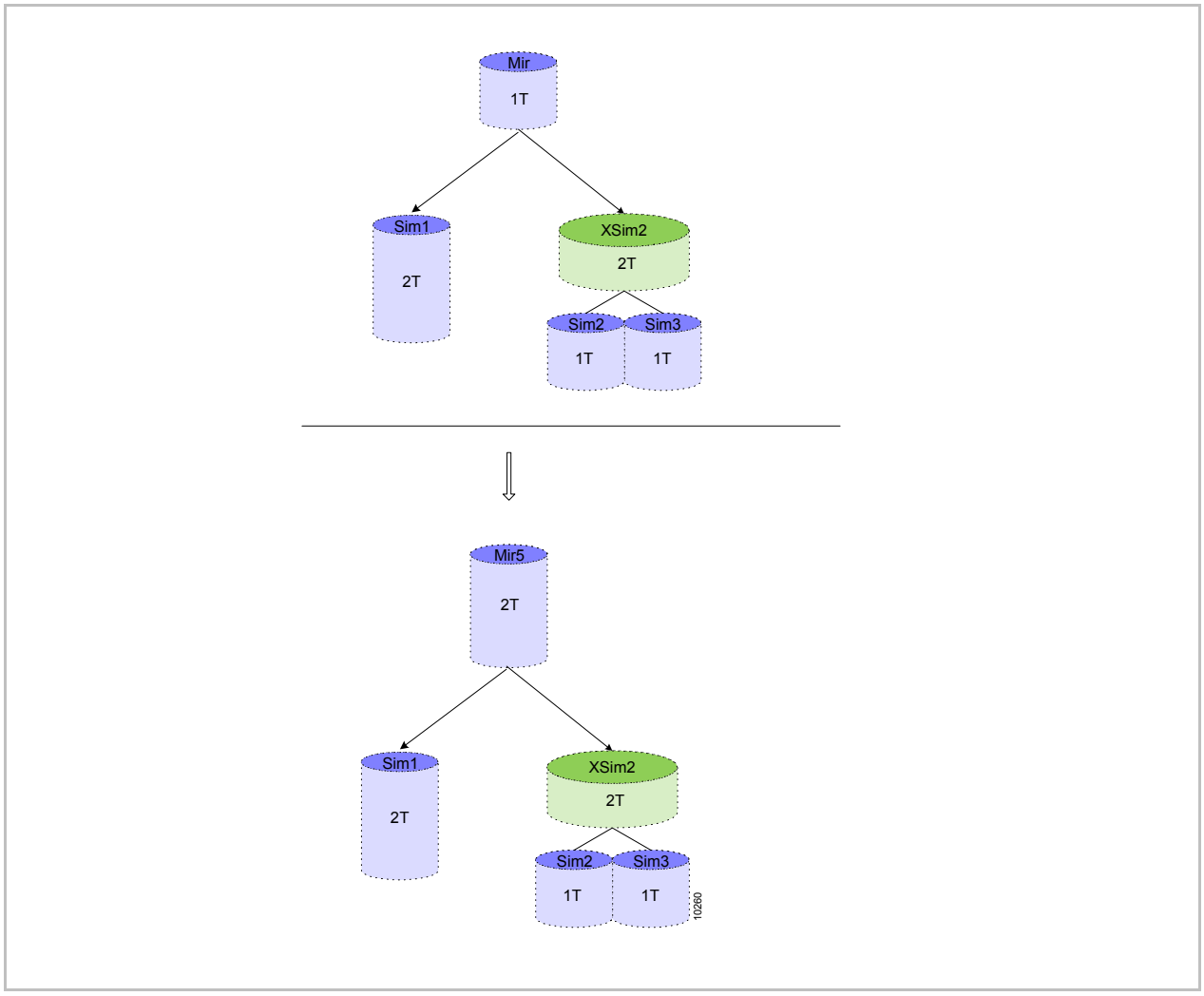


Figure 3-14. Expanding XSim2

Renaming a Volume

After creating a volume you can rename it. Renaming a volume will have no negative effect on the volume hierarchies built on the renamed volume.

volume set

Switch	Definition	Type	Values/Remarks
-NA	NEW ALIAS	MANDATORY	ASCII STRING (MAXIMUM 10 CHARACTERS)
-VOL	ALIAS OF VOLUME TO CHANGE	MANDATORY	ASCII STRING (MAXIMUM 10 CHARACTERS)

Example:

volume set –vol Concat1 –n JPGRepos

Removing a Volume

You can remove a volume. The volume must be inactive, that is not exposed, and it must be at the top level of its volume hierarchy. For example, you cannot remove a simple volume from within a set of volumes creating a striped volume. The striped volume is at the top of the hierarchy must be removed first.

volume remove

Switch	Definition	Type	Values/Remarks
-VOL	ALIAS OF VOLUME	MANDATORY	ASCII STRING (MAXIMUM 10 CHARACTERS)
-ALL	REMOVES A VOLUME AND **ALL VOLUMES COMPOSING IT** IN THE HIERARCHY	OPTIONAL	DO NOT SPECIFY, NO VALUE ALLOWED FOR SWITCH

Example:

The top-level volume Stripe 1 is removed while the component volumes, Simple 2, 4, 8 & 10, remain intact.

volume remove –vol Stripe1

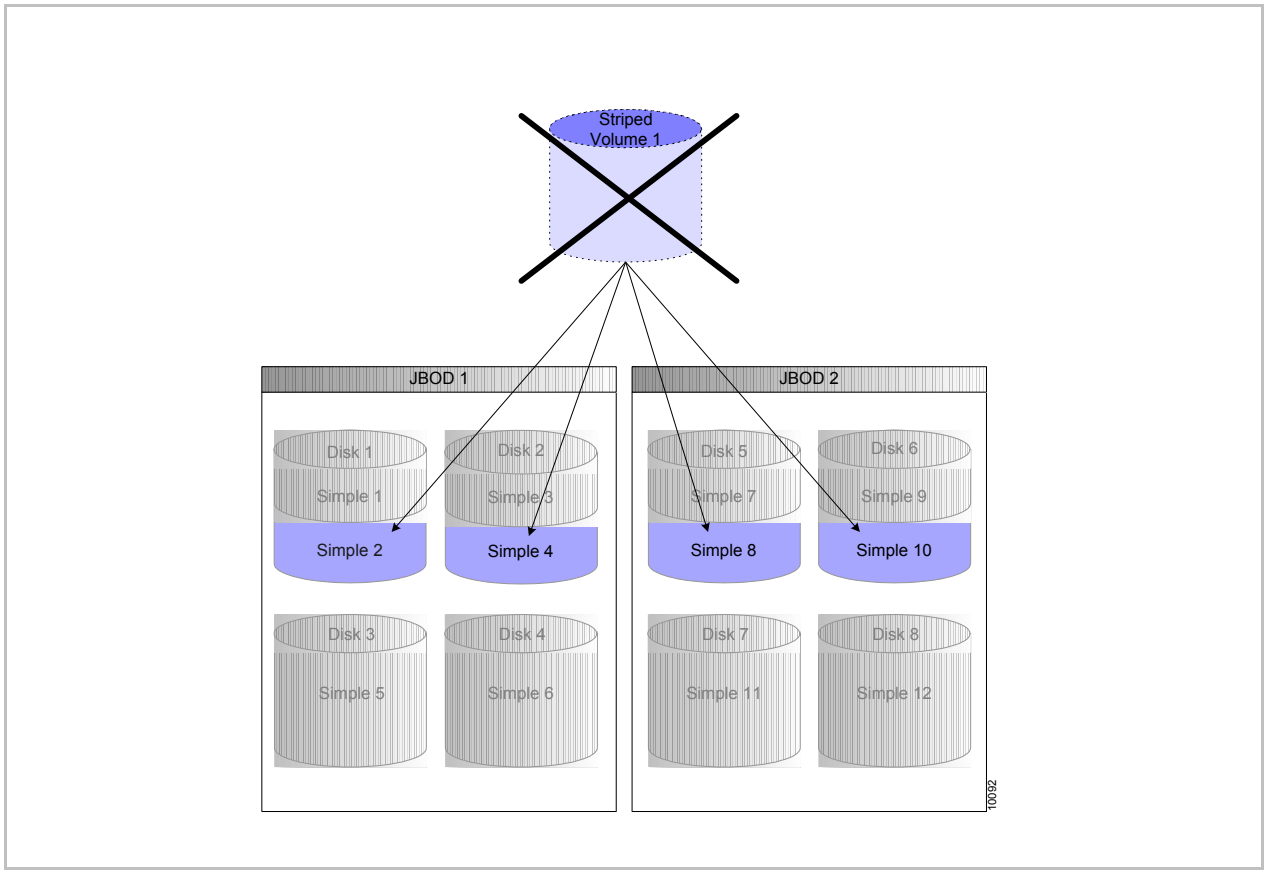


Figure 3-15. Stripe 1 Volume Removed

You can remove a volume and all of its component volumes in a volume hierarchy. The volume must be at the top of the hierarchy. The volume cannot be exposed; the volume LUN must be inactivated. Simple volumes will convert back to subdisks.

volume remove

Switch	Definition	Type	Values/Remarks
-VOL	ALIAS OF VOLUME	MANDATORY	ASCII STRING (MAXIMUM 10 CHARACTERS)
-ALL	REMOVES A VOLUME AND **ALL VOLUMES COMPOSING IT** IN THE HIERARCHY	OPTIONAL	DO NOT SPECIFY, NO VALUE ALLOWED FOR SWITCH

Example:

The top-level volume Stripe 1 is removed along with its component volumes, Simple 2, 4, 8 & 10.

volume remove -all –vol Stripe1

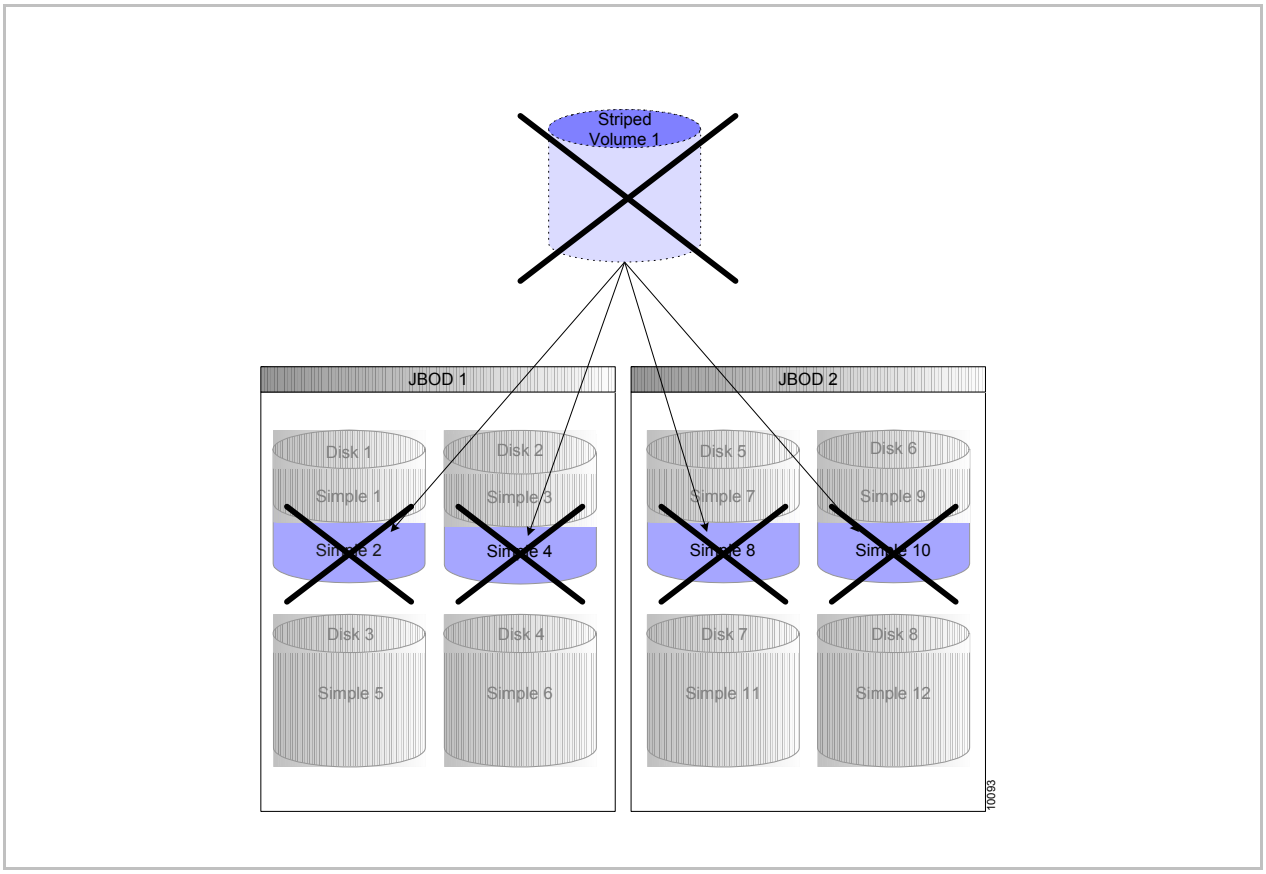


Figure 3-16. Stripe 1 Volume and Supporting Hierarchy Removed

Replacing a Volume

You can replace a volume with another volume. Use the CLI command **volume replace** after a disk failure to replace a volume used in a storage hierarchy with a volume on a functional disk. This is only a 'physical' replacement. The data on the failed disk is not copied to the new volume.

volume replace

Switch	Definition	Type	Values/Remarks
-NVOL	ALIAS OF NEW VOLUME	MANDATORY	ASCII STRING (MAXIMUM 10 CHARACTERS)
-VOL	ALIAS OF VOLUME	MANDATORY	ASCII STRING (MAXIMUM 10 CHARACTERS)

You can replace a failed volume in a mirror. You must then synchronize the new volume to the original mirrored volumes.

volume mirror sync start

Switch	Definition	Type	Values/Remarks
-DST	DESTINATION VOLUME	MANDATORY	ASCII STRING (MAXIMUM 10 CHARACTERS)
-SRC	SOURCE VOLUME	MANDATORY	ASCII STRING (MAXIMUM 10 CHARACTERS)

Example:

The volume Simple3 is synchronized to the volume Simple5.

volume mirror sync –src Simple3 –dst Simple5

If you are working in a cluster, the volume will be displayed in the state need sync on both i serieses. Synchronize the volume on the exposing i series using the CLI command **volume mirror sync**.

Chapter 4
Monitoring & Statistics

The i series enables RFC standards compliant health, interface and session monitoring of all i series interfaces.

For specific details on a monitoring parameter, consult the RFC standard 2863.

Health Monitoring

You can monitor the health of the i series hardware for fan malfunctions that could lead to overheating as well as power supply malfunctions both of which can nullify high availability and lead to i series failover.

system hardware show

This command shows all hardware interface connection statistics.

system hardware show

Table 4-1: System Hardware

MAX NUMBER OF POWER SUPPLIES:	2
PS STATUS:	1 WORKING
MAX NUMBER OF FANS:	2
FAN STATUS:	2 WORKING
MEMORY STATUS	OK
CPU TEMPERATURE (C):	59
CPU TEMPERATURE THRESHOLD (C):	WARNING 90; FAULTY 100
CPU TEMPERATURE STATUS:	OK
ON-BOARD TEMPERATURE (C):	33
ON-BOARD TEMPERATURE THRESHOLD (C):	WARNING 50; FAULTY 70
ON-BOARD TEMPERATURE STATUS	OK

You can change the default temperature scale to Fahrenheit using the CLI command device set –temperature_units f.

Interface Statistics

You can monitor interface traffic and errors for each i series interface to aid in system diagnostics. The interface monitoring has two components: the interface configuration and the counters.

interface statistics show

This command shows interface connection statistics.

interface statistics show

Switch	Definition	Type	Values/Remarks
-TABLE	DISPLAYS DATA IN TABLE FORMAT	OPTIONAL	DEFAULT DISPLAY
-RECORD	DISPLAYS DATA IN RECORD FORMAT	OPTIONAL	
-DETAILS	DISPLAYS DETAILS ABOUT INTERFACE	OPTIONAL[1]	
-IF	INTERFACE ALIAS	OPTIONAL	ASCII STRING (MAXIMUM 10 CHARACTERS)

Dependencies

optional[1]: switch -if is mandatory for details view

Table 4-2: Interface Statistics Show

Alias	In Octets	Out Octets	In Errors
CONS	0	0	0
MGMT	42040	129772	0
FC3	647295438498	390488847341	0
FC4	0	0	0
ETH1	535709973551	857473339209	0
ETH2	0	0	0
ETH3	0	0	0

Table 4-3: Interface Statistics Details

Alias:	eth1
DISCONTINUITY:	2 DAYS 1H:37M:9 SEC
IN/OUT OCTETS:	535709973551
IN/OUT UNICAST PKTS:	857473339209
IN/OUT DISCARDS:	0/0
IN/OUT ERRORS:	0/0
IN/OUT MULTICAST PKTS:	96251/0
IN/OUT BROADCAST PKTS:	403010/0

TCP/IP Statistics

ip statistics show

This command shows statistics for IP protocol counters.

ip statistics show

Table 4-4: IP Statistics

IN RECEIVES:	161853270
IN HEADER ERRORS:	683
IN ADDRESS ERRORS:	65177
IN UNKNOWN PROTOS:	0
IN DISCARDS:	0
IN DELIVERS:	161200809
OUT REQUESTS:	162958810
OUT DISCARDS:	0
OUT NO ROUTES:	3596
REASM. FRAGMENTS RECEIVED:	0
REASM. FRAGMENTS OK:	0
REASM. FAILURES:	0
FRAGMENTS OK:	0

IN RECEIVES:	161853270
FAILED TO FRAGMENT:	0
NUMBER GENERATED FRAG.:	0
ROUTING DISCARDS:	0

icmp statistics show

This command displays statistics for all the ICMP counters.

icmp statistics show

Table 4-5: ICMP Statistics

MESSAGES RECEIVED / SENT:	13/4
ERRORS IN / OUT:	0/0
DEST. UNREACH IN / OUT:	0/0
TIME EXCDS IN / OUT:	0/0
PARAM. PROBLEMS IN / OUT:	0/0
SRC QUENCH IN / OUT:	0/0
REDIRECT IN / OUT:	0/0
ECHOS IN / OUT:	4/0
ECHO REPLY IN / OUT:	0/4
TIMESTAMPS RECEIVED / SENT:	0/0
TIMESTAMPS REPLY RECEIVED / SENT:	0/0
ADDRESS MASKS RECEIVED / SENT:	0/0
ADDRESS MASKS REPLIES RECEIVED / SENT:	0/0

tcp connection show

This command shows all TCP connections.

tcp connection show

Table 4-6: TCP Connections

Local Address	Local Port	Remote Address	Remote Port	State
0.0.0.0	23	0.0.0.0	0	LISTEN
0.0.0.0	427	0.0.0.0	0	LISTEN
10.0.0.110	23	10.0.0.26	4943	ESTABLISHED
11.11.11.110	3260	0.0.0.0	0	LISTEN
11.11.11.110	3260	11.11.11.26	2176	ESTABLISHED
22.22.22.110	3260	0.0.0.0	0	LISTEN

tcp statistics show

This command shows all TCP connection counters.

tcp statistics show

Table 4-7: TCP Statistics

#CURRENT CONNECTIONS:	4
ACTIVE OPEN:	0
PASSIVE OPEN:	5
ATTEMPT FAILURES:	0
RESET ESTABLISHMENTS:	0
SEGMENTS RECEIVED:	16078975
SEGMENTS SENT:	162950234
SEGMENTS RETRANSMITTED:	3794
ERRORS RECEIVED:	50
RESET SENT:	0

udp listeners show

This command shows all UDP listeners.

udp listeners show

Local Address	Local Port
0.0.0.0	427
0.0.0.0	17185
0.0.0.0	56789
0.0.0.0	65532
10.0.0.110	161
127.0.0.1	65538

udp statistics show

This command shows all UDP connection counters.

udp statistics show

Table 4-8: UDP Statistics

Datagrams Received	408815
WRONG PORT DATAGRAMS	0
ERRORS DATAGRAMS	18681
DATAGRAMS SENT	78999

iSCSI Session Statistics

You can monitor iSCSI sessions including:

- All iSCSI sessions in and out of the i series.
- All iSCSI sessions for a specific initiator or target.
- Specific iSCSI session details.

iscsi session show

This command shows all iSCSI sessions, both in and out of the i series.

iscsi session show

Switch	Definition	Type	Values/Remarks
-TABLE	DISPLAYS DATA IN TABLE FORMAT	OPTIONAL	DEFAULT DISPLAY
-RECORD	DISPLAYS DATA IN RECORD FORMAT	OPTIONAL	
-DETAILS	DISPLAYS SPECIFIC DETAILS	OPTIONAL[1]	
-ID	iSCSI SESSION ID	OPTIONAL[1]	
-ADV	ADVANCED iSCSI SESSION DETAILS	OPTIONAL	DO NOT SPECIFY, NO VALUE ALLOWED FOR SWITCH

Dependencies

optional[1]: switch -id is mandatory for details view

Table 4-9: iSCSI Sessions

ID	Initiator	ISID	Target	TSIH
1.1.1	IQN.199*~	400001370000	NMS151	B701
1.2.1	IQN.199*~	400001370000	NMS151	7701
1.3.1	IQN.199*~	400001370000	NMS154	3B01
1.4.1	IQN.199*~	400001370000	NMS155	5701

This command details all statistics, either basic or advanced, for a specific iSCSI session.

iscsi session show -details -id

Table 4-10: Basic iSCSI Session Details

INITIATOR ALIAS:	NMS153
INITIATOR NAME:	IQN.1991-05.COM.MICROSOFT:QA-2.QA.TEST.COM
ISID:	400001370000
TARGET ALIAS:	NMS154DR
TARGET NAME:	NMS154DR
TSIH:	B701
TYPE:	NORMAL
AUTHENTICATION	DEF_ALL
CONNECTION ID:	1
STATE:	FULL (2)
LOCAL ADDRESS:	11.11.11.110
LOCAL PORT:	3260
REMOTE ADDRESS:	11.11.11.26
REMOTE PORTAL:	2178

Table 4-11: Advanced iSCSI Session Details

INITIAL R2T	FALSE
IMMEDIATE DATA	TRUE
MAX OUTSTANDING R2T	1
FIRST BURST SIZE	65536
MAX BURST SIZE	262114
NUMBER OF CONNECTIONS	1
SEQUENCE IN ORDER	TRUE
PDU IN ORDER	TRUE
ERROR RECOVERY LEVEL	0

iscsi session statistics

This command lists the statistics of all iSCSI sessions in and out of the i series.

iscsi session statistics

Switch	Definition	Type	Values/Remarks
-TA	TARGET ALIAS FOR STATISTICS	MANDATORY	ASCII STRING (MAXIMUM 10 CHARACTERS)
-TYPE	INITIATOR TYPE	MANDATORY	CRP, TXRX, ERROR

Example:

List the statistics of all iSCSI sessions for the target finance to initiator iqn.1991-05.microsoft:steven.brocade type crp.

iscsi session statistics –ta finance -initiator iqn.1991-05.microsoft:steven.brocade –type crp

Table 4-12: CRP iSCSI Session Details

ID	Initiator	ISID	TSIH	Cmd PDUs	Rsp PDUs
1	NMS153	400001370000	B701	36941394	36938928

Table 4-13: TXRX iSCSI Session Details

ID	Initiator	ISID	TSID	Tx Octets	Rx Octets
1	NMS153	400001370000	B701	2513649168	227187

Table 4-14: Error iSCSI Session Details

ID	Initiator	ISID	TSIH	Digests Err	Timeout Err
1	NMS153	400001370000	B701	0	0

iSCSI Connection Statistics

You can monitor iSCSI connections including:

- All iSCSI connections in and out of the i series.
- All iSCSI connections for a specific initiator or target.
- Specific iSCSI connection details.

iscsi session connection show

This command lists all connections in the i series.

iscsi session connection show

Switch	Definition	Type	Values/Remarks
-TABLE	DISPLAYS DATA IN TABLE FORMAT	OPTIONAL	DEFAULT DISPLAY
-RECORD	DISPLAYS DATA IN RECORD FORMAT	OPTIONAL	
-DETAILS	DISPLAYS SPECIFIC DETAILS	OPTIONAL[1]	
-ID	iSCSI CONNECTION ID	OPTIONAL[1]	
-ADV	ADVANCED PARAMETERS	OPTIONAL	DO NOT SPECIFY, NO VALUE ALLOWED FOR SWITCH

Dependencies

optional[1]: switch -id is mandatory for details view

Table 4-15: iSCSI Session Connections

ID	Cid	State	Local Address	Port	Remote Address	Port
1.1.1	0		11.11.11.110	3260	11.11.11.26	2178
1.2.1	0		11.11.11.110	3260	11.11.11.26	2176
1.3.1	0		11.11.11.110	3260	11.11.11.26	2177

iscsi session connection details

This command lists all connections of a specific session.

iscsi session connection details

Switch	Definition	Type	Values/Remarks
-ID	iSCSI CONNECTION ID	MANDATORY	X.X.X WHERE X.X.X IS THE VALUE SHOWN IN **'ISCSI SESSION CONNECTION SHOW'**
-ADV	ADVANCED PARAMETERS	OPTIONAL	DO NOT SPECIFY, NO VALUE ALLOWED FOR SWITCH

Table 4-16: iSCSI Session Connection Details

CONNECTION ID:	1
STATE:	FULL
LOCAL ADDRESS:	11.11.11.110
LOCAL PORT:	3260
REMOTE ADDRESS:	11.11.11.26
REMOTE PORT:	2178

Table 4-17: Advanced iSCSI Session Connection Details

RX DATA SEGMENT LENGTH:	65536
TX DATA SEGMENT LENGTH	65536
HEADER INTEGRITY	
DATA INTEGRITY	

SCSI Port Statistics

You can monitor both the SCSI/iSCSI target and initiator ports.

scsi target port statistics show

This command lists SCSI/iSCSI target port statistics.

scsi target port statistics show

Table 4-18: SCSI/iSCSI Initiator Port Statistics

Target	Port	Trans	In Commands	Read MB	Written MB
NMS154DR	42929	ISCSI	0	230845	244372
MNS155DR	42929	ISCSI	0	3863197	2498873

Remote iSCSI Initiator Statistics

You can monitor remote iSCSI initiators including:

- All initiators connected to the i series.
- All initiators connections to a specific target.
- Statistics of all connected initiators.

The CLI has a twenty-character display limit for initiator WWUIs. Use i series manager to view a WWUI longer than twenty characters.

iscsi rinitiator show

This command shows all remote iSCSI initiators connected to the i series.

iscsi rinitiator show

Switch	Definition	Type	Values/Remarks
-TABLE	DISPLAYS DATA IN TABLE FORMAT	OPTIONAL	DEFAULT DISPLAY
-RECORD	DISPLAYS DATA IN RECORD FORMAT	OPTIONAL	
-TA	DISPLAYS DATA FOR TARGET ALIAS	OPTIONAL	ASCII STRING (MAXIMUM 10 CHARACTERS)

Table 4-19: All Connected Remote iSCSI Initiators

Target Alias	Initiator Alias	Initiator Name
NMS154DR	IQN.1991-05.COM.MICR	IQN.1991-05.COM.MICR
NMS155DR	IQN.1991-05.COM.MICR	IQN.1991-05.COM.MICR

iscsi rinitiator list

This command lists the statistics of all remote iSCSI initiators connected to the i series.

iscsi rinitiator show -ta

Table 4-20: Connected Remote iSCSI Initiators on a Target

Name	Alias	ISID
IQN.1991*~	IQN.1991*~	40001370000

iscsi rinitiator statistics show

This command lists the statistics of all iSCSI remote initiators connected to the i series.

iscsi rinitiator statistics show

Target	Initiator	Attached Times	Out Commands	Written MB	Read MB
TA1	IQN.199*~	1	0	4848612	7382819
TA2	IQN.199*~	1	0	3914422	8773472
TA3	IQN.199*~	1	0	146699	399844

Logical Unit (LU) Statistics

This command shows all statistics for configured LUNs on the i series.

lu statistics show

Table 4-21: LU Statistics

LUN	Target	Commands	Read (MB)	Written (MB)	In Resets	OutTask SetFull
0	TA1	36938947	2308445	0	0	0
77	TA1	32638777	1	407972	0	0
0	TA2	199543	203571	22314	0	0
222	TA2	3209004	1661175	415591	0	0

Chapter 5
Command Line Interface Reference

The CLI is available via:

- Console port with a direct RS232 connection.
- 1 Gbit Ethernet network port (Eth1/Management 10/100) with a Telnet session.

The CLI is used to implement all i series management functions, including switching, virtualization and security.

> **Note:**
> *All CLI commands must be entered in lower case. Inputted data is case sensitive and can include upper and lowercase letters.*

The CLI command prompt is **>**.

All CLI commands in this chapter are listed first with the basic command followed by a table of command switches; their explanations and status (mandatory or optional). Default values are listed as **bold and underlined**.

The CLI supports the use of the following hot keys for the listed functions:

Table 5-1: Hot Keys

Command	Description
?	LIST OF COMMANDS WITH A SHORT DESCRIPTION OF EACH.
!	RETURN TO MAIN MENU. **NOTE:** ! CANNOT BE USED AS A VALUE OR PART OF ANY FIELD.
ESC	ABORT CURRENT COMMAND.
#	DISPLAYS PREVIOUS COMMAND IN COMMAND HISTORY. **NOTE: #** CANNOT BE USED AS A VALUE OR PART OF ANY FIELD.
TAB	USE THE TAB TO SKIP THROUGH ALL THE DIFFERENT COMMANDS. THE TAB CAN BE USED TO AUTO-COMPLETE PARTIALLY ENTERED COMMANDS.
↑ ↓	USE THE ARROWS SCROLL THROUGH PREVIOUS COMMANDS.
← →	USE THE ARROWS TO MOVE CURSOR LEFT/RIGHT WITHIN THE CLI COMMAND LINE.

Table 5-2 and Table 5-3 list the deprecated commands in version 3.3.X.

Table 5-2: Deprecated Command in Version 3.5

Command	Replaced By	Page
SYSTEM SET	SYSTEM CF SET	5-52
SYSTEM COPY	SYSTEM CF COPY	5-49
SYSTEM SHOW	SYSTEM CF SHOW	5-49

Table 5-3: Deprecated Command in Version 3.3

Command	Replaced By	Page
ACL DETAILS	ACL SHOW -TA	5-8
ACL IDENTITY DETAILS	ACL IDENTITY SHOW -DETAILS	5-8
FT EXPORT	FT UPLOAD TECHINFO	5-18
FT UPDATE	FT DOWNLOAD FIRMWARE	5-16
INFO	INTERFACE SHOW -DETAILS -IF	5-20
INTERFACE DETAILS	INTERFACE SHOW -DETAILS	5-20
INTERFACE STATISTICS DETAILS	INTERFACE STATISTICS SHOW -DETAILS -IF	5-20
IP STATISTICS ICMP SHOW	ICMP STATISTICS SHOW	5-18
IP STATISTICS IP SHOW	IP STATISTICS SHOW	5-25
ISCSI INITIATOR DETAILS	ISCSI INITIATOR SHOW	5-27
ISCSI RINITIATOR LIST	ISCSI RINITIATOR SHOW -TA	5-29
ISCSI RTARGET DETAILS	ISCSI RTARGET SHOW -DETAILS -RTA	5-30
ISCSI RTARGET RPORTAL LIST	ISCSI RTARGET RPORTAL SHOW -DETAILS -RTA	5-31
ISCSI SESSION CONNECTION DETAILS	ISCSI SESSION CONNECTION SHOW -DETAILS -ID	5-32
ISCSI SESSION DETAILS	ISCSI SESSION SHOW -DETAILS -ID	5-33
ISCSI TARGET ALIAS	ISCSI TARGET SHOW -RECORD	5-30
ISCSI TARGET DETAILS	ISCSI TARGET SHOW -DETAILS -TA	5-35
LU DETAILS	LU SHOW -DETAILS -TA'	5-36
NEIGHBOR DETAILS	NEIGHBOR SHOW -DETAILS -NB	5-38
STORAGE ALIAS	STORAGE SHOW -RECORD	5-46
STORAGE DETAILS	STORAGE SHOW -DETAILS -S	5-46
SUBDISK ALIAS	SUBDISK SHOW -RECORD -D	5-48

SUBDISK DETAILS	SUBDISK SHOW -DETAILS	5-48
VOLUME ALIAS	VOLUME SHOW -RECORD	5-65
VOLUME DETAILS	USE VOLUME SHOW -DETAILS -VOL	5-65
VOLUME SNAPSHOT LIST	VOLUME SNAPSHOT SHOW -VOL	5-65

i series CLI Commands

These commands enable you to configure and view the basic i series parameters needed to operate the i series.

-A-

acl add

Use the command **acl add** to link an identity to a target.

acl add

Switch	Definition	Type	Values/Remarks
-ID	IDENTITY ALIAS	MANDATORY	ASCII STRING (MAXIMUM 10 CHARACTERS)
-TA	ISCSI TARGET ALIAS	MANDATORY	ASCII STRING (MAXIMUM 10 CHARACTERS)
-ACC	ACCESS RIGHTS TO THE TARGET	OPTIONAL	**RW**, RO, NA
-POS	ACCESS PRIORITY LEVEL (POSITION) *	OPTIONAL	INTEGER 1-2147482646 * THE NEXT FREE POSITION

acl details

The command 'acl details' has been replaced by 'acl show -ta' (see page 5-8).

acl identity add chap

This command adds CHAP authentication credentials to an identity.

acl identity add chap

Switch	Definition	Type	Values/Remarks
-ID	IDENTITY ALIAS	MANDATORY	ASCII STRING (MAXIMUM 10 CHARACTERS)
-UN	HOST NAME	OPTIONAL [1]	ASCII STRING
-PW	HOST PASSWORD	OPTIONAL [1]	ASCII STRING [6-20 CHARACTERS]
-RADIUS	RADIUS SERVER	OPTIONAL [1]	FLAG

Dependencies

optional[1]:

when using '-radius': -id, -radius are mandatory, -un is optional, -pw is not an option

when not using '-radius': -id, -un, -pw are mandatory, -radius is not an option

acl identity add name

This command adds an iSCSI initiator to an identity.

acl identity add name

Switch	Definition	Type	Values/Remarks
-ID	IDENTITY ALIAS	MANDATORY	ASCII STRING (MAXIMUM 10 CHARACTERS)
-NAME	WWUI OF INITIATOR	MANDATORY	ISCSI WORLD WIDE UNIQUE IDENTIFIER (ASCII STRING OF MAX. 223 CHARACTERS)

acl identity add srp

This command adds SRP authentication credentials to an identity.

acl identity add srp

Switch	Definition	Type	Values/Remarks
-ID	IDENTITY ALIAS	MANDATORY	ASCII STRING (MAXIMUM 10 CHARACTERS)
-PW	HOST PASSWORD	MANDATORY	ASCII STRING [6-20 CHARACTERS]
-UN	HOST NAME	MANDATORY	ASCII STRING (MAXIMUM 80 CHARACTERS)

acl identity create

This command creates an identity.

acl identity create

Switch	Definition	Type	Values/Remarks
-ALIAS	IDENTITY ALIAS	MANDATORY	ASCII STRING (MAXIMUM 10 CHARACTERS)
-INFO	IDENTITY INFORMATION	OPTIONAL	ASCII STRING

acl identity delete

This command deletes an identity from the i series.

acl identity delete

Switch	Definition	Type	Values/Remarks
-ID	IDENTITY ALIAS	MANDATORY	ASCII STRING (MAXIMUM 10 CHARACTERS)

acl identity details

The command 'acl identity details' has been replaced by 'acl identity show -details' (see page 5-8)

acl identity remove chap

This command removes a CHAP authentication credential from an identity.

acl identity remove chap

Switch	Definition	Type	Values/Remarks
-ID	IDENTITY ALIAS	MANDATORY	ASCII STRING (MAXIMUM 10 CHARACTERS)
-UN	HOST NAME	OPTIONAL[1]	ISCSI WORLD WIDE UNIQUE IDENTIFIER (ASCII STRING OF MAX. 223 CHARACTERS)

Dependencies

optional[1]: mandatory if not using RADIUS

acl identity remove name

This command removes an iSCSI initiator from an identity.

acl identity remove name

Switch	Definition	Type	Values/Remarks
-ID	IDENTITY ALIAS	MANDATORY	ASCII STRING (MAXIMUM 10 CHARACTERS)
-NAME	HOST NAME	MANDATORY	ISCSI WORLD WIDE UNIQUE IDENTIFIER (ASCII STRING OF MAX. 223 CHARACTERS)

acl identity remove srp

This command removes an SRP authentication credential from an identity.

acl identity remove srp

Switch	Definition	Type	Values/Remarks
-ID	IDENTITY ALIAS	MANDATORY	ASCII STRING (MAXIMUM 10 CHARACTERS)
-UN	HOST NAME	OPTIONAL[1]	ISCSI WORLD WIDE UNIQUE IDENTIFIER (ASCII STRING OF MAX. 223 CHARACTERS)

Dependencies

optional[1]: mandatory if not using RADIUS

acl identity set

This command allows changes to an identity.

acl identity set

Switch	Definition	Type	Values/Remarks
-ID	IDENTITY ALIAS	MANDATORY	ASCII STRING (MAXIMUM 10 CHARACTERS)
-INFO	IDENTITY INFORMATION	OPTIONAL	ASCII STRING
-NA	NEW ALIAS FOR IDENTITY	OPTIONAL	ASCII STRING (MAXIMUM 10 CHARACTERS)

acl identity show

This command lists the identities in a i series.

acl identity show

Switch	Definition	Type	Values/Remarks
-TABLE	DISPLAYS DATA IN TABLE FORMAT	OPTIONAL	DEFAULT DISPLAY
-RECORD	DISPLAYS DATA IN RECORD FORMAT	OPTIONAL	
-DETAILS	DISPLAYS SPECIFIC DETAILS	OPTIONAL	
-ID	USER-ASSIGNED ALIAS FOR IDENTITY	OPTIONAL[1]	ASCII STRING (MAXIMUM 10 CHARACTERS)

Dependencies

optional[1]: switch -id is mandatory for details view

acl remove

This command removes an identity from the access control list of a specific target.

acl rem

Switch	Definition	Type	Values/Remarks
-ID	IDENTITY ALIAS	MANDATORY	ASCII STRING (MAXIMUM 10 CHARACTERS)
-TA	ISCSI TARGET ALIAS	MANDATORY	ASCII STRING (MAXIMUM 10 CHARACTERS)

acl set

Use the command **acl set** to modify a target's access rights and identity position.

acl set

Switch	Definition	Type	Values/Remarks
-ID	IDENTITY ALIAS	MANDATORY	ASCII STRING (MAXIMUM 10 CHARACTERS)
-TA	ISCSI TARGET ALIAS	MANDATORY	ASCII STRING (MAXIMUM 10 CHARACTERS)
-ACC	ACCESS RIGHTS TO THE TARGET	OPTIONAL [1]	RW, RO, NA
-POS	ACCESS PRIORITY LEVEL (POSITION)	OPTIONAL [1]	

Dependencies

optional [1]: one of the optional switches is mandatory when changing

acl show

This command shows all target access per identity for the i series.

acl show

Switch	Definition	Type	Values/Remarks
-TABLE	DISPLAYS DATA IN TABLE FORMAT	OPTIONAL	DEFAULT DISPLAY
-RECORD	DISPLAYS DATA IN RECORD FORMAT	OPTIONAL	
-TA	USER-ASSIGNED ALIAS FOR TARGET	OPTIONAL	ASCII STRING (MAXIMUM 10 CHARACTERS)

admin add

This command adds a user name to the list of valid user login names for the i series. A user name can be from 1 to 19 characters long, including spaces. A password can be from 6 to 11 characters long, including spaces.

admin add

Switch	Definition	Type	Values/Remarks
-PW	USER PASSWORD	MANDATORY	ASCII STRING 6-11 CHARACTERS
-UN	USER NAME	MANDATORY	ASCII STRING 1—19 CHARACTERS

admin password

This interactive command enables a user to change their login password for their user name on the i series. You can only change the password of the current active user.

admin password

admin remove

This command deletes a user name from the list of valid user login names for the i series. Any user name, except the logged in user name, can be deleted.

admin remove

Switch	Definition	Type	Values/Remarks
-UN	USER NAME	MANDATORY	ASCII STRING 1—19 CHARACTERS

admin show

This command shows all valid user login names for the i series.

admin show

-C-

cluster failover disable

This command disables the cluster failover functionality. This command must be executed on both iSCSI Gateways in the cluster.

cluster failover disable

cluster failover enable

This command enables the cluster failover functionality. This command must be executed on both i serieses in the cluster.

cluster failover enable

cluster failover force

This command forces the switch to take over.

cluster failover force

cluster set

This command allows you to modify a cluster's parameters.

cluster set

Switch	Definition	Type	Values/Remarks
-FINT	FAILOVER INTERVAL TIME WHEN SUSPICIOUS INTERVAL IS EXCEEDED	OPTIONAL[1]	
-KAI	KEEP ALIVE INTERVAL TIME BETWEEN KEEP ALIVE SIGNALS FROM NEIGHBORS	OPTIONAL[1]	
-SINT	SUSPICIOUS INTERVAL TIME FROM WHEN A SIGNAL WAS EXPECTED BUT NOT RECEIVED	OPTIONAL[1]	

Dependencies

optional[1]: at least one of the switches is mandatory

cluster show

This command shows the cluster parameters.

cluster show

cluster synchronize lusn

This command allows you to synchronize the serial number of the logical units in case the master was configured before the neighbor.

cluster synchronize lusn

-D-

debug

This command is used for advanced troubleshooting operations and requires a password from Technical Support.

Note:
Do not use this command unless instructed to do so by technical support.

debug

device advance set

This command redefines the specified advanced parameter of the i series.

device advance set

Switch	Definition	Type	Values/Remarks
-PARAM	THE EXACT NAME OF PARAMETER IN CONFIG FILE	MANDATORY	ASCII STRING
-VAL	NEW VALUE TO WRITE TO CONFIG FILE	OPTIONAL [1]	ASCII STRING
-DEFAULT	RESET THE PARAMETER TO DEFAULT FACTORY VALUE	OPTIONAL [1]	ASCII STRING

Dependencies

optional [1]: one of the optional switches is mandatory

device advance show

This command shows the specified advanced parameter of the i series.

device show

Switch	Definition	Type	Values/Remarks
-PARAM	THE EXACT NAME OF PARAMETER IN CONFIG FILE	MANDATORY	ASCII STRING

device set

Use the CLI command **device set** to add or change management parameters. This command will not appear in the CLI menu until the i series is initialized.

device set

Switch	Definition	Type	Values/Remarks
-C	CONTACT PERSON IN THE EVENT OF A SYSTEM MALFUNCTION	OPTIONAL [1]	ASCII STRING
-D	LOCAL DATE	OPTIONAL [1]	DD/MM/YYYY
-ID	I SERIES ID IN A CLUSTER	OPTIONAL [1]	0, 1* *EACH I SERIES MUST HAVE A DIFFERENT ID
-IF	MANAGEMENT PORT ALIAS	OPTIONAL [1]	ETH1: (DEFAULT FOR I SERIES 2000) MGNT: (DEFAULT FOR I SERIES 3000, 38000, NOT AVAILABLE FOR I SERIES 2000)

Switch	Definition	Type	Values/Remarks
-IM	MANAGEMENT PORT IP MASK	OPTIONAL[1]	IP NETWORK MASK **255.255.255.0**
-IP	MANAGEMENT PORT IP ADDRESS	OPTIONAL[1]	IP ADDRESS
-LOC	LOCATION OF THE CONTACT PERSON	OPTIONAL[1]	ASCII STRING
-N	I SERIES NAME	OPTIONAL[1]	ASCII STRING
-P	PORT THROUGH WHICH ALL SNMP COMMUNICATIONS WILL FLOW	OPTIONAL[1]	INTEGER IN RANGE 0..65535 **161**
-RCOM	READ COMMUNITY	OPTIONAL[1]	ASCII STRING (MAXIMUM 80 CHARACTERS) **PUBLIC**
-RLD	REPORT LUN DISCOVERY	OPTIONAL[1]	**Y**(ES), N(O)
-T	LOCAL TIME	OPTIONAL[1]	HH:MM
-TELNET	TELNET PORT FOR I SERIES COMMUNICATIONS	OPTIONAL[1]	**23**
-TEMPERATURE_UNITS	TEMPERATURE DISPLAY SCALE	OPTIONAL[1]	**C**(ELCIUS), F(AHRENHEIT)
-WCOM	WRITE COMMUNITY	OPTIONAL[1]	ASCII STRING (MAXIMUM 80 CHARACTERS) **PRIVATE**

Dependencies

optional[1]: at least one of the switches is mandatory

-E-

exit

This command closes the Telnet/SSH session. It is not available when connected via RS-232 connection.

exit

-F-

fc interface show

This command shows each FC port and its World Wide Port Name (WWPN).

Note:
This command is available only when an FC interface is present.

fc interface show

fc node show

This command shows the i series World Wide Node Name (WWNN).

Note:
This command is available only when an FC interface is present.

fc node show

fc set

This command allows you to set the speed of the FC communication.

Note:
This command is available only when an FC interface is present.

fc set

Switch	Definition	Type	Values/Remarks
-IF	STORAGE PORT	MANDATORY	ASCII STRING (MAXIMUM 10 CHARACTERS)
-CM	CONNECTION MODE	OPTIONAL	**AUTO** (AUTO DETECT)* FAB (FABRIC), PUL (PUBLICLOOP), PRL (PRIVATELOOP) PTP (POINT-TO-POINT)
-SP	FC COMMUNICATION SPEED	OPTIONAL	0: AUTO **1**: 1 GB 2: 2 GB 4: 4 GB

* **Note:** auto detect and ptp are not available for versions prior to 3.3.

ft autoupload disable

This command stops the automatic export of logs.

ft autoupload enable

This command starts the automatic upload/export of the logs.

ft autoupload enable

Switch	Definition	Type	Values/Remarks
-IP	IP ADDRESS OF TELNET STATION WHERE TFTP APPLICATION SITS	MANDATORY	IP ADDRESS
-PORT	UDP PORT NUMBER	OPTIONAL	INTEGER IN RANGE 0..65535 **69**
-FD	DIRECTORY TO EXPORT FILES TO	OPTIONAL*	ASCII STRING (MAXIMUM 10 CHARACTERS)
-TIMEOUT	TIMEOUT IN SECONDS	OPTIONAL	1..**15**
-RETRIES	NUMBER OF RETRIES	OPTIONAL	1..**3**..8

* **Note:** Some TFTP servers do not accept the '\' option. These servers should be configured to "Allow '\' as virtual root" by the user.

ft autoupload show

This command displays the configuration of the autoupload feature.

ft autoupload show

Switch	Definition	Type	Values/Remarks
-TABLE	DISPLAYS DATA IN TABLE FORMAT	OPTIONAL	DEFAULT DISPLAY
-RECORD	DISPLAYS DATA IN RECORD FORMAT	OPTIONAL	
-DETAILS	DISPLAYS DETAILS	OPTIONAL	

ft download <x>

where <x> = config/db/firmware

This command downloads the config/database/firmware file.

ft download <X>

Switch	Definition	Type	Values/Remarks
-IP	IP ADDRESS OF TELNET STATION WHERE TFTP APPLICATION SITS	MANDATORY	IP ADDRESS
-PORT	UDP PORT NUMBER	OPTIONAL	INTEGER IN RANGE 0..65535 **69**
-FN	DIRECTORY TO EXPORT FILES TO	MANDATORY	ASCII STRING MUST END WITH '\' OR '/'
-TIMEOUT	TIMEOUT IN SECONDS	OPTIONAL	1..**15**
-RETRIES	NUMBER OF RETRIES	OPTIONAL	1..**3**..8

ft export

The command 'ft export' has been replaced by 'ft upload techinfo' (see page 5-18).

ft show

The command displays information about the file transfer status.

ft show

Switch	Definition	Type	Values/Remarks
-TABLE	DISPLAYS DATA IN TABLE FORMAT	OPTIONAL	DEFAULT DISPLAY
-RECORD	DISPLAYS DATA IN RECORD FORMAT	OPTIONAL	
-DETAILS	DISPLAYS SPECIFIC DETAILS	OPTIONAL	
-DATE	DATE OF TRANSFER IN DD/MM/YYYY	OPTIONAL	ASCII STRING (MAXIMUM 10 CHARACTERS)
-TIME	TIME OF TRANSFER IN HH:MM	OPTIONAL[1]	
-LATEST	LAST TRANSFER	OPTIONAL[2]	

Dependencies

optional[1]: switch -date is mandatory for with -time.
optional[2]: switch cannot be used with -date or -time.

ft update

The command 'ft update' has been replaced by 'ft download firmware' (see page 5-16).

ft upload <x>

where <x> = config /db/log/map/techinfo

This command uploads a i series <x> file from the i series to the local TFTP server.

ft upload <x>

Switch	Definition	Type	Values/Remarks
-IP	TFTP SERVER IP ADDRESS	MANDATORY	IP ADDRESS
-FD	DIRECTORY TO EXPORT FILES TO	OPTIONAL[1]	ASCII STRING EXISTS ONLY FOR MAP
-FN	FILE DIRECTORY AND FILENAME	MANDATORY	ASCII STRING
-PORT	UDP PORT NUMBER	OPTIONAL	INTEGER IN RANGE 0..65535 **69**
-RETRIES	NUMBER OF RETRIES	OPTIONAL	1..**3**..8
-TIMEOUT	TIMEOUT IN SECONDS	OPTIONAL	1..**15**

Dependencies

optional[1]: switch -fd is optional and exists only for map

-|-

icmp statistics show

This command displays statistics for all the icmp counters.

icmp statistics show

info

This command displays the current i series configuration and serial number.

info

The command 'info' has been replaced by 'interface show -details -if' (see page 5-20).

interface details

The command 'interface details' has been replaced by 'interface show -details' (see page 5-20).

interface reset

This command resets the specified interface alias.

interface reset

Switch	Definition	Type	Values/Remarks
-IF	CURRENT INTERFACE ALIAS	MANDATORY	ASCII STRING (MAXIMUM 10 CHARACTERS)

interface set

This command renames the specified interface alias. Leaving the new alias field blank will return the alias to its default setting. You can disable the interface.

interface set

Switch	Definition	Type	Values/Remarks
-IF	CURRENT INTERFACE ALIAS	MANDATORY	ASCII STRING (MAXIMUM 10 CHARACTERS)
-NA	NEW ALIAS	OPTIONAL	ASCII STRING (MAXIMUM 10 CHARACTERS)
-ENABLE	ENABLES INTERFACE	OPTIONAL	INTERFACE SHOW COMMAND STATUS IS: LINK UP, LINK DOWN
-DISABLE	DISABLES INTERFACE	OPTIONAL	INTERFACE SHOW COMMAND STATUS IS: DISABLED

interface show

This command shows the i series interfaces (ports) and their parameters.

interface show

Switch	Definition	Type	Values/Remarks
-TABLE	DISPLAYS DATA IN TABLE FORMAT	OPTIONAL	DEFAULT DISPLAY
-RECORD	DISPLAYS DATA IN RECORD FORMAT	OPTIONAL	
-DETAILS	DISPLAYS DETAILS ABOUT INTERFACE	OPTIONAL	
-IF	INTERFACE ALIAS	OPTIONAL[1]	ASCII STRING (MAXIMUM 10 CHARACTERS)

Dependencies

optional[1]: mandatory with -details

interface statistics details

The command 'interface statistics details' has been replaced by 'interface statistics show -details -if' (see page 5-20).

interface statistics show

This command shows all interface connection statistics.

interface statistics show

Switch	Definition	Type	Values/Remarks
-TABLE	DISPLAYS DATA IN TABLE FORMAT	OPTIONAL	DEFAULT DISPLAY
-RECORD	DISPLAYS DATA IN RECORD FORMAT	OPTIONAL	
-DETAILS	DISPLAYS DETAILS ABOUT INTERFACE	OPTIONAL[1]	
-IF	INTERFACE ALIAS	OPTIONAL	ASCII STRING (MAXIMUM 10 CHARACTERS)

Dependencies

optional[1]: switch -if is mandatory for details view

ip config remove

This command removes an IP address from an interface.

ip config remove

Switch	Definition	Type	Values/Remarks
-IP	IP ADDRESS TO REMOVE FROM THE NETWORK INTERFACE PORT	MANDATORY	IP ADDRESS

ip config set

This command configures a new IP address or edits an existing one.

ip config set

Switch	Definition	Type	Values/Remarks
-IP	IP ADDRESS ASSIGNED TO INTERFACE PORT	MANDATORY	IP ADDRESS
-IF	NETWORK INTERFACE PORT	MANDATORY[1]	ETH1, ETH2, ETH3 (FOR NEW CONFIGURATION)
-ACT	ACTIVITY STATUS IF IP ADDRESS IS ACTIVE TO EXPOSE VOLUMES. USE INACTIVE STATUS TO ALLOW FAILOVER.	OPTIONAL	**1** (ACTIVE), 2 (INACTIVE) RELEVANT ONLY IN CLUSTER
-IM	IP NETWORK MASK	OPTIONAL	IP NETWORK MASK **255.255.255.0**

Dependencies

mandatory[1]: necessary for new configurations

ip config show

This command displays the i series IP configurations.

ip config show

Switch	Definition	Type	Values/Remarks
-TABLE	DISPLAYS DATA IN TABLE FORMAT	OPTIONAL	DEFAULT DISPLAY
-RECORD	DISPLAYS DATA IN RECORD FORMAT	OPTIONAL	

ip isns add

This command adds an iSNS server's IP address to the i series iSNS client.

ip isns add

Switch	Definition	Type	Values/Remarks
-IP	IP ADDRESS OF ISNS SERVER	MANDATORY	IP ADDRESS UP TO 2 ISNS SERVERS

ip isns remove

This command removes an iSNS server's IP address from the i series iSNS client.

ip isns remove

Switch	Definition	Type	Values/Remarks
-IP	IP ADDRESS OF ISNS SERVER	MANDATORY	IP ADDRESS

ip isns show

This command shows all iSNS servers configured on the i series.

ip isns show

Switch	Definition	Type	Values/Remarks
-TABLE	DISPLAYS DATA IN TABLE FORMAT	OPTIONAL	DEFAULT DISPLAY
-RECORD	DISPLAYS DATA IN RECORD FORMAT	OPTIONAL	

ip radius add

This command adds a RADIUS server IP address to the i series RADIUS client.

ip radius add

Switch	Definition	Type	Values/Remarks
-IP	IP ADDRESS OF RADIUS SERVER	MANDATORY	IP ADDRESS UP TO 2 RADIUS SERVERS
-K	SHARED SECRET BETWEEN I SERIES AND RADIUS SERVER	MANDATORY	ASCII STRING (MAXIMUM 80 CHARACTERS) MIN 16 CHARACTERS
-P	UDP PORT NUMBER TO SEND REQUESTS TO RADIUS SERVER	OPTIONAL	INTEGER IN RANGE 0..65535 **1812**

ip radius remove

This command removes a RADIUS server IP address from the i series RADIUS client.

ip radius remove

Switch	Definition	Type	Values/Remarks
-IP	IP ADDRESS OF RADIUS SERVER	MANDATORY	IP ADDRESS
-P	UDP PORT NUMBER TO SEND REQUESTS TO RADIUS SERVER	OPTIONAL	INTEGER IN RANGE 0..65535

ip radius set

This command allows changes to a RADIUS server configuration on the i series RADIUS client.

ip radius set

Switch	Definition	Type	Values/Remarks
-IP	IP ADDRESS OF RADIUS SERVER	MANDATORY	IP ADDRESS
-K	SHARED SECRET BETWEEN I SERIES AND RADIUS SERVER	OPTIONAL[1]	ASCII STRING MINIMUM 16 CHARACTERS
-P	UDP PORT NUMBER TO SEND REQUESTS TO RADIUS SERVER	OPTIONAL[1]	INTEGER IN RANGE 0..65535 **1812**

Dependencies

optional[1]: at least one of the switches is mandatory

ip radius show

This command shows all IP addresses for RADIUS servers configured on the i series RADIUS client.

Switch	Definition	Type	Values/Remarks
-TABLE	DISPLAYS DATA IN TABLE FORMAT	OPTIONAL	DEFAULT DISPLAY
-RECORD	DISPLAYS DATA IN RECORD FORMAT	OPTIONAL	

ip route add

This command adds an IP route to a network port.

ip route add

Switch	Definition	Type	Values/Remarks
-DIP	DESTINATION IP	MANDATORY	IP ADDRESS
-GW	GATEWAY ROUTER IP ADDRESS	MANDATORY	IP ADDRESS
-IF	INTERFACE ALIAS	MANDATORY	ASCII STRING (MAXIMUM 10 CHARACTERS)
-DMASK	HOST DESTINATION IP MASK	OPTIONAL[1]	**255.255.255.255**

Dependencies

optional[1]: mandatory when '-dip = subnet IP' (network route)

ip route default

This command sets a default IP route to a network port.

ip route default

Switch	Definition	Type	Values/Remarks
-GW	IP ADDRESS OF THE DEFAULT GATEWAY ROUTER	MANDATORY	IP ADDRESS
-IF	INTERFACE ALIAS	OPTIONAL	**ETH1**, MGNT

ip route remove

This command removes an IP route from a network port.

ip route remove

Switch	Definition	Type	Values/Remarks
-DIP	HOST DESTINATION IP ADDRESS	MANDATORY	IP ADDRESS
-DMASK	HOST DESTINATION IP MASK	OPTIONAL	IP NETWORK MASK **255.555.255.255**
-GW	GATEWAY TO HOST STATION IP ADDRESS	OPTIONAL	IP ADDRESS

ip route show

This command shows all IP routes on a i series.

ip route show

Switch	Definition	Type	Values/Remarks
-TABLE	DISPLAYS DATA IN TABLE FORMAT	OPTIONAL	DEFAULT DISPLAY
-RECORD	DISPLAYS DATA IN RECORD FORMAT	OPTIONAL	

ip statistics icmp show

The command 'ip statistics icmp show' has been replaced by 'icmp statistics show ' (see page 5-18).

ip statistics ip show

The command 'ip statistics ip show' has been replaced by 'ip statistics show ' (see page 5-25).

ip statistics show

This command shows statistics for IP protocol counters.

ip statistics show

iscsi discovery rportal add

This command creates a new portal to discover remote targets.

iscsi discovery rportal add

Switch	Definition	Type	Values/Remarks
-IP	NETWORK PORT IP ADDRESS	MANDATORY	IP ADDRESS
-PERIOD	PERIOD FOR REDISCOVER IN SECONDS	OPTIONAL	INTEGER IN RANGE 0..65535 **1800**
-PORT	TCP PORT FOR ISCSI COMMUNICATION	OPTIONAL	INTEGER IN RANGE 0..65535 **3260**

iscsi discovery rportal discover

This command performs a manual discovery for specific remote ports.

Switch	Definition	Type	Values/Remarks
-IP	NETWORK PORT IP ADDRESS	MANDATORY	IP ADDRESS
-PORT	TCP PORT FOR ISCSI COMMUNICATION	OPTIONAL	INTEGER IN RANGE 0..65535 **3260**

iscsi discovery rportal remove

This command removes specific remote discovery ports.

Switch	Definition	Type	Values/Remarks
-IP	NETWORK PORT IP ADDRESS	MANDATORY	IP ADDRESS
-PORT	TCP PORT FOR ISCSI COMMUNICATION	OPTIONAL	INTEGER IN RANGE 0..65535 **3260**

iscsi discovery rportal set

This command sets remote portals for discovery.

iscsi discovery rportal set

Switch	Definition	Type	Values/Remarks
-IP	NETWORK PORT IP ADDRESS	MANDATORY	IP ADDRESS
-PERIOD	PERIOD FOR REDISCOVER IN SECONDS	OPTIONAL[1]	INTEGER IN RANGE 0..65535 **1800**
-PORT	TCP PORT FOR ISCSI COMMUNICATION	OPTIONAL[1]	INTEGER IN RANGE 0..65535 **3260**

Dependencies

optional[1]: at least one of the switches is mandatory

iscsi discovery rportal show

This command shows remote portals configured for discovery.

iscsi discovery rportal show

Switch	Definition	Type	Values/Remarks
-TABLE	DISPLAYS DATA IN TABLE FORMAT	OPTIONAL	DEFAULT DISPLAY
-RECORD	DISPLAYS DATA IN RECORD FORMAT	OPTIONAL	

iscsi initiator details

This command has been replaced by 'iscsi initiator show' (see page 5-27).

iscsi initiator set

This command sets the iSCSI initiator.

iscsi initiator set

Switch	Definition	Type	Values/Remarks
-CHAPNUM	CHAP USER NAME	OPTIONAL	
-CHAPPW	CHAP PASSWORD	OPTIONAL	
-SRPUN	SRP USERNAME	OPTIONAL	
-SRPPW	SRP PASSWORD	OPTIONAL	

iscsi initiator show

This command shows details for the configured iSCSI initiator.

iscsi initiator show

iscsi portal create

This command creates an iSCSI portal on a 1 Gb (network) port.

iscsi portal create

Switch	Definition	Type	Values/Remarks
-IP	NETWORK PORT IP ADDRESS	MANDATORY	IP ADDRESS
-P	TCP PORT FOR iSCSI COMMUNICATION	OPTIONAL	INTEGER IN RANGE 0..65535 **3260**

iscsi portal remove

This command removes an iSCSI portal on a 1 Gb (network) port.

iscsi portal remove

Switch	Definition	Type	Values/Remarks
-IP	NETWORK PORT IP ADDRESS	MANDATORY	IP ADDRESS
-P	TCP PORT FOR iSCSI COMMUNICATION	MANDATORY	INTEGER IN RANGE 0..65535

iscsi portal show

This command shows the portals defined for iSCSI on the i series with which you are communicating.

iscsi portal show

Switch	Definition	Type	Values/Remarks
-TABLE	DISPLAYS DATA IN TABLE FORMAT	OPTIONAL	DEFAULT DISPLAY
-RECORD	DISPLAYS DATA IN RECORD FORMAT	OPTIONAL	

iscsi rinitiator list

The command 'iscsi rinitiator list' has been replaced by 'iscsi rinitiator show -ta' (see page5-29).

iscsi rinitiator show

This command shows all remote initiators.

iscsi rinitiator show

Switch	Definition	Type	Values/Remarks
-TABLE	DISPLAYS DATA IN TABLE FORMAT	OPTIONAL	DEFAULT DISPLAY
-RECORD	DISPLAYS DATA IN RECORD FORMAT	OPTIONAL	
-TA	DISPLAYS DATA FOR TARGET ALIAS	OPTIONAL	ASCII STRING (MAXIMUM 10 CHARACTERS)

iscsi rinitiator statistics show

This command shows the statistics for remote initiators.

Switch	Definition	Type	Values/Remarks
-TABLE	DISPLAYS DATA IN TABLE FORMAT	OPTIONAL	DEFAULT DISPLAY
-RECORD	DISPLAYS DATA IN RECORD FORMAT	OPTIONAL	

iscsi rtarget create

This command creates a new remote iSCSI target.

iscsi rtarget create

Switch	Definition	Type	Values/Remarks
-RTN	REMOTE TARGET NAME	MANDATORY	ISCSI WORLD WIDE UNIQUE IDENTIFIER (ASCII STRING OF MAX. 223 CHARACTERS)
-RTA	REMOTE ISCSI TARGET ALIAS	OPTIONAL	ASCII STRING (MAXIMUM 10 CHARACTERS)

iscsi rtarget details

The command 'iscsi rtarget details' has been replaced by 'iscsi rtarget show -details -rta' (see page 5-30).

iscsi rtarget remove

This command removes a remote iSCSI target.

iscsi rtarget remove

Switch	Definition	Type	Values/Remarks
-RTA	REMOTE ISCSI TARGET ALIAS	MANDATORY	ASCII STRING (MAXIMUM 10 CHARACTERS)

iscsi rtarget set

This command renames a target alias.

iscsi target set

Switch	Definition	Type	Values/Remarks
-RTA	ALIAS OF RTARGET	MANDATORY	ASCII STRING (MAXIMUM 10 CHARACTERS)
-CHAPPW	USER PASSWORD FOR CHAP AUTHENTICATION	MANDATORY[1]	ASCII STRING
-CHAPUN	USER NAME FOR CHAP AUTHENTICATION	MANDATORY[1]	ASCII STRING
-RADIUS		MANDATORY[1]	ASCII STRING

Dependencies

mandatory[1]: mandatory with CHAP password

iscsi rtarget show

This command shows all remote targets.

iscsi rtarget show

Switch	Definition	Type	Values/Remarks
-TABLE	DISPLAYS DATA IN TABLE FORMAT	OPTIONAL	DEFAULT DISPLAY
-RECORD	DISPLAYS DATA IN RECORD FORMAT	OPTIONAL	
-DETAILS	DISPLAYS DETAILS ABOUT INTERFACE	OPTIONAL[1]	
-RTA	REMOTE ISCSI TARGET ALIAS	OPTIONAL	ASCII STRING (MAXIMUM 10 CHARACTERS)

Dependencies

optional[1]: switch -rta is mandatory for details view

iscsi rtarget rportal create

This command creates an iSCSI remote portal for a specified remote target.

iscsi rtarget rportal create

Switch	Definition	Type	Values/Remarks
-RIP	REMOTE IP ADDRESS	MANDATORY	IP ADDRESS
-RTA	REMOTE ISCSI TARGET ALIAS	MANDATORY	ASCII STRING (MAXIMUM 10 CHARACTERS)
-RPORT	TCP PORT FOR ISCSI COMMUNICATION	OPTIONAL	INTEGER IN RANGE 0..65535 **3260**
-RTAG	REMOTE PORTAL TAG	OPTIONAL	DEVICE ID OF THE REMOTE I SERIES **-1**

iscsi rtarget rportal list

The command 'iscsi rtarget rportal list' has been replaced by 'iscsi rtarget rportal show -details -rta' (see page 5-31).

iscsi rtarget rportal remove

This command removes the remote portals for a specified remote target..

iscsi rtarget rportal remove

Switch	Definition	Type	Values/Remarks
-RIP	REMOTE TARGET NAME	MANDATORY	IP ADDRESS
-RPORT	TCP PORT FOR ISCSI COMMUNICATION	MANDATORY	INTEGER IN RANGE 0..65535
-RTA	REMOTE ISCSI TARGET ALIAS	MANDATORY	ASCII STRING (MAXIMUM 10 CHARACTERS)

iscsi rtarget rportal show

This command shows all remote targets.

iscsi rtarget show

Switch	Definition	Type	Values/Remarks
-TABLE	DISPLAYS DATA IN TABLE FORMAT	OPTIONAL	DEFAULT DISPLAY
-RECORD	DISPLAYS DATA IN RECORD FORMAT	OPTIONAL	
-DETAILS	DISPLAYS DETAILS ABOUT INTERFACE	OPTIONAL[1]	
-RTA	REMOTE ISCSI TARGET ALIAS	OPTIONAL	ASCII STRING (MAXIMUM 10 CHARACTERS)

Dependencies

optional[1]: switch -rta is mandatory for details view

iscsi session connection details

The command 'iscsi session connection details' has been replaced by 'iscsi session connection show -details -id' (see page 5-32).

iscsi session connection show

This command shows all connections for all iSCSI sessions.

iscsi session connection show

Switch	Definition	Type	Values/Remarks
-TABLE	DISPLAYS DATA IN TABLE FORMAT	OPTIONAL	DEFAULT DISPLAY
-RECORD	DISPLAYS DATA IN RECORD FORMAT	OPTIONAL	
-DETAILS	DISPLAYS SPECIFIC DETAILS	OPTIONAL[1]	
-ID	ISCSI CONNECTION ID	OPTIONAL[1]	
-ADV	ADVANCED PARAMETERS	OPTIONAL	DO NOT SPECIFY, NO VALUE ALLOWED FOR SWITCH

Dependencies

optional[1]: switch -id is mandatory for details view

iscsi session details

The command 'iscsi session details' has been replaced by 'iscsi session show -details -id' (see page 5-33).

iscsi session show

This command shows all iSCSI sessions.

iscsi session show

Switch	Definition	Type	Values/Remarks
-TABLE	DISPLAYS DATA IN TABLE FORMAT	OPTIONAL	DEFAULT DISPLAY
-RECORD	DISPLAYS DATA IN RECORD FORMAT	OPTIONAL	
-DETAILS	DISPLAYS SPECIFIC DETAILS	OPTIONAL[1]	
-ID	iSCSI SESSION ID	OPTIONAL[1]	
-ADV	ADVANCED iSCSI SESSION DETAILS	OPTIONAL	DO NOT SPECIFY, NO VALUE ALLOWED FOR SWITCH

Dependencies

optional[1]: switch -id is mandatory for details view

iscsi session statistics show

This command lists the statistics for a specific inbound session for a specified local target.

iscsi session statistics show

Switch	Definition	Type	Values/Remarks
-TA	TARGET ALIAS FOR STATISTICS	MANDATORY	ASCII STRING (MAXIMUM 10 CHARACTERS)
-TYPE	INITIATOR TYPE	MANDATORY	CRP, TXRX, ERROR

iscsi target alias

The command 'iscsi target alias' has been replaced by 'iscsi target show -record' (see page 5-30).

iscsi target create

This command creates an iSCSI target without creating LU0, attaching volumes or exposing the target. Targets can be created in advance and only later have LUNs created and exposed.

iscsi target create

Switch	Definition	Type	Values/Remarks
-TA	USER-ASSIGNED ALIAS FOR ISCSI TARGET	MANDATORY	ASCII STRING (MAXIMUM 10 CHARACTERS)
-TN	USER-ASSIGNED WORLD-WIDE UNIQUE IDENTIFIER FOR THE TARGET	MANDATORY	ISCSI WORLD WIDE UNIQUE IDENTIFIER (ASCII STRING OF MAX. 223 CHARACTERS)
-DEVICE	ALIAS OF I SERIES TO EXPOSE TARGET ON	OPTIONAL	ASCII STRING RELEVANT ONLY IN CLUSTER

iscsi target details

The' iscsi target details' command has been replaced by 'iscsi target show -details -ta' (see page 5-35).

iscsi target remove

This command removes an iSCSI target.

iscsi target remove

Switch	Definition	Type	Values/Remarks
-TA	ISCSI TARGET ALIAS TO REMOVE	MANDATORY	ASCII STRING (MAXIMUM 10 CHARACTERS)

iscsi target set

This command renames a target alias.

iscsi target set

Switch	Definition	Type	Values/Remarks
-TA	ALIAS OF TARGET TO RENAME	MANDATORY	ASCII STRING (MAXIMUM 10 CHARACTERS)
-DEVICE	ALIAS OF I SERIES TO EXPOSE TARGET ON	OPTIONAL	ASCII STRING
-NA	NEW ALIAS FOR TARGET	OPTIONAL	ASCII STRING (MAXIMUM 10 CHARACTERS)
-CHAPPW	USER PASSWORD FOR CHAP AUTHENTICATION (FOR DUAL AUTHENTICATION)	OPTIONAL[1]	ASCII STRING
-CHAPUN	USER NAME FOR CHAP AUTHENTICATION (FOR DUAL AUTHENTICATION)	OPTIONAL[2]	ASCII STRING

Dependencies

optional[1]: mandatory with CHAP username

optional[2]: mandatory with CHAP password

iscsi target show

This command shows all created targets.

iscsi target show

Switch	Definition	Type	Values/Remarks
-TABLE	DISPLAYS DATA IN TABLE FORMAT	OPTIONAL	DEFAULT DISPLAY
-RECORD	DISPLAYS DATA IN RECORD FORMAT	OPTIONAL	
-DETAILS	DISPLAYS SPECIFIC DETAILS	OPTIONAL[1]	
-TA	USER-ASSIGNED ALIAS FOR ISCSI TARGET	OPTIONAL	ASCII STRING (MAXIMUM 10 CHARACTERS)

Dependencies

optional[1]: switch -ta is mandatory for details view

-L-

lu details

The command 'lu details' has been replaced by 'lu show -details -ta' (see page 5-36).

lu remove

This command removes the LU from its target. The LU must be inactive before being removed. This command is the opposite of **volume expose**.

lu remove

Switch	Definition	Type	Values/Remarks
-TA	TARGET ALIAS OF LU	MANDATORY	ASCII STRING (MAXIMUM 10 CHARACTERS)
-LUN	LOGICAL UNIT NUMBER	OPTIONAL	**0**

lu show

This command shows all LUNs defined in the database.

lu show

Switch	Definition	Type	Values/Remarks
-TABLE	DISPLAYS DATA IN TABLE FORMAT	OPTIONAL	DEFAULT DISPLAY
-RECORD	DISPLAYS DATA IN RECORD FORMAT	OPTIONAL	
-DETAILS	DISPLAYS SPECIFIC DETAILS	OPTIONAL[1]	
-TA	TARGET ALIAS OF LU	OPTIONAL	ASCII STRING (MAXIMUM 10 CHARACTERS)
-LUN	LOGICAL UNIT NUMBER	OPTIONAL	**0**

Dependencies

optional[1]: switch -ta is mandatory for details view

lu statistics show

This command shows all statistics for configured LUs on the i series.

lu statistics show

Switch	Definition	Type	Values/Remarks
-TABLE	DISPLAYS DATA IN TABLE FORMAT	OPTIONAL	DEFAULT DISPLAY
-RECORD	DISPLAYS DATA IN RECORD FORMAT	OPTIONAL	

-N-

neighbor add

This command adds a neighbor to a cluster.

neighbor add

Switch	Definition	Type	Values/Remarks
-IP	IP ADDRESS OF MGMT PORT ON NEIGHBOR	MANDATORY	IP ADDRESS
-NB	ALIAS OF NEIGHBOR TO ADD TO CLUSTER	MANDATORY	ASCII STRING (MAXIMUM 10 CHARACTERS)

neighbor details

The command 'neighbor details' has been replaced by 'neighbor show -details -nb' (see page 5-38).

neighbor remove

This command removes a i series from a cluster.

neighbor remove

Switch	Definition	Type	Values/Remarks
-NB	ALIAS OF NEIGHBOR TO ADD TO CLUSTER	MANDATORY	ASCII STRING (MAXIMUM 10 CHARACTERS)

neighbor set

This command resets a neighbor IP address in a cluster.

neighbor set

Switch	Definition	Type	Values/Remarks
-IP	IP ADDRESS OF MGMT PORT ON NEIGHBOR	MANDATORY	IP ADDRESS
-NB	ALIAS OF NEIGHBOR TO ADD TO CLUSTER	MANDATORY	ASCII STRING (MAXIMUM 10 CHARACTERS)

neighbor show

This command lists the neighbor(s) in a cluster.

neighbor show

Switch	Definition	Type	Values/Remarks
-TABLE	DISPLAYS DATA IN TABLE FORMAT	OPTIONAL	DEFAULT DISPLAY
-RECORD	DISPLAYS DATA IN RECORD FORMAT	OPTIONAL	
-DETAILS	DISPLAYS SPECIFIC DETAILS	OPTIONAL[1]	
-NB	ALIAS OF NEIGHBOR IN CLUSTER	OPTIONAL	ASCII STRING (MAXIMUM 10 CHARACTERS)

Dependencies

optional[1]: switch -nd is mandatory for details **view**

-P-

ping

This command pings any IP-connected device from the i series port.

ping

Switch	Definition	Type	Values/Remarks
-IP	IP ADDRESS TO PING	MANDATORY	IP ADDRESS
-IF	INTERFACE ALIAS THAT ISSUES ICMP REQUESTS	OPTIONAL	ASCII STRING (MAXIMUM 10 CHARACTERS)

pscsi set busid

This command sets a storage port's SCSI bus ID.

Note:
This command is available only when a pSCSI interface is present.

pscsi set busid

Switch	Definition	Type	Values/Remarks
-IF	INTERFACE ALIAS	MANDATORY	ASCII STRING (MAXIMUM 10 CHARACTERS)
-ID	SCSI BUS IDENTITY	OPTIONAL	0..**7**..15

pscsi show

This command shows all SCSI storage ports and their corresponding SCSI bus IDs.

Note:
This command is available only when a pSCSI interface is present.

pscsi show

Switch	Definition	Type	Values/Remarks
-TABLE	DISPLAYS DATA IN TABLE FORMAT	OPTIONAL	DEFAULT DISPLAY
-RECORD	DISPLAYS DATA IN RECORD FORMAT	OPTIONAL	

-S-

scsi initiator port statistics show

This command shows statistics the SCSI target ports.

scsi initiator port statistics show

Switch	Definition	Type	Values/Remarks
-TABLE	DISPLAYS DATA IN TABLE FORMAT	OPTIONAL	DEFAULT DISPLAY
-RECORD	DISPLAYS DATA IN RECORD FORMAT	OPTIONAL	

scsi target port statistics show

This command shows statistics the SCSI target ports.

scsi target port statistics show

Switch	Definition	Type	Values/Remarks
-TABLE	DISPLAYS DATA IN TABLE FORMAT	OPTIONAL	DEFAULT DISPLAY
-RECORD	DISPLAYS DATA IN RECORD FORMAT	OPTIONAL	

snmp manager add

This command adds a manager to the i series.

snmp manager add

Switch	Definition	Type	Values/Remarks
-IP	MANAGER IP ADDRESS	MANDATORY	IP ADDRESS
-P	RECEIVE TRAPS THROUGH SPECIFIC PORT	OPTIONAL	INTEGER IN RANGE 0..65535 **162**
-RCOM	READ COMMUNITY	OPTIONAL	ASCII STRING (MAXIMUM 80 CHARACTERS) **PUBLIC**
-TRAP	SEND TRAPS TO MANAGER	OPTIONAL	**Y** (SEND), N (DO NOT SEND)
-WCOM	WRITE COMMUNITY	OPTIONAL	ASCII STRING (MAXIMUM 80 CHARACTERS) **PRIVATE**

snmp manager remove

This command removes a manager from the i series.

snmp manager remove

Switch	Definition	Type	Values/Remarks
-IP	MANAGER IP ADDRESS	MANDATORY	IP ADDRESS
-P	RECEIVE TRAPS THROUGH SPECIFIED PORT	MANDATORY	INTEGER IN RANGE 0..65535

snmp manager set

This command modifies parameters of existing managers.

snmp manager set

Switch	Definition	Type	Values/Remarks
-IP	MANAGER IP ADDRESS	MANDATORY	IP ADDRESS
-P	PORT TO RECEIVE TRAPS THROUGH	MANDATORY	INTEGER IN RANGE 0..65535
-NP	NEW PORT FOR RECEIVING TRAPS	OPTIONAL[1]	INTEGER IN RANGE 0..65535
-RCOM	READ COMMUNITY	OPTIONAL[1]	ASCII STRING (MAXIMUM 80 CHARACTERS) **PUBLIC**
-TRAP	SEND TRAPS TO MANAGER	OPTIONAL[1]	**Y** (SEND), N (DO NOT SEND)
-WCOM	WRITE COMMUNITY	OPTIONAL[1]	ASCII STRING (MAXIMUM 80 CHARACTERS) **PRIVATE**

Dependencies

optional[1]: at least one of the switches is mandatory

snmp manager show

This command displays the managers of the i series.

snmp manager show

Switch	Definition	Type	Values/Remarks
-TABLE	DISPLAYS DATA IN TABLE FORMAT	OPTIONAL	DEFAULT DISPLAY
-RECORD	DISPLAYS DATA IN RECORD FORMAT	OPTIONAL	

storage alias

The command ‘storage alias’ has been replaced by 'storage show -record' (see page 5-46).

storage blink abort

This command stops a storage device from blinking.

storage blink abort

Switch	Definition	Type	Values/Remarks
-S	ALIAS OF DEVICE TO BLINK	MANDATORY	ASCII STRING (MAXIMUM 10 CHARACTERS)

storage blink start

This command allows you to blink a storage device to identify it.

storage blink start

Switch	Definition	Type	Values/Remarks
-S	DEVICE ALIAS TO BLINK	MANDATORY	ASCII STRING (MAXIMUM 10 CHARACTERS)
-T	LENGTH OF TIME TO BLINK DEVICE	OPTIONAL	1..3600 SEC **0**: FOREVER

storage create

This command creates a new storage.

storage create

Switch	Definition	Type	Values/Remarks
-S	STORAGE ALIAS **NOTE:** IF NO NAME IS SPECIFIED, STOR_* WILL BE ASSIGNED WHERE * IS THE NEXT AVAILABLE NUMBER.	OPTIONAL	ASCII STRING (MAXIMUM 10 CHARACTERS)
-SN	SERIAL NUMBER FOR STORAGE	OPTIONAL	ASCII STRING (1..255)
-TRANS	TYPE OF TRANSPORT	OPTIONAL	FCP, **ISCSI**
-LUN	LUN	OPTIONAL[1]	0..255
-RTN	USER-ASSIGNED WORLD WIDE UNIQUE IDENTIFIER FOR THE RTARGET	OPTIONAL[1]	ISCSI WORLD WIDE UNIQUE IDENTIFIER (ASCII STRING OF MAX. 223 CHARACTERS)

Dependencies

optional[1]: both should appear

storage details

The command 'storage details' has been replaced by 'storage show -details -s' (see page 5-46).

storage discovery start

This command resets the Fiber Channel loop and reregisters all attached storage devices. In most cases, the i series automatically discovers new storage. Use this command after adding or removing storage devices from the i series topography if it is not automatically discovered. Because this command resets the FC loop, it may cause a failure of any I/O operations being executed when the command is invoked.

storage discovery start

storage discovery show

This command shows the state of the storage discovery process.

storage discovery show

storage disk set

This command allows you to enable or disable write cache for a disk.

storage disk set

Switch	Definition	Type	Values/Remarks
-D	DISK DEVICE	MANDATORY	ASCII STRING (MAXIMUM 10 CHARACTERS)
-ALLOC	ALLOCATES STORAGE TO HOST	OPTIONAL	YES, **NO**
-WCE	WRITE CACHE ENABLED	OPTIONAL	TRUE, FALSE

storage disk show

This command 'storage disk show' has been replaced by 'storage show -disk' (see page 5-46).

storage expose

This command exposes a storage device.

storage expose

Switch	Definition	Type	Values/Remarks
-S	STORAGE ALIAS TO REMOVE	MANDATORY	ASCII STRING (MAXIMUM 10 CHARACTERS)
-TA	TARGET ALIAS	MANDATORY	ASCII STRING (MAXIMUM 10 CHARACTERS)
-LUN		OPTIONAL	
-NEW	EXPOSE VOLUME ON NEW TARGET	OPTIONAL[1]	
-TN	TARGET NAME	OPTIONAL[1]	
-DEVICE	NAME OF DEVICE TO BE EXPOSED ON	OPTIONAL[1]	

Dependencies

optional[1]: Mandatory on new target

storage override

This command overrides missing storage.

Note:
Do not use this command unless instructed to do so by technical support.

storage ovveride

Switch	Definition	Type	Values/Remarks
-S	STORAGE ALIAS	MANDATORY	ASCII STRING (MAXIMUM 10 CHARACTERS)
-NS	NEW STORAGE ALIAS	MANDATORY	ASCII STRING (MAXIMUM 10 CHARACTERS)

storage remove

This command removes a storage device from the database only if the storage device state is defined as *StorageIsMissing*.

storage remove

Switch	Definition	Type	Values/Remarks
-S	STORAGE ALIAS TO REMOVE	MANDATORY	ASCII STRING (MAXIMUM 10 CHARACTERS)

storage set

This command allows you to edit storage device parameters.

storage set

Switch	Definition	Type	Values/Remarks
-S	STORAGE ALIAS TO MODIFY	MANDATORY	ASCII STRING (MAXIMUM 10 CHARACTERS)
-INFO	INFORMATION ON STORAGE TO SET	OPTIONAL[1]	ASCII STRING
-NA	NEW ALIAS FOR STORAGE	OPTIONAL[1]	ASCII STRING (MAXIMUM 10 CHARACTERS)

Dependencies

optional[1] : at least one of the switches is mandatory

storage show

This command shows all storage devices connected to the i series.

storage show

Switch	Definition	Type	Values/Remarks
-TABLE	DISPLAYS DATA IN TABLE FORMAT	OPTIONAL	DEFAULT DISPLAY
-RECORD	DISPLAYS DATA IN RECORD FORMAT	OPTIONAL	
-DETAILS	DISPLAYS SPECIFIC DETAILS	OPTIONAL[1]	
-S	STORAGE ALIAS	OPTIONAL	ASCII STRING (MAXIMUM 10 CHARACTERS)
-DISK	DISK DEVICE	OPTIONAL	ASCII STRING (MAXIMUM 10 CHARACTERS)

Dependencies

optional[1]: switch -s is mandatory for details view

storage unexpose

This command unexposes a storage device.

storage expose

Switch	Definition	Type	Values/Remarks
-S	STORAGE ALIAS TO REMOVE	MANDATORY	ASCII STRING (MAXIMUM 10 CHARACTERS)

subdisk alias

The command 'subdisk alias' has been replaced by 'subdisk show -record -d' (see page 5-48).

subdisk create

This command allows you to create subdisks.

subdisk create

Switch	Definition	Type	Values/Remarks
-D	DISK ALIAS	MANDATORY	ASCII STRING (MAXIMUM 10 CHARACTERS)
-SD	SUBDISK ALIAS	MANDATORY	ASCII STRING (MAXIMUM 10 CHARACTERS)
-SL	LENGTH OF DISK IN BLOCKS	MANDATORY	1 BLOCK = 512 BYTES
-SA	START ADDRESS	OPTIONAL	**0**

subdisk details

The command 'subdisk details' has been replaced by 'subdisk show -details' (see page 5-48).

subdisk remove

This command removes a specified subdisk.

subdisk remove

Switch	Definition	Type	Values/Remarks
-SD	ALIAS OF SUBDISK TO SHOW	MANDATORY	ASCII STRING (MAXIMUM 10 CHARACTERS)

subdisk set

This command allows you to change subdiskparameters.

subdisk set

Switch	Definition	Type	Values/Remarks
-SD	SUBDISK ALIAS	MANDATORY	ASCII STRING (MAXIMUM 10 CHARACTERS)
-NA	NEW SUBDISK ALIAS	OPTIONAL	ASCII STRING (MAXIMUM 10 CHARACTERS)
-INFO	INFORMATION ABOUT THE SUBDISK	OPTIONAL	

subdisk show

This command shows all/specified subdisks connected to the V Switch.

subdisk show

Switch	Definition	Type	Values/Remarks
-TABLE	DISPLAYS DATA IN TABLE FORMAT	OPTIONAL	DEFAULT DISPLAY
-RECORD	DISPLAYS DATA IN RECORD FORMAT	OPTIONAL	
-DETAILS	DISPLAYS SPECIFIC DETAILS	OPTIONAL[1]	
-D	ALIAS OF DISK TO SHOW SUBDISKS ON	OPTIONAL	ASCII STRING (MAXIMUM 10 CHARACTERS)
-SD	ALIAS OF SUBDISK TO SHOW	OPTIONAL	ASCII STRING (MAXIMUM 10 CHARACTERS)

Dependencies

optional[1]: switch -d & -sd are mandatory for details view

system boot

This command forces the i series to boot in Safe Mode.

system boot

Switch	Definition	Type	Values/Remarks
-SM	SAFE MODE LEVEL	MANDATORY	0: NORMAL 1: LAST GOOD CONFIGURATION 2: DEFAULT DATABASE 3: DEFAULT FACTORY SYSTEM

system cf format

This command formats the compact flash.

system cf format

system cf show

This command identifies the presence of the compact flash and its replication state.

system cf show

system show

> The command 'system show' has been replaced by 'system cf show'.

system cf copy

This command copies the external compact flash to the internal flash.

system cf copy

Switch	Definition	Type	Values/Remarks
-FROM	SPECIFIES FROM WHERE TO COPY THE FILE (E.G. EXTERNAL COMPACT FLASH TO LOCAL FLASH)	MANDATORY	FLASH, CFLASH
-PREVIOUS	COPIES THE PREVIOUS FILE FROM COMPACT FLASH	OPTIONAL	

system copy

The command ‘system copy’ has been replaced by 'system cf copy'.

system hardware show

This command shows all hardware interface connection statistics.

system hardware show

system log realtime show

This command shows realtime log events.

system log realtime show

Switch	Definition	Type	Values/Remarks
-INFO	DISPLAYS EVENTS WITH SEVERITY INFO	OPTIONAL	
-WARN	DISPLAYS EVENTS WITH SEVERITY WARN	OPTIONAL	
-ERROR	DISPLAYS EVENTS WITH SEVERITY ERROR	OPTIONAL	
-FATAL	DISPLAYS EVENTS WITH SEVERITY FATAL	OPTIONAL	

system log show

This command shows log events filtered by user specified criteria.

system log show

Switch	Definition	Type	Values/Remarks
-STARTDATE	DISPLAYS EVENTS STARTING FROM THIS DATE	OPTIONAL	
-STARTTIME	DISPLAYS EVENTS STARTING FROM THIS TIME	OPTIONAL	
-ENDDATE	DISPLAYS EVENTS UP UNTIL THIS DATE	OPTIONAL	
-ENDTIME	DISPLAYS EVENTS UP UNTIL THIS TIME	OPTIONAL	
-SKIP	THE NUMBER OF EVENTS TO SKIP	OPTIONAL	
-EVENTCOUNT	THE NUMBER OF EVENTS TO DISPLAY	OPTIONAL	
-INFO	DISPLAYS EVENTS WITH SEVERITY INFO	OPTIONAL	
-WARN	DISPLAYS EVENTS WITH SEVERITY WARN	OPTIONAL	
-ERROR	DISPLAYS EVENTS WITH SEVERITY ERROR	OPTIONAL	
-FATAL	DISPLAYS EVENTS WITH SEVERITY FATAL	OPTIONAL	

system reset

This command performs a remote soft reset of the i series. All configuration databases will be maintained on the i series, including user names and passwords; network port aliases; configured volumes and iSCSI targets.

system reset

system reset_default_factory

This command resets the i series to factory default settings. It is available only when connected via RS-232.

system reset_default_factory

system cf set

This command sets the replication mode status.

system cf set

Switch	Definition	Type	Values/Remarks
-REP	REPLICATION MODE STATUS	MANDATORY	YES NO

system set

The command 'system set' has been replaced by 'system cf set'.

-T-

tcp connection show

This command shows all TCP connections.

tcp connection show

Switch	Definition	Type	Values/Remarks
-TABLE	DISPLAYS DATA IN TABLE FORMAT	OPTIONAL	DEFAULT DISPLAY
-RECORD	DISPLAYS DATA IN RECORD FORMAT	OPTIONAL	

tcp statistics show

This command shows all TCP connection counters.

tcp statistics show

traceroute

Switch	Definition	Type	Values/Remarks
-IP	DESTINATION IP ADDRESS	MANDATORY	IP ADDRESS
-FIRSTTTL	FIRST TTL VALUE	OPTIONAL	1-255 DEFAULT 1
-GW	IP ADDRESS OF GATEWAY FOR SOURCE ROUTING	OPTIONAL	IP ADDRESS
-ICMP	ICMP DATAGRAMS	OPTIONAL	
-IF	NAME OF OUTGOING NETWORKING INTERFACE	OPTIONAL	ETH1, ETH2, ETH3
-MAXTTL	MAXIMUM TTL VALUE	OPTIONAL	1-255, DEFAULT 30
-LENGTH	SIZE IN BYTES OF OUTGOING PACKETS	OPTIONAL	DEFAULT 40
-NOFRAG	DO NOT FRAGMENT	OPTIONAL	
-NOROUTE	DO NOT ROUTE	OPTIONAL	
-NUMPROBE	NUMBER OF PACKETS SENT PER HOP	OPTIONAL	DEFAULT 3
-PORT	UDP DESTINATION PORT	OPTIONAL	DEFAULT 33434
-PROBEMTU	PROBING PATH MTU	OPTIONAL	
-SHOWTTL	SHOW RECEIVED TTL	OPTIONAL	
-SRC	OUTGOING SOURCE IP ADDRESS	OPTIONAL	IP ADDRESS
-TIMEOUT	TIMEOUT IN SECONDS TO WAIT FOR REPLY	OPTIONAL	DEFAULT 5
-TOS	SET THE TYPE-OF-SERVICE	OPTIONAL	0-255, DEFAULT 0

-U-

udp listeners show

This command shows all UDP listeners.

udp listeners show

Switch	Definition	Type	Values/Remarks
-TABLE	DISPLAYS DATA IN TABLE FORMAT	OPTIONAL	DEFAULT DISPLAY
-RECORD	DISPLAYS DATA IN RECORD FORMAT	OPTIONAL	

udp statistics show

This command shows all UDP connection counters.

udp statistics show

-V-

volume alias

The command 'volume alias' has been replaced by 'volume show -record' (see page 5-65).

volume copy abort

This command aborts an off-line volume copy operation.

volume copy abort

Switch	Definition	Type	Values/Remarks
-SRC	SOURCE	MANDATORY	ASCII STRING (MAXIMUM 10 CHARACTERS)
-DST	DESTINATION	MANDATORY	ASCII STRING (MAXIMUM 10 CHARACTERS)

volume copy create

This command creates an off-line volume copy.

volume copy create

Switch	Definition	Type	Values/Remarks
-DST	DESTINATION	MANDATORY	ASCII STRING (MAXIMUM 10 CHARACTERS)
-SRC	SOURCE	MANDATORY	ASCII STRING (MAXIMUM 10 CHARACTERS)

volume copy show

This command shows all on-going and previously executed copy operations on volumes

volume copy show

Switch	Definition	Type	Values/Remarks
-TABLE	DISPLAYS DATA IN TABLE FORMAT	OPTIONAL	DEFAULT DISPLAY
-RECORD	DISPLAYS DATA IN RECORD FORMAT	OPTIONAL	

volume create concatenated

This command creates a concatenated volume across the specified volumes in the order listed.

volume create concatenated

Switch	Definition	Type	Values/Remarks
-VOL	ALIAS OF VOLUME TO CREATE	MANDATORY	ASCII STRING (MAXIMUM 10 CHARACTERS)
-CH	ALIAS OF EACH VOLUME TO INCLUDE IN CONCATENATED VOLUME	MANDATORY[1, 3]	ASCII STRING (MAXIMUM 10 CHARACTERS)
-NBC	NUMBER OF VOLUMES TO CONCATENATE ACROSS	OPTIONAL[1, 2]	**2**..16

Dependencies

[1]: order must be as follows: '-nbc' must be before '-ch'

[2]: mandatory if greater than 2

[3]: can be used up to 16 times

volume create mirror

This command creates a mirrored volume the specified number of volumes.

volume create mirror

Switch	Definition	Type	Values/Remarks
-VOL	ALIAS OF VOLUME TO CREATE	MANDATORY	ASCII STRING (MAXIMUM 10 CHARACTERS)
-CH	ALIAS OF EACH VOLUME TO INCLUDE IN CONCATENATED VOLUME	MANDATORY[1, 3]	ASCII STRING (MAXIMUM 10 CHARACTERS)
-NBC	NUMBER OF VOLUMES TO CONCATENATE ACROSS	OPTIONAL[1, 2]	**2**..16

Dependencies

[1]: order must be as follows: '-nbc' must be before '-ch'

[2]: mandatory if greater than 2

[3]: can be used up to 16 times

volume create simple

This command creates a simple volume out of a disk or subdisk.

volume create simple

Switch	Definition	Type	Values/Remarks
-VOL	ALIAS OF VOLUME TO CREATE	OPTIONAL	ASCII STRING (MAXIMUM 10 CHARACTERS)
-SD	SUBDISK ALIAS	OPTIONAL[1]	ASCII STRING (MAXIMUM 10 CHARACTERS)
-D	DISK ALIAS	OPTIONAL[1]	ASCII STRING (MAXIMUM 10 CHARACTERS)

Dependencies

optional[1]: at least one of the switches is mandatory

volume create snapshot

This command creates a snapshot volume.

volume create snapshot

Switch	Definition	Type	Values/Remarks
-CH	ALIAS OF EACH VOLUME TO INCLUDE	MANDATORY	ASCII STRING (MAXIMUM 10 CHARACTERS)
-SRC	SOURCE VOLUME ALIAS	MANDATORY	ASCII STRING (MAXIMUM 10 CHARACTERS)
-VOL	ALIAS OF VOLUME TO CREATE	MANDATORY	ASCII STRING (MAXIMUM 10 CHARACTERS)
-ACTIVATE	ACTIVATION OF SNAPSHOT VOLUME	OPTIONAL	DO NOT SPECIFY, NO VALUE ALLOWED FOR SWITCH
-LT	THRESHOLD LOAD %	OPTIONAL	5..**80**..100

volume create stripe

This command creates a striped volume across the specified volumes in the order listed.

volume create stripe

Switch	Definition	Type	Values/Remarks
-SUS	STRIPE UNIT SIZE	MANDATORY	INTEGER
-VOL	ALIAS OF VOLUME TO CREATE	MANDATORY	ASCII STRING (MAXIMUM 10 CHARACTERS)
-CH	ALIAS OF EACH VOLUME TO INCLUDE IN CONCATENATED VOLUME	MANDATORY[1, 3]	ASCII STRING (MAXIMUM 10 CHARACTERS)
-NBC	NUMBER OF VOLUMES TO CONCATENATE ACROSS	OPTIONAL[1, 2]	**2**..16

Dependencies

[1]: order must be as follows: '-nbc' must be before '-ch'

[2]: mandatory if greater than 2

[3]: can be used up to 16 times

volume create transparent

This command creates a transparent volume out of a disk.

volume create transparent

Switch	Definition	Type	Values/Remarks
-D	DISK ALIAS	MANDATORY	ASCII STRING (MAXIMUM 10 CHARACTERS)
-VOL	ALIAS OF VOLUME TO CREATE	OPTIONAL	ASCII STRING (MAXIMUM 10 CHARACTERS)

volume details

This command 'volume details' has been replaced by 'volume show -details -vol' (see page 5-65).

volume expand

This command expands a volume's actual capacity to match its potential capacity.

volume expand

Switch	Definition	Type	Values/Remarks
-VOL	ALIAS OF VOLUME	MANDATORY	ASCII STRING (MAXIMUM 10 CHARACTERS)

volume expose

This command exposes a volume.

volume expose

Switch	Definition	Type	Values/Remarks
-TA	TARGET ALIAS	MANDATORY	ASCII STRING (MAXIMUM 10 CHARACTERS)
-VOL	ALIAS OF VOLUME	MANDATORY	ASCII STRING (MAXIMUM 10 CHARACTERS)
-NEW	EXPOSE VOLUME ON NEW TARGET	MANDATORY [1]	DO NOT SPECIFY, NO VALUE ALLOWED FOR SWITCH
-TN	USER-ASSIGNED WORLD WIDE UNIQUE IDENTIFIER FOR THE TARGET	MANDATORY [1]	ISCSI WORLD WIDE UNIQUE IDENTIFIER (ASCII STRING OF MAX. 223 CHARACTERS)
-LUN	LUN	MANDATORY[2]	0..255
-DEVICE	I SERIES ALIAS TO EXPOSE TARGET ON	OPTIONAL [1]	ASCII STRING (MAXIMUM 10 CHARACTERS)

Dependencies

mandatory [1] : mandatory on new target

mandatory[2] : mandatory on existing target

optional[1]: optional on new target

volume hierarchy show

This command shows the volumes composing the specified volume.

volume hierarchy show

Switch	Definition	Type	Values/Remarks
-VOL	ALIAS OF VOLUME	MANDATORY	ASCII STRING (MAXIMUM 10 CHARACTERS)

volume mirror add

This command adds an on-line volume copy to a mirror or the head of a hierarchy.

volume mirror add

Switch	Definition	Type	Values/Remarks
-CH	NEW CHILD TO ADD TO MIRROR	MANDATORY	ASCII STRING (MAXIMUM 10 CHARACTERS)
-VOL	ALIAS OF VOLUME	MANDATORY	ASCII STRING (MAXIMUM 10 CHARACTERS)
-NOSYNC	DISABLES AUTOMATIC MIRROR SYNC	OPTIONAL	DO NOT SPECIFY, NO VALUE ALLOWED FOR SWITCH

volume mirror break

This command removes a child from a mirror volume.

volume mirror break

Switch	Definition	Type	Values/Remarks
-CH	CHILD TO BE REMOVED FROM MIRROR	MANDATORY	ASCII STRING (MAXIMUM 10 CHARACTERS)
-VOL	ALIAS OF VOLUME	MANDATORY	ASCII STRING (MAXIMUM 10 CHARACTERS)

volume mirror sync abort

This command aborts the synchronization of mirrored volumes. Use this command after adding another volume to a group of mirrored volumes or to restore a mirrored volume on a disk after a disk failure.

volume mirror sync abort

Switch	Definition	Type	Values/Remarks
-DST	DESTINATION VOLUME	MANDATORY	ASCII STRING (MAXIMUM 10 CHARACTERS)
-SRC	SOURCE VOLUME	MANDATORY	ASCII STRING (MAXIMUM 10 CHARACTERS)

volume mirror sync start

This command synchronizes mirrored volumes. Use this command after adding another volume to a group of mirrored volumes or to restore a mirrored volume on a disk after a disk failure.

volume mirror sync start

Switch	Definition	Type	Values/Remarks
-DST	DESTINATION VOLUME	MANDATORY	ASCII STRING (MAXIMUM 10 CHARACTERS)
-SRC	SOURCE VOLUME	MANDATORY	ASCII STRING (MAXIMUM 10 CHARACTERS)

volume mirror sync show

This command shows all mirrors that were/are in mirror sync state.

volume mirror sync show

Switch	Definition	Type	Values/Remarks
-TABLE	DISPLAYS DATA IN TABLE FORMAT	OPTIONAL	DEFAULT DISPLAY
-RECORD	DISPLAYS DATA IN RECORD FORMAT	OPTIONAL	

volume remove

This command removes a volume from the system. The volume must be at the top of the hierarchy. The volume cannot be exposed; the volume LU must be inactivated. Simple volumes will convert back to their component disks or subdisks.

volume remove

Switch	Definition	Type	Values/Remarks
-VOL	ALIAS OF VOLUME	MANDATORY	ASCII STRING (MAXIMUM 10 CHARACTERS)
-ALL	REMOVES A VOLUME AND **ALL VOLUMES COMPOSING IT** IN THE HIERARCHY	OPTIONAL	DO NOT SPECIFY, NO VALUE ALLOWED FOR SWITCH

volume replace

This command replaces a volume with another volume. Use this command after a disk failure to replace a volume used in a storage hierarchy with a volume on a functional disk.

If you are replacing a volume used as part of a mirrored volume, use the CLI command **volume mirror-synch** to synchronize the replacement volume with the other mirrored volume(s).

volume replace

Switch	Definition	Type	Values/Remarks
-NVOL	ALIAS OF NEW VOLUME	MANDATORY	ASCII STRING (MAXIMUM 10 CHARACTERS)
-VOL	ALIAS OF VOLUME	MANDATORY	ASCII STRING (MAXIMUM 10 CHARACTERS)

volume resize

This command increases a simple, cubed or concatenated volume.

volume resize

Switch	Definition	Type	Values/Remarks
-VOL	ALIAS OF VOLUME TO RESIZE	MANDATORY	ASCII STRING (MAXIMUM 10 CHARACTERS)
-WITH	VOLUME TO RESIZE WITH	MANDATORY	ASCII STRING (MAXIMUM 10 CHARACTERS)
-A	NEW ALIAS OF RESIZED VOLUME	OPTIONAL	ASCII STRING (MAXIMUM 10 CHARACTERS)

volume retract

This command retracts a volume by deleting all added volumes use to resize the volume. This command only works if the resized volume has not been expanded. The head of the volume hierarchy is retracted, not the resized volume.

volume retract

Switch	Definition	Type	Values/Remarks
-VOL	ALIAS OF VOLUME	MANDATORY	ASCII STRING (MAXIMUM 10 CHARACTERS)

volume set

This command will change a volume alias or load threshold.

volume set

Switch	Definition	Type	Values/Remarks
-NA	NEW ALIAS	MANDATORY	ASCII STRING (MAXIMUM 10 CHARACTERS)
-VOL	ALIAS OF VOLUME TO CHANGE	MANDATORY	ASCII STRING (MAXIMUM 10 CHARACTERS)

volume snapshot activate

This command activates a snapshot volume.

volume snapshot activate

Switch	Definition	Type	Values/Remarks
-VOL	ALIAS OF VOLUME	MANDATORY	ASCII STRING (MAXIMUM 10 CHARACTERS)

volume snapshot deactivate

This command deactivates a snapshot volume.

volume snapshot deactivate

Switch	Definition	Type	Values/Remarks
-VOL	ALIAS OF VOLUME	MANDATORY	ASCII STRING (MAXIMUM 10 CHARACTERS)

volume snapshot list

The command 'volume snapshot list' has been replaced by 'volume snapshot show -vol' (see page 5-65).

volume snapshot rollback abort

This command aborts snapshot rollback.

volume snapshot rollback abort

Switch	Definition	Type	Values/Remarks
-SNAP	ALIAS OF SNAPSHOT VOLUME	MANDATORY	ASCII STRING (MAXIMUM 10 CHARACTERS)

volume snapshot rollback show

This command shows snapshot rollback details.

volume snapshot rollback show

Switch	Definition	Type	Values/Remarks
-TABLE	DISPLAYS DATA IN TABLE FORMAT	OPTIONAL	DEFAULT DISPLAY
-RECORD	DISPLAYS DATA IN RECORD FORMAT	OPTIONAL	

volume snapshot rollback start

This command starts snapshot rollback.

volume snapshot rollback start

Switch	Definition	Type	Values/Remarks
-SNAP	ALIAS OF SNAPSHOT VOLUME	MANDATORY	ASCII STRING (MAXIMUM 10 CHARACTERS)
-FORCE	SKIP CONFIRMATION	OPTIONAL	DO NOT SPECIFY, NO VALUE ALLOWED FOR SWITCH

volume snapshot show

This command shows all source volumes and their snapshot volumes.

volume snapshot show

Switch	Definition	Type	Values/Remarks
-TABLE	DISPLAYS DATA IN TABLE FORMAT	OPTIONAL	DEFAULT DISPLAY
-RECORD	DISPLAYS DATA IN RECORD FORMAT	OPTIONAL	
-VOL	ALIAS OF VOLUME	OPTIONAL	ASCII STRING (MAXIMUM 10 CHARACTERS)

volume snapshot set

This command sets snapshot parameters.

volume snapshot set

Switch	Definition	Type	Values/Remarks
-LT	NEW VOLUME THRESHOLD %	MANDATORY	5-100
-VOL	ALIAS OF VOLUME TO CHANGE	MANDATORY	ASCII STRING (MAXIMUM 10 CHARACTERS)

volume show

This command shows all volumes defined in the database.

volume show

Switch	Definition	Type	Values/Remarks
-TABLE	DISPLAYS DATA IN TABLE FORMAT	OPTIONAL	DEFAULT DISPLAY
-RECORD	DISPLAYS DATA IN RECORD FORMAT	OPTIONAL	
-DETAILS	DISPLAYS SPECIFIC DETAILS	OPTIONAL[1]	
-VOL	ALIAS OF VOLUME	OPTIONAL	ASCII STRING (MAXIMUM 10 CHARACTERS)

Index

S

T

W