# i series manager
# Graphical User Interface

# Table of Contents

# 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.brocade.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

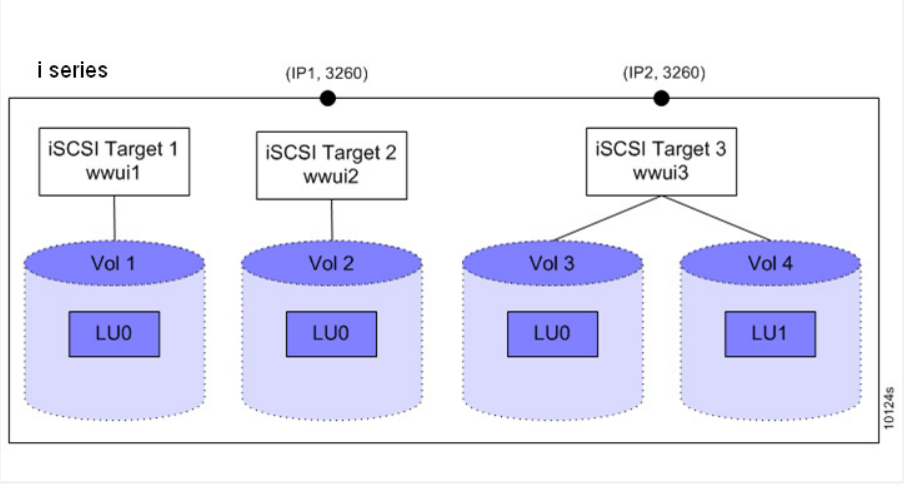



*Figure 1-1. iSCSI Target Access*

## 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.

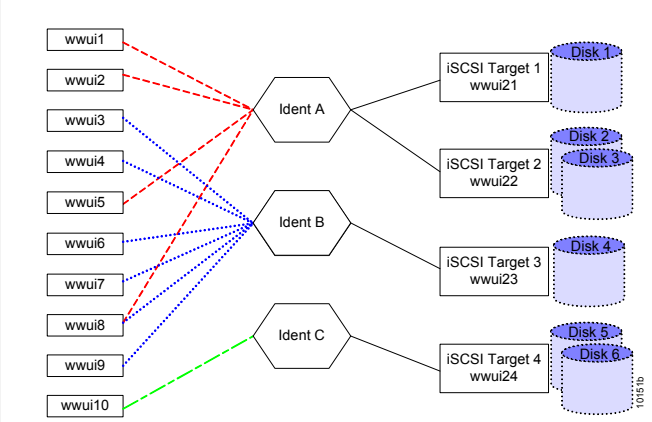
**Note:**
*If you are working with an iSNS server, all hosts are able to see all targets but only those hosts with access rights are able to connect to the authorized targets.*

**Example:**

In Figure 1-2 identities are coupled with iSCSI targets to limit iSCSI initiator access to

- 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

- 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.

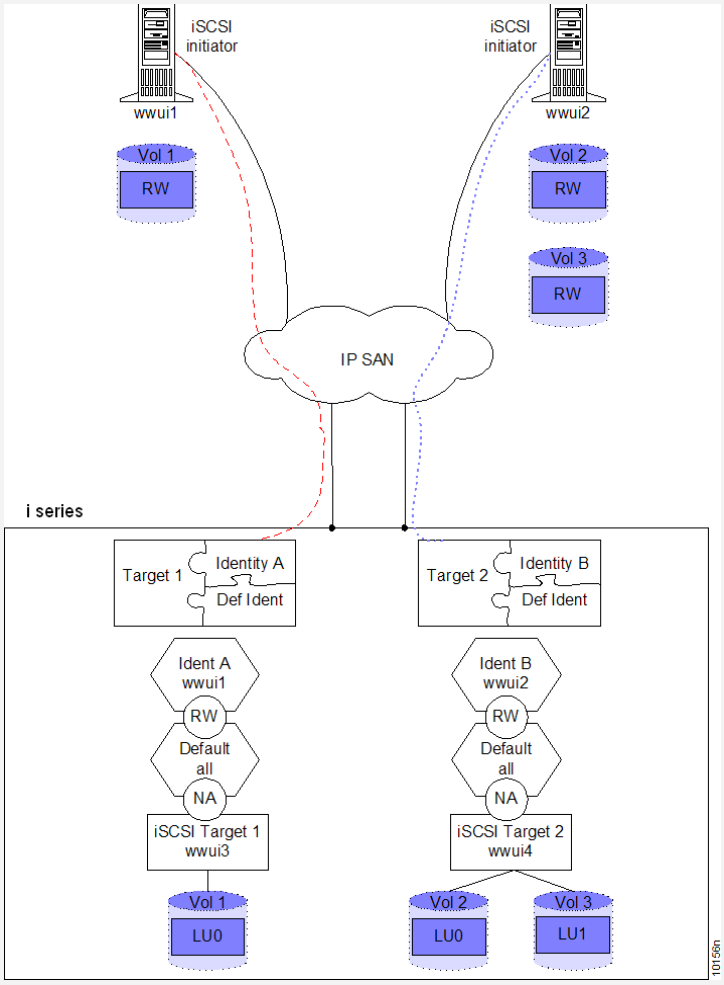



*Figure 1-3. Default Identities*

## 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.

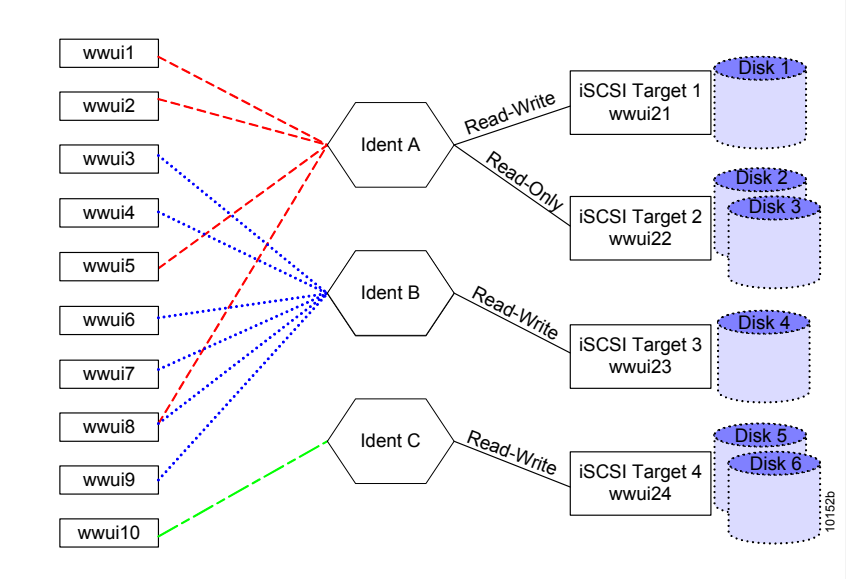



*Figure 1-4. Access Rights per Identity-Target Pair*

## *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.

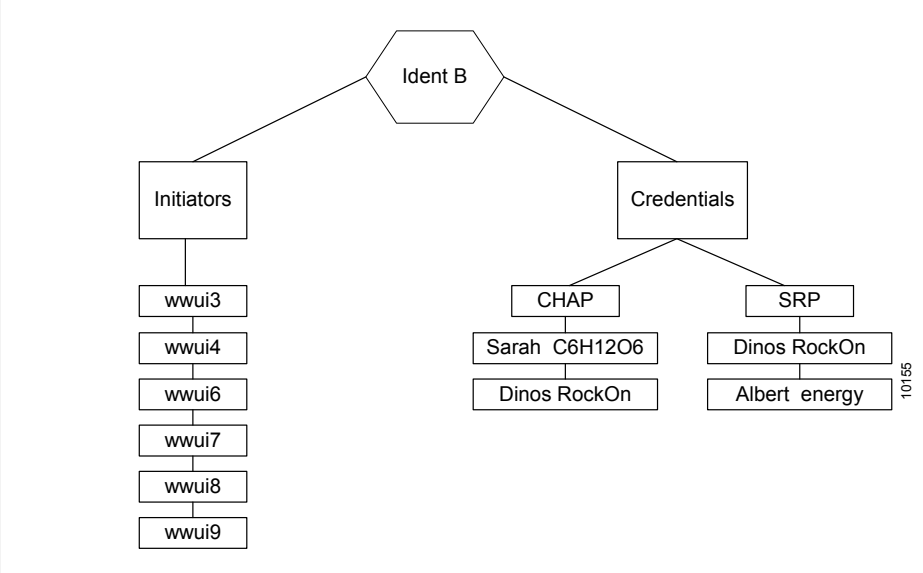



*Figure 1-5. Identity with iSCSI Initiators and Credentials*

### *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.

- 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.

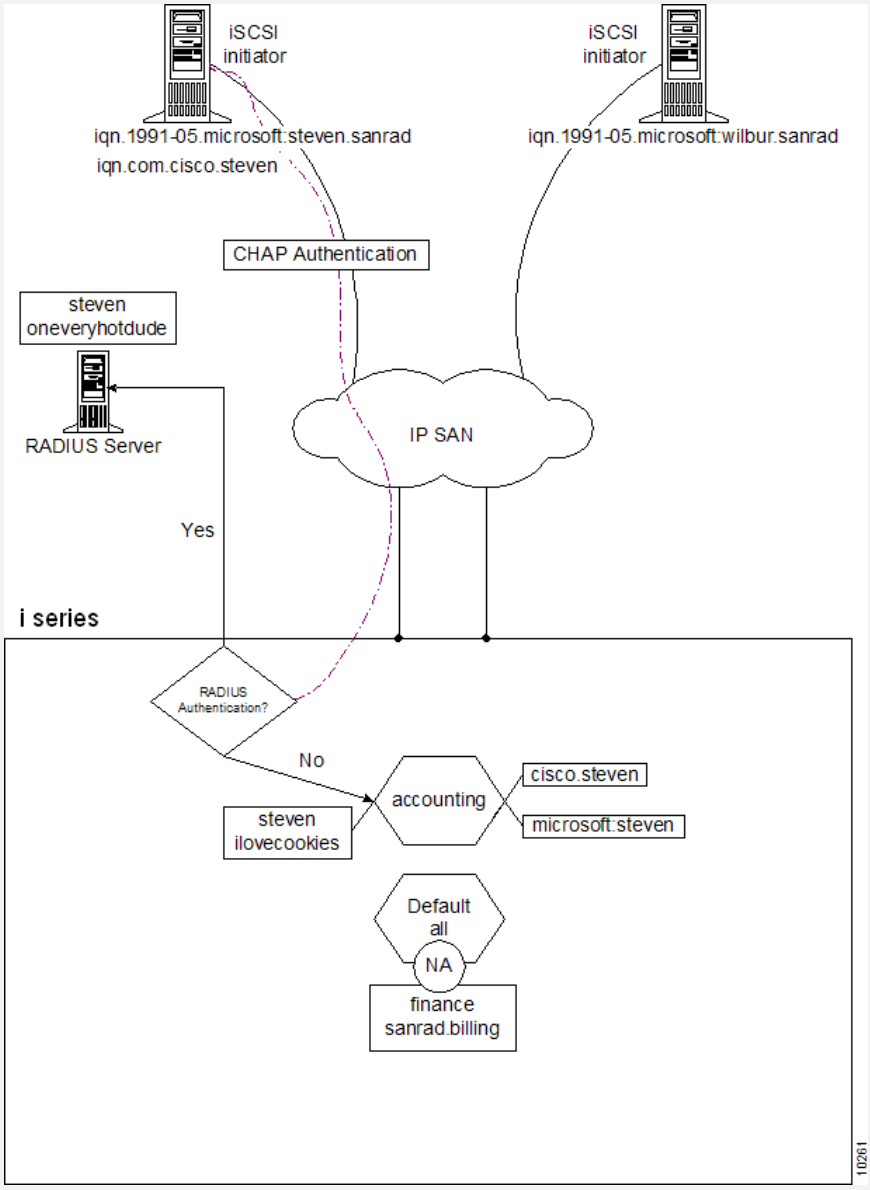



*Figure 1-6. Sending a CHAP Authentication Challenge*

# 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,

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.

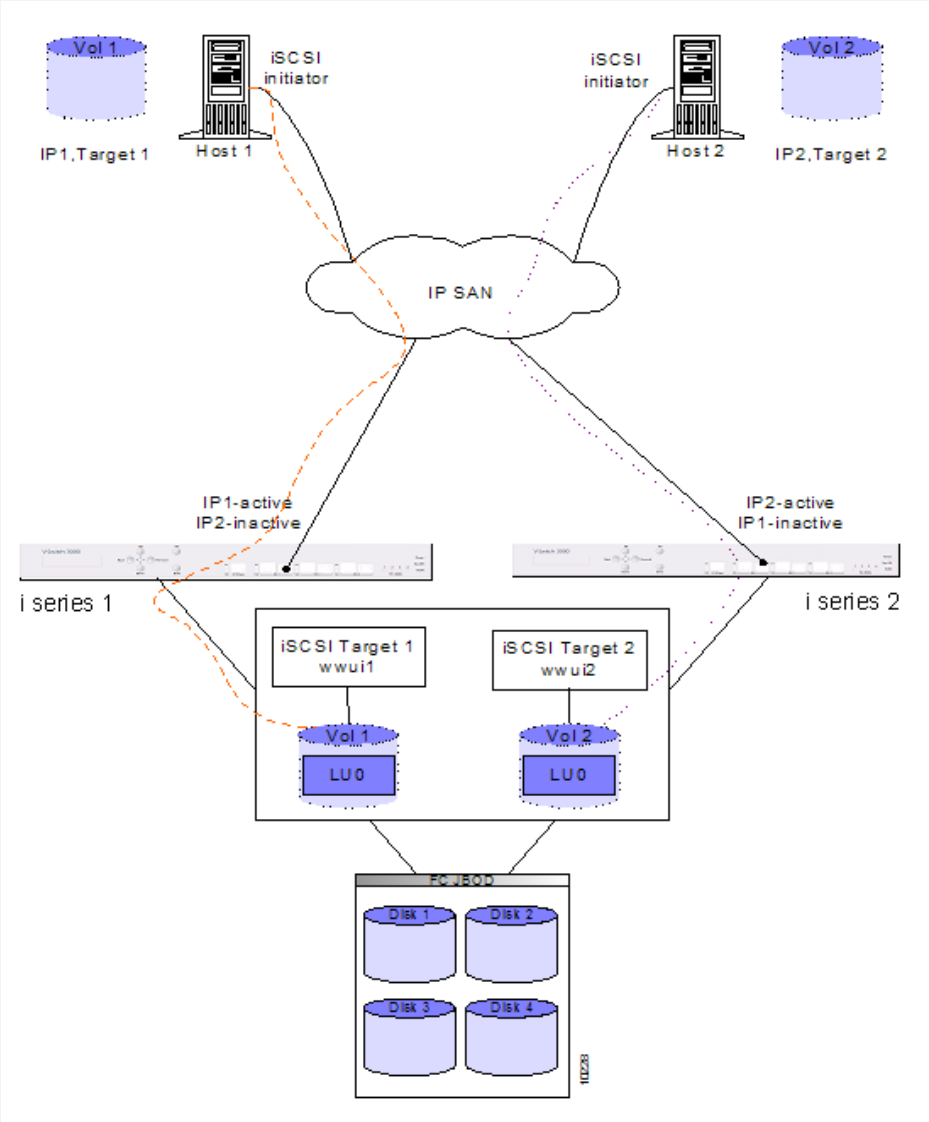



*Figure 1-7. i series Cluster Configuration*

**Example**

In Figure 1-8, i series 1 has gone off-line.  i series 2 activates i series 1's IP address and

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.

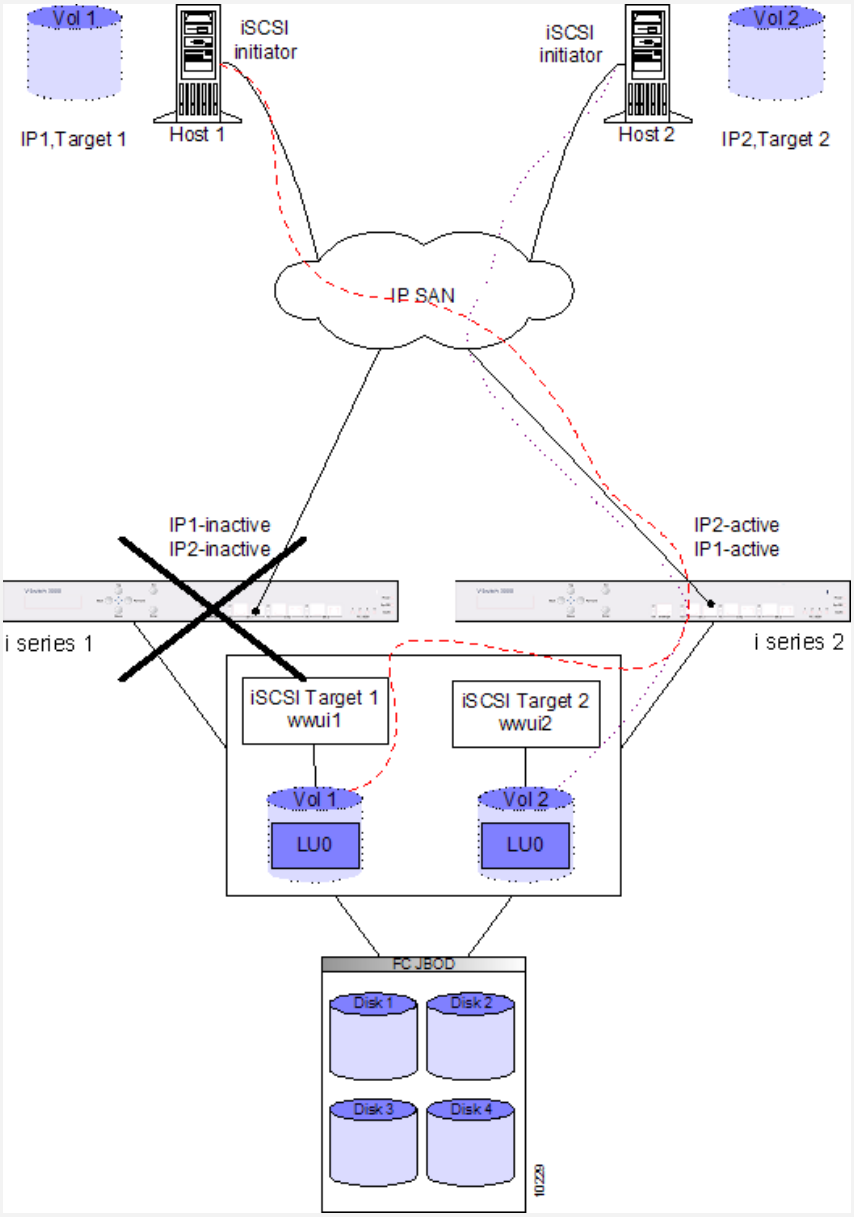



*Figure 1-8.  Re-Routing Storage Access with Off-line i series*

## 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.

## Synchronizing a Cluster

If disks or targets are created on one i series operating alone, when another i series is added, its database must be synchronized to the first i series's database. This can happen in three situations:

1. A new i series is added to a configured and functioning i series to form a cluster.
2. An offline i series in a cluster comes back online.
3. CLI is used to make an isolated configuration change in one i series.

When an element is not synchronized, a yellow exclamation mark appears to the left of it instead of a green check mark and the alarm *Object not redundant* is displayed. Synchronization is possible at every level of i series manager: Cluster, i series, Target and Disk.

Synchronization is carried out from the selected level down. Synchronization at the cluster level will synchronize the i series and their disks. You cannot synchronize IP addresses or IP routes as well as CHAP/SRP passwords.

# 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. For more information, see ***Transparent Volumes in Chapter 4.***

**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. For more information see ***Creating Subdisks (LUN Carving) in Chapter 4.***

**Example:**

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

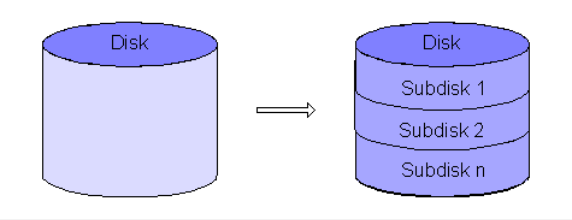



*Figure 1-9. Concatenated Volume Block Distribution*

## 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. For more information see ***Concatenated Volumes in Chapter 4.***

**Example:**

In Figure 1-10, the volume is divided into two equitable chunks to be mapped across

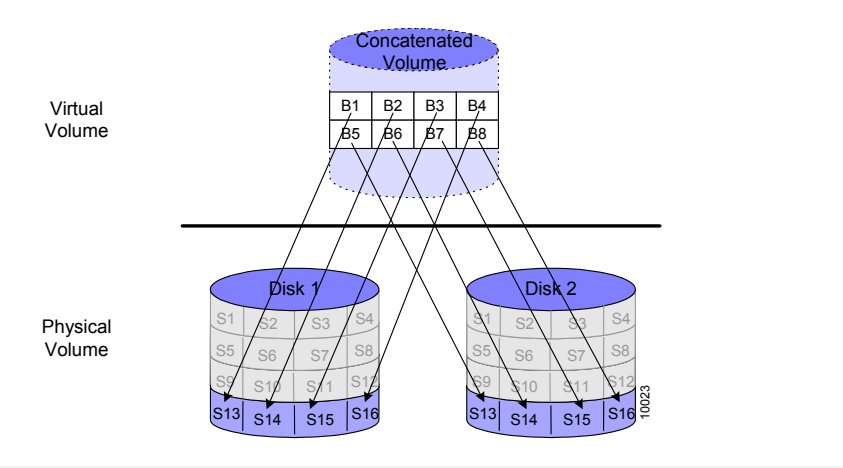



*Figure 1-10. Concatenated Volume Block Distribution*

## *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. For more information see ***Striped Volumes in Chapter 4.***

**Note:**

*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

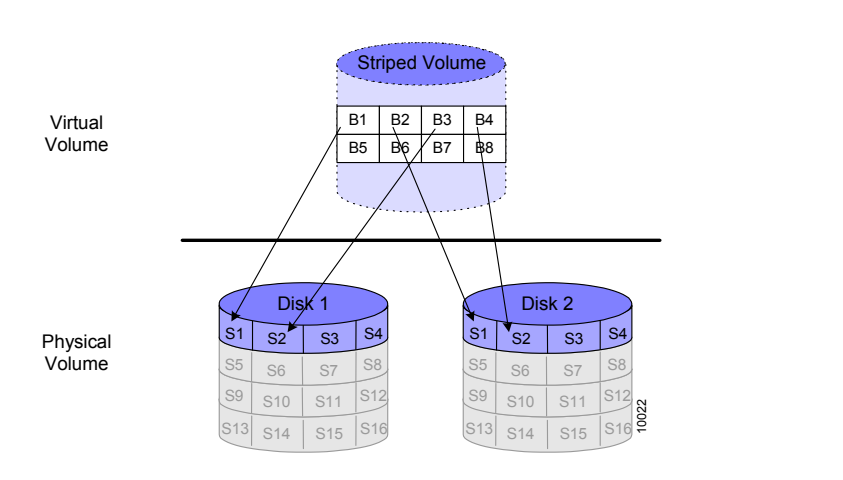



*Figure 1-11. Striped Volume Block Distribution*

## *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.  For more information see ***Mirrored Volumes in Chapter 4.***

**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

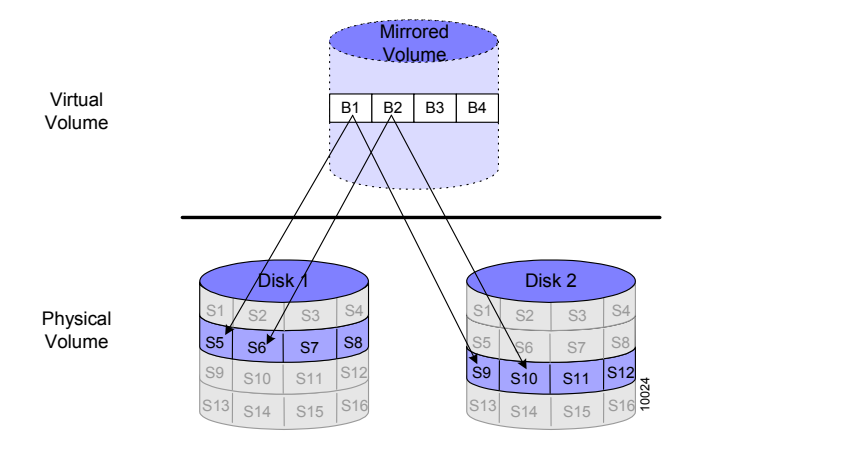



*Figure 1-12. Mirrored Volume Block Distribution*

## *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. For more information see ***Creating a Stripe over Mirrored Volumes in Chapter 4.***
- **RAID 0+1 is mirror over striped**
  Create striped volumes and then create mirrored volumes of the striped volumes. For more information see ***Creating a Mirror over Striped Volumes in Chapter 4.***

**Example**

In Figure 1-13, in the first mirrored volume, data block 1 is mapped to both block 1 on

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.

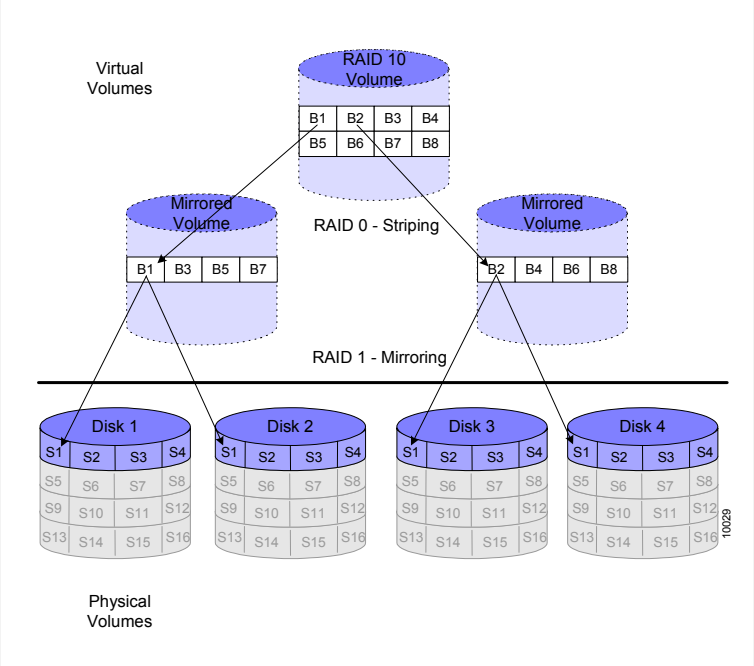



*Figure 1-13. RAID 10 Volume Block Distribution*

# 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. For more information see ***Offline Copy in Chapter 4.***

### *Online Copy or Volume Migration*

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:

1. 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). For more information see ***Migrating Volumes*** or ***Online Copy in Chapter 4.***

**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

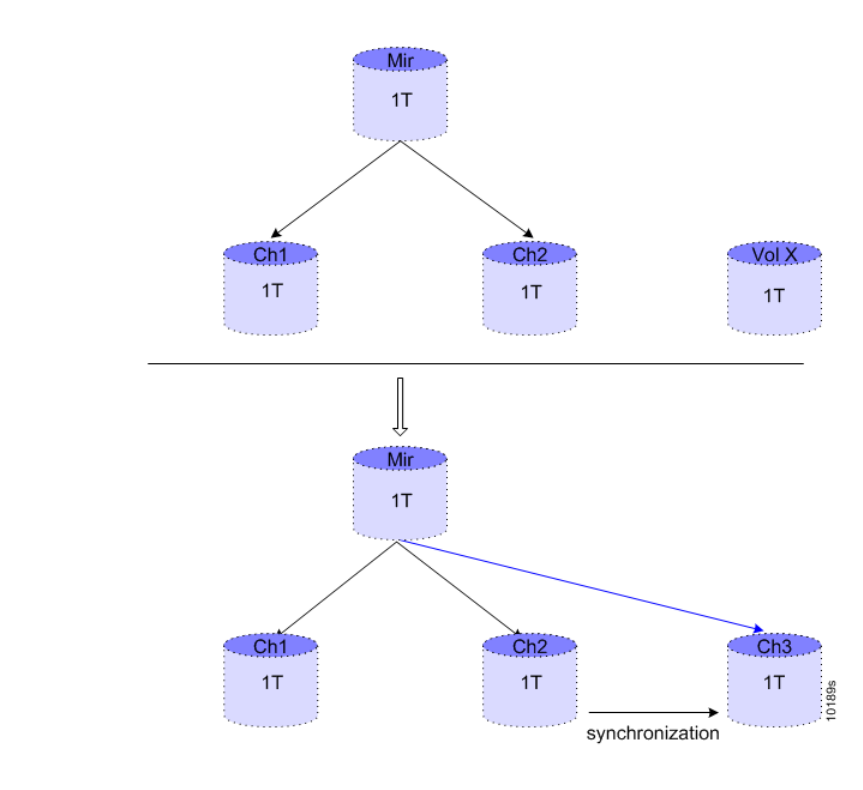



*Figure 1-14. Adding Another Child to a Mirror*

**Example**

In Figure 1-15, a concatenated volume becomes one child of a new mirrored volume.

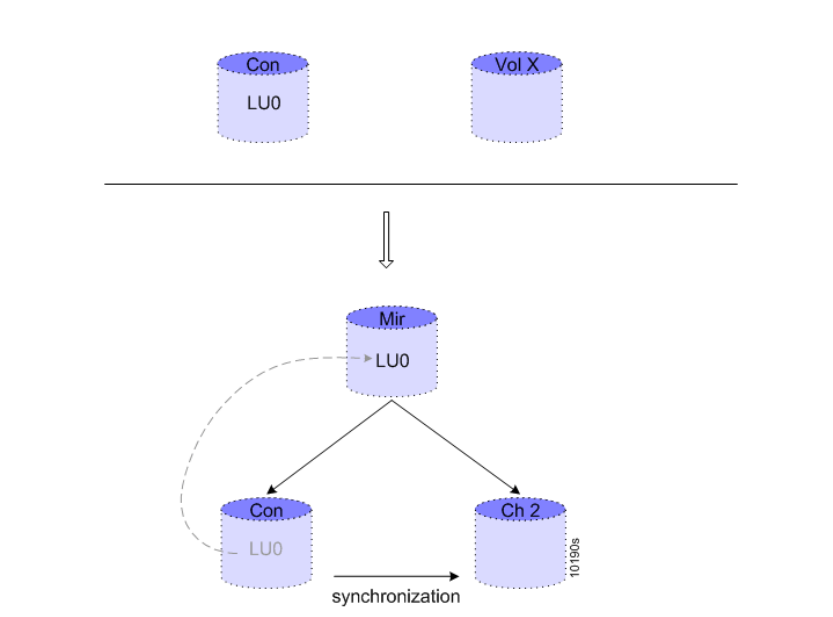



*Figure 1-15. Creating a Mirror to Add Data Redundancy*

**2.** 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). For more information see ***Breaking a Mirror in Chapter 4.***

**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

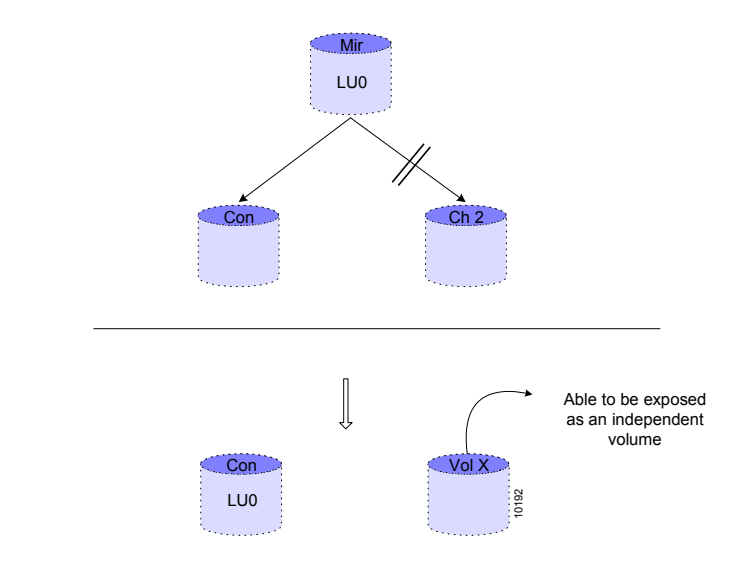



*Figure 1-16. Breaking a Mirror*

## 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. For more information see ***Snapshot Operations in Chapter 4.***

### *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

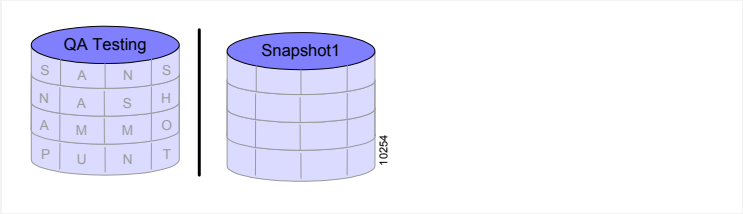



*Figure 1-17. 1st Snapshot Created*

**Example**

Figure 1-18 shows the same source and snapshot volume after a write operation to

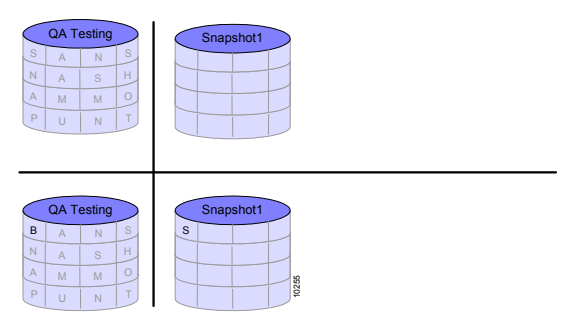



*Figure 1-18. 1st Write to Source and Update to 1st Snapshot*

**Example**

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


*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

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.

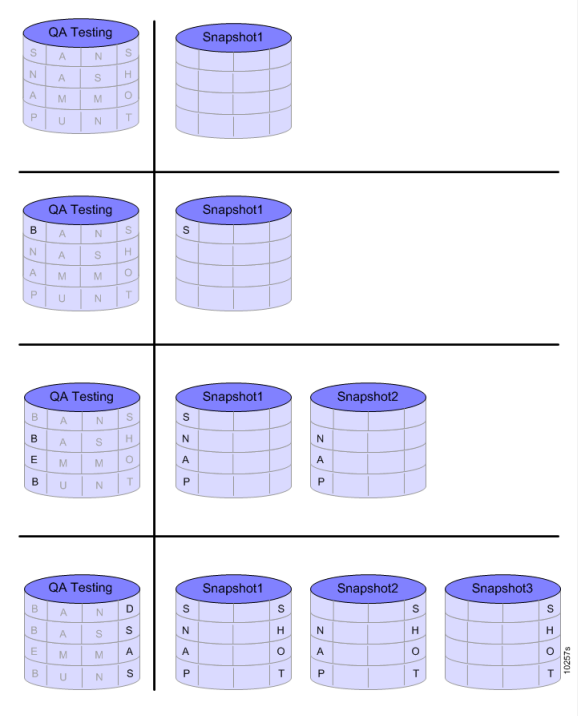



*Figure 1-20. 3rd Snapshot Created, Write to Source and Update to 1st & 2nd Snapshot*

## 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).

**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).

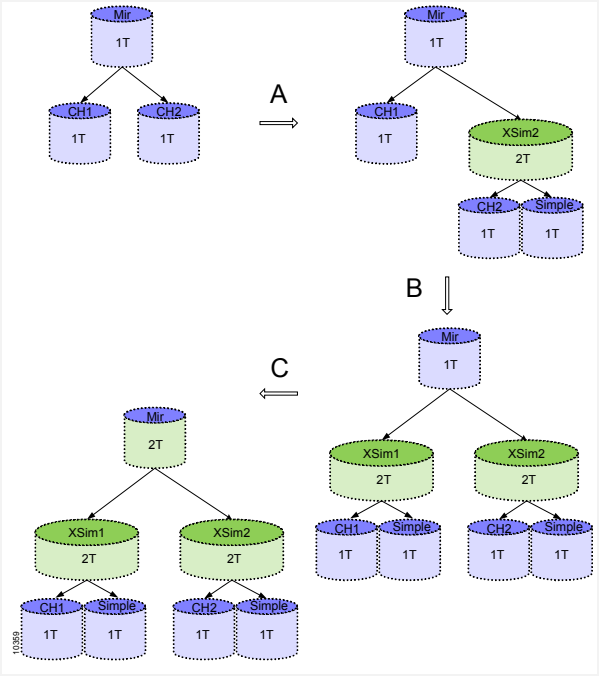



*Figure 1-21. Resizing a Volume*

# i series manager Overview

i series manager is a network management system for the i series.

- i series manager centrally manages multiple i series.
- Automatically synchronizes parameters in both devices when they are part of a cluster.
- i series manager manages virtualization processes (e.g. creating, expanding, exposing volumes).
- i series manager manages advanced volume operations (e.g. copying, snapshots, replicating volumes).
- i series manager provides performance monitoring for advanced diagnostics.
- i series manager provides detailed alarm reporting including email notification and alarm propagation.

## Managing the i series

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, using the i series LCD panel (for i series 3000 only) or via a console or dumb terminal to open a direct connection with the i series's RS232 console port.

The i series can be managed in one of three different ways. Each way requires a different configuration.

- **In-band**
  The management terminal (Telnet, SSH, SP server) connects to the i series's Eth1 port. The Eth1 port is used by the i series for management as well as by the hosts for accessing data accessing storage data (refer to B, Figure 1-22).
- **RS232**
  The console connects to the i series's RS232 port in a direct connection (refer to C, Figure 1-22). The RS232 port is used mainly for initial configuration: setting up the management IP, Mask and i series name. For more information on RS232 Serial Connection refer to ***RS232 Serial Connection in Chapter 3.***
- **Out-of-band (**certain versions only**)**
  The management terminal (Telnet, SSH, SP server) connects to the i series's dedicated 10/100 management port via a fast Ethernet network (refer to A, Figure 1-22). The i series's default IP (10.11.12.123) can be used to connect to the i series from remote (via telnet). For more information on Telnet/SSH connection refer to ***Telnet/SSH Connection in Chapter 3.***

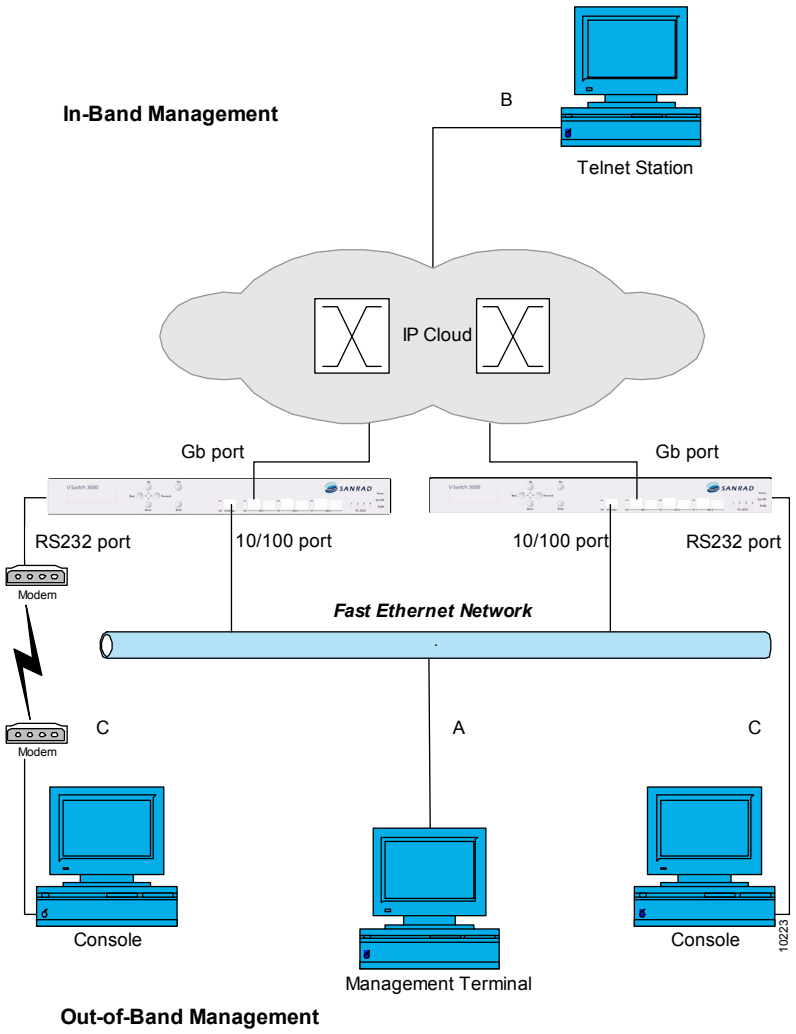



*Figure 1-22. i series Management Options*

# Chapter 2
# Installation

i series manager installation runs on Win32 and Linux platforms and works on a client-server model with the following access options:

- Client installed locally on the same host server.
- Client and server installed remotely with the remote client accessing the local server with a Web browser as a JAVA applet.
- Stand-alone client installed remotely accessing the local server.

## Windows Platform

The following section is for Win32 platform only. If you are using Linux, refer to ***Linux Platform***.

### Installing i series manager on a Windows Platform

**Notes:**

*If you have a previous version of i series manager installed, you must remove the previous version before upgrading your i series manager system.*

*To install and run i series manager, you must have the JAVA Runtime Environment (JRE) installed. If you have both a server and client installed, you need to install the JRE in both places.*

*i series manager will not run if the correct version of the JRE is not properly installed on the host machine. The correct version of Java is included on the installation CDROM. Additionally, the JRE can be downloaded from* **http://java.sun.com**.

***To install i series manager on Windows platform:***

1. Double click on the i series manager.exe file in the i series manager folder on the NEXSAN CD shipped with the i series.

   The i series manager Installation Wizard opens.

2. Click **Next** to begin installation.

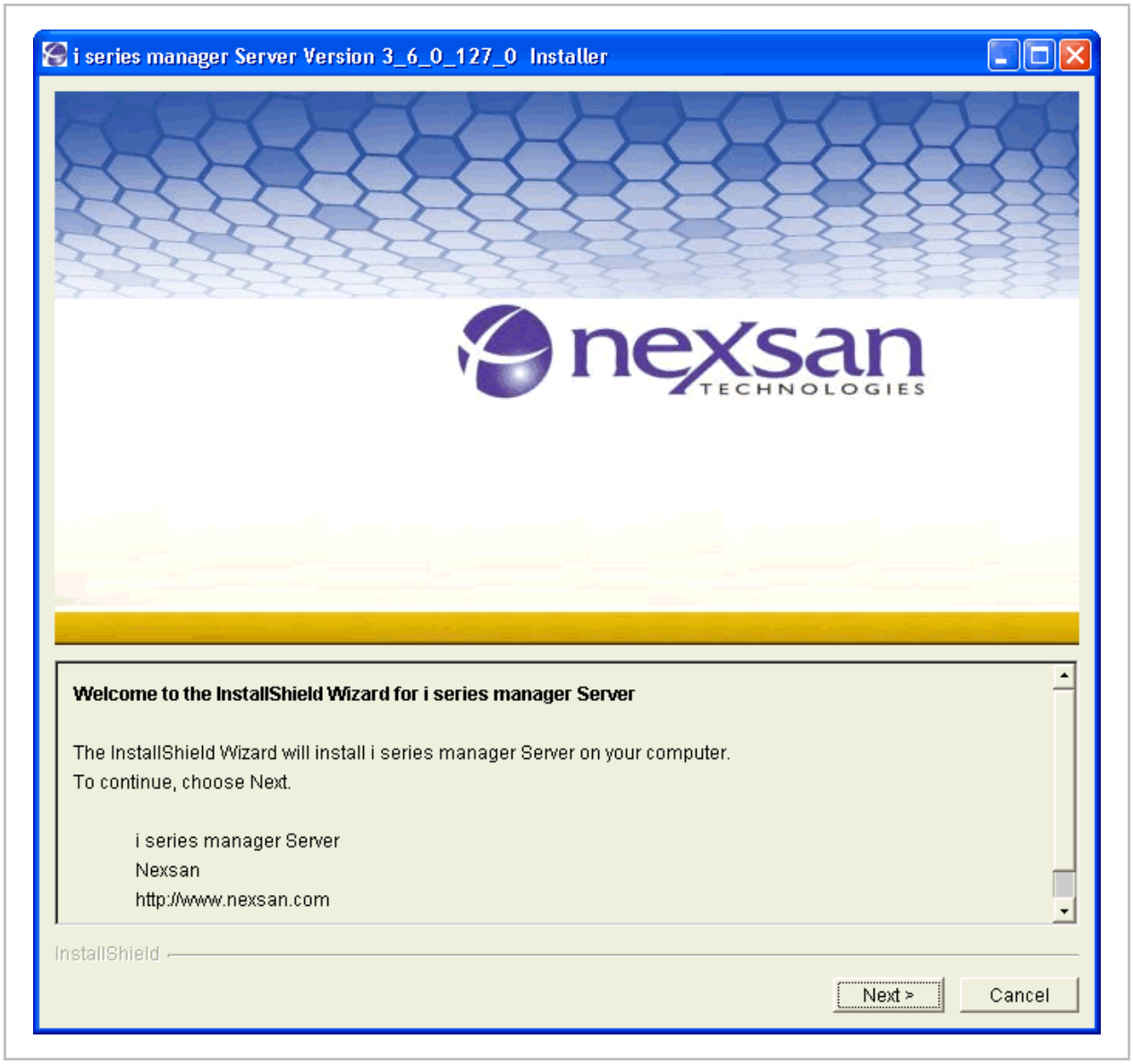



*Figure 2-1. i series manager Server Installation Wizard*

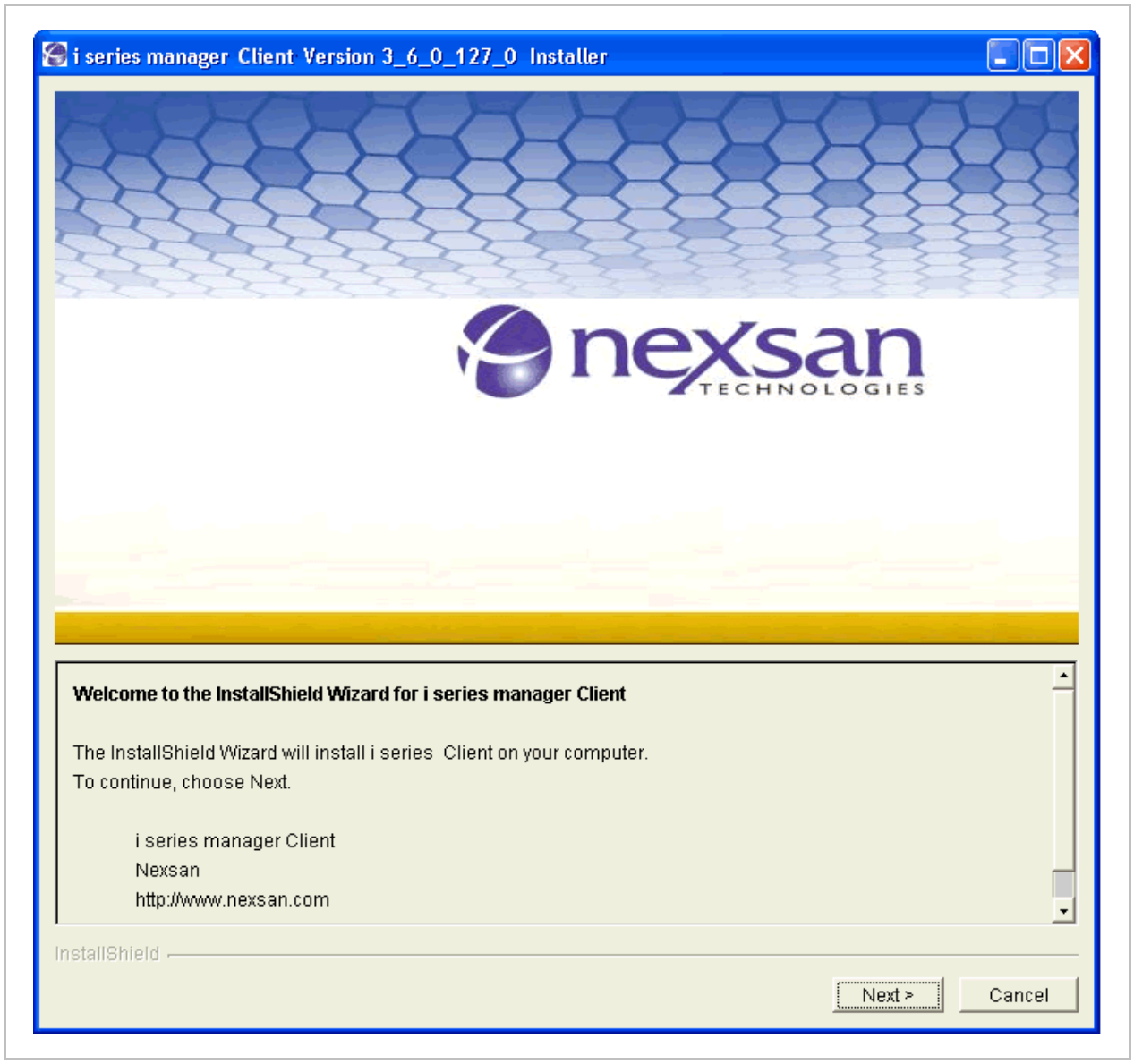



*Figure 2-2. Stand-Alone Client Installation Wizard*

3. Install i series manager in the default location or use the Browse to specify an alternate location.

**Note:**
*If the i series manager user will be accessing i series manager through a Web browser, i series manager must be installed under your system's Web server documents root.*

4. Click **Next**.

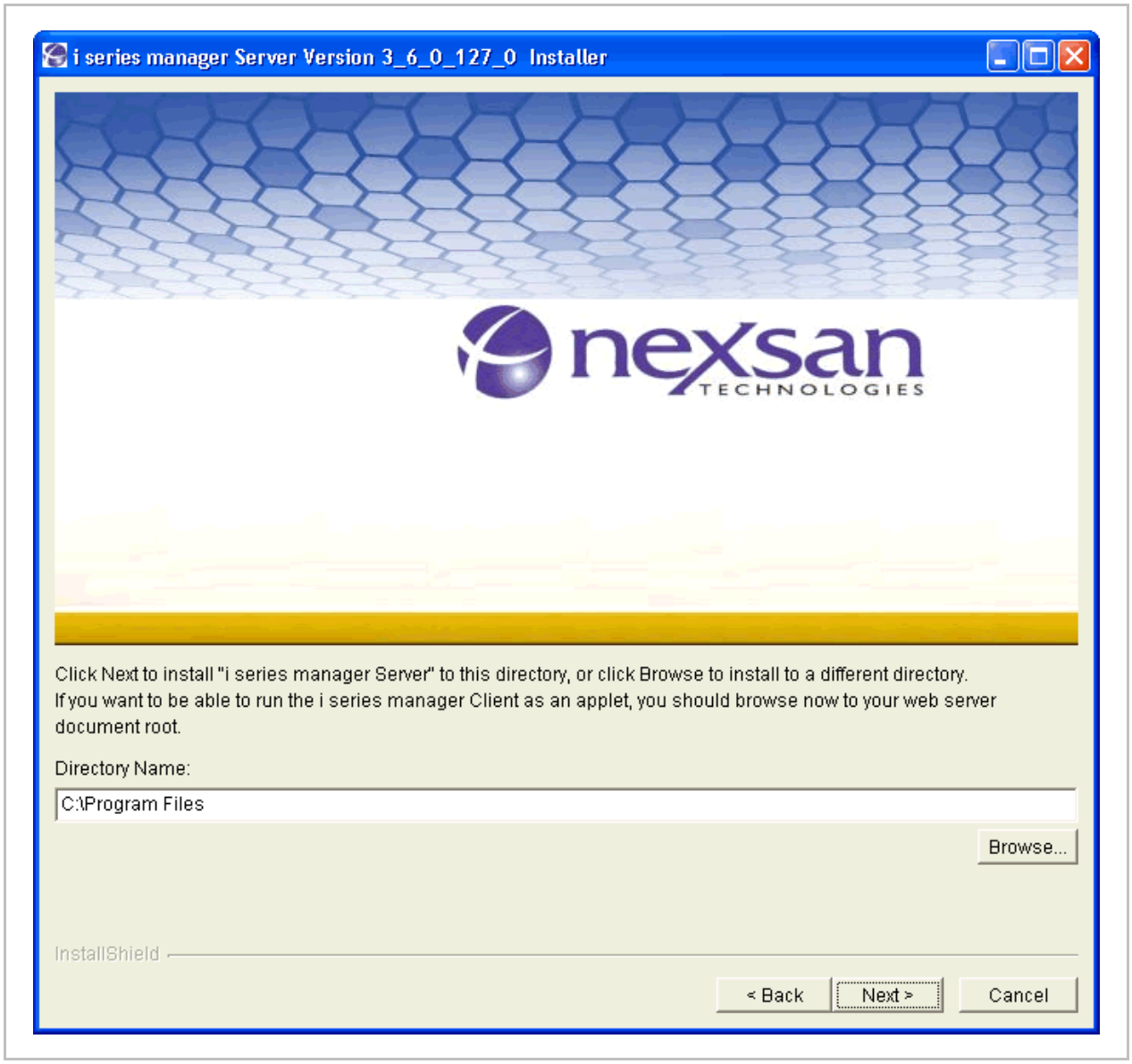



*Figure 2-3. i series manager Installation Location*

5. Confirm installation location and click **Next**.

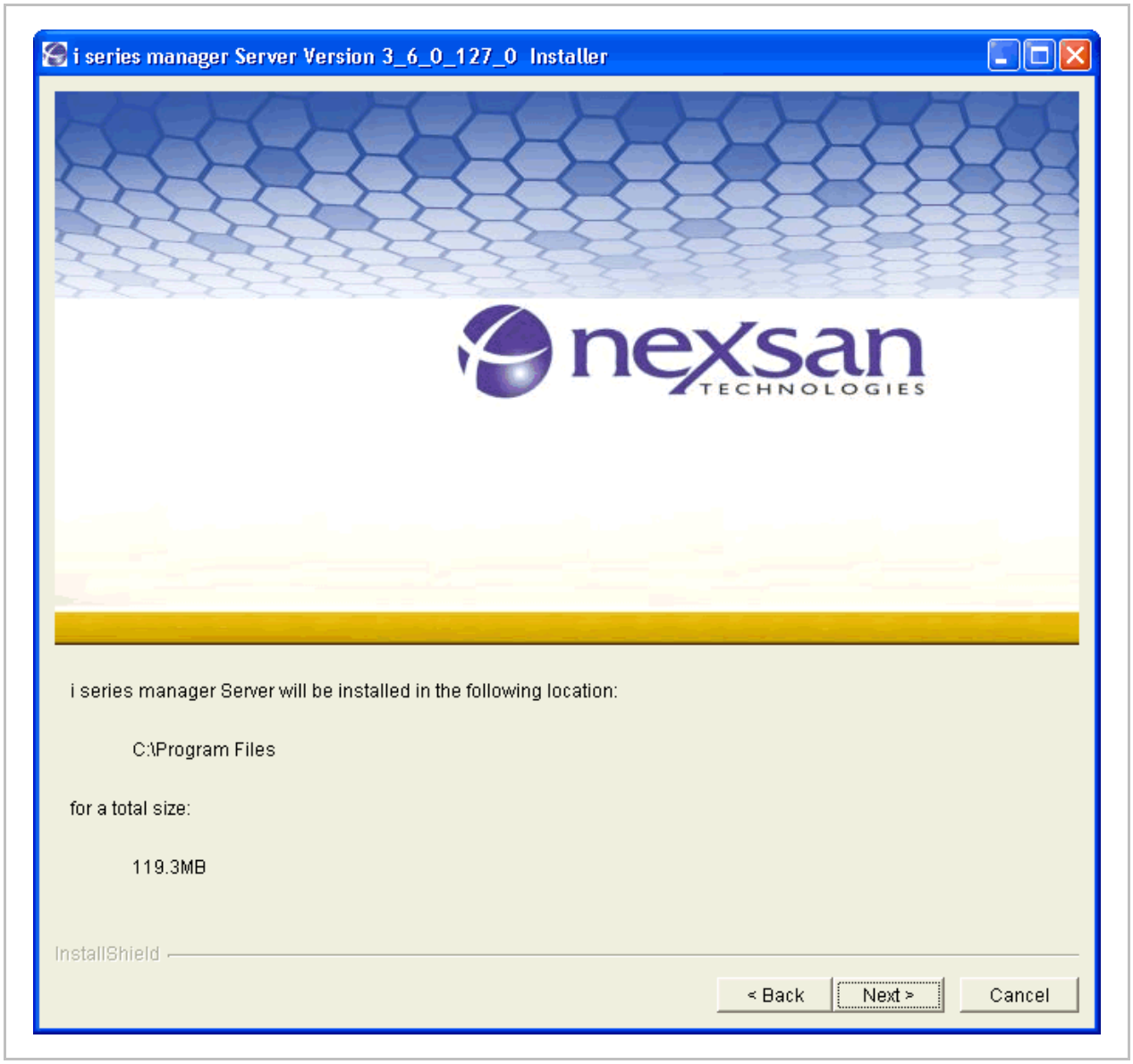



*Figure 2-4. i series manager Installation Location Confirmation*

The i series manager Management System files are installed in the designated location.

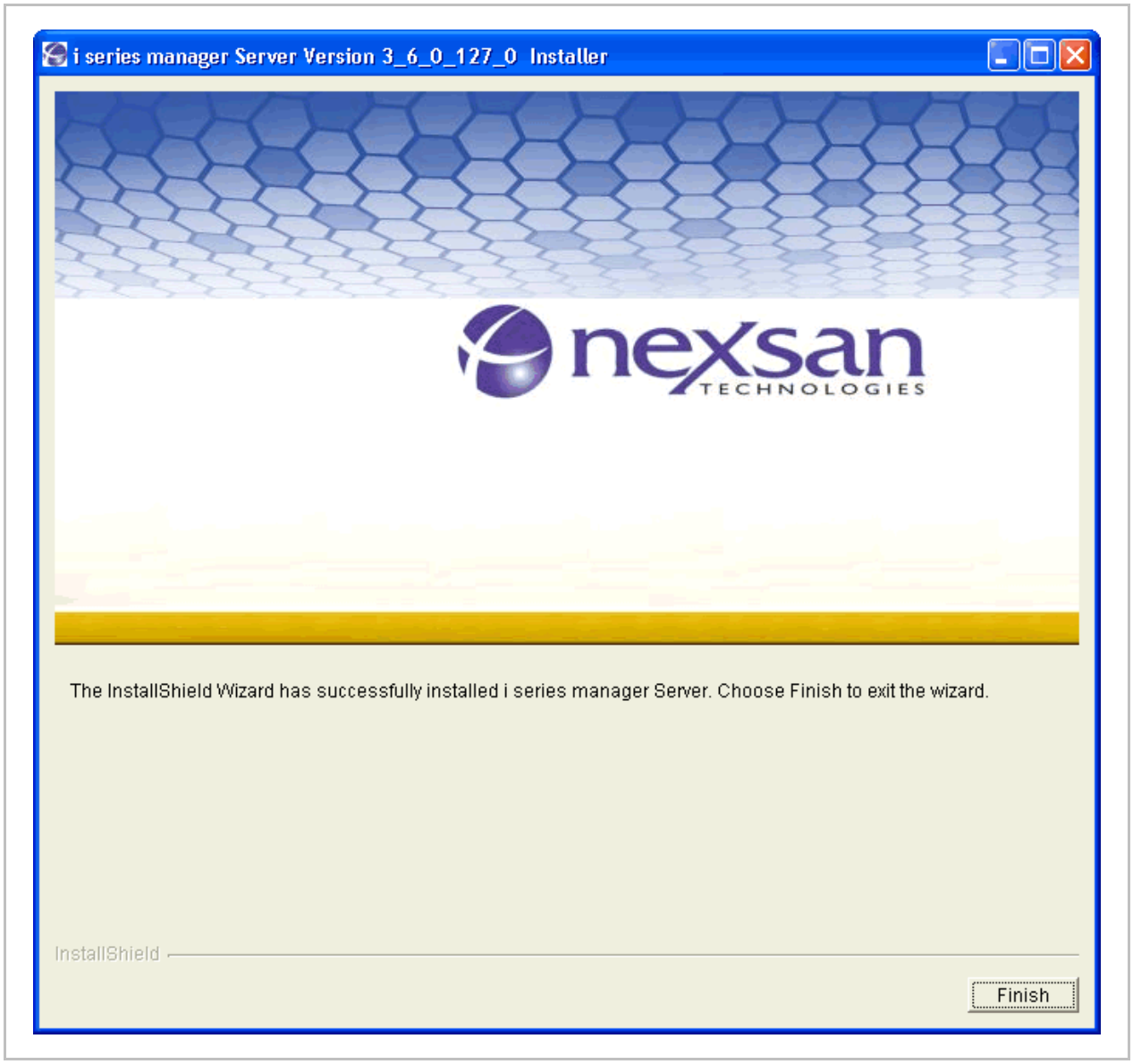



*Figure 2-5. Complete Installation*

6. Click **Finish** to complete the installation wizard instructions and close the wizard.

## Running i series manager Server

The i series manager Server starts automatically. You can Stop/Restart/Run the server.

***To stop/restart/start the i series manager server***

1. From the Programs menu:
   **Start > Programs > NEXSAN > i series manager > Server > Start/Stop/Restart.**

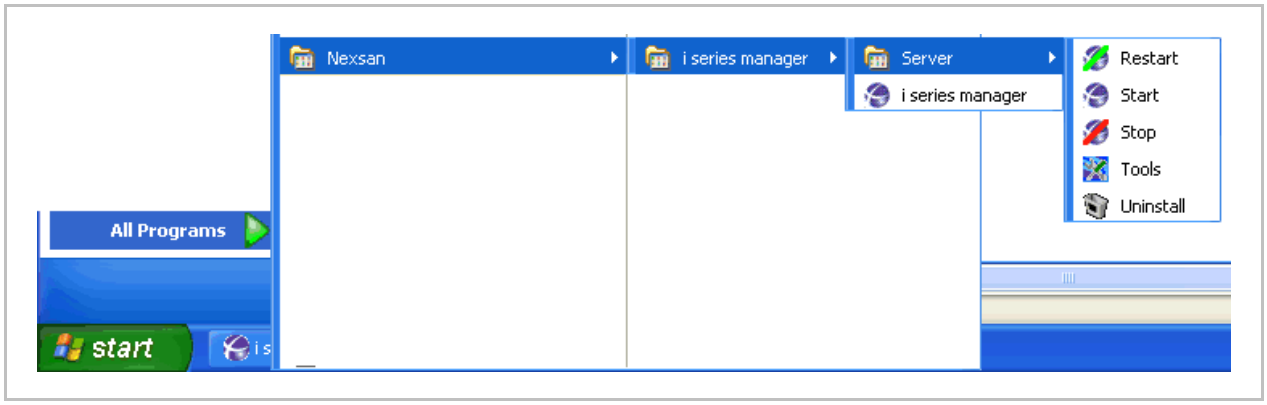



*Figure 2-6. i series manager Server Location*

### *i series manager Server Located Behind NAT*

You need to configure the i series manager server host machine alias or IP address if the i series manager server host machine is located behind a NAT (Network Translation) environment. If the i series manager server host machine is not located behind a NAT environment, the System Configuration Hostname must be left blank.

***To configure system parameters:***

1. From the Programs menu:
   **Start > Programs > NEXSAN > i series manager > Server > Tools.**

   The Tools icon appears in the system tray (Figure 2-7).

2. In the system tray, right click on the Tool icon and select **Network Configuration...**

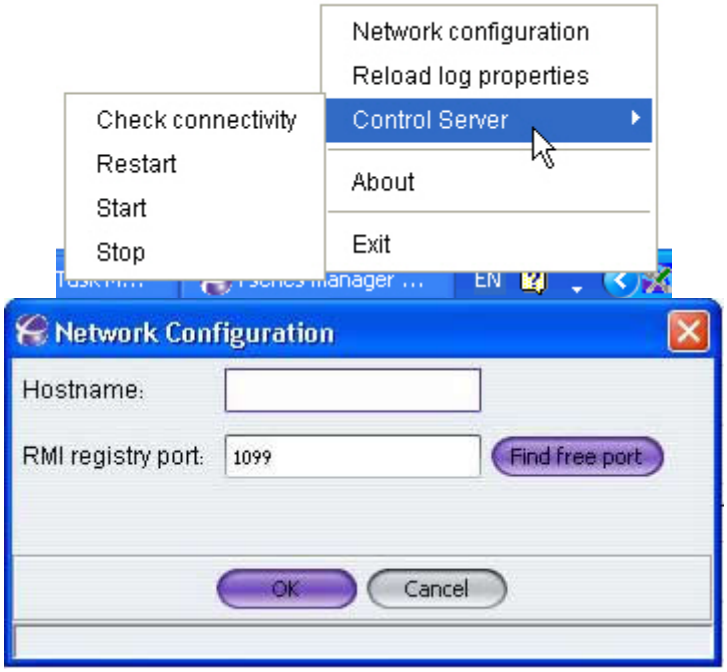



*Figure 2-7. Tools Menu*

The Network Configuration dialog box opens.

3. Enter the **Hostname** (use i series manager server host machine alias or IP address).
4. Enter the **RMI registry port**.
5. Click **OK**.

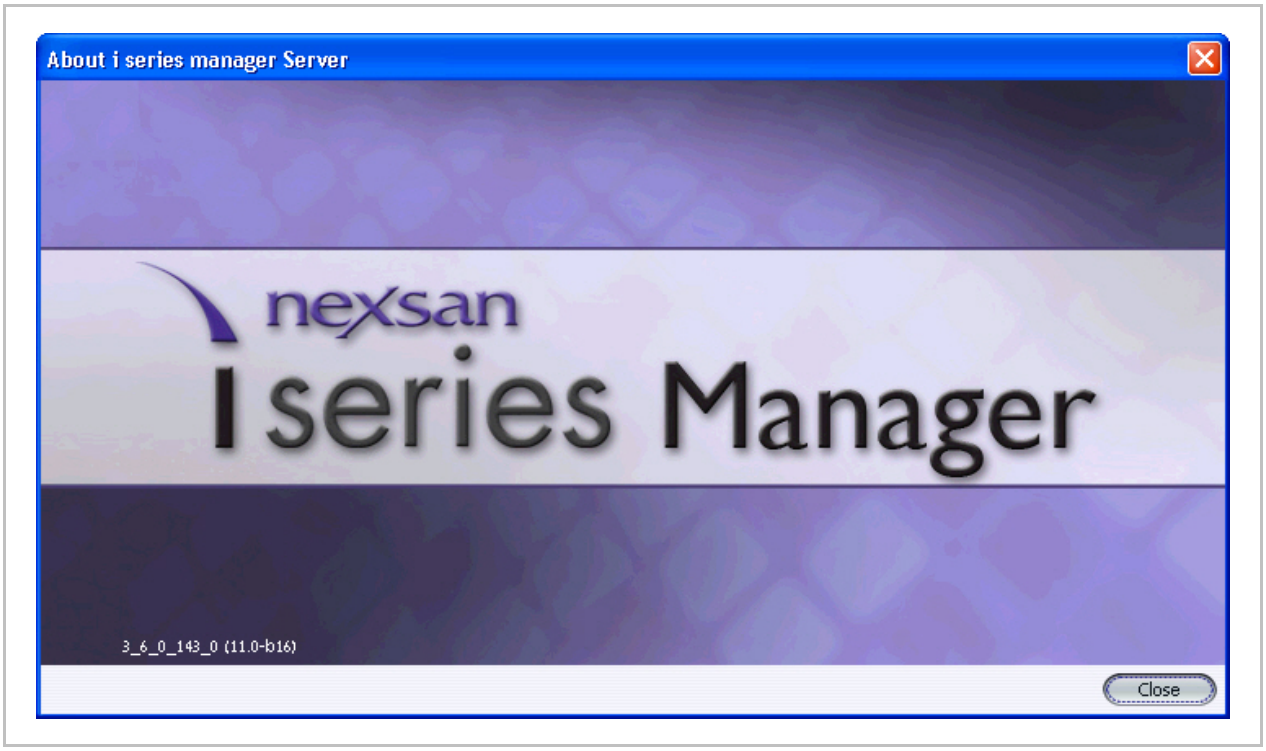



*Figure 2-8. System Configuration Dialog Box*

## Running i series manager Client

After installing i series manager and running the i series manager server, you can open the i series manager client at any time either by running the i series manager Client on the local management station, on another station or through a Web browser.

> **Note:**
> *When accessing i series manager through a Web browser, i series manager must be installed under your system's Web server documents root. The i series manager URL is in the form:*
> *http://<ip of host terminal or host name>/NEXSAN/i series manager/index.html*

### *Accessing i series manager on the Local Management Station*

***To start the client:***

1. From the Programs menu:
   **Start > Programs > NEXSAN > i series manager > i series manager**

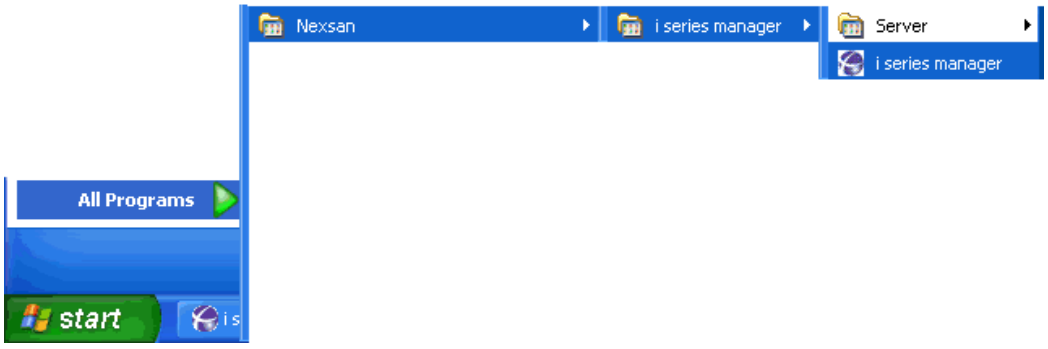



*Figure 2-9. i series manager Location*

The i series manager screen opens.

2. Enter the default **User Name** and **Password: *admin***.

> **Note:**
> *If the i series manager client is located on a different host server from the i series manager server, you must enter the i series manager server host name and server port to enable communication between the client and server.*

3. If necessary, enter **Server Host** and **Server Port.**
4. Click **OK**.

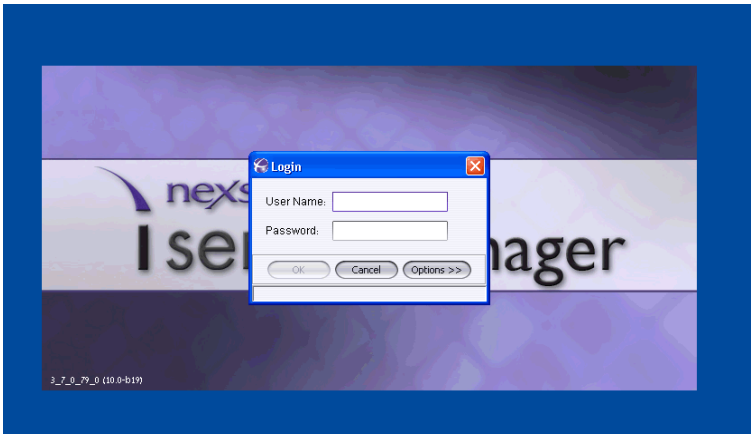



*Figure 2-10. i series manager Client Login Screen*

You can now add your i series to i series manager.

# Chapter 3
# i series Operations

i series manager communicates with the i series via the i series management port IP address. The i series communicates with hosts via iSCSI portals which are configured via i series manager. i series manager automatically discovers all disks and LUNs connected to the i series storage ports. i series manager enables multi-cluster management.

## Initial i series Configuration

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.

### Assigning a 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***

Change your computer's IP Address to anything on the same subnet 10.11.12.*

Connect to the management port on the i series.

Telnet to 10.11.12.123.

Enter Username and Password: ***admin***.

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

1. IP Address.

IP Mask.

i series name.
This name will appear in the i series manager Navigation Pane. If you don't enter a name, i series manager will use the last section of its IP address. This name can be changed later via the i series Properties tab if there is only one i series present.

Management port (Mgnt or ETH1).

## RS232 Serial Connection

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

1. Connect the cable to the appropriate port on the management server, and open a Terminal session. Set the following parameters in the terminal:
   **Bits per second = 115200**, **Flow Control = None**, **Emulation = Autodetect**.

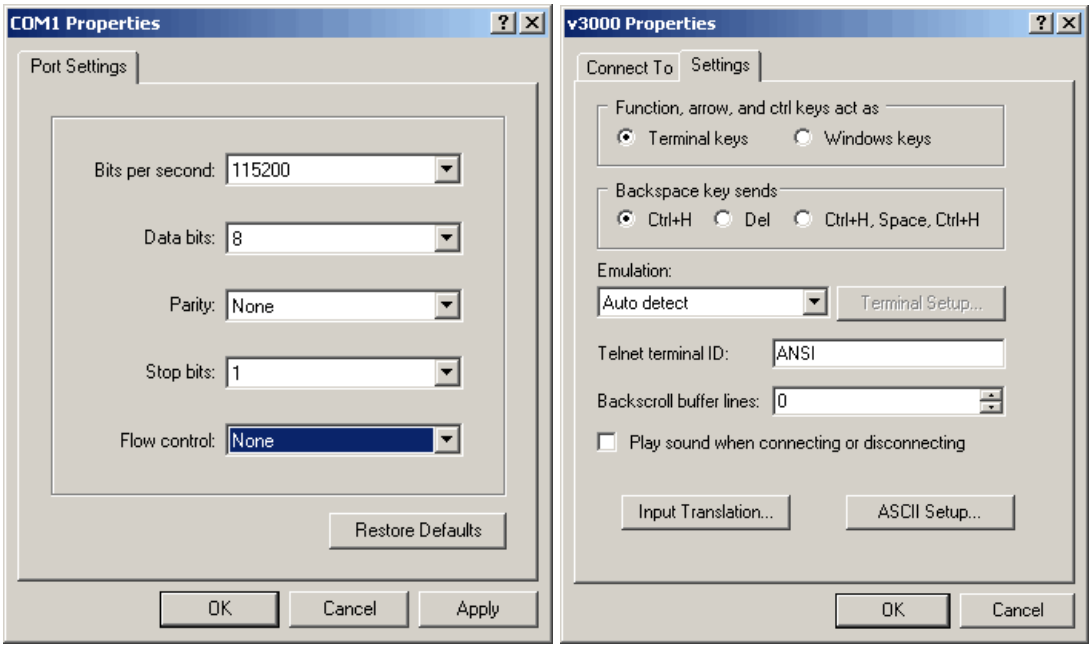



*Figure 3-1. Terminal Properties*

Enter Username and Password: ***admin***.

Set the default IP Address.

Set the default IP Mask.

Set the default i series name. This name will appear in the i series manager Navigation Pane. If you don't enter a name, i series manager will use the last section of its IP address. This name can be changed later via the i series Properties tab if there is only one i series present.

Set the default management port (Mgnt or ETH1).

# i series manager User Login Profiles

> **Note:**
> *Once you add a user profile, the default username and password is erased.*

**User Name:** The default user name for i series manager is **admin.**

User names can be any string up to 79 characters long.

**Password:** The default password for i series manager is **admin.**

Passwords must be at least 6 and not more than 12 characters long.

### *To configure a user profile:*

1. From the **i series manager** menu bar, select **Secure** > i series manager **Users…**

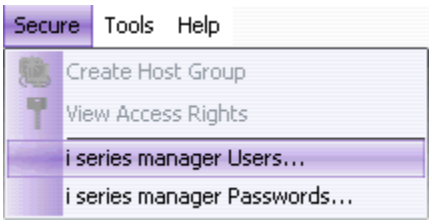



*Figure 3-2. Secure Menu*

The Users window opens.

Click **Add**.

The **Add User** dialog box opens.

Enter the user name and password in the appropriate fields.

Click **OK**.

The Add User dialog box closes. The new user name now appears in the Users window. You can sort the user names by clicking the sort arrow.

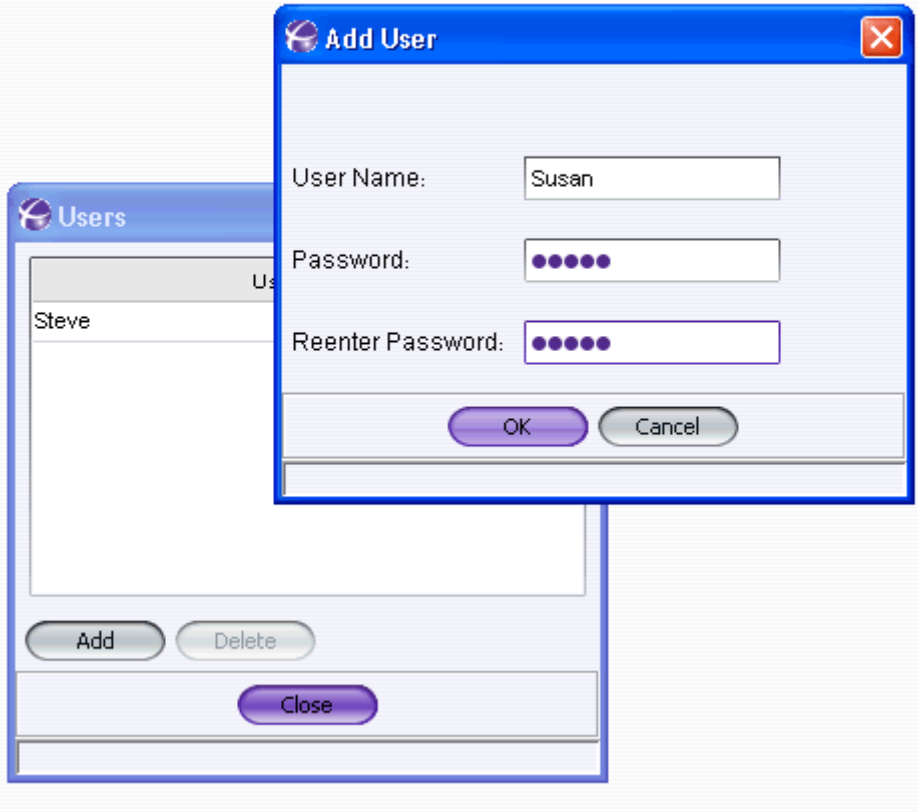



*Figure 3-3. Users Window*

# Changing the User Password

***To change the current user password:***

1. From the i series manager menu bar, select **Secure** > i series manager **Passwords…**

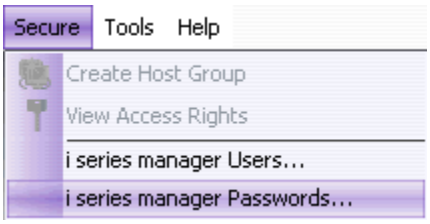



*Figure 3-4. Secure Menu*

The Change Password window opens.

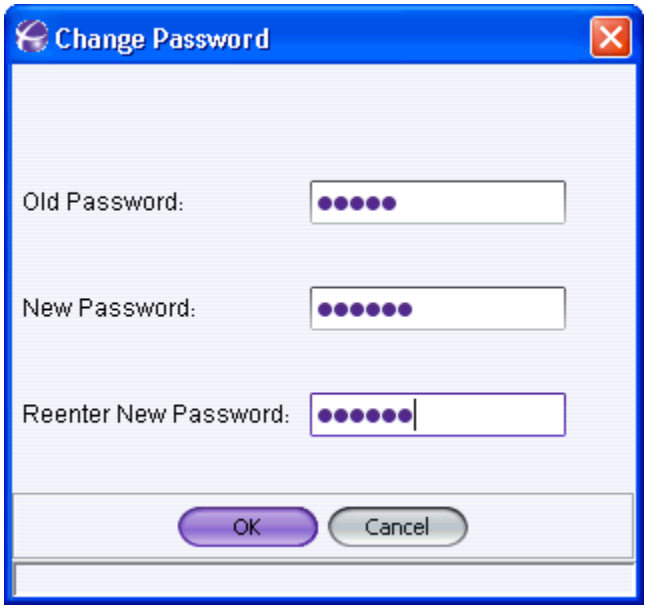



*Figure 3-5. Change Password*

2. Enter the old and new password and click **OK**.

# i series & Cluster Configuration

A *cluster* is a group of FC storage units and switches that function as one unit for virtualization. Clusters provide high availability in the event of i series failover.

i series manager enables you to make a cluster from two i serieses and configure both at the same time. Additionally, a cluster can be made by adding a new i series to an already configured stand-alone i series and then synchronizing the cluster.

> **Note:**
> *This section details the steps necessary for configuring a single, stand alone i series. When additional steps must be taken for cluster configuration, they are noted .*

## Adding a New i series

All stand alone i series must be added to i series manager.

***To add a new i series:***

1. From the Quick Launch:
   **Configure > Create System Entity > Storage Resource Group [Single Switch]…**

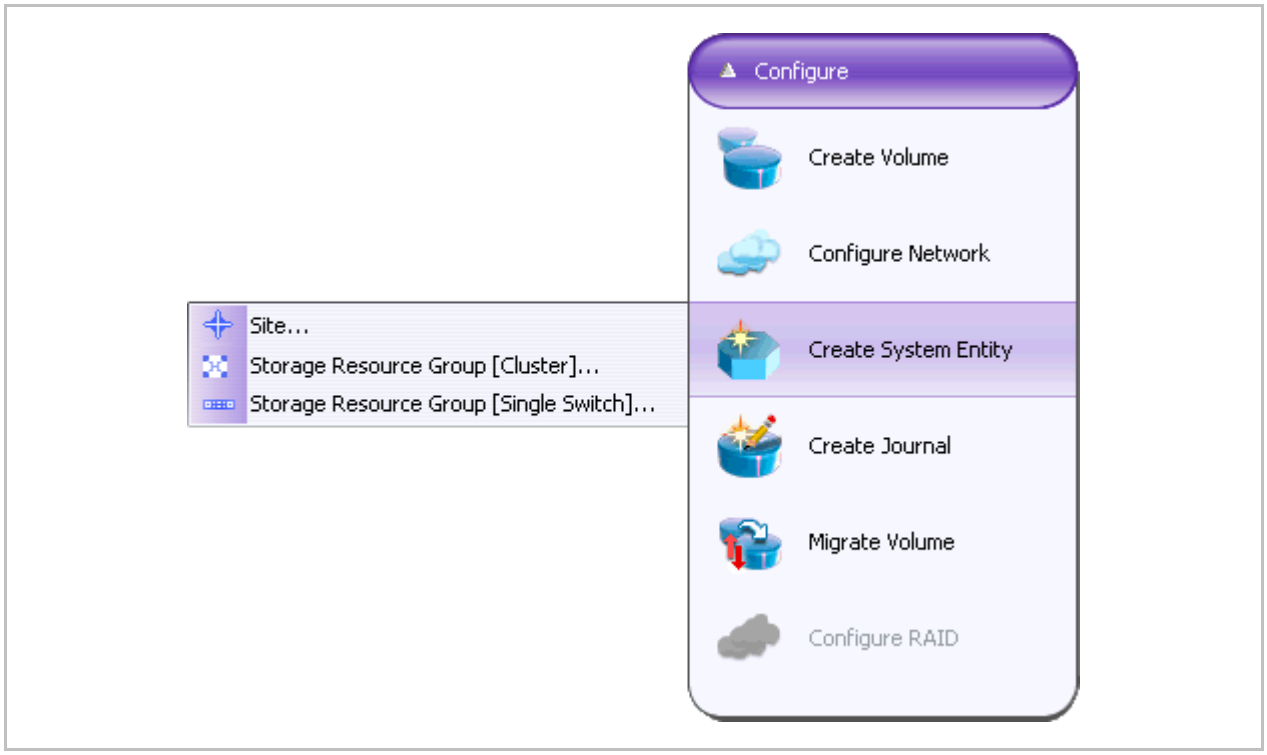



*Figure 3-6. New Storage Resource Group (Single Switch)*

The New i series dialog box opens.

Enter the i series configuration parameters in the dialog box.

**Note:**
*The IP address is mandatory. The remaining fields contain default values.*

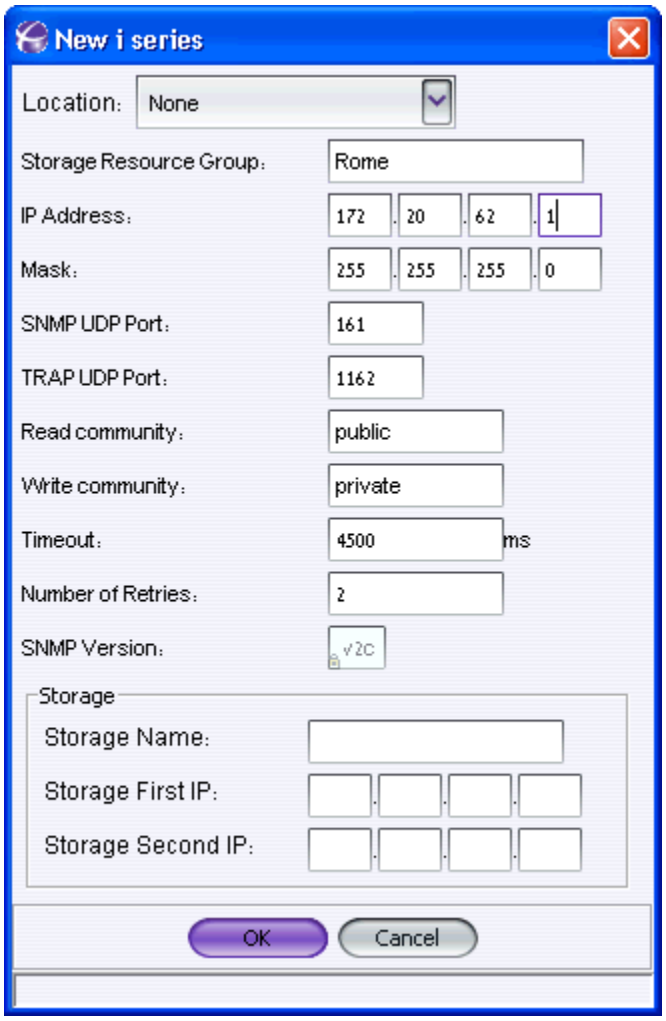



*Figure 3-7. New i series*

*Table 3-1. i series Management Parameters*

| Parameter | Definition |
|---|---|
| Location | Location in the navigation tree |
| Storage Resource Group | i series Name |
| IP Address | IP address of the management interface configured on i series during initial setup. |
| Mask | IP mask for the management interface |
| SNMP UDP Port | UDP port on which SNMP manager-agent communications run |
| TRAP UDP Port | UDP port on which the SNMP agent will issue traps |
| Read Community | Defined group granted read access to data |
| Write Community | Defined group granted write access to data |
| Timeout | Time in milliseconds before an SNMP session is considered closed. |
| Number of Retries | Number of times to try to re-establish an active SNMP session |
| SNMP Version | SNMP protocol version being used to establish i series manager communications with the specified i series |
| Storage Name | Storage Name |
| Storage First IP | IP address of first storage |
| Storage Second IP | IP address of second storage |

The new i series appears in the Navigation pane and is represented by two entities: a "**virtual entity**" and a "**physical entity**". The menu options differ for the two different types of entities. The virtual entity is referred to as "cluster level".

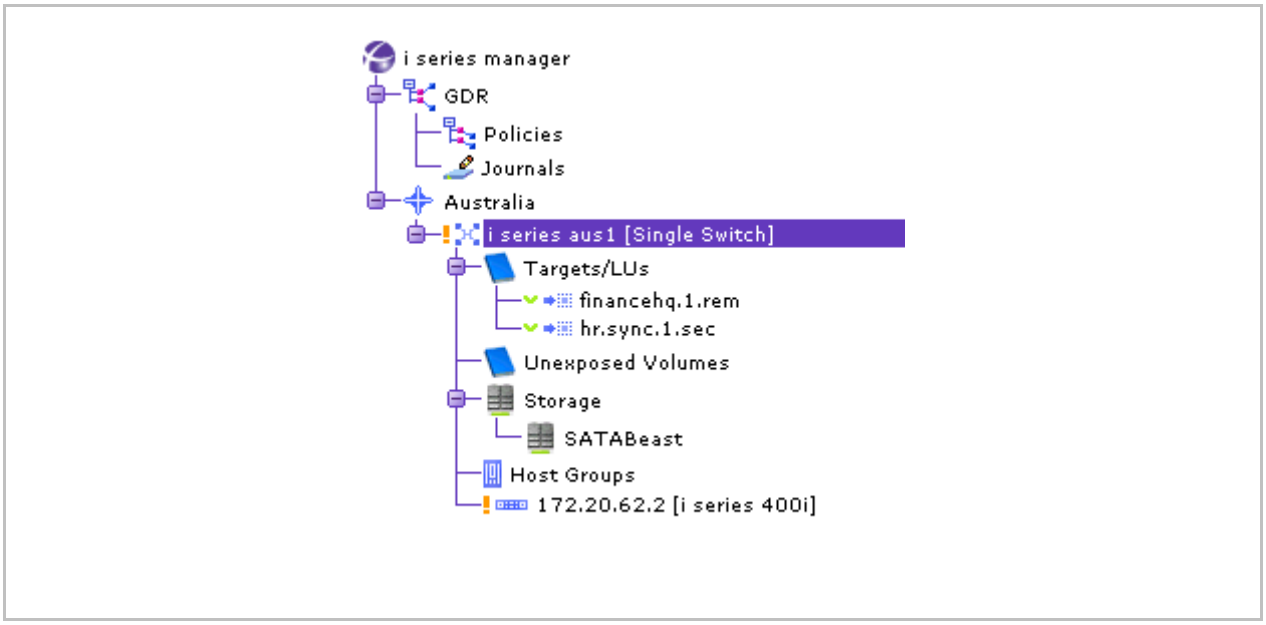



*Figure 3-8. i series Entity (Cluster Level)*

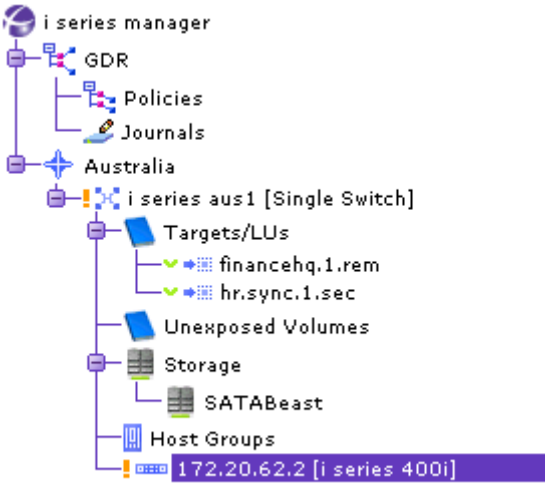



*Figure 3-9. i series Physical Entity*

## Setting i series Properties

You can change i series properties via the different tabs in the Properties Window (Figure 3-12).

***To display i series properties:***

1. From the Quick Launch:
   select **Configure > Configure Network.**

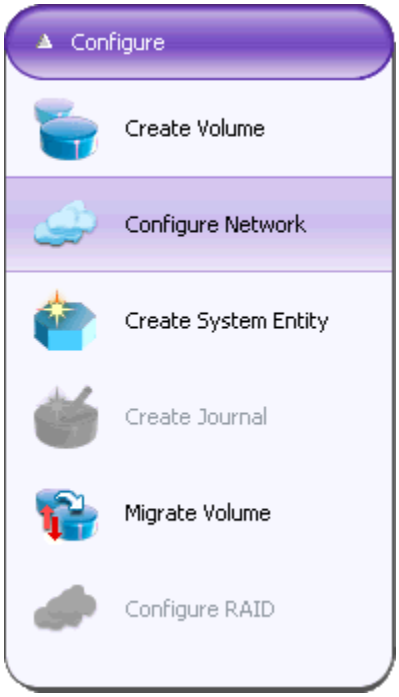



*Figure 3-10. Properties (i series Menu)*

The i series Properties dialog box opens.

Select the i series from the drop down list box at the top.

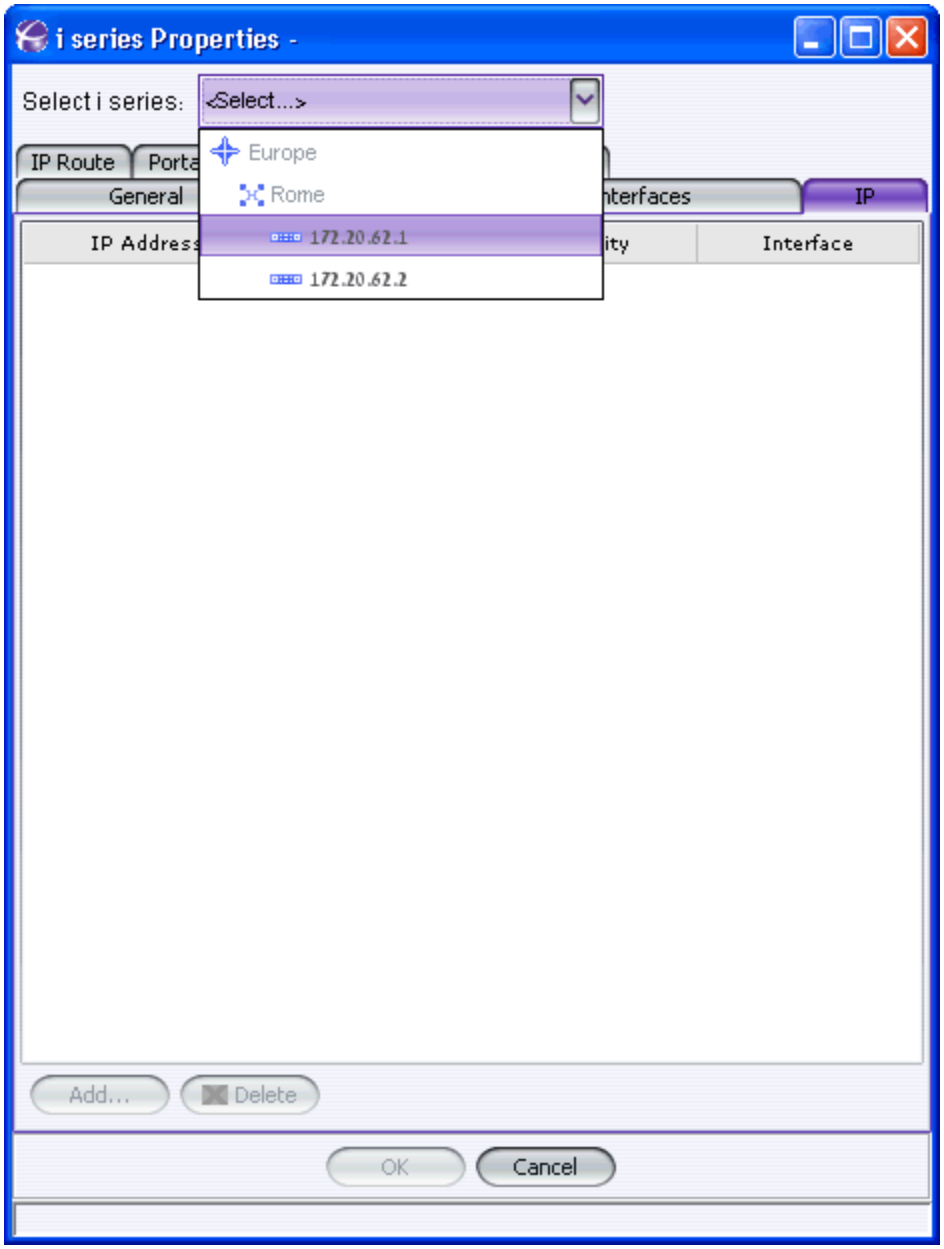



*Figure 3-11. Select (i series Menu)*

The i series Properties dialog box opens displaying different tabs.

Toggle between these tabs to configure the different i series properties.

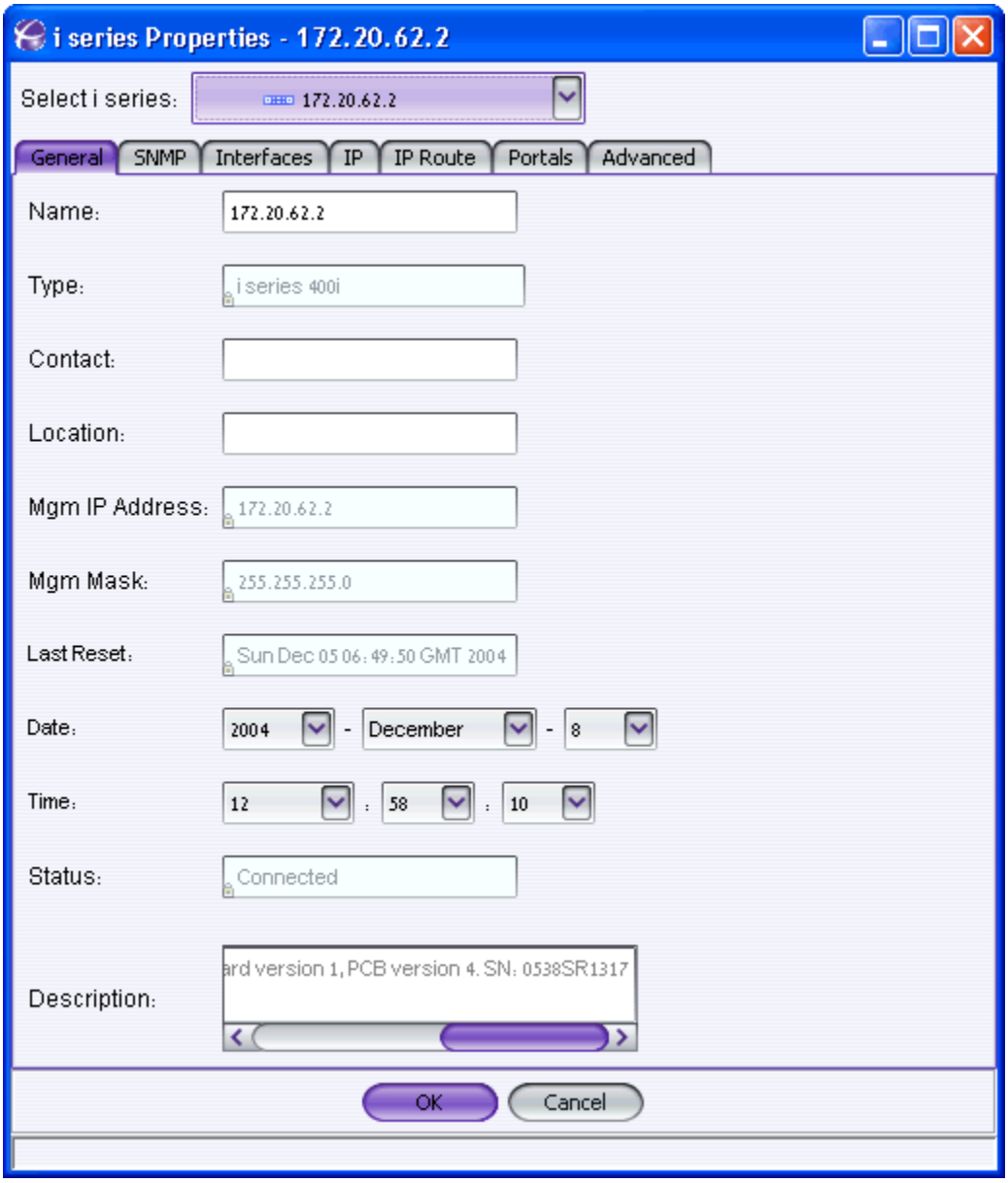



*Figure 3-12. i series Properties*

*Table 3-2. General Tab*

| Parameter | Definition |
|---|---|
| Name | Name of the i series |
| Contact | Contact person for technical support |
| Location | Location of the contact person |
| Mgmt IP Address | IP address of the i series management interface |
| Mgmt Mask | IP mask for the management interface |
| Last Reset | Date and time since the last i series reset |
| Date | Local date |
| Time | Local time |
| Status | i series connection status |
| Description | Description of i series hardware and software |

## Date and Time

You can set the local date and time on a i series.

> **Note:**
> *Alarms are time-stamped according to the computer clock that is running the i series manager server.*

***To set i series date and time:***

1. From the i series Properties Window (Figure 3-12), select the **Properties** tab.

   The i series **Properties** dialog box opens.

Select the year, month and day for the i series (Figure 3-13).

Select the hour, minutes and seconds.

Select AM or PM. Select AM for morning, PM for evening (12:00 AM=midnight, 12:00 PM=noon).

Click **OK**.

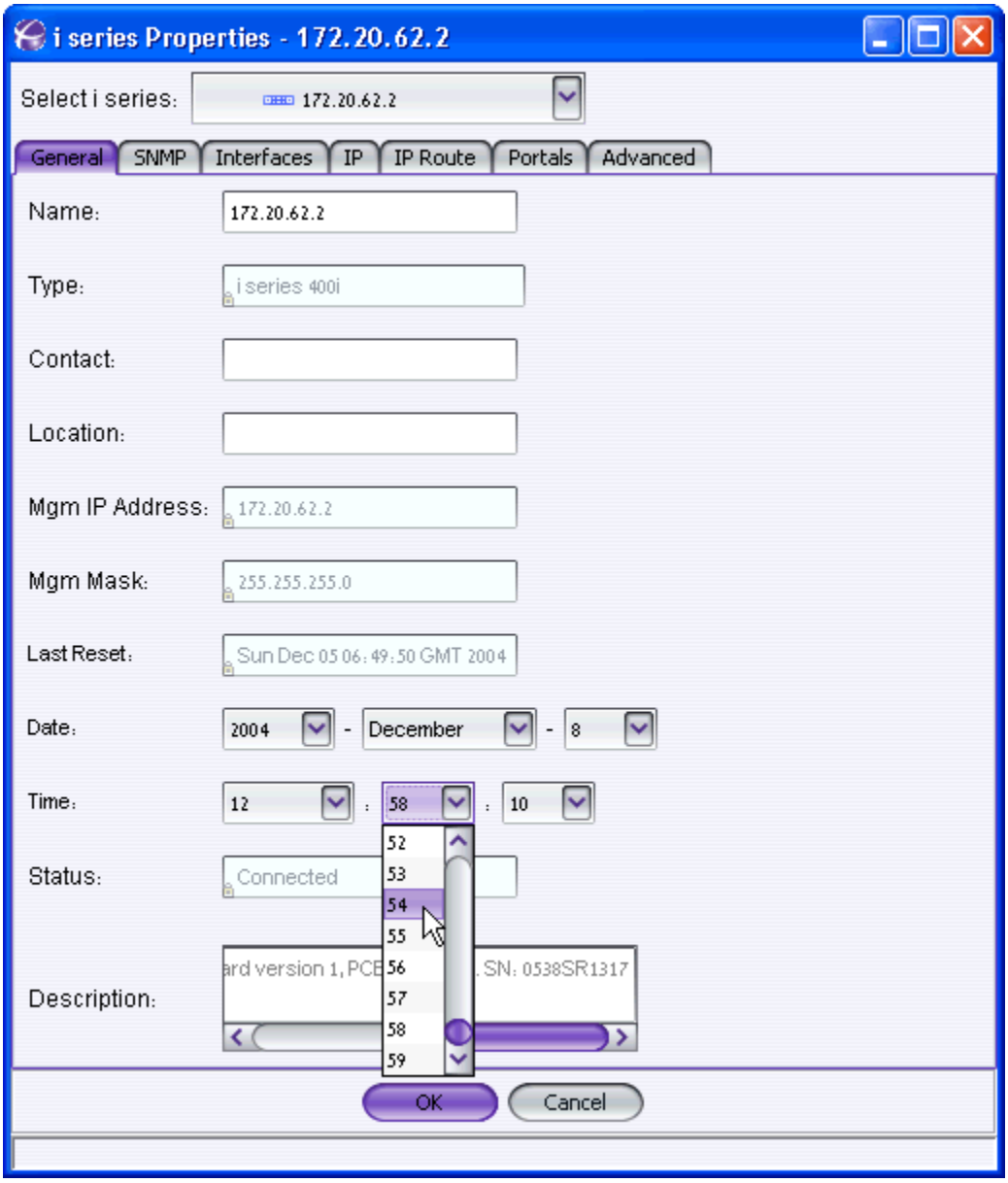



*Figure 3-13. Setting the i series Date*

## *IP Address*

To enable a host to communicate with the i series, an IP address must be assigned to the port. After adding an IP address, configure an iSCSI portal on the IP address (see Portals).

- Each network port can have multiple IP addresses assigned to it.
- i series 2000 has two 1Gb Ethernet network ports. All other i seriess have three 1 Gb Ethernet network ports.

> **Note:**
> *If you are adding a network port IP address in a cluster, assign the IP address as active on one i series and inactive on the second i series. In the event of a i series failover, the second i series will activate its inactive IP addresses and begin exposing the IP address' target LUNs.*

### *To add network IP addresses:*

1. From the i series Properties Window (Figure 3-12), select the **IP** tab.

Click **Add**.

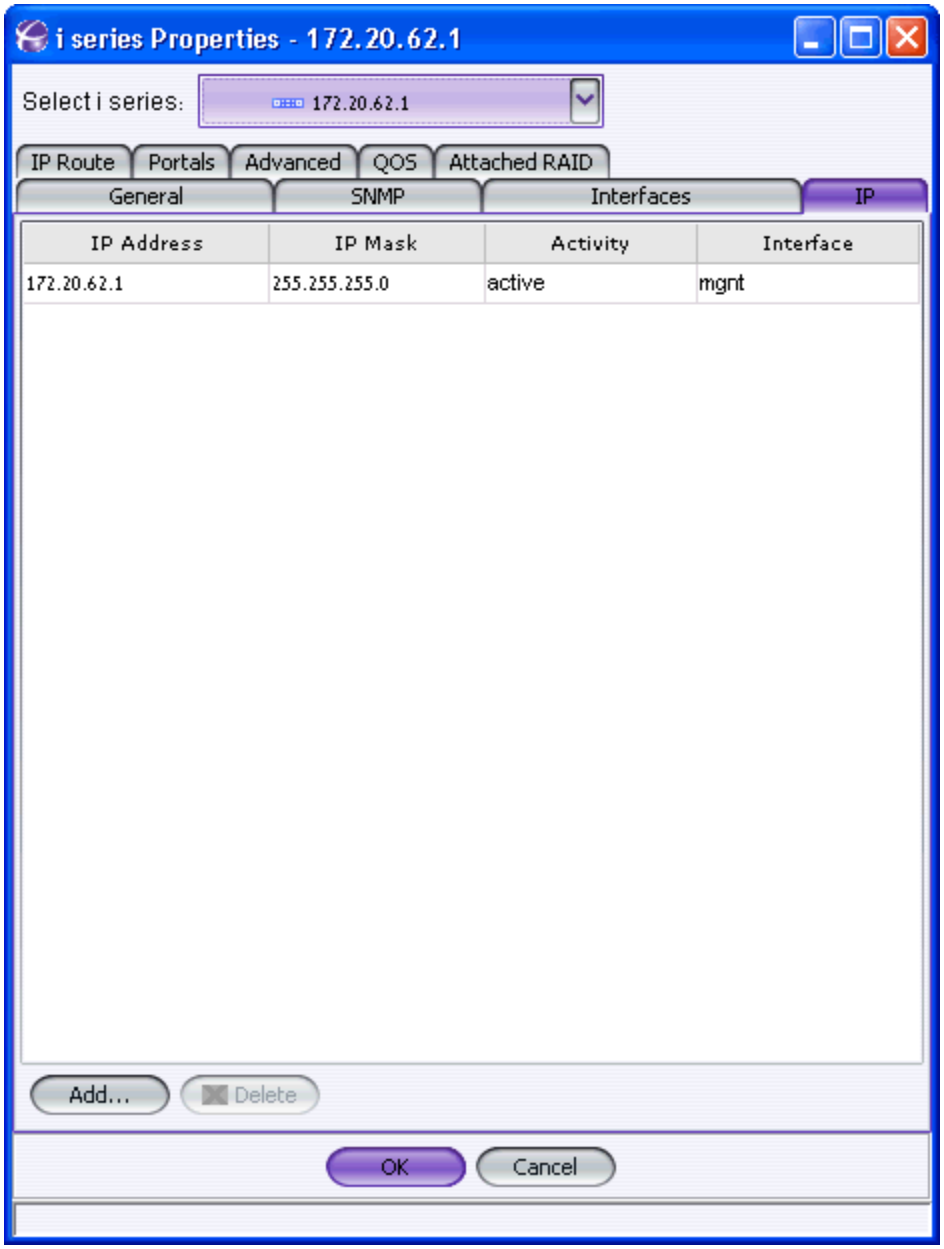



*Figure 3-14. Add Network Port IP Parameters*

The Add IP dialog box opens (Figure 3-15).

1. Enter the **IP Address**.

   Enter the **IP Mask**.

   Configure the **Activity** as active or inactive.

   Configure the **Interface**.

Add this IP to the neighbor in the cluster by checking the checkbox.

Click **OK**.

The new network port IP address is listed in the IP tab.

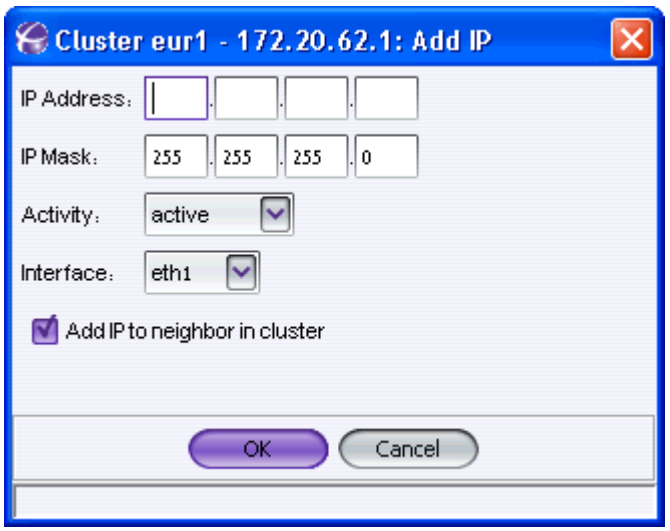



*Figure 3-15. Add Network Port IP Parameters*

*Table 3-3. Network Port Parameters*

| Parameter | Description |
|---|---|
| IP Address | IP address of interface |
| IP Mask | IP mask of interface |
| Activity | IP address state |
| Interface | Interface name |

**Cluster Note:**

- IP addresses configured as active on the first i series will be configured as inactive on the second.
- In the event of failover, the inactivate IP addresses are activated on the functioning i series to take over target LUN exposure. The IP address's activity will be shown as switched.

## Portals

A portal is the combination of an interface IP address and a TCP port. You must assign iSCSI portals to enable communications between an iSCSI initiator and iSCSI target.

***To add an iSCSI portal:***

1. From the i series Properties Window (Figure 3-12), select the **Portals** tab.

Click **Add**.

The Add Portal dialog box opens.

Select the IP address from the drop-down menu of existing IP address and enter the port number. Click **OK**.

> **Cluster Note:**
> *When you add an iSCSI portal to a i series in a cluster, you need to add the portal to the second i series as well. In the event of a i series failover, this allows the second i series to begin exposing the failed i series's target LUNs through the portal.*

2. When working in a cluster, click the **Add portal to neighbor in cluster** checkbox.
3. Click **OK**.

   The iSCSI portal is added to the i series Properties tab.
4. Click **OK**.

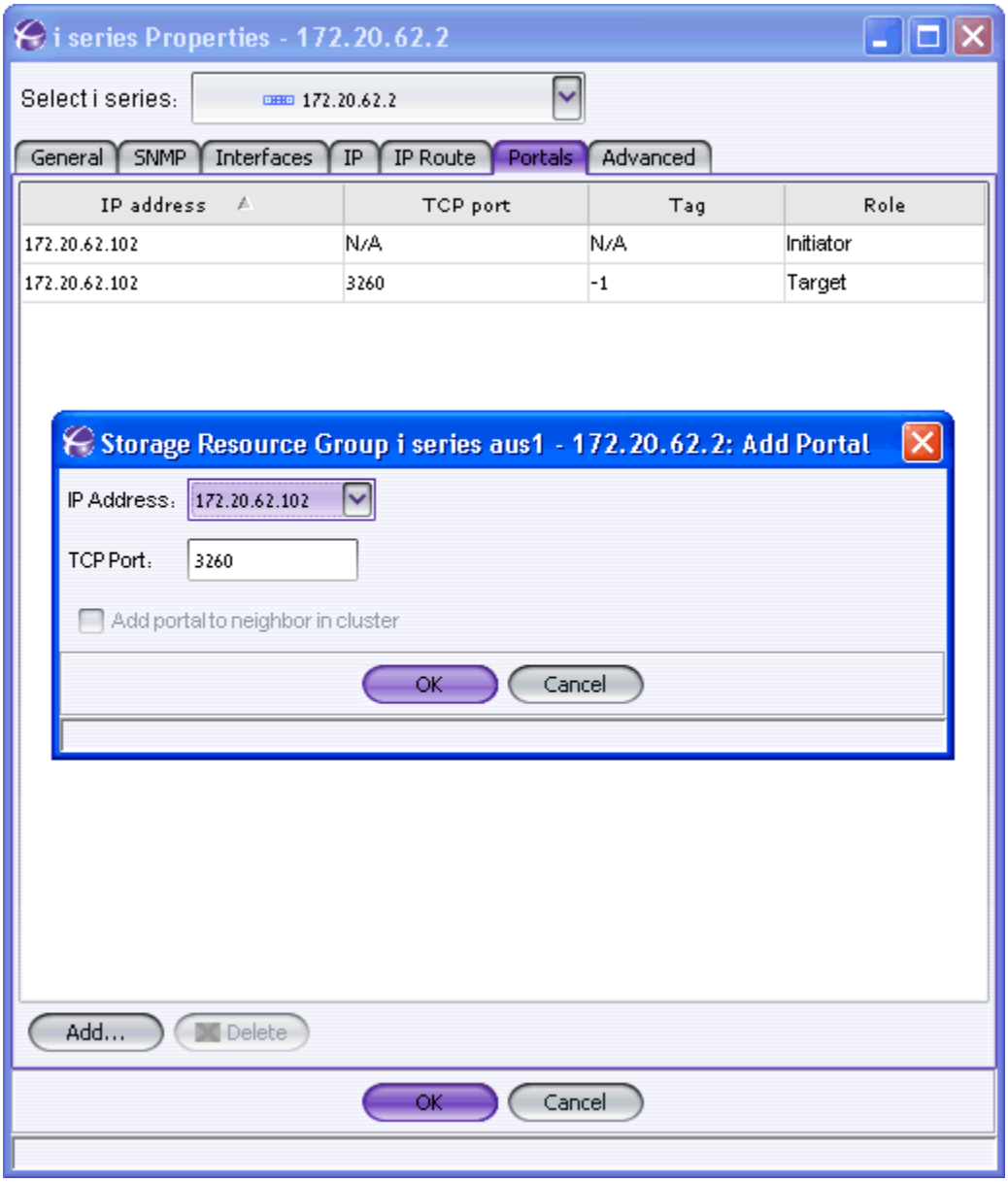



*Figure 3-16. Portal Values*

*Table 3-4. Portal Parameters*

| Parameter | Description |
|---|---|
| IP Address | User-assigned IP address of an interface |
| Port | TCP port through which the iSCSI protocol passes (usually 3260) |

***To delete an iSCSI portal:***

1. In the Navigation pane, right click on the i series and select **Properties.**

   The i series **Properties** dialog box opens (Figure 3-12).

Toggle to the **Portals** tab.

Select desired portal and click **Delete**.

A dialog box appears asking if you want to delete selected portals. Click **Yes** to confirm delete.

## *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.

- Each i series can have only one IP route designated to a specific external network, even if there is more than one possible physical path to that network.

> **Cluster Note:**
> *In a cluster, an IP route must be added to both i serieses. In the event of a i series failover, the second i series will be able to establish communications through the route and expose the failed i series's target LUNs.*

***To add an IP route:***

1. From the i series Properties Window (Figure 3-12), select the **IP Route** tab.

Click **Add**.

The Add IP Route dialog box opens.

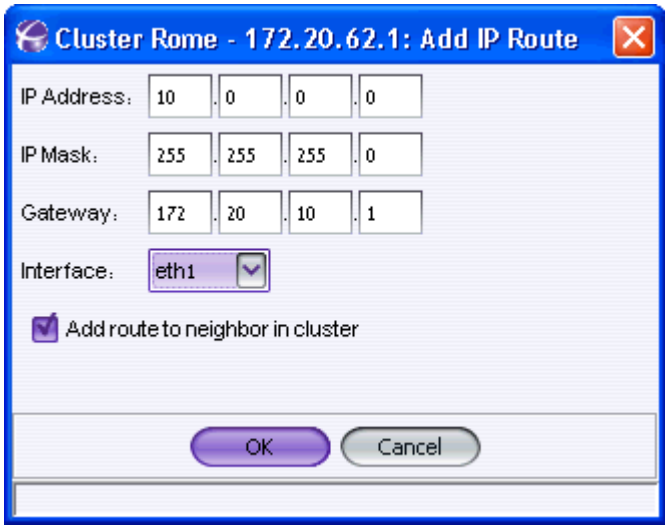



*Figure 3-17. Add IP Route Dialog Box*

Enter the routing values (see Table 3-5).

You can configure a default gateway for each port, including the management port, for routing all traffic not otherwise specified in the i series routing table by using 0.0.0.0 for both the IP address and IP Mask.

**Cluster Note:**

- If you are working in a cluster, select *'Add route to neighbor in cluster'* to add the route to the second i series.
- Don't select the checkbox if you want to exclude the route from the second i series in the cluster.

Click **OK**. The **Add IP Route** dialog box closes. The new IP route is listed in the **IP Route** tab (Figure 3-18).

*Table 3-5. IP Routing Parameters*

| Parameter | Description |
|---|---|
| Dest IP Address | IP address of destination network<br>Use IP address 0.0.0.0 to create a default gateway |
| Dest IP Mask | IP mask of destination network<br>Use IP mask 0.0.0.0 to create a default gateway |
| Gateway | IP address of gateway router |
| Interface | Network interface to open route through |

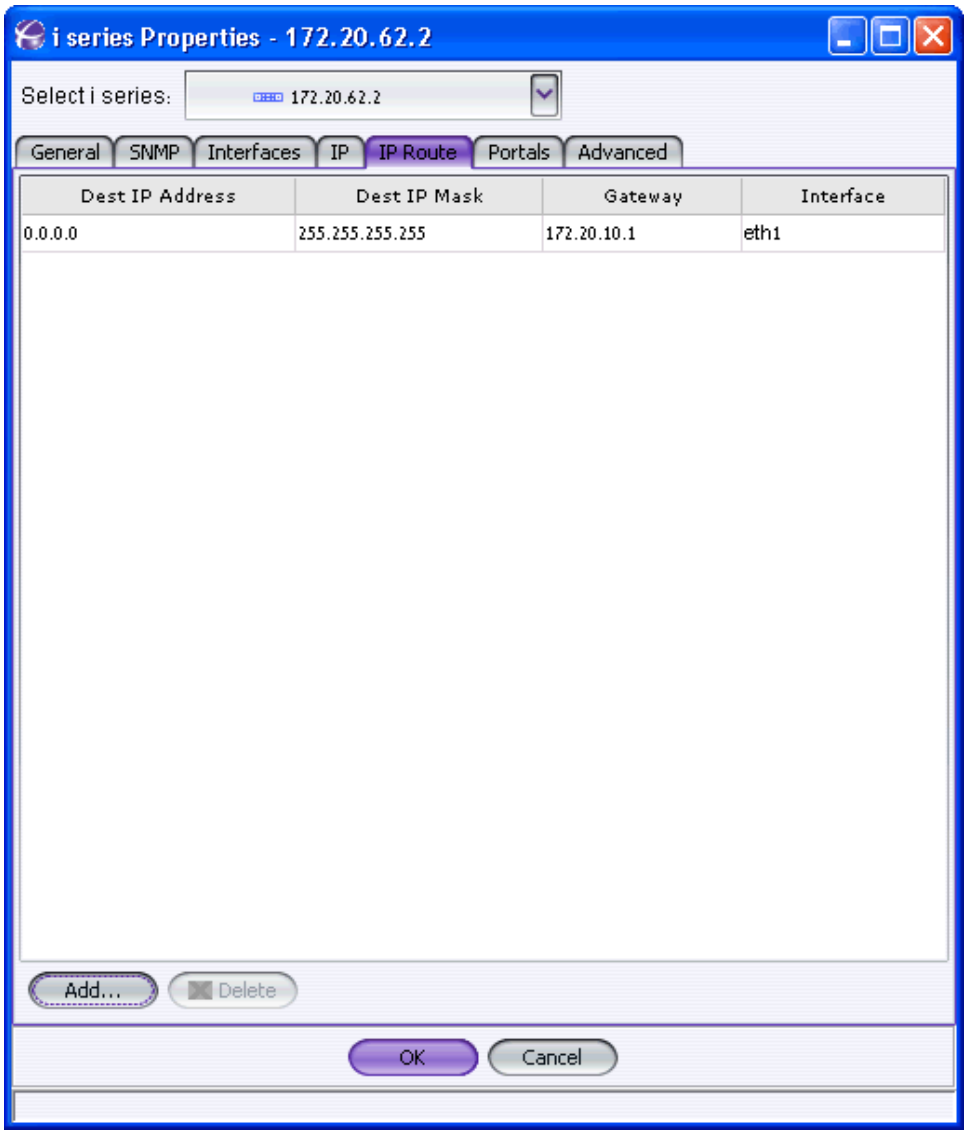



*Figure 3-18. New IP Route Dialog Box*

## Creating a New Storage Resource Group (Cluster)

i series manager enables you to easily configure network port IP addresses, iSCSI portals and IP routes simultaneously on both i serieses in the cluster.

***To add a new cluster from two new i seriess:***

1. From the *Quick Launch*:
   **Configure > Create System Entity > Storage Resource Group [Cluster]…**

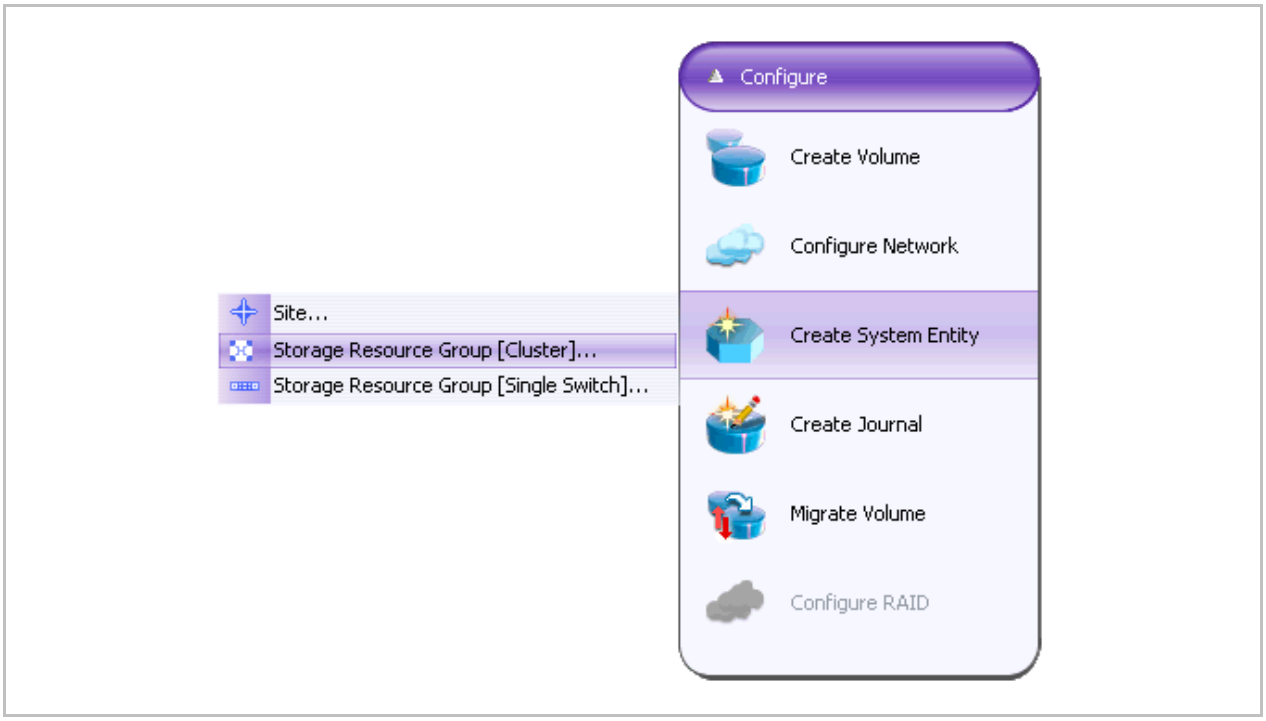



*Figure 3-19. New Storage Resource Group (Cluster)*

The New Cluster dialog box opens.

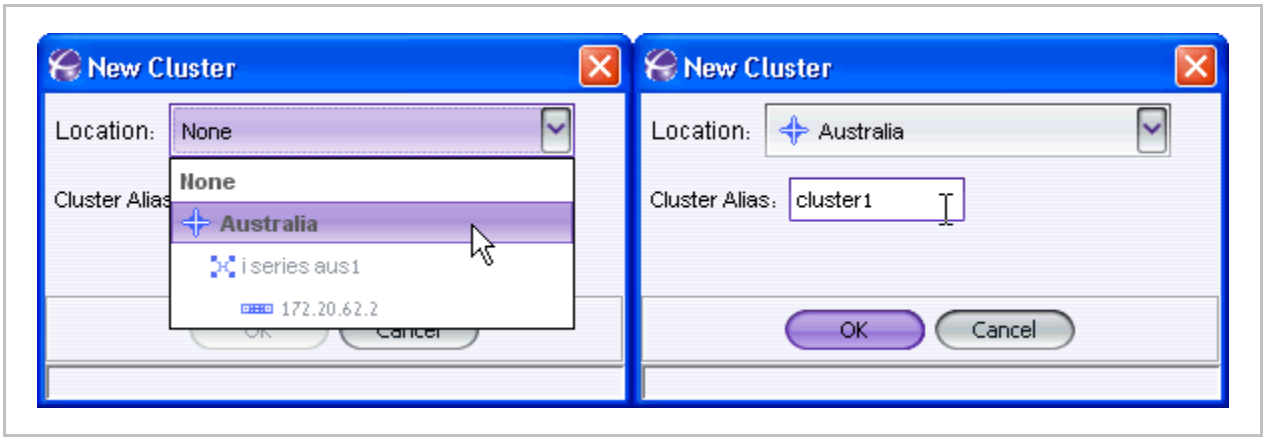



*Figure 3-20. New Cluster Dialog Box*

Select location to create the cluster from the drop down list box.

Enter the cluster alias.

Click **OK**.

Add i serieses to the cluster (refer to Adding a New ).

## Creating a Cluster by Adding New i series to Stand-Alone i series

***To make a cluster by adding a new i series to a stand alone i series:***

1. In the Navigation pane, right click on the stand alone i series (at cluster level), and select **New** > i series**...**

> **Cluster Note:**
> *Both i serieses in a cluster must have different aliases. If you add a second i series with the same alias as the first i series, no cluster will be created and no failover will be possible.*
> *The i series will be listed in the i series manager navigation pane with an orange exclamation mark (major alarm) and the Alarms window will display the alarm i serieses are not neighbors. For i series manager to create a cluster, you need to rename the second i series via the i series Properties.*

Synchronize the new i series by following the steps outlined in Synchronizing a Cluster.

Define the i series parameters for the second i series (V2) as follows:

- IP of V1 as passive
- Portals of V1
- Routing of V1

Manually configure the Credentials (Passwords, CHAP/SRP) from the Identities level (refer to *Assigning Identity Credentials*).

### *Synchronizing a Cluster*

If volumes or targets are created on one i series operating alone, when another i series is added, its database must be synchronized to the first i series's database. This can happen in three situations:

1. A new i series is added to a configured and functioning i series to form a cluster.

An offline i series in a cluster comes back online.

CLI is used to make an isolated configuration change in one i series.

When an element is not synchronized, a yellow exclamation mark may appear to the left of it (instead of a green check mark ) meaning that the alarm *Object not redundant* is opened (see Viewing Alarm Properties in Chapter 6).

***To synchronize a cluster:***

1. Select the cluster to synchronize.

Right click and select **Cluster Sync** from the open menu (Figure 3-21).

Synchronization is instantaneous. During synchronization, a yellow exclamation mark at the selected element's level (and below) are converted to green check marks . The green check marks indicate that synchronization has completed.

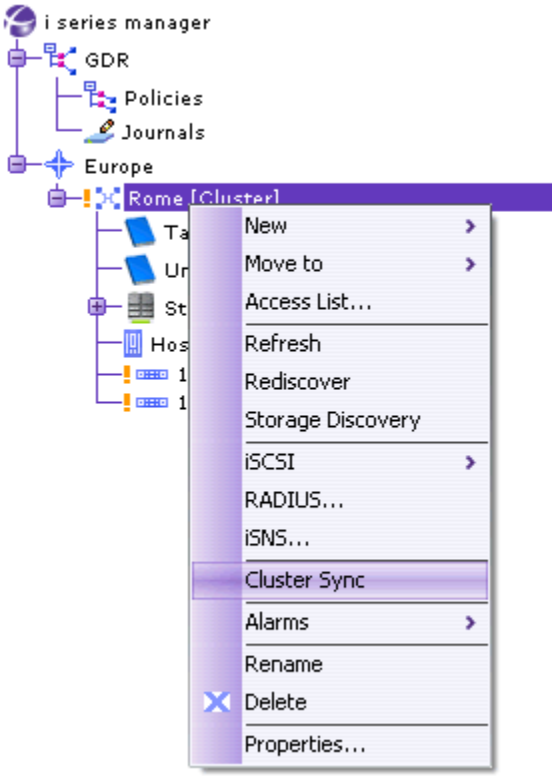



*Figure 3-21. Synchronize Selected*

## Setting Cluster Properties

The Cluster Properties dialog box (Figure 3-23) allows you to configure general

## *Keep Alive, Suspicious and Faulty Intervals*

The i series sends out *keep alive* signals to the other i series (its neighbor) in a cluster. Suspicious and Faulty Intervals define the time interval for the i series to not get Keep-alive signals from its neighbor and subsequently change its neighbors' state to suspicious and faulty. The faulty state triggers a takeover procedure.

***To configure keep alive, suspicious and faulty intervals:***

1. In the Navigation pane, right click the cluster and select **Properties...**

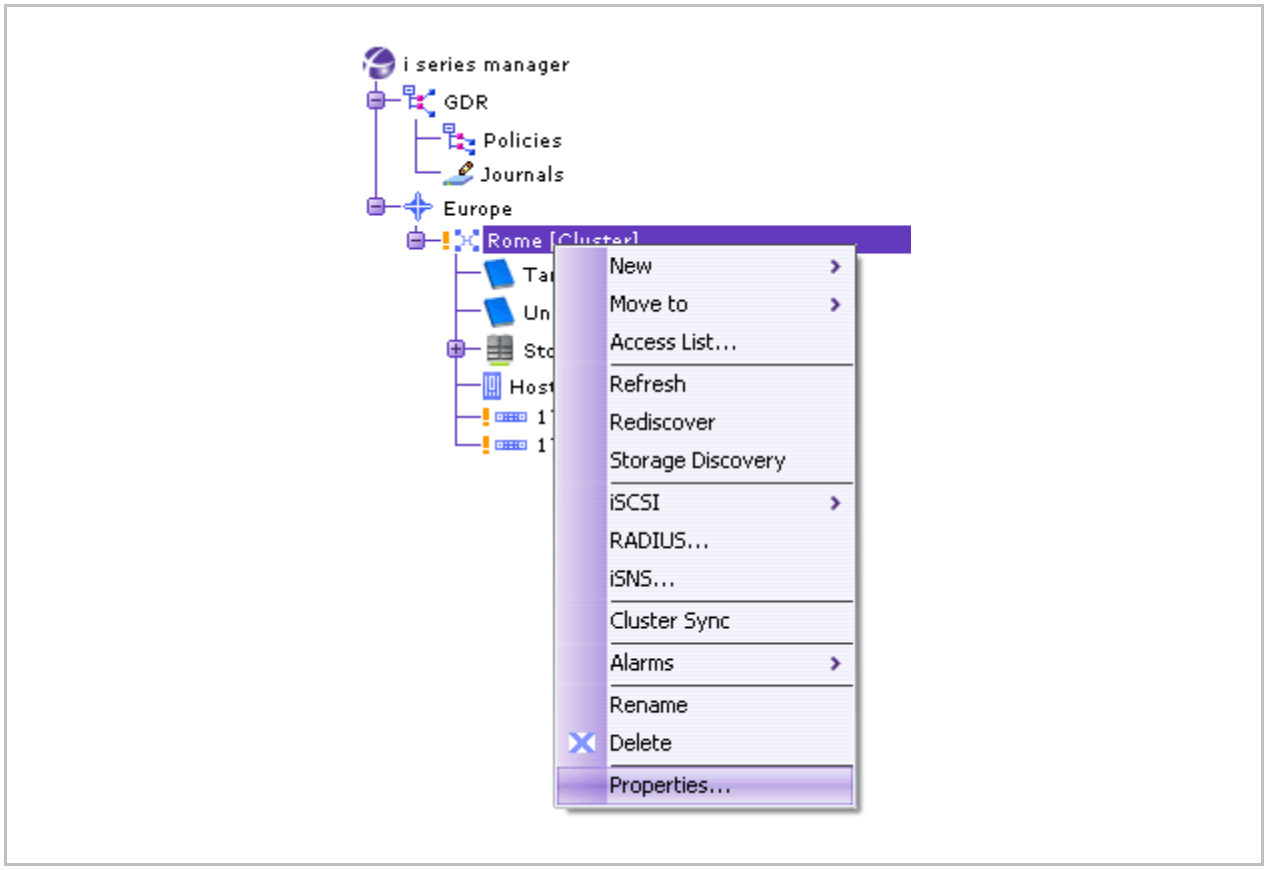



*Figure 3-22. Properties Selected*

Enter the desired intervals for Keep-alive Intervals, Suspicious Intervals, and Faulty Intervals.

Click **OK**.

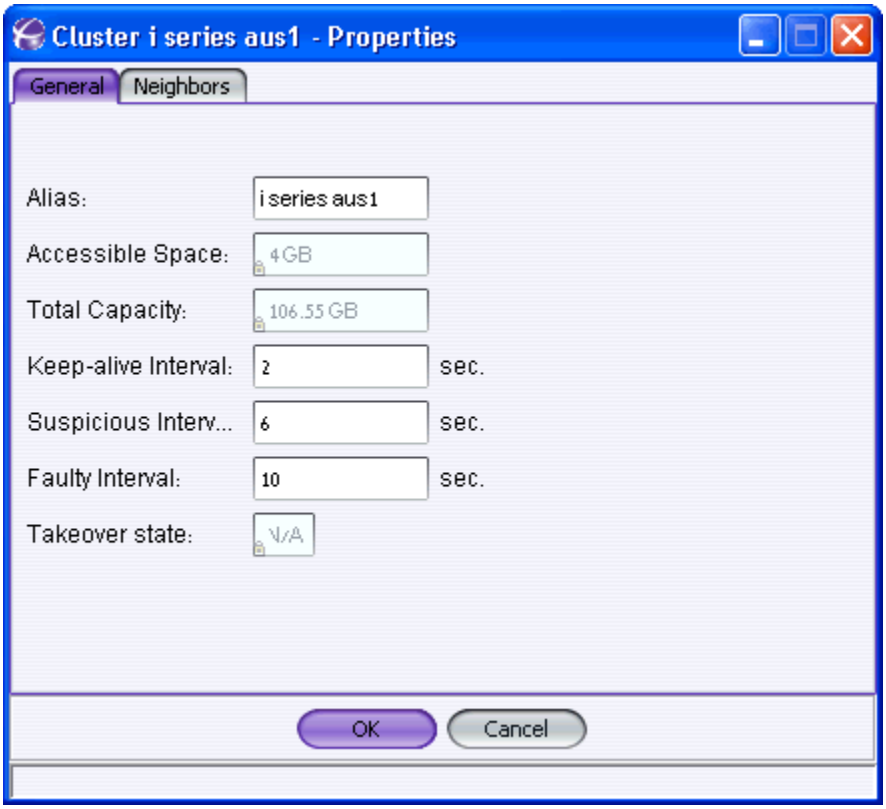



*Figure 3-23. Cluster Properties Dialog Box*

***To view neighbor properties for a cluster:***

1. In the Navigation pane, right click and select **Properties…**

   The **Cluster Properties** dialog box opens.

Click the Neighbors tab.

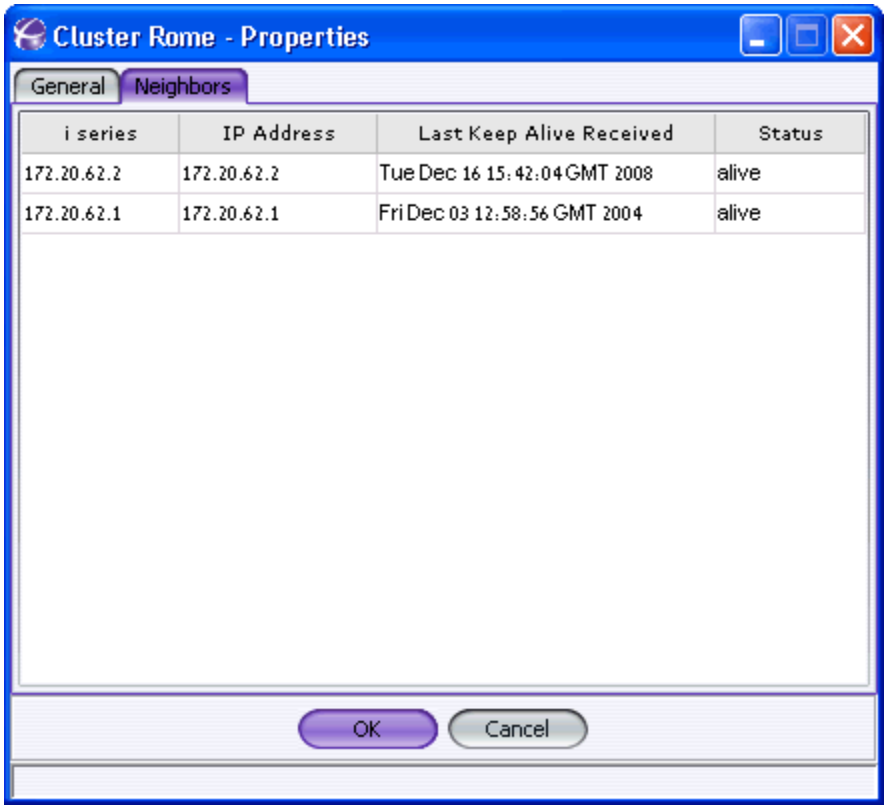



*Figure 3-24. Cluster Properties Dialog Box – Neighbors Tab*

## Breaking a Cluster

You can break a cluster by removing one of its neighbors (i series). A i series can be deleted from a cluster only after it is offline and i series manager recognizes it as disconnected.

**Cluster Note:**

- If you remove a i series from a cluster, all of its configurations will be automatically transferred to its neighbor. However, the activity of the IP addresses will be active and not switched.
- If the removed i series is re-connected, the IP addresses will not failback to the re-connected i series. The IP addresses and their exposed targets will be exposed on both i serieses.
- If the removed i series is re-connected, then duplicate IP addresses will exist.

### *To break a cluster:*

1. Disconnect (turn off) the i series from the system.

   The offline i series is marked with a red exclamation mark .

The remaining i series is marked with a blue exclamation mark to show that it has taken over exposing the offline i series's targets.

Right click on the offline i series and select **Delete**.

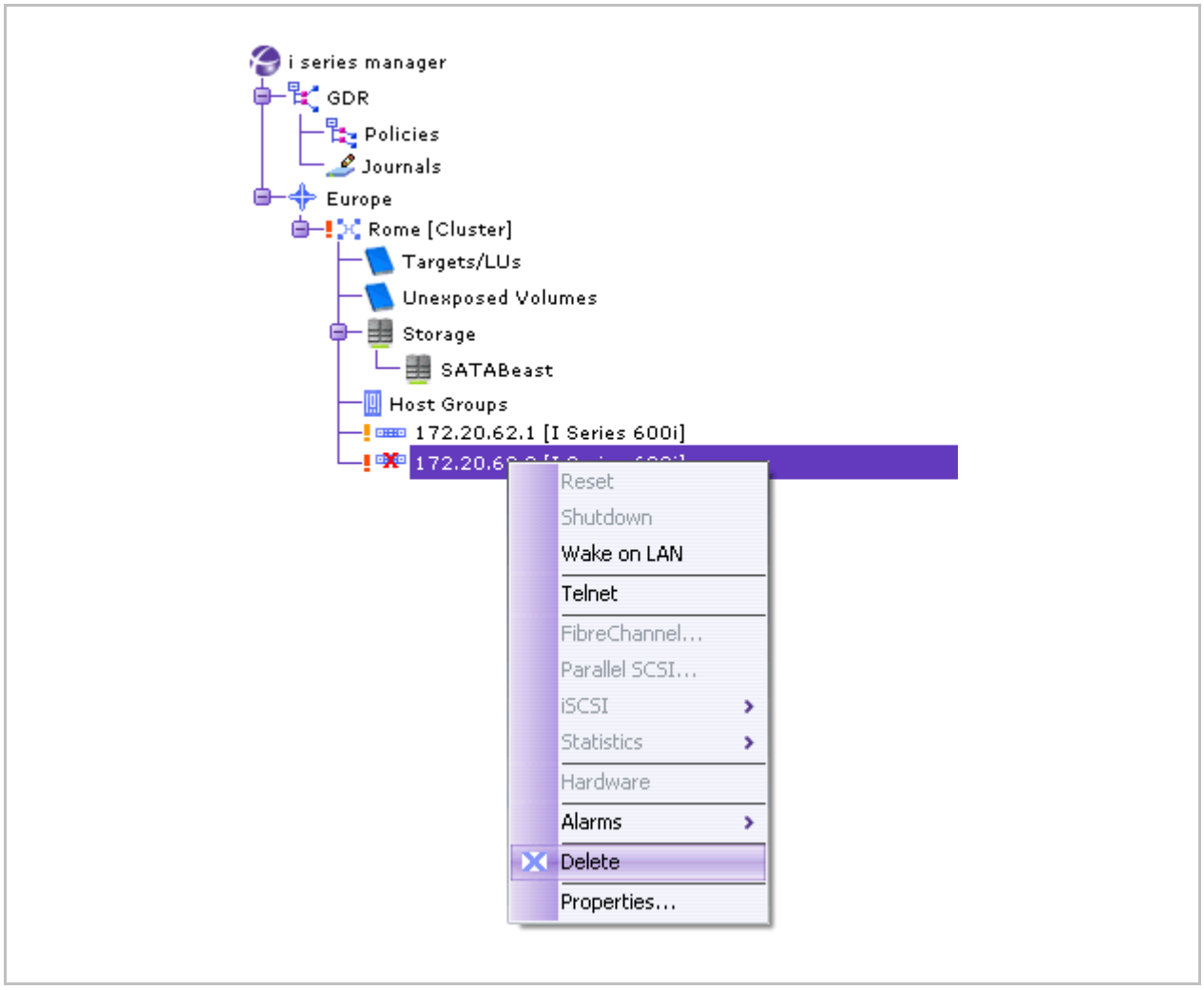



*Figure 3-25. Delete Offline i series*

A Dialog box opens asking if you want to delete the offline i series. Click **Yes.**

i series manager begins removing the offline i series from the i series manager database.

The **Navigation** pane displays the remaining i series in the cluster.

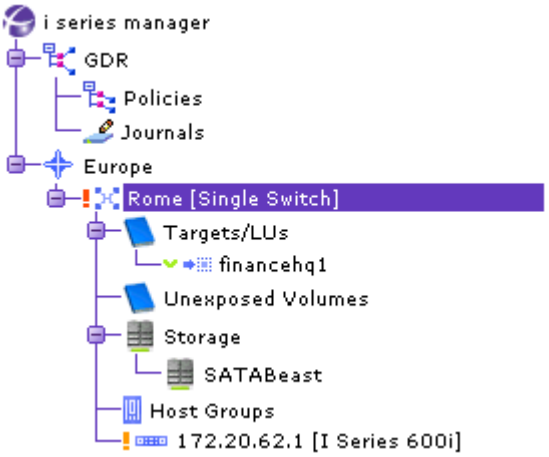



*Figure 3-26. Navigation Pane with Remaining i series*

## Additional i series Functionality

This section describes routine and optional i series configuration operations.

### *FC Storage Port Configuration*

The i series default configuration for FC connections is Auto NL_Port in a public loop. Each storage port connected to an FC device can be reconfigured to change the connection speed, port type and connection mode.

***To change FC/SCSI storage port parameters:***

1. In the Navigation pane, select the i series, right click and select **Fibre Channel...**

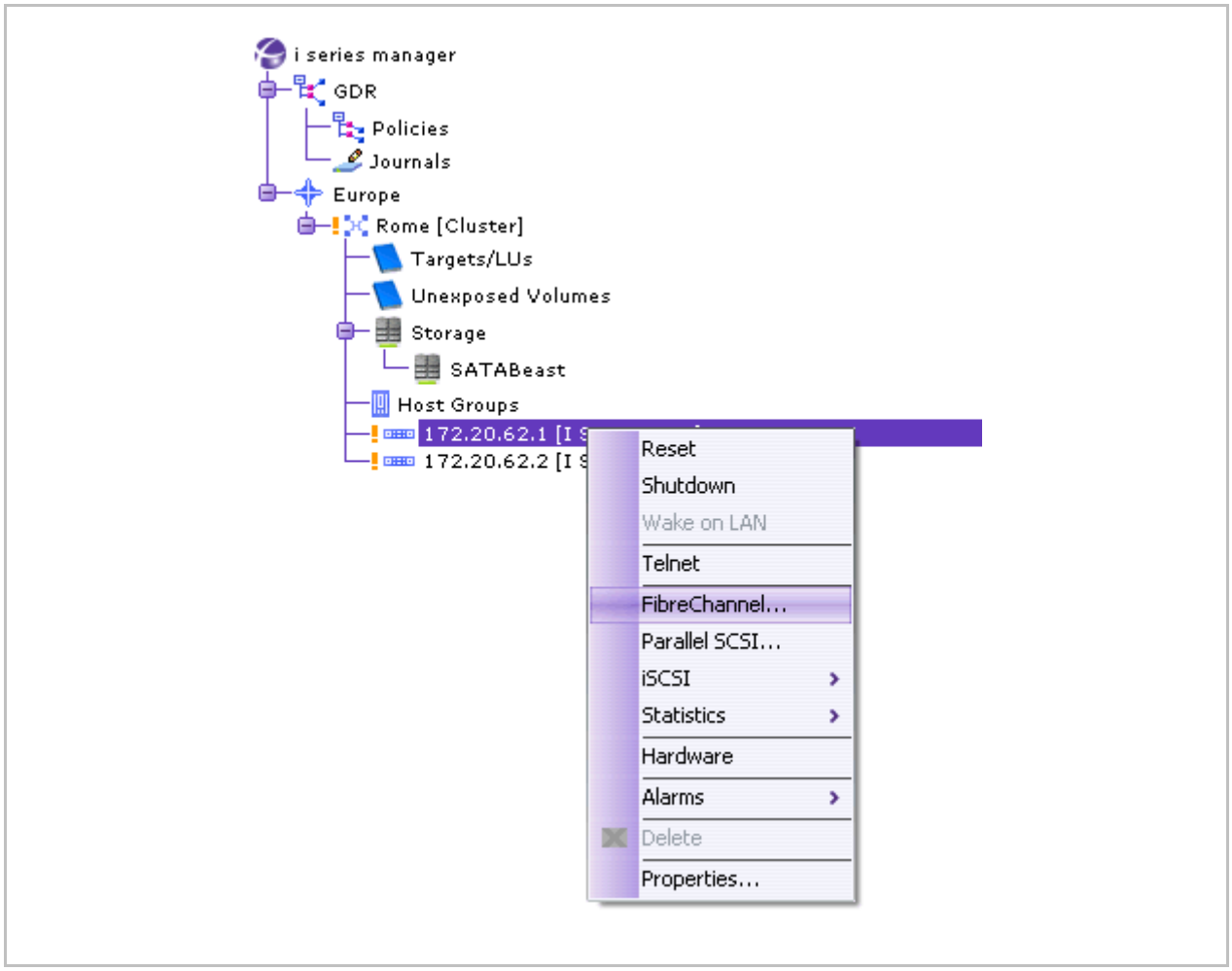



*Figure 3-27. i series Fibre Channel Option*

The Fibre Channel Parameters dialog box opens.

Toggle to the **Interfaces** tab.

Configure parameters for **Speed** and **Topology** by selecting them from the drop down menus.

Click **OK**.

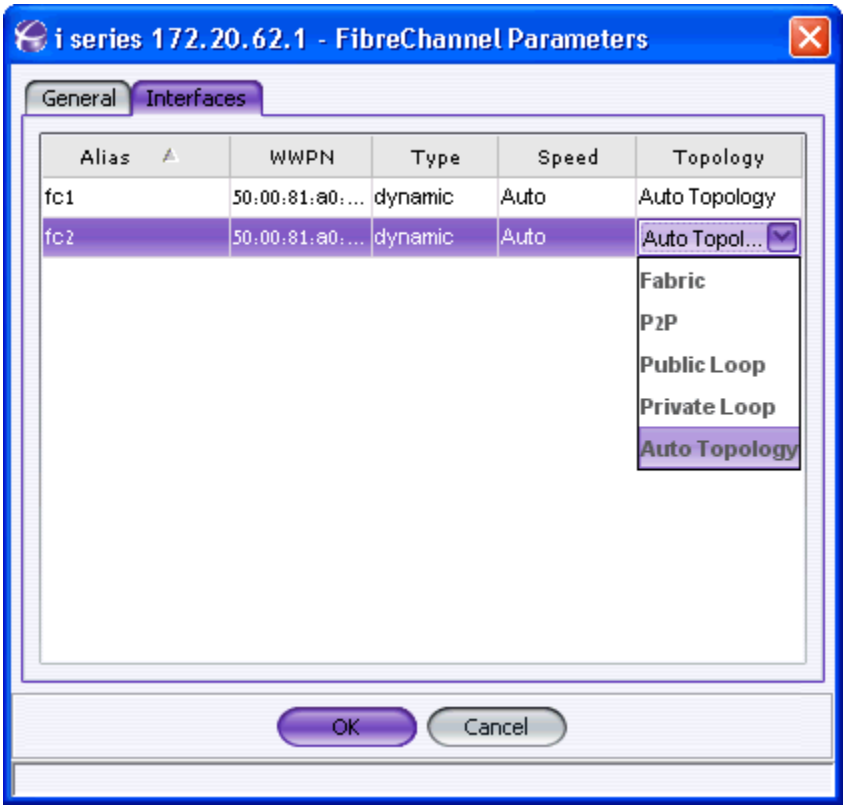



*Figure 3-28. Setting FC Port Speed*

*Shouldn't we explain what does it mean? What is P2P, Public Loop and so on?*

## Wake on LAN (V3XXX only)

Certain i series versions have advanced shutdown and wake up functionality. You can shutdown and wake up the i series directly from i series manager.

> **Note:**
> *In order to use this feature, the management port must be set to Mgnt and not Eth1.*

***To shutdown the i series:***

- In the Navigation pane, right click on the i series and select **Shutdown.**

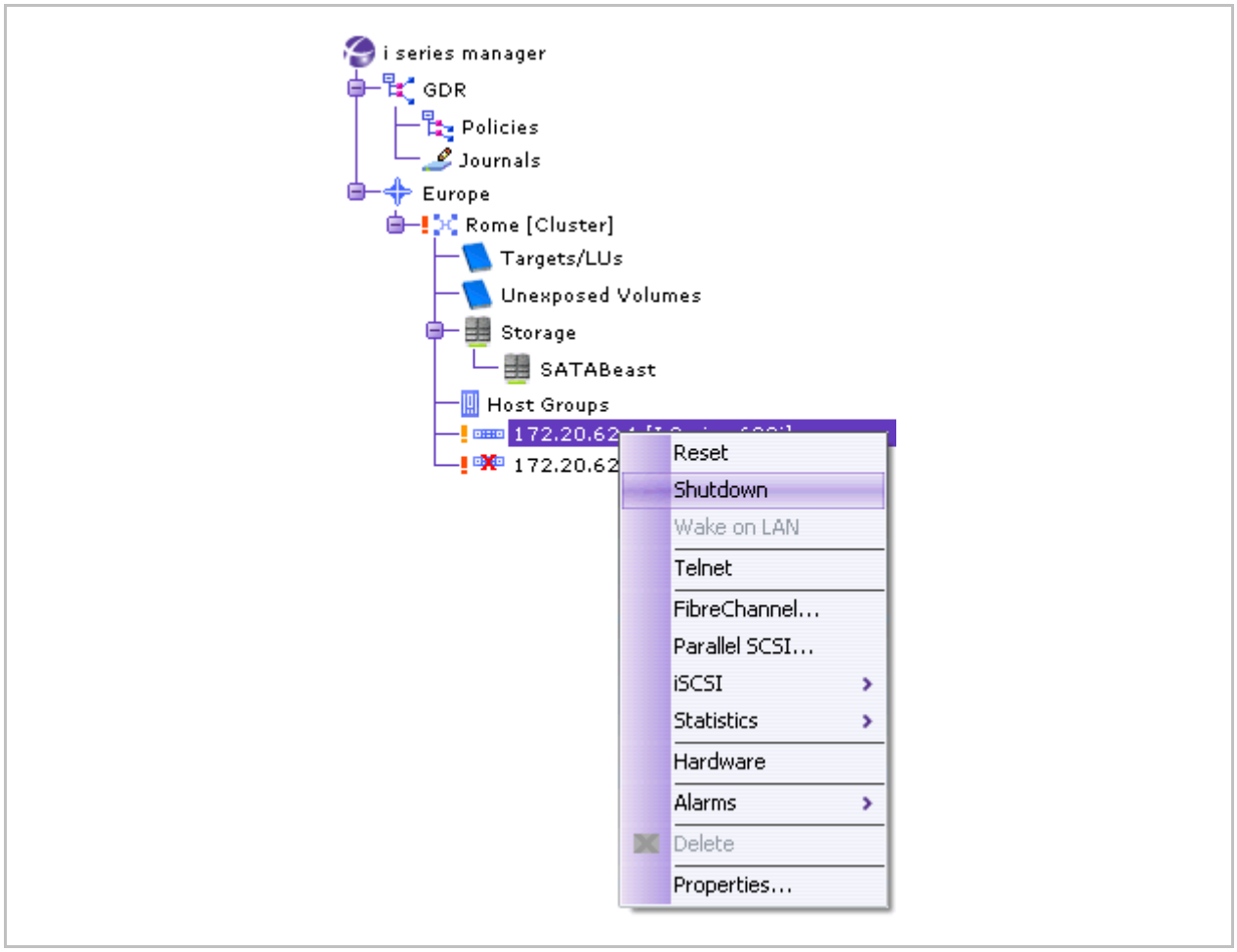



*Figure 3-29. Shutdown*

***To wake up the i series:***

- In the Navigation pane, right click on the i series and select **Wake on LAN.**

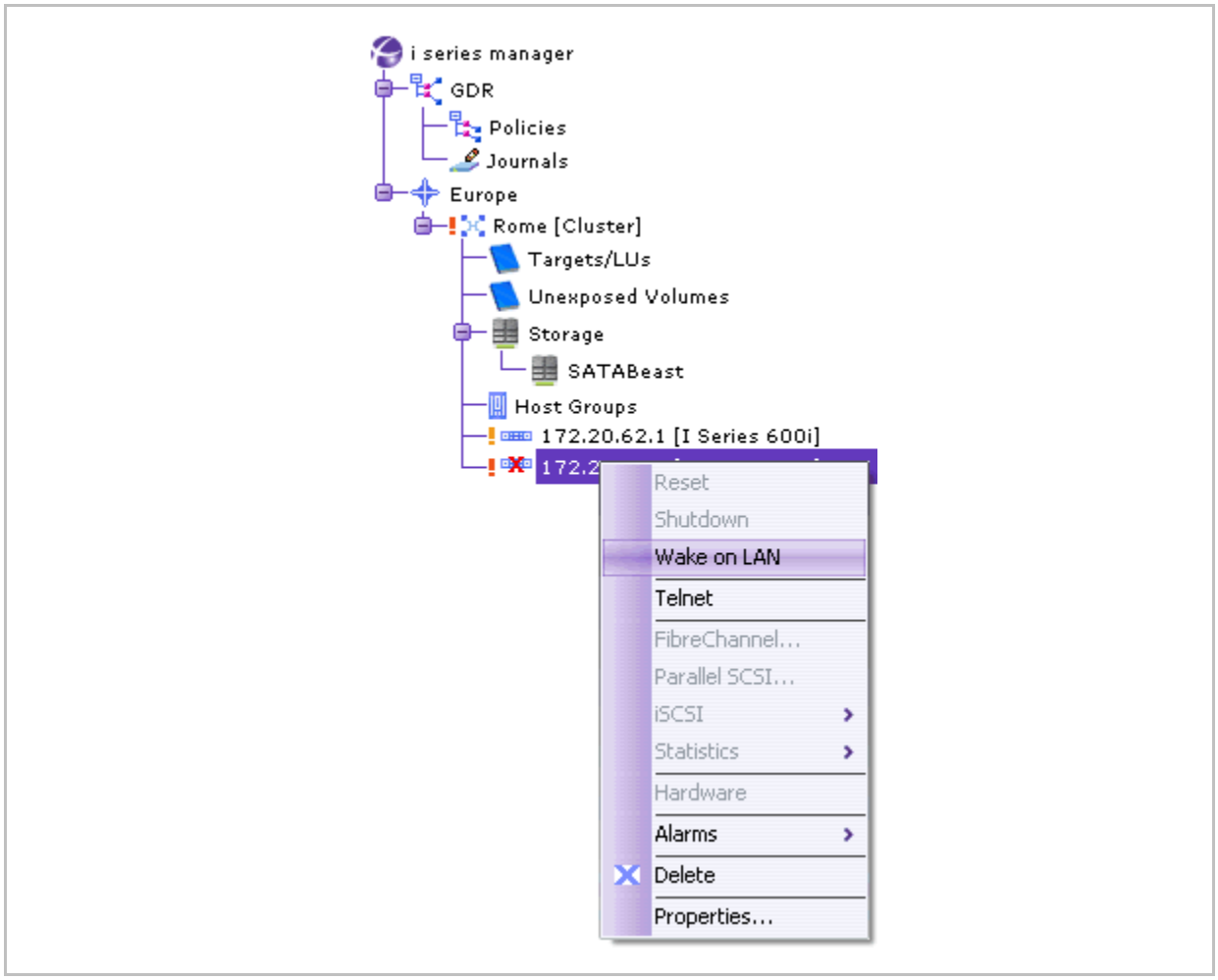



*Figure 3-30. Wake on LAN*

## SFP Properties

**Note:** *SFP parameters are available for the i series 34xx and 38xx.*

You can view SFP parameters for FC Interfaces.

### To view SFP parameters:

1. In the Navigation pane, right click on the i series and select **Properties…**

   The i series **Properties** dialog box opens (Figure 3-12).

2. Toggle to the Interfaces Tab.

3. Select the desired interface, right click and select **SFP** (Figure 3-31).

   The SFP Properties dialog box appears.

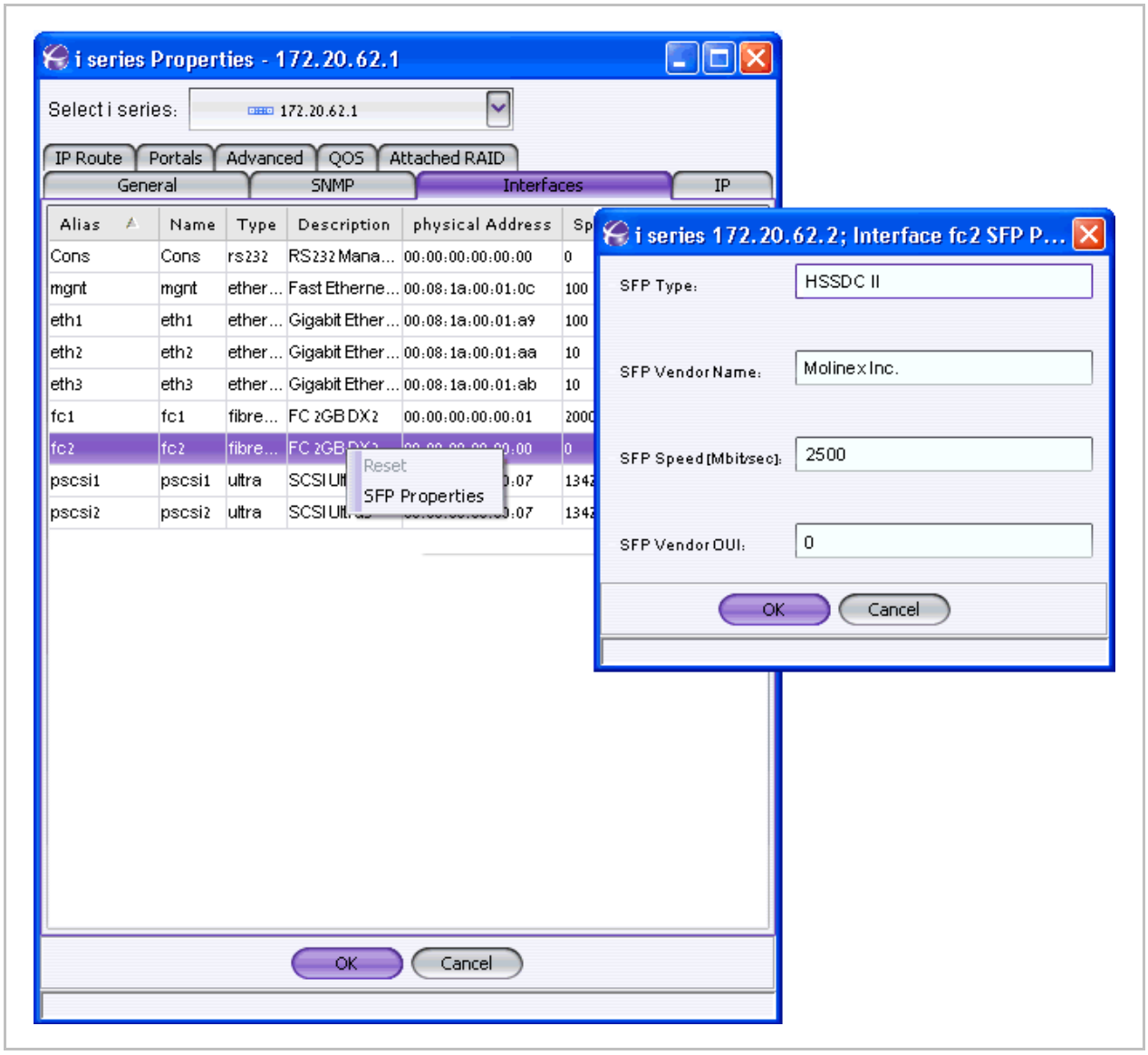



*Figure 3-31. SFP Properties*

## Discovery of iSCSI Storage Devices

An iSCSI device can have many portals. Each portal can have remote targets associated with it. In order for the i series to recognize a portal's remote targets, you must define the IP Address of the iSCSI portal. Once defined, the i series will automatically receive the list of remote targets attached to the portal.

There are two ways to discover remote iSCSI targets:

1. Discover all remote targets attached to an iSCSI device.

Discover a specific remote target.

***To discover remote targets attached to an iSCSI device:***

1. In the Navigation pane, right click on the Cluster and select **iSCSI > Remote Portals**.

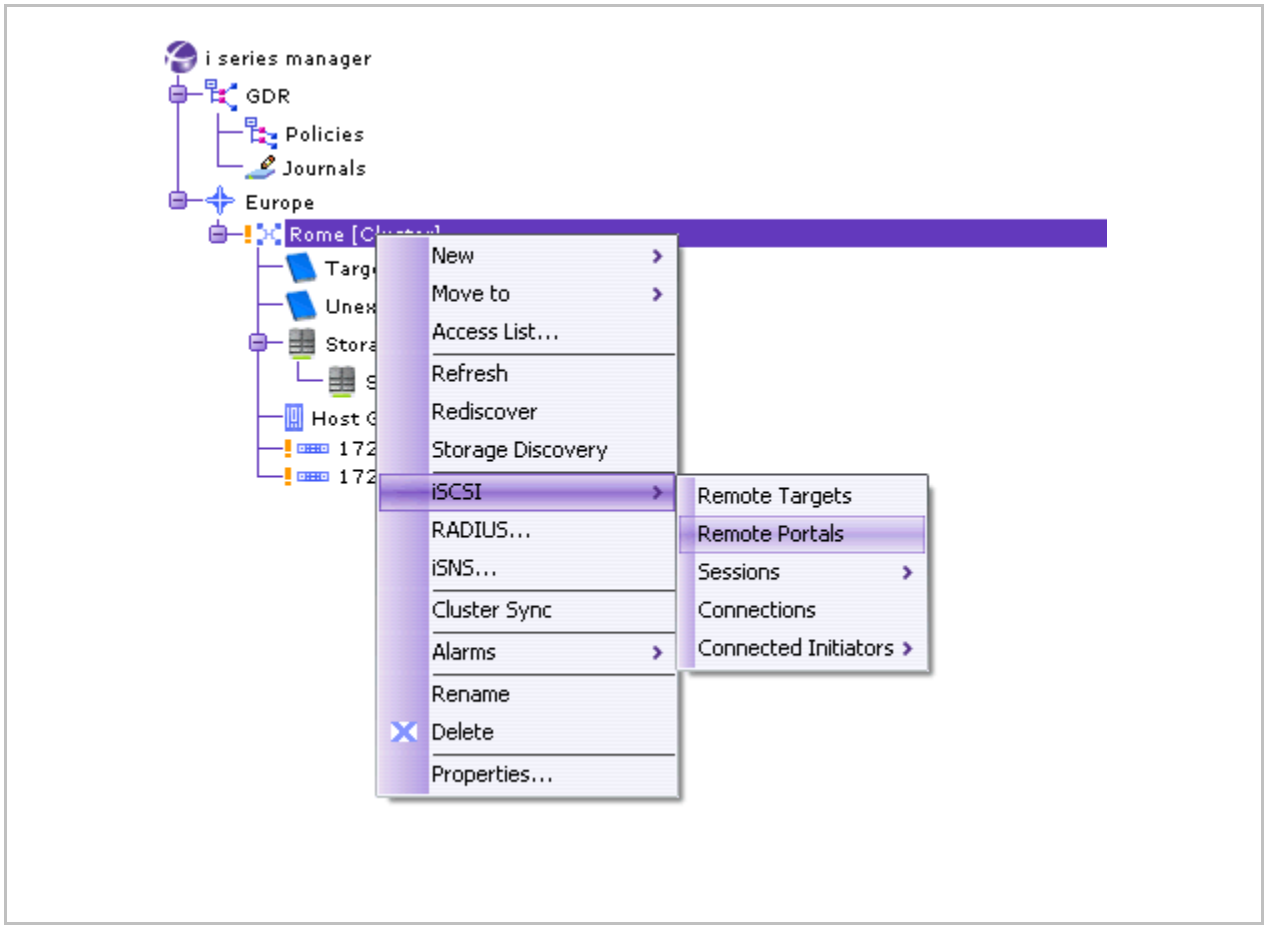



*Figure 3-32. Remote Portals*

The iSCSI Remote Portals window appears.

Click **Add**.

Enter **IP Address** and click **OK**.

The Portals are added to the iSCSI Remote Portals window.

Click **Close**.

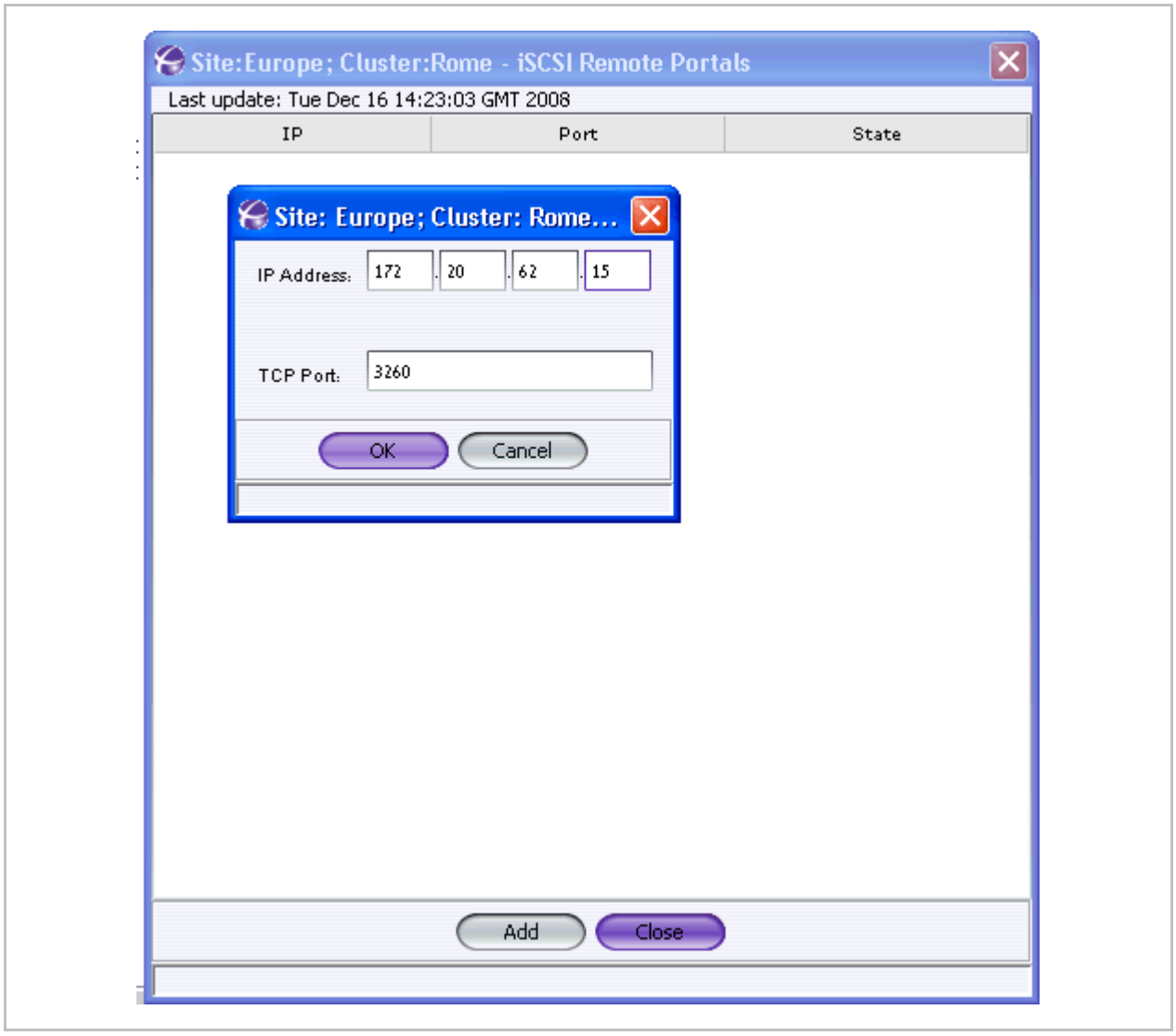



*Figure 3-33. iSCSI Remote Portals*

***To discover a specific remote iSCSI target:***

1. Select the i series, right click and select **New > iSCSI Remote Target…**

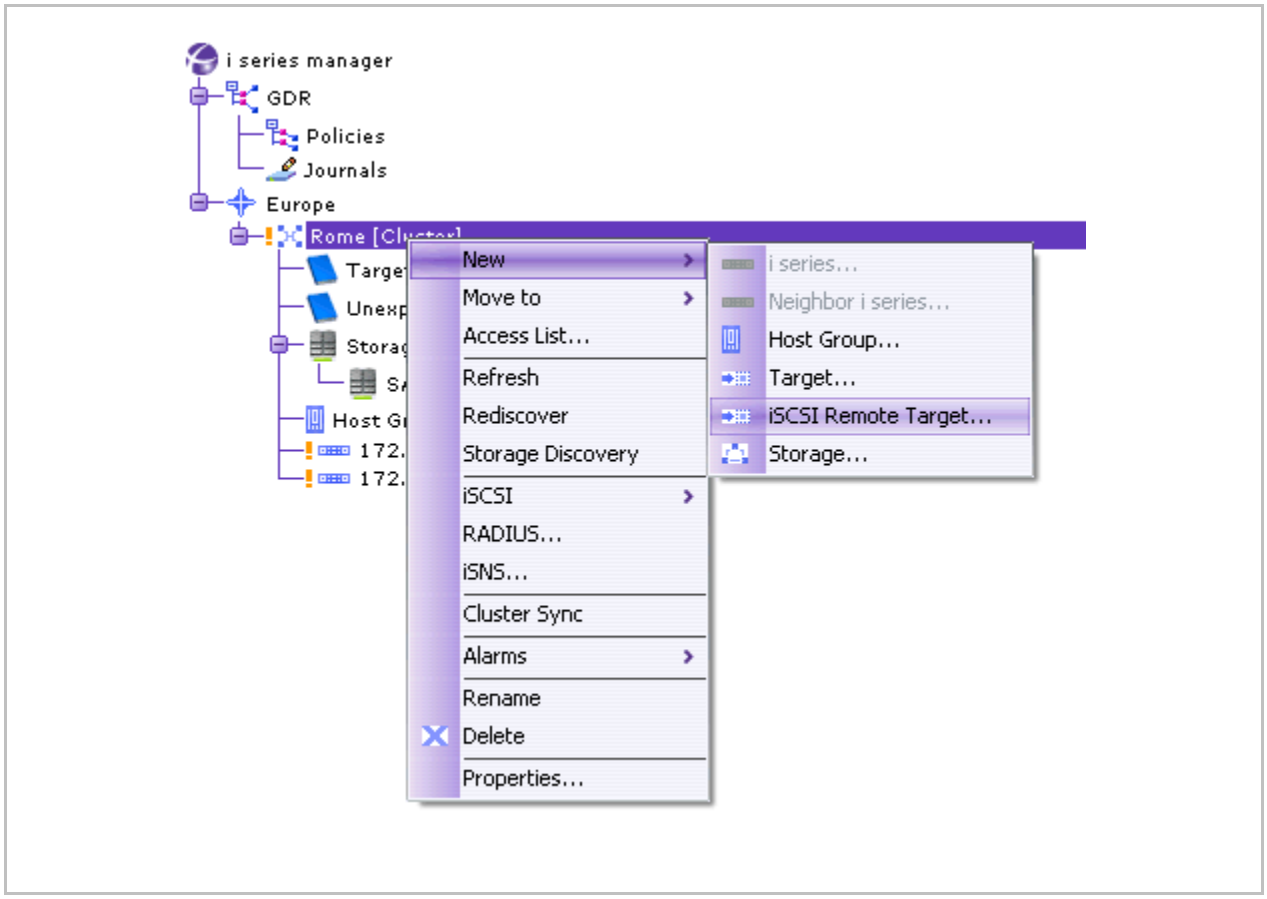



*Figure 3-34. New Remote Target*

The New iSCSI Remote target window appears.

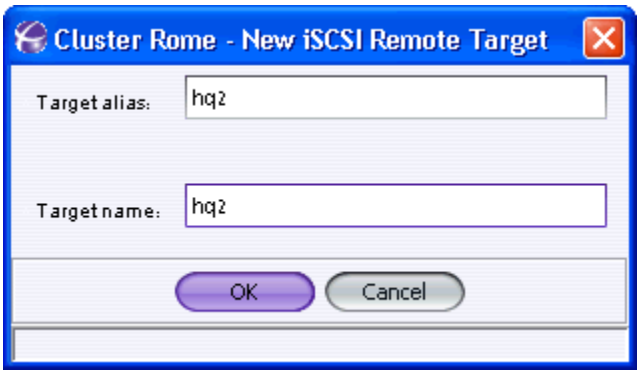



*Figure 3-35. iSCSI Remote Target*

Configure **Target alias** and **Target name** for existing remote target.

Click **OK**.

Select the i series, right click and select **iSCSI > Remote Target…**

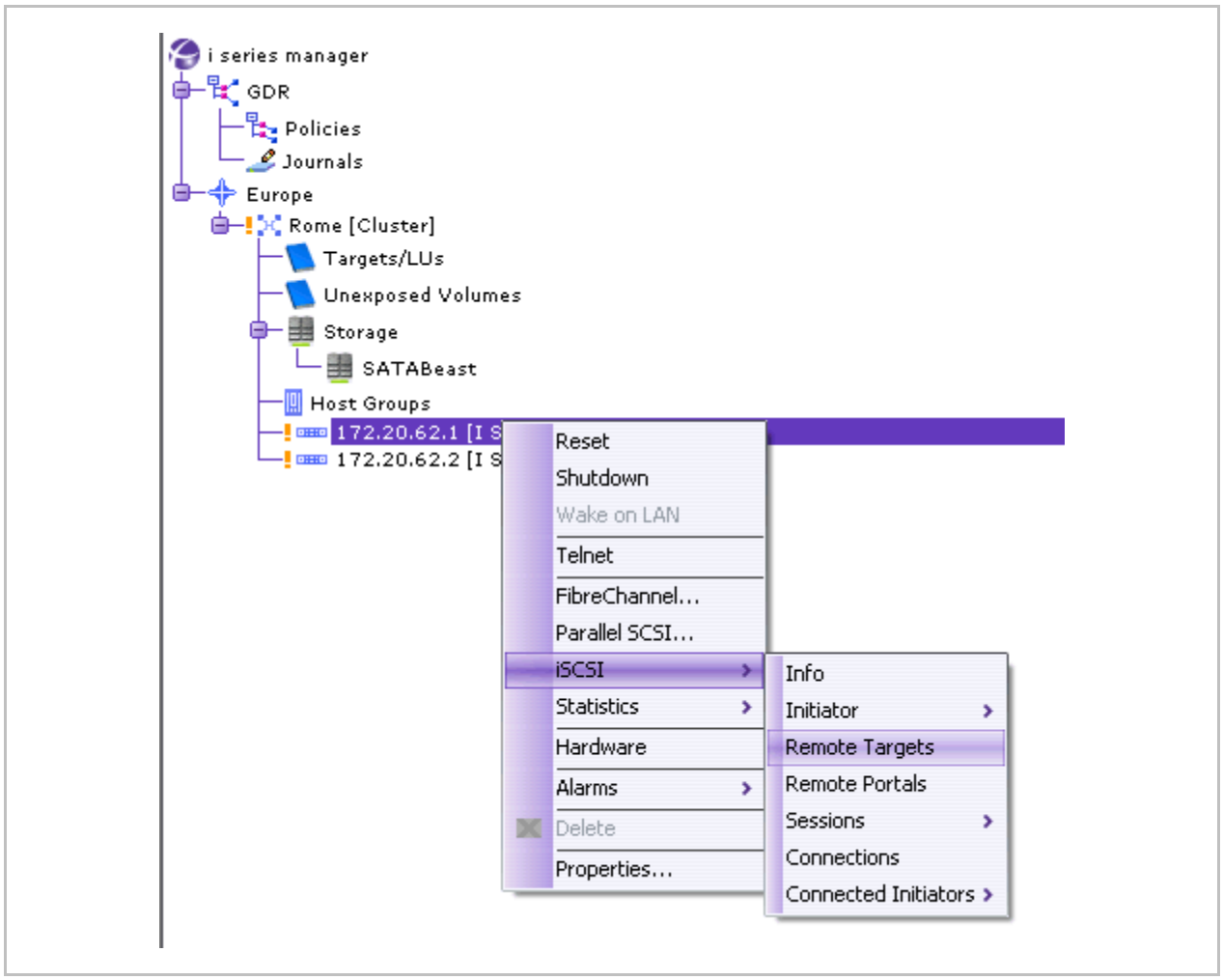



*Figure 3-36. Discover Remote Target*

The iSCSI Remote Targets window appears.

Select the remote target, right click and select **Add Portal.**

The Add Portal window appears.

Configure the IP Address, TCP Port and Group Portal Tag for the Portal.

Click **OK**.

The Portal is added and remote target is now connected.

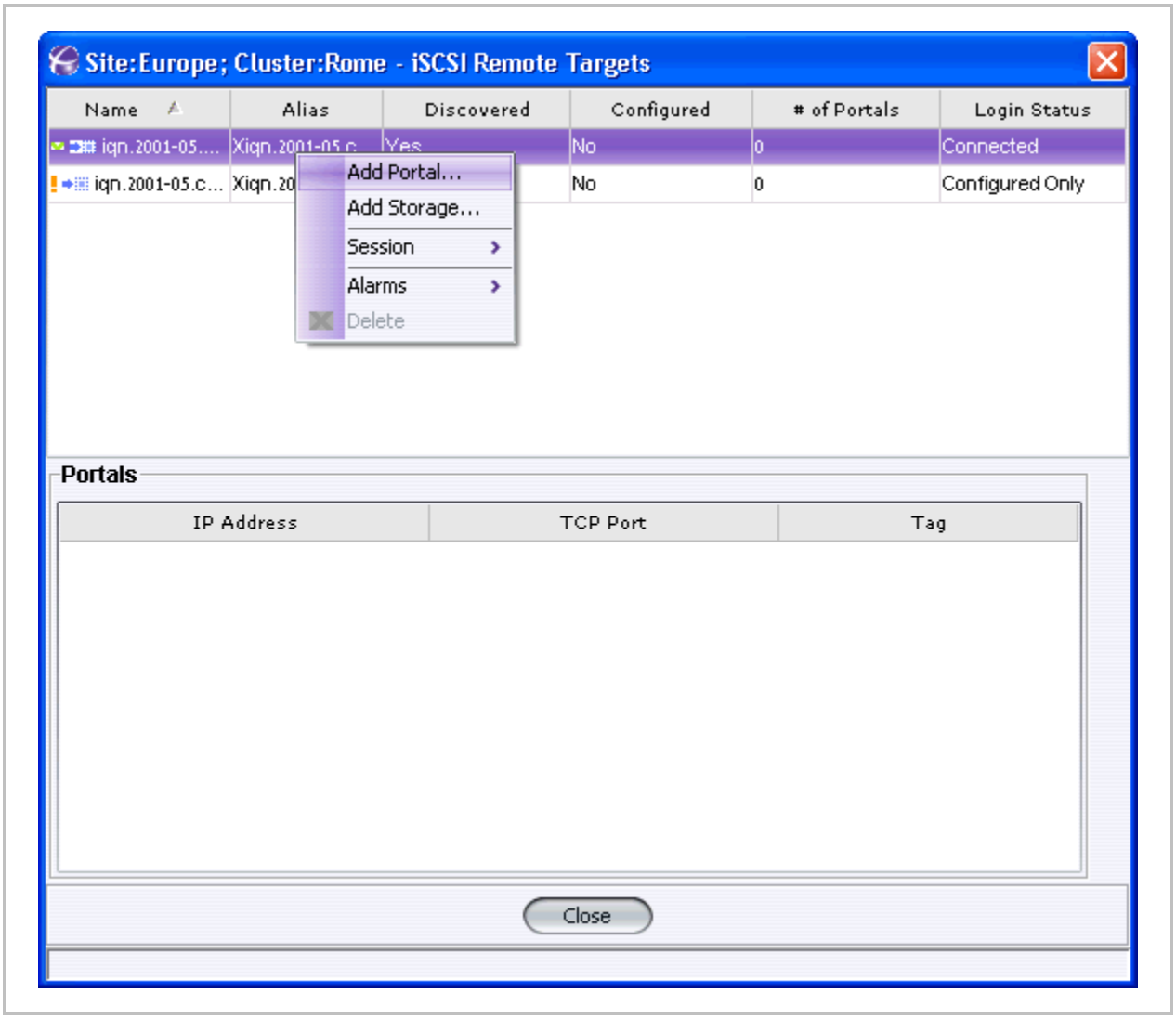



*Figure 3-37. Configure Remote Target Portal*

## iSNS Configuration

The i series supports Internet Storage Name Service (iSNS) protocol for advertising its targets and portals on the iSNS server. This enables iSCSI initiators in the IP-SAN to locate the i series targets automatically. Targets defined by the i series's Access Control List (ACL) as having controlled access are accessible only to those servers defined as having access to the target.

### To add an iSNS server:

1. In the Navigation pane, right click on desired cluster and select **iSNS…**

   The **iSNS Servers** dialog box opens.

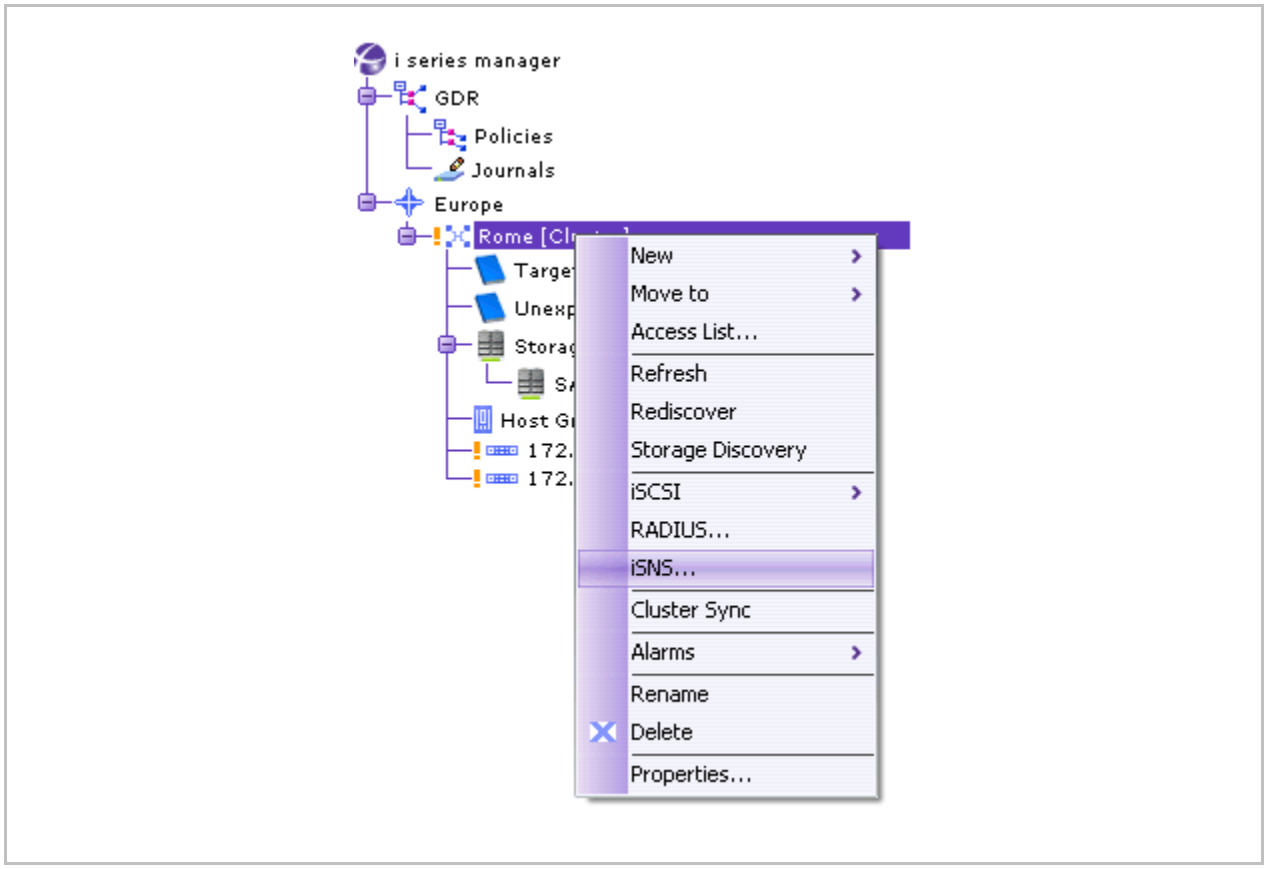



*Figure 3-38. i series Selected*

Click **Add** to open the New iSNS Server dialog box (Figure 3-39).

Enter the iSNS server IP address and click **OK**.

The IP address is added to the iSNS Server dialog box.

Click **OK**.

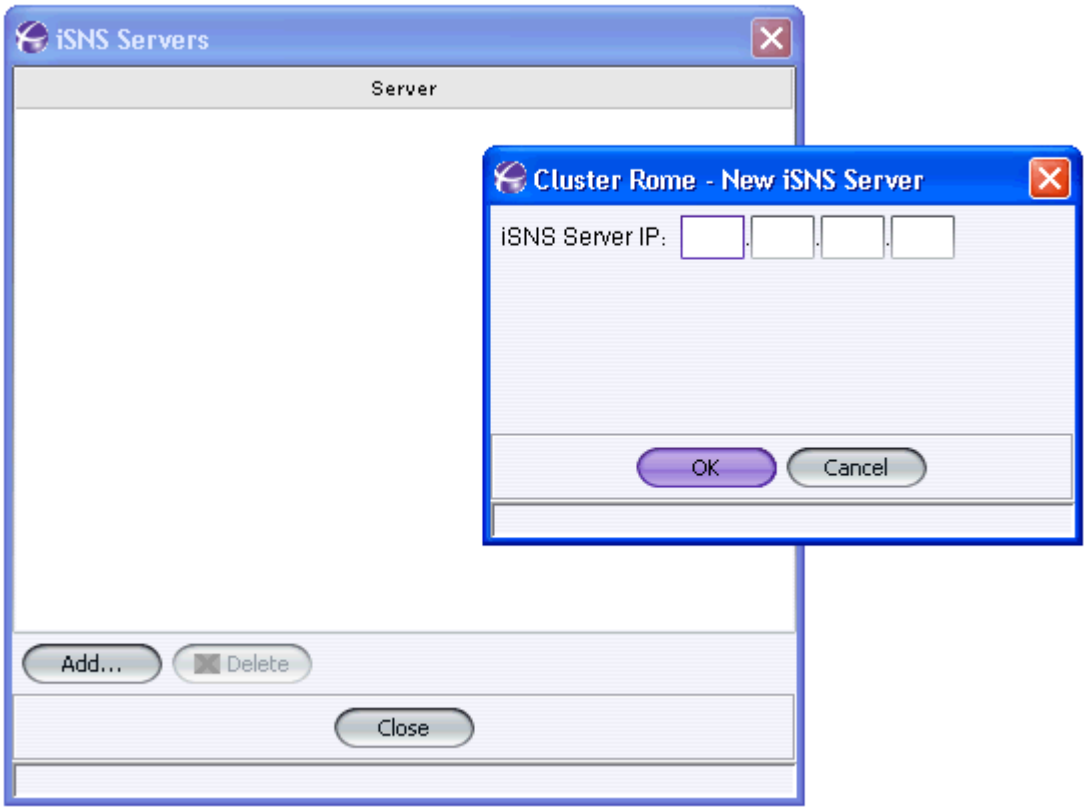



*Figure 3-39. New iSNS Server Dialog Box*

## RADIUS Server Configuration

A 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.

### To configure a Radius server:

1. From the Navigation pane, select the cluster or stand-alone i series. Right click and select **RADIUS** from the open menu.

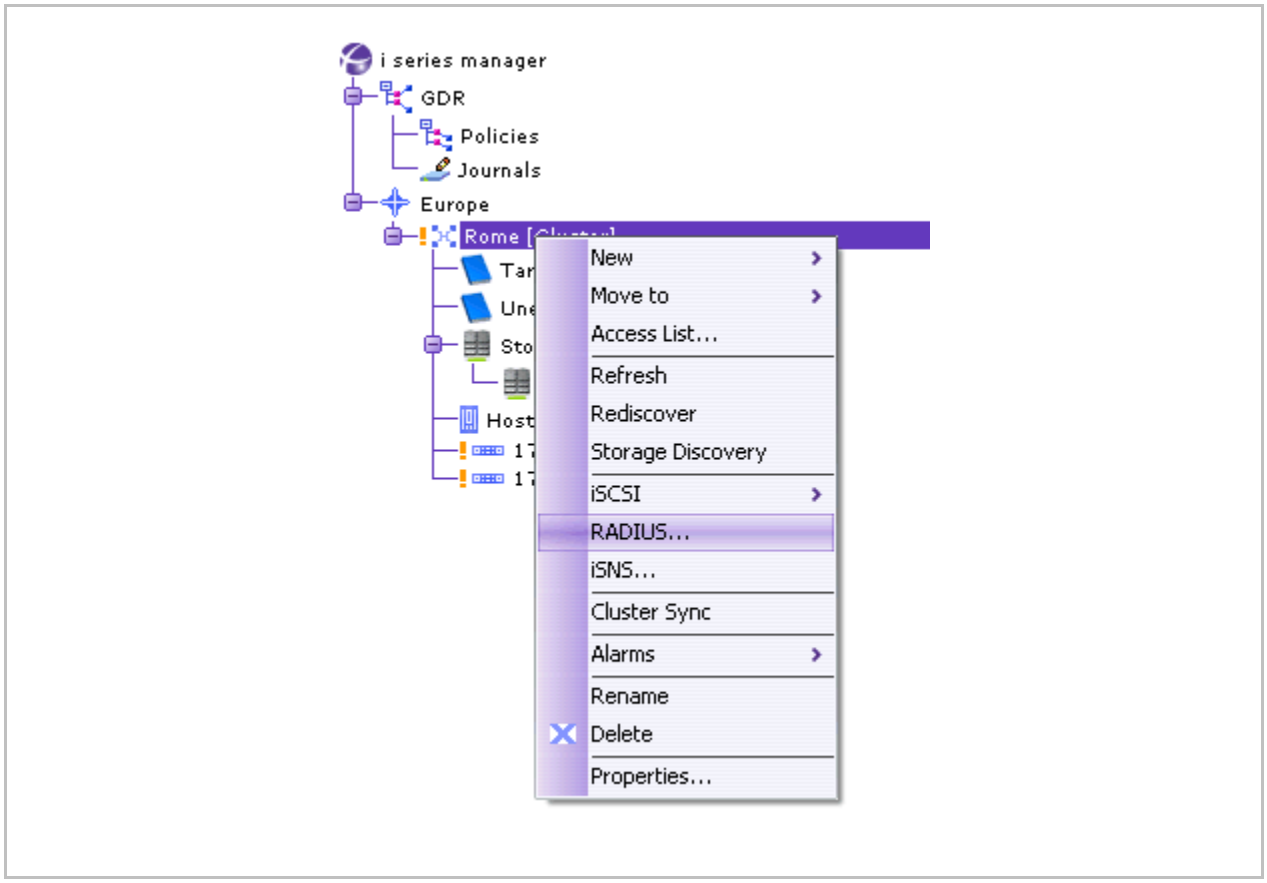



*Figure 3-40. i series Selected*

The RADIUS Servers dialog box opens.

Click Add.

The Add RADIUS Server dialog box opens.

Enter the new RADIUS server parameters.

Click **OK**.

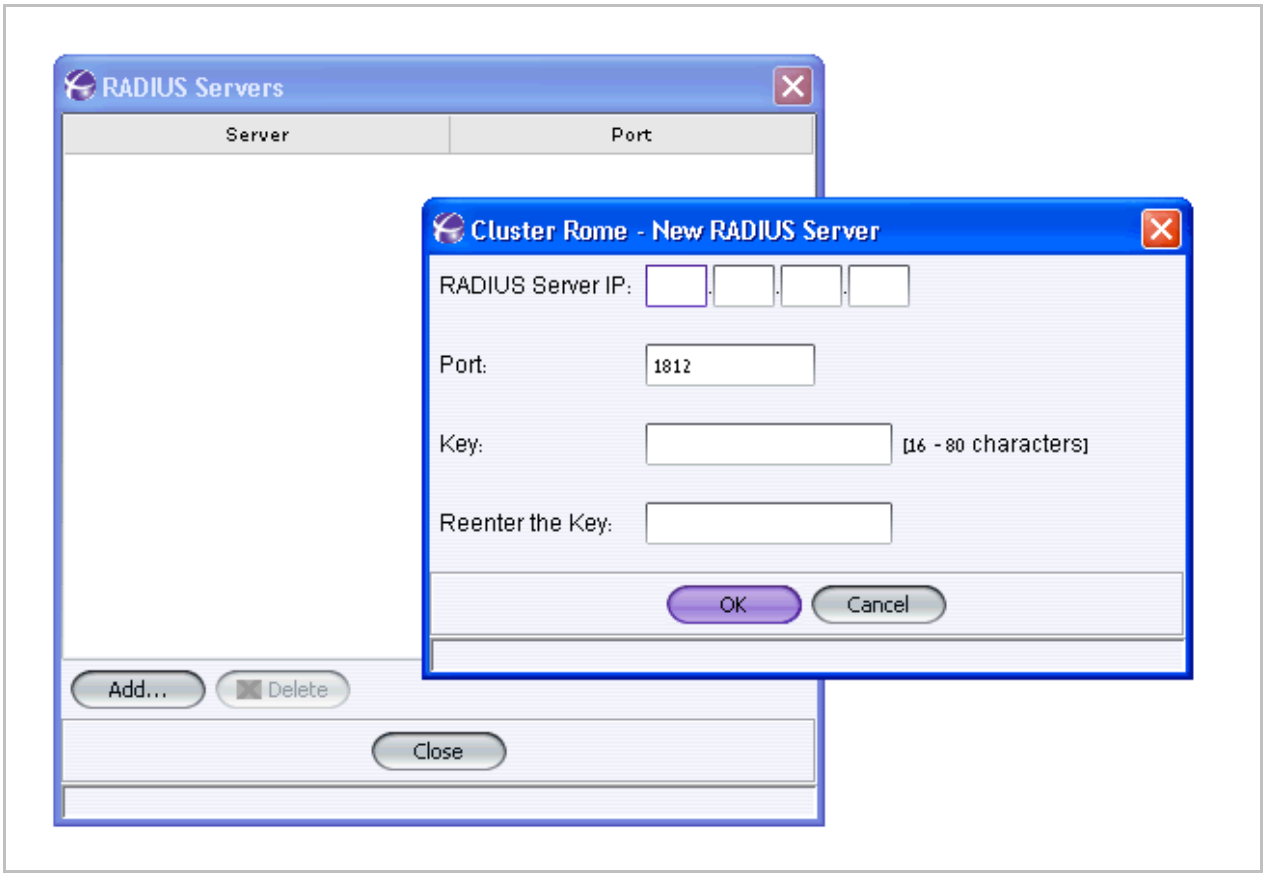



*Figure 3-41. RADIUS Server Configuration*

### *SNMP Configuration*

SNMP and trap port configurations are editable from this tab.

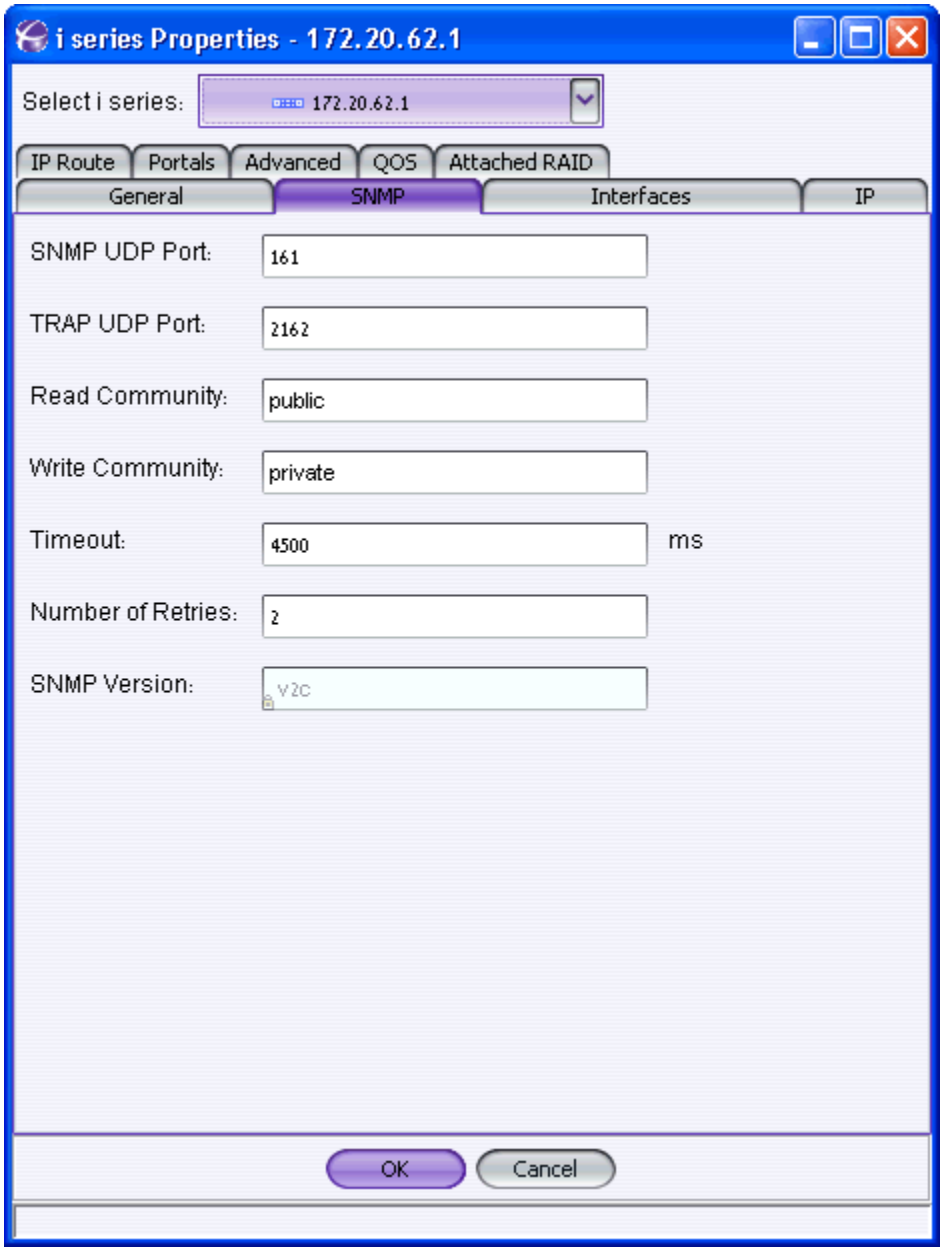



*Figure 3-42. SNMP Tab*

*Table 3-6. SNMP Tab Parameters*

| Parameter | Definition |
|---|---|
| SNMP UDP Port | UDP port on which SNMP manager-agent communications run |
| TRAP UDP Port | UDP port on which the SNMP agent will issue traps |
| Read Community | defined group granted read access to data |
| Write Community | defined group granted write access to data |
| Timeout | time in milliseconds before an SNMP session is considered closed |
| Number of Retries | number of times to re-establish an active SNMP session |
| SNMP Version | SNMP protocol version being used to establish i series manager communications with the specified i series |

## Telnet Port Designation

If your network topology includes a management station communicating with the i series via CLI, you can enable Telnet communications to be transported through a port other than the standard Telnet port 23. If your Telnet communications connection to the i series traverses a firewall, the standard Telnet port 23 may be blocked by the firewall as a security measure. The designated port can be opened in the firewall for dedicated i series - management terminal communications.

***To designate a telnet port:***

1. In the Navigation pane, select the i series.

Right click on the i series and select **Properties**. The i series **Properties** dialog box opens (Figure 3-12).

Toggle to the **Advanced** tab (Figure 3-43).

Enter the new Telnet port and click **OK**.

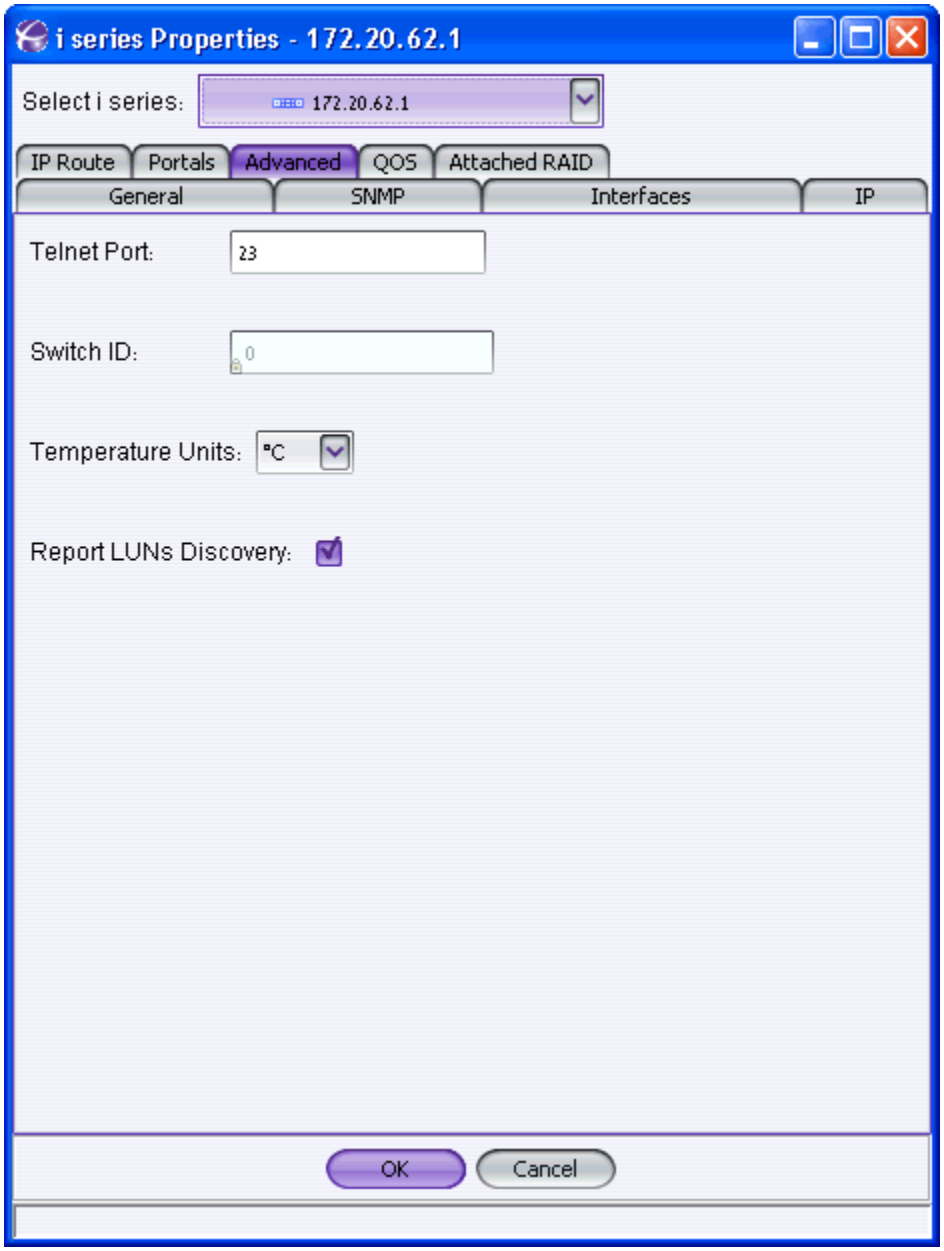



*Figure 3-43. Setting Telnet Port*

A message box opens stating that you must reset the i series for the new Telnet port properties to take effect. Click **OK**.

Reset the i series (see Reset ).

Check that the new Telnet port was applied by checking the **Advanced** tab in the i series **Properties** dialog box (Figure 3-43).

## *Report LUNs Command (Discovering Storage Devices)*

The i series default algorithm for storage devices discovery uses the SCSI command *REPORT LUNS*. Certain storage devices either do not support this command or do not respond according to the SCSI standard.

**Cluster Note:**
*When working with devices that do not support the SCSI command REPORT LUNS, 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, disable or re-enable device discovery using REPORT LUNs.*

### *To disable/enable report LUNs command:*

1. In the **Navigation** pane, right click on the i series and select **Properties**.

   The i series **Properties** dialog box opens (Figure 3-12).

Toggle to the **Advanced** tab (Figure 3-44).

Disable (uncheck) or re-enable (check) **Report LUNs Discovery**.

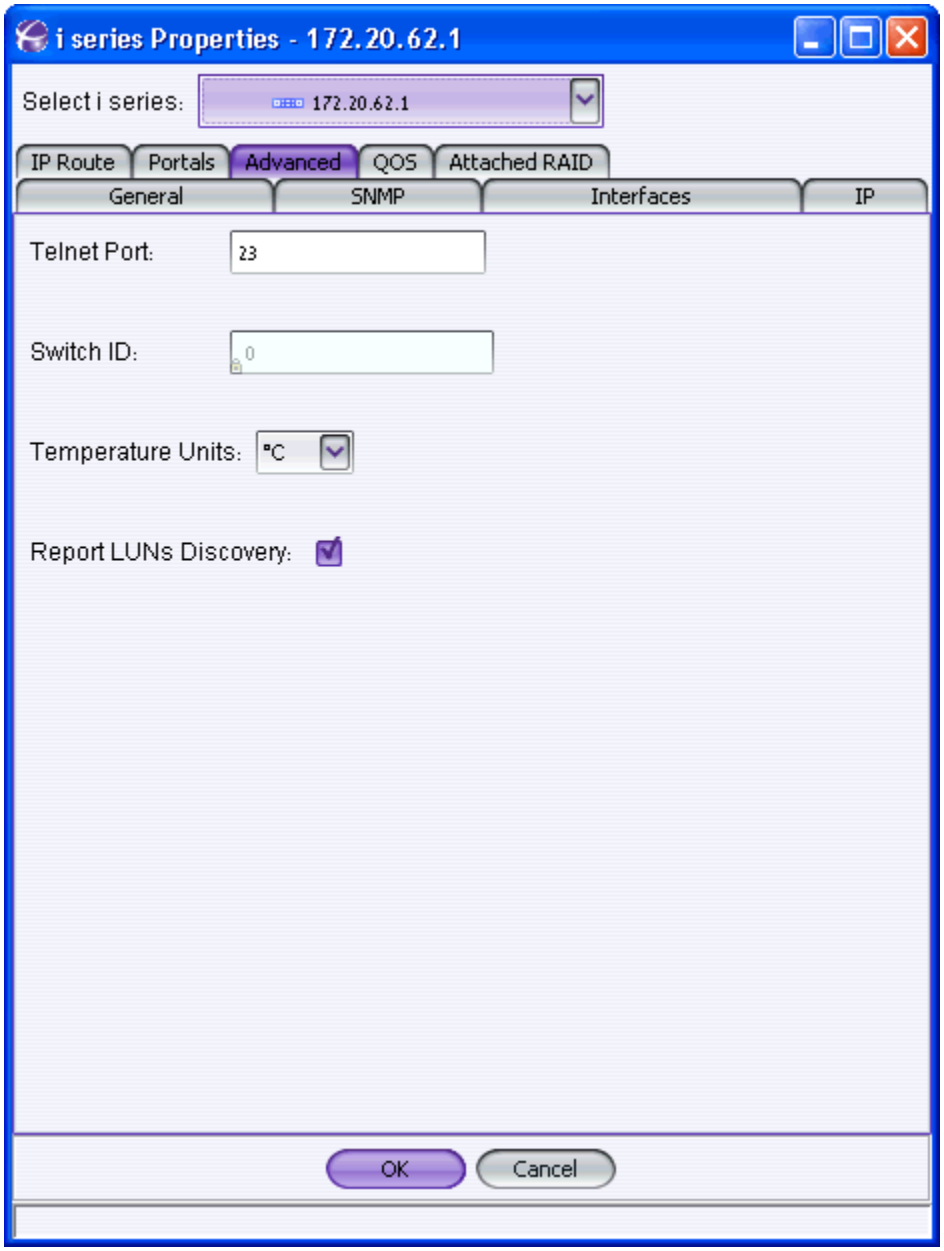



*Figure 3-44. Report LUNs Discovery Box*

### *Rediscover i series or Cluster Database*

Rediscover causes i series manager to refresh the information and update its database.

**Note:**

- The command ***Rediscover*** rediscovers the database for the i series or cluster.
- The command ***Storage Discovery*** rediscovers the physical disks attached to the i series.

### *To rediscover the database for the i series or cluster:*

1. Right click on cluster and select **Rediscover** (Figure 3-45).

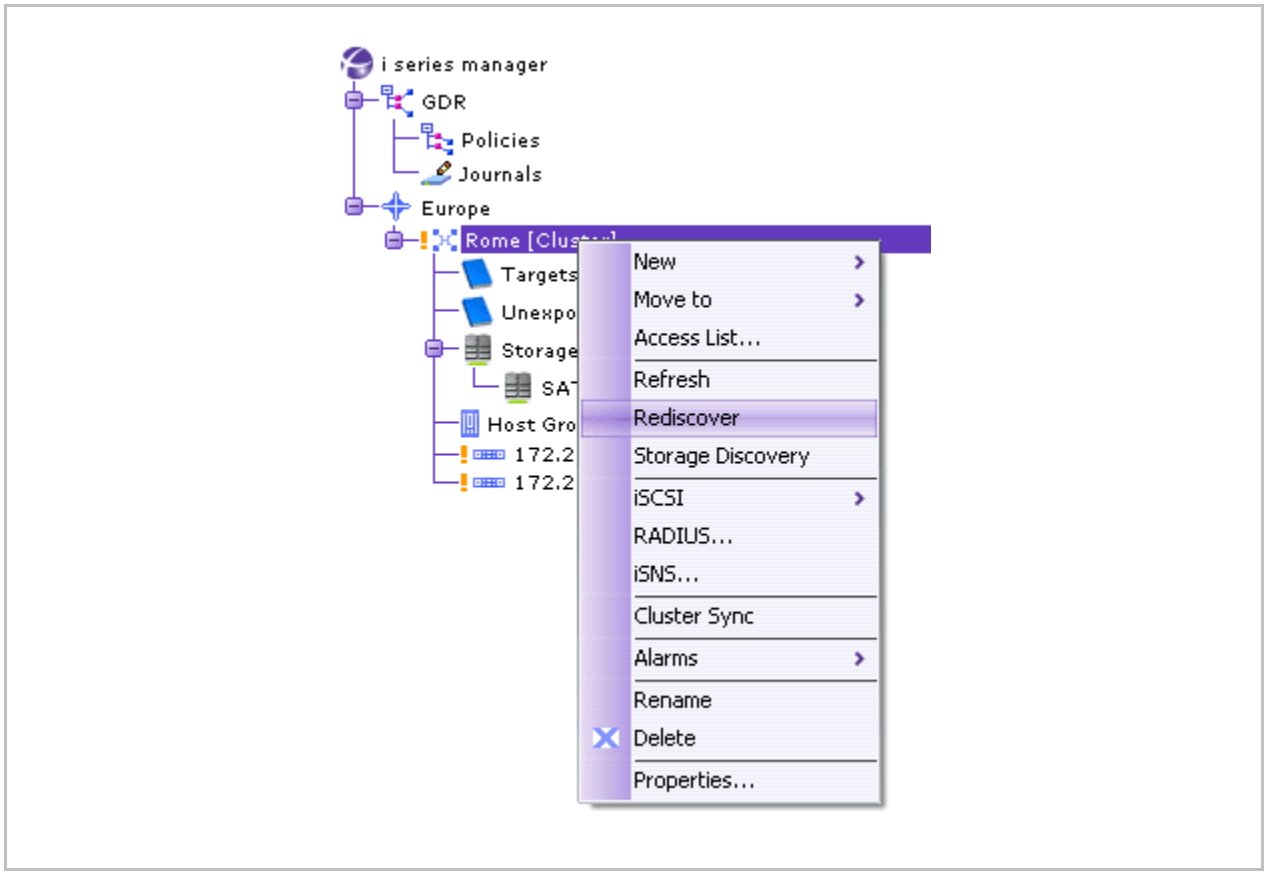



*Figure 3-45. Rediscover*

A confirmation window appears asking if you want to rediscover the i series. Click **Yes**.

A status window appears at the bottom of the screen indicating that Discovery has started.

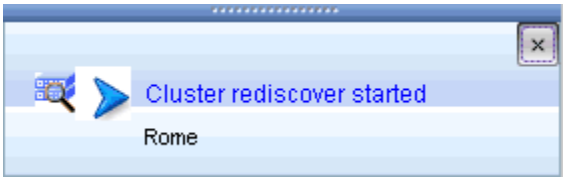



*Figure 3-46. Discovery Started*

When all attached storage devices, system configurations and virtual volumes have been discovered, the status window indicates that the operation has completed.

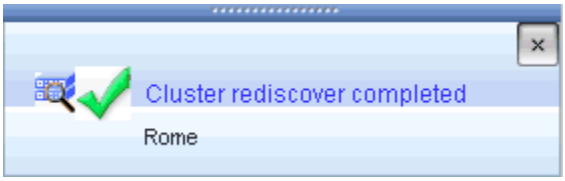



*Figure 3-47. Discovery Completed*

## Storage Discovery

Storage Discovery rediscovers the physical disks attached to the i series.

***To rediscover the physical disks attached to the i series:***

1. Right click on cluster and select **Storage Discovery** (Figure 3-48).

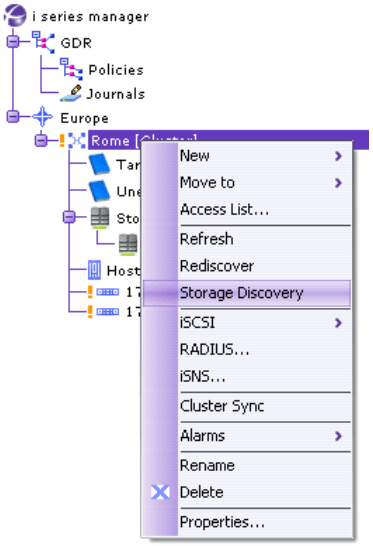



*Figure 3-48. Storage Discovery*

A confirmation window appears asking if you want to initiate the storage discovery. Click **Yes**.

## Reset i series

You can reset the i series from i series manager. All configuration databases will be maintained on the i series, including network port aliases and all configured volumes and targets.

> **Note:**
> *In the case of a cluster, Reset will cause the second i series to takeover.*

### To reset a i series:

1. In the **Navigation** pane, select the i series.

Right click on the i series and select **Reset**.

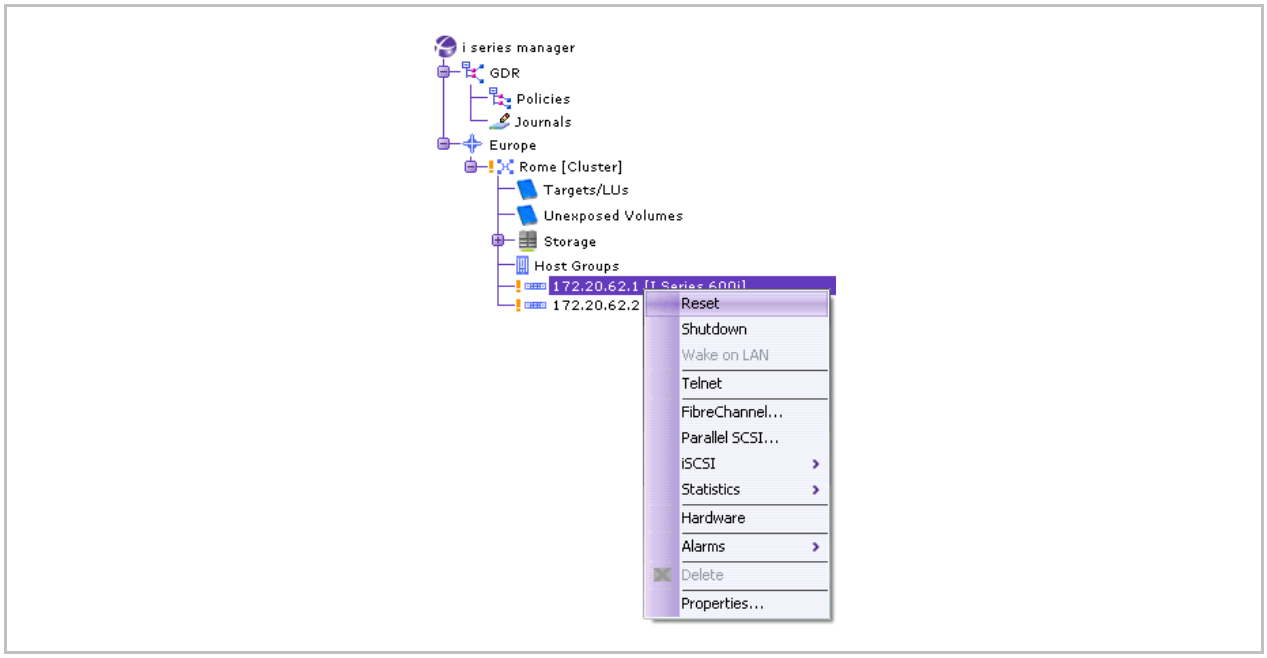



*Figure 3-49. Reset Selected From i series Menu*

A confirmation window appears asking if you want to Reset the i series. Click **Yes**.

The status bar displays ***Resetting*** i series while the i series is being reset.

As part of the reset process, i series manager rediscovers the i series. After the discovery process has completed, you can resume work. The status bar will display ***Ready***.


*Figure 3-50. Ready Status*

**Note:**
*If the reset i series is part of a cluster, you may have to synchronize the cluster. See Synchronizing a Cluster.*

## Removing i series from a Cluster

Removing the i series will remove all management configurations for the i series from i series manager (see *Breaking a Cluster*).

# Chapter 4
# Volume Operations

This chapter describes the volume management offered by i series manager. i series manager enables you to create and operate volume built from physical storage attached to the i series.

## Displaying Storage

Volume operations are performed from the Storage View Main Window (Figure 4-1) or from the Advanced Volume Creation Window (Figure 4-3).

***To display the storage view window:***

- Click on **Storage** in the navigation pane.

  The Available Storage Devices and Subdisks Details (partitioned disks) panels appear in the main window.

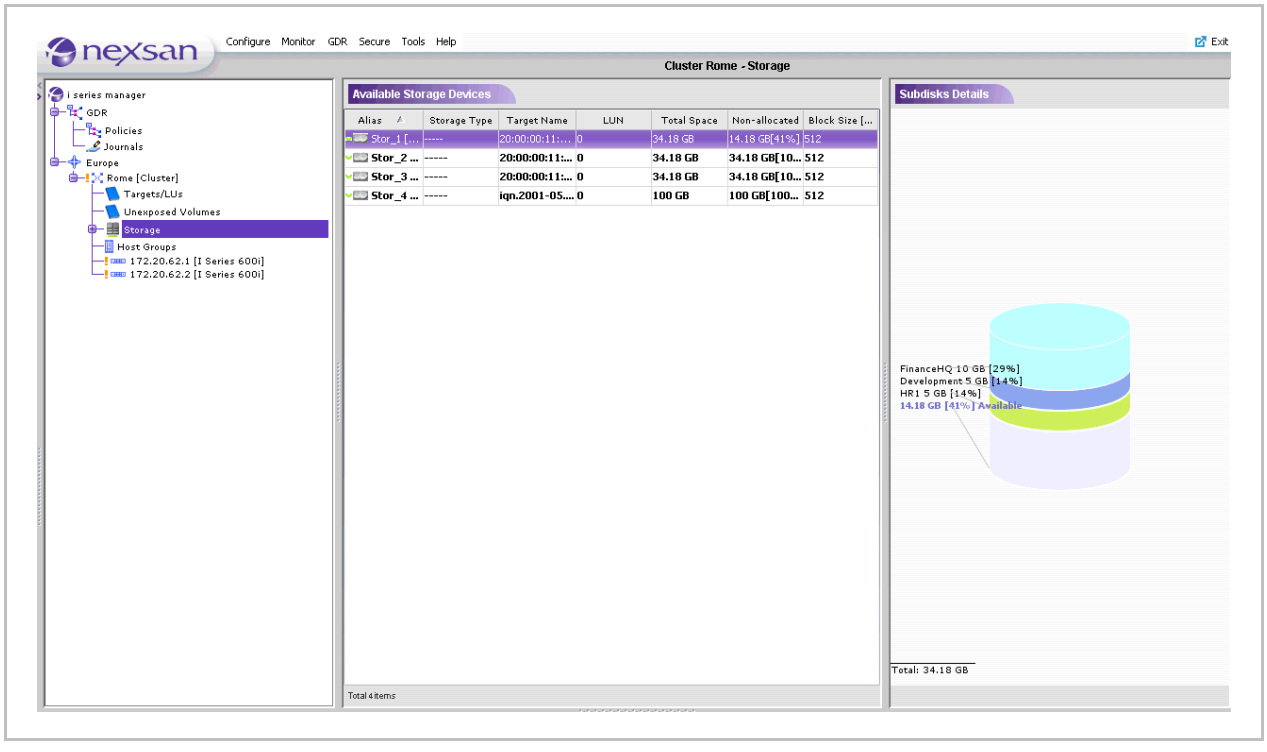



*Figure 4-1. Storage View Focus*

### *To display the Advanced Volume Creation Window:*

1. From the *Quick Launch:*
   **Configure > Create Volume > Advanced…**

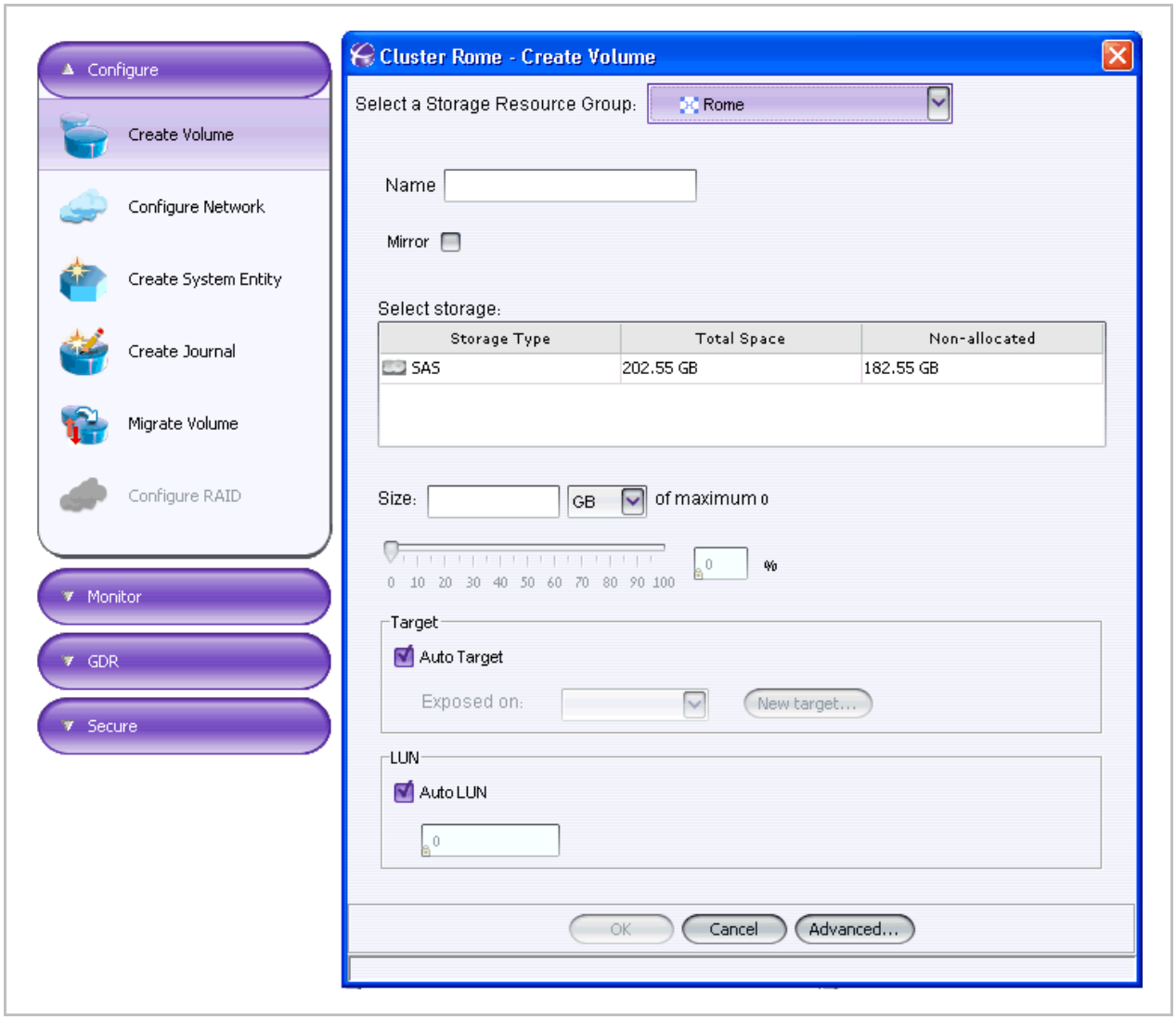



*Figure 4-2. Accessing Advanced Volume Operations*

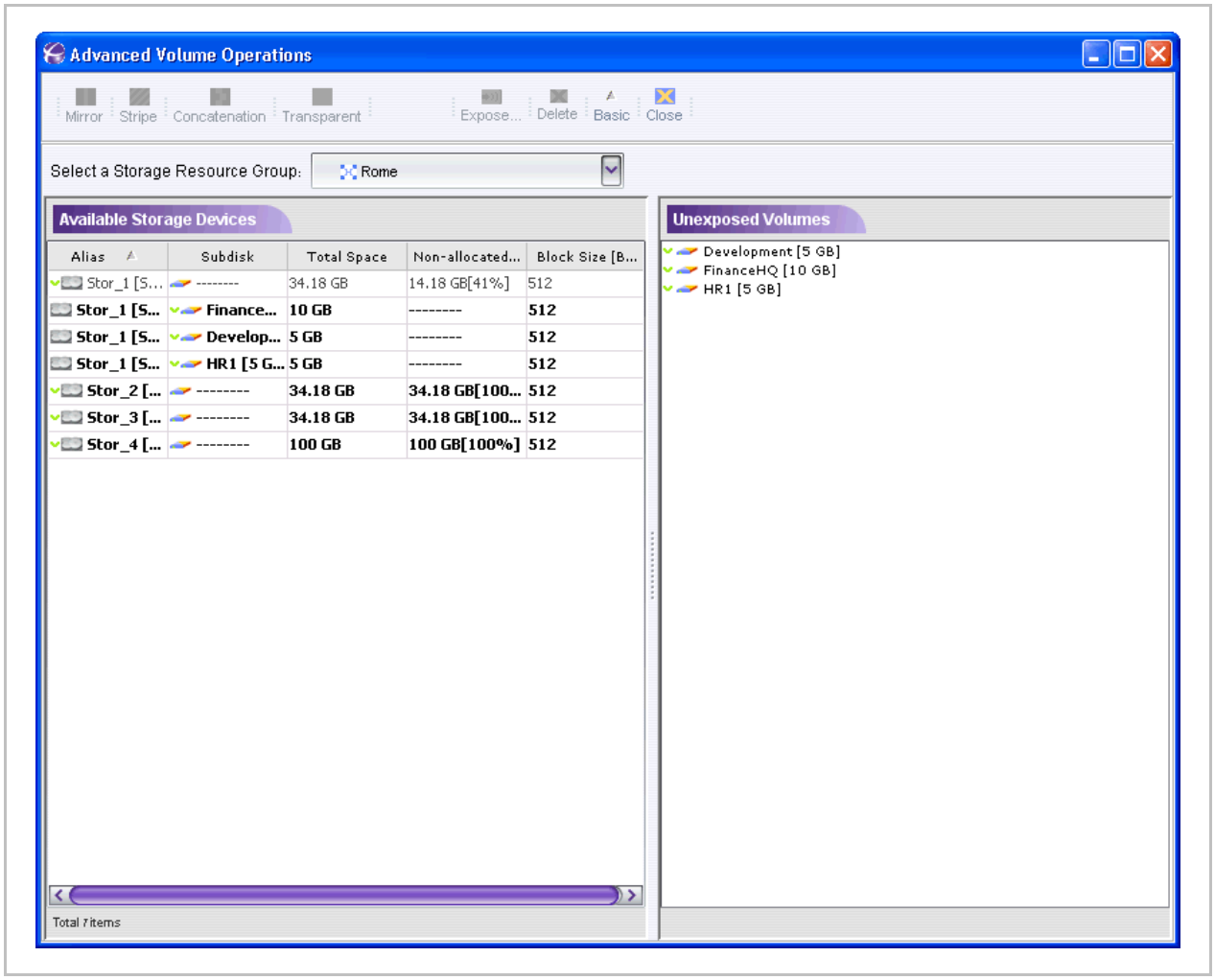



*Figure 4-3. Advanced Volume Creation Window*

## Storage Properties

***To display or modify available storage properties:***

1. Select the desired storage device by clicking on its name from the Available Storage Devices panel (Figure 4-5).
2. Right click and select **Properties**.

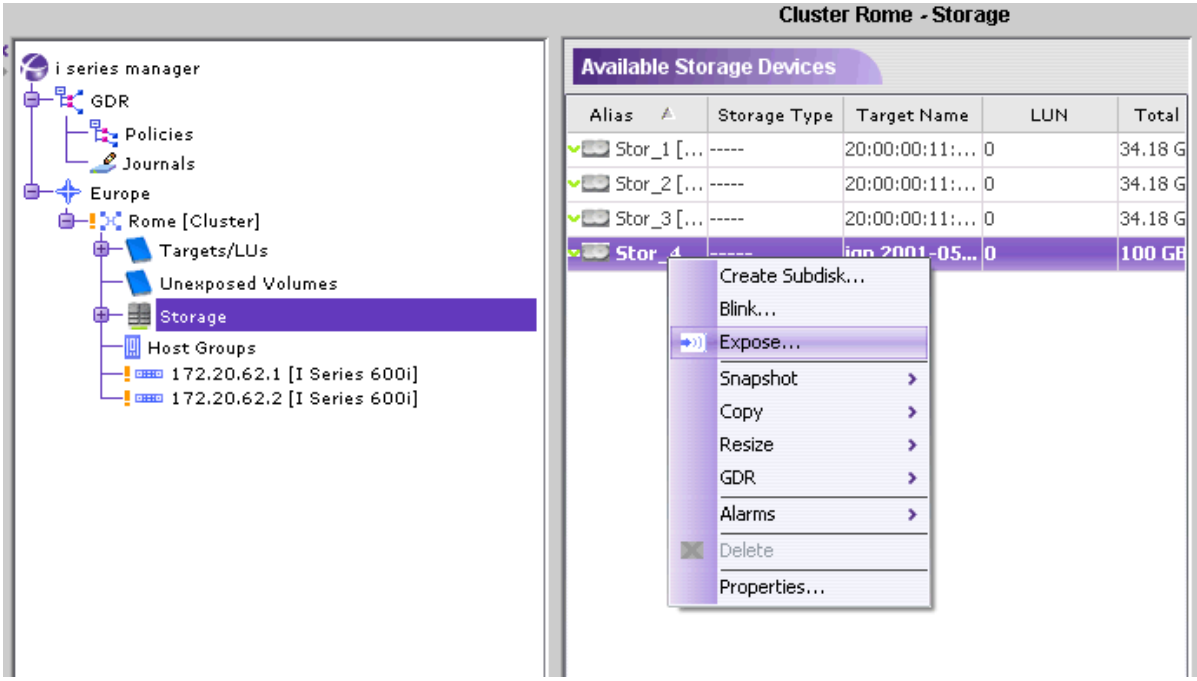



*Figure 4-4. Disk Properties Menu*

The Disk Properties dialog box opens. If subdisks exist, you can view them by clicking on the subdisks tab (Figure 4-6).

3. The fields **Alias**, **Information**, **Write Cache Enabled** and **Allocable** are editable
4. Configure parameters and click **OK**.

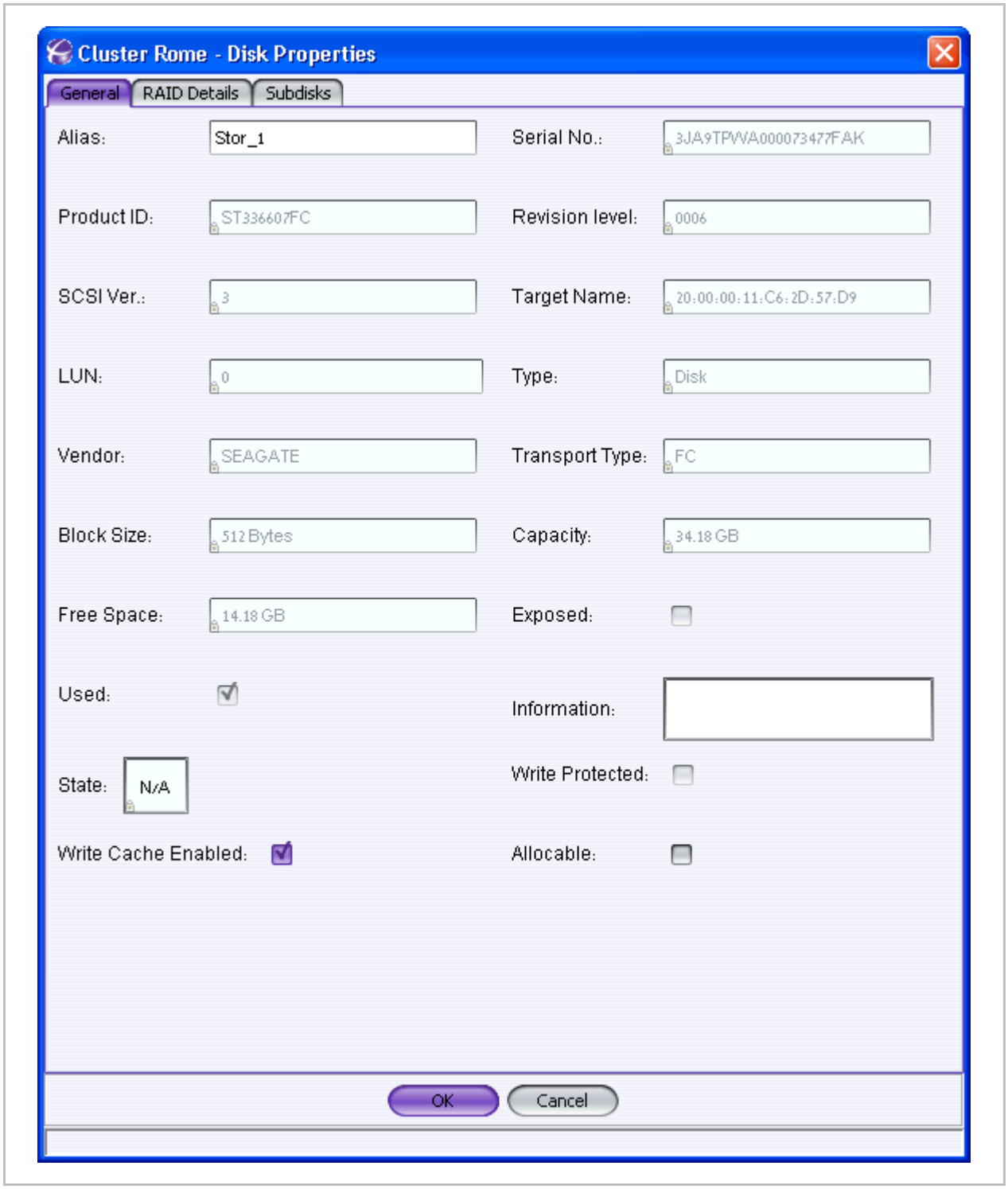



*Figure 4-5. General Tab - Disk Properties*

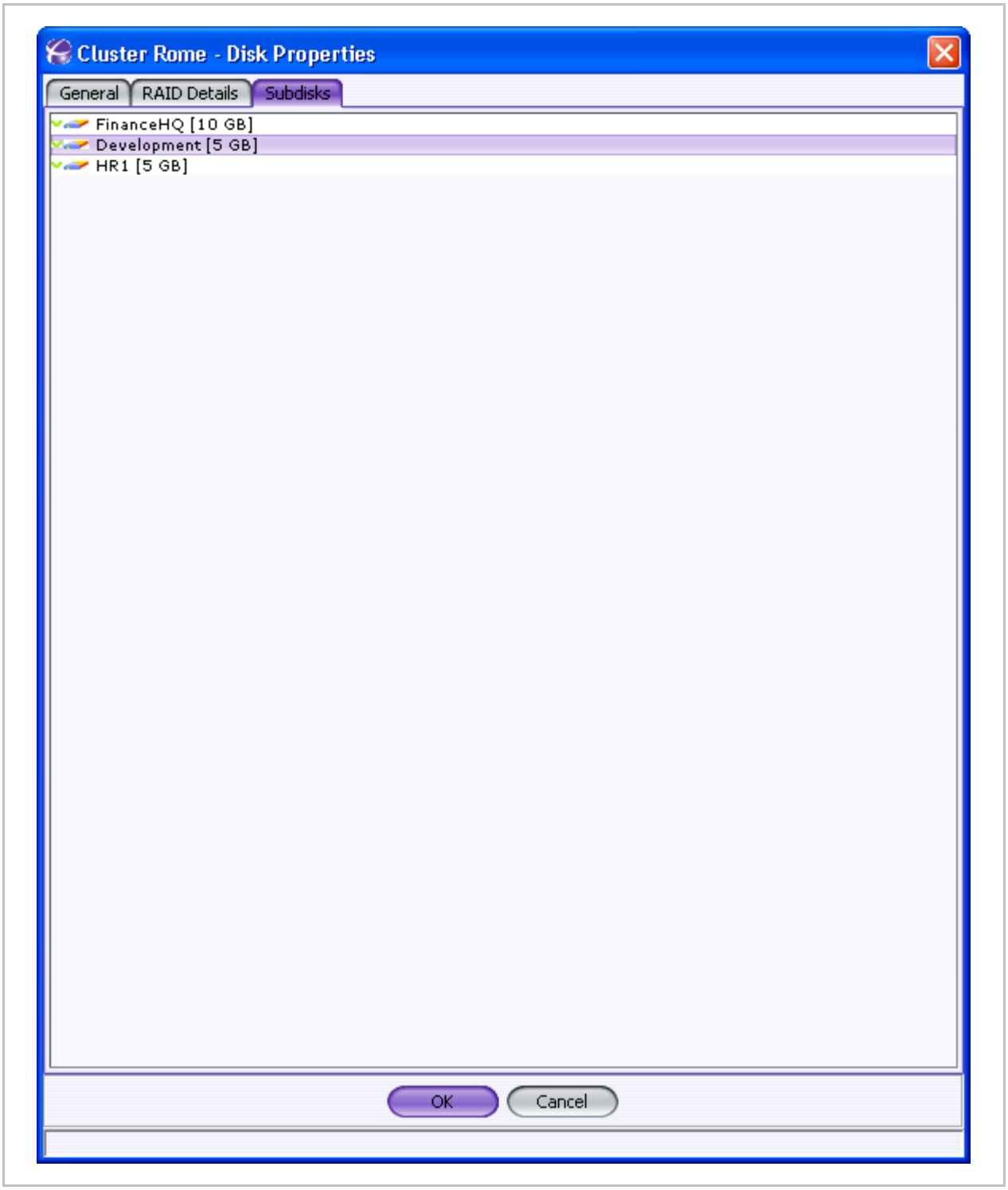



*Figure 4-6. Subdisks Tab - Disk Properties*

# Creating Volumes

This section describes the steps to create the virtual volume from the actual physical volumes. There are two main steps to volume creation:

1. Creating the virtual volume from a physical disk.
   Volumes can be made from the whole physical disk, or partitioned into subdisks.
2. Exposing the virtual volume.
   Volumes cannot be accessible by servers until they have been exposed. For information on exposing the volumes, see Volume Exposure & Targets.

## Express Volume Creation

Express volume creation allows you to create and expose a volume from one dialog box.

***To express create volumes:***

1. From the *Quick Launch:*
   **Configure > Create Volume**


*Figure 4-7. Quick Launch - Create Volume*

The Create Volume window appears.

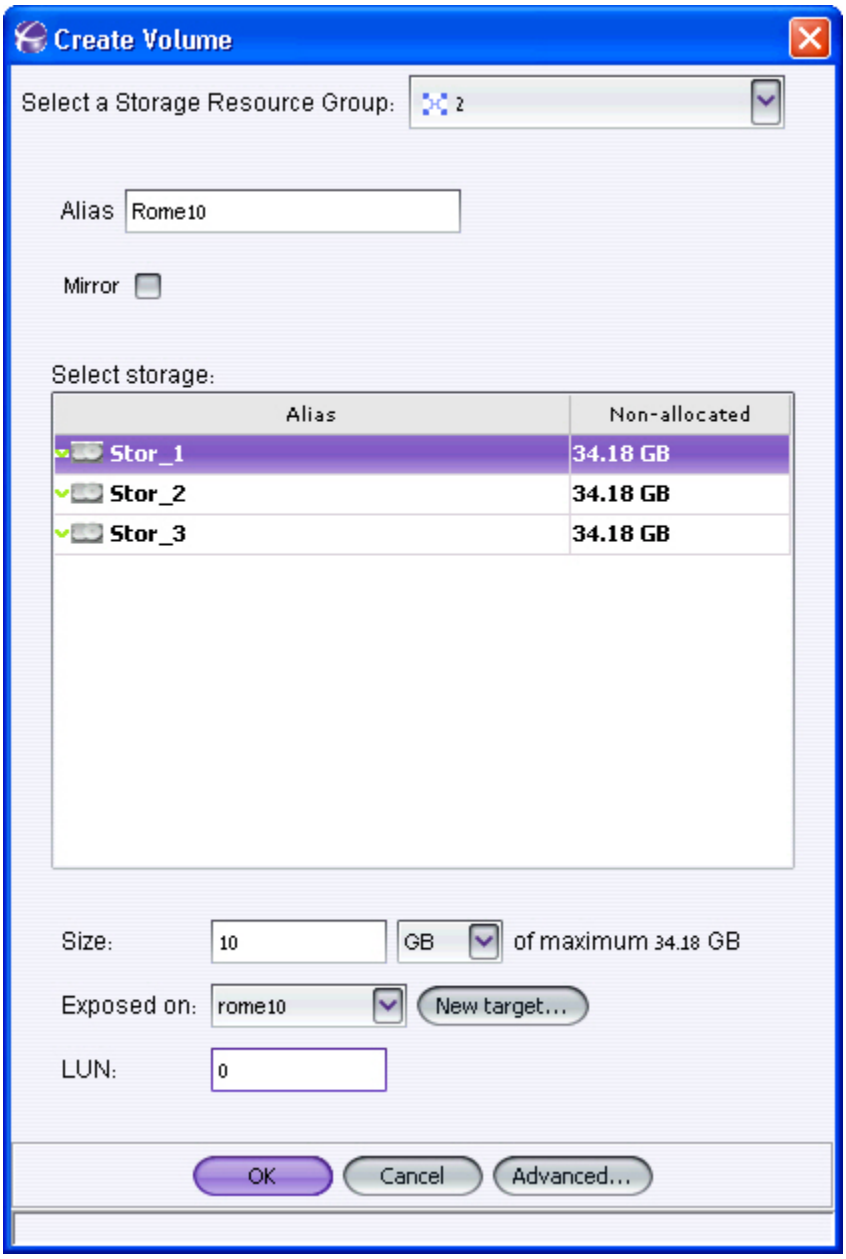



*Figure 4-8. Create Volume*

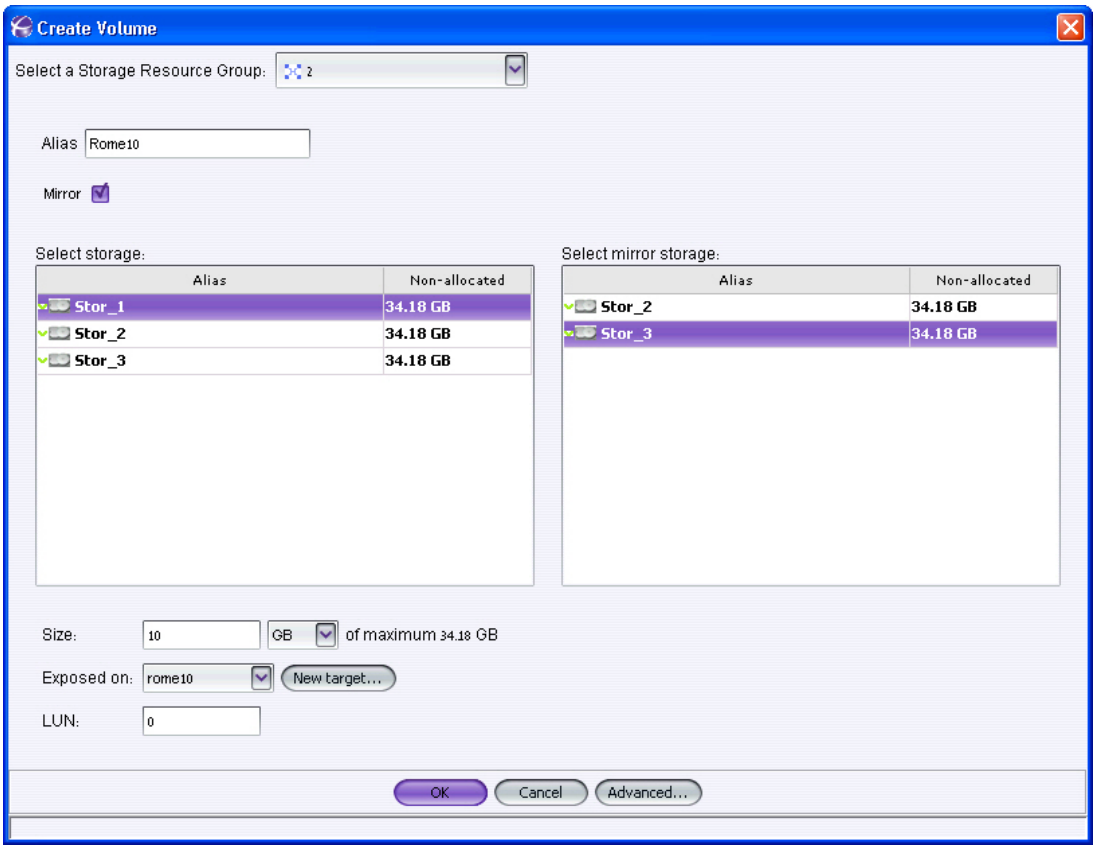



*Figure 4-9. Create Volume with Mirror*

2. Select a storage resource group from the list.
3. Assign an alias for the volume you are about to create.
4. If you want to create a mirrored volume check the Mirror checkbox.
5. Select a storage from which to create this volume from the list of available storage. When creating a mirrored volume you must do the same for the mirrored volume from the list of available storage on the right.
6. Specify the size of the volume to create. Select the units for the volume MB, GB or TB.
7. Select a target to expose this volume on. If you want to create a new target, click **New Target…**
8. Specify a LUN for the target.
9. Click **OK**.

## Creating Volumes from the Whole Physical Disk

Volumes must be exposed in order for them to be used by FS Applications.

> **Note:**
> *Only disks that don't have subdisks configured on them, or are not being used, can be directly exposed.*

***To create a volume from the whole physical disk:***

1. From the list of available storage devices, select the physical volume to expose.
2. Right click the mouse and select **Expose…** Volume Exposure is discussed below in Creating Subdisks (LUN Carving).

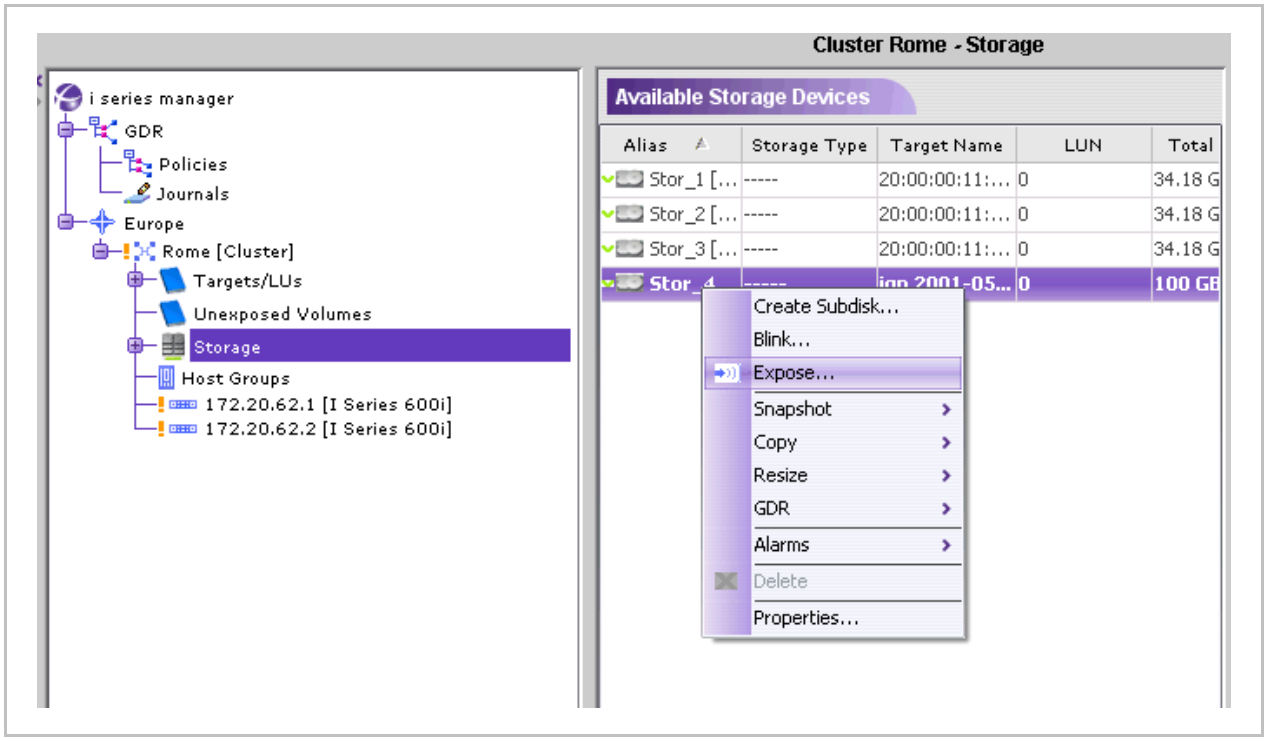



*Figure 4-10. Expose Volume*

## Creating Subdisks (LUN Carving)

Volumes can be created from partitioned disks (subdisks).

> **Note:**
> *Subdisks have start block and end block addresses within the disk in hexadecimal form.*

### *To create a subdisk:*

1. Select the disk you want to partition from the list of available disks (Figure 4-10).

   The disk appears in the Subdisks Details pane on the right. The available space on the disk is listed as free.

2. Right click and select Create Subdisk from the open menu (Figure 4-11).

   The Create Subdisk dialog box opens.

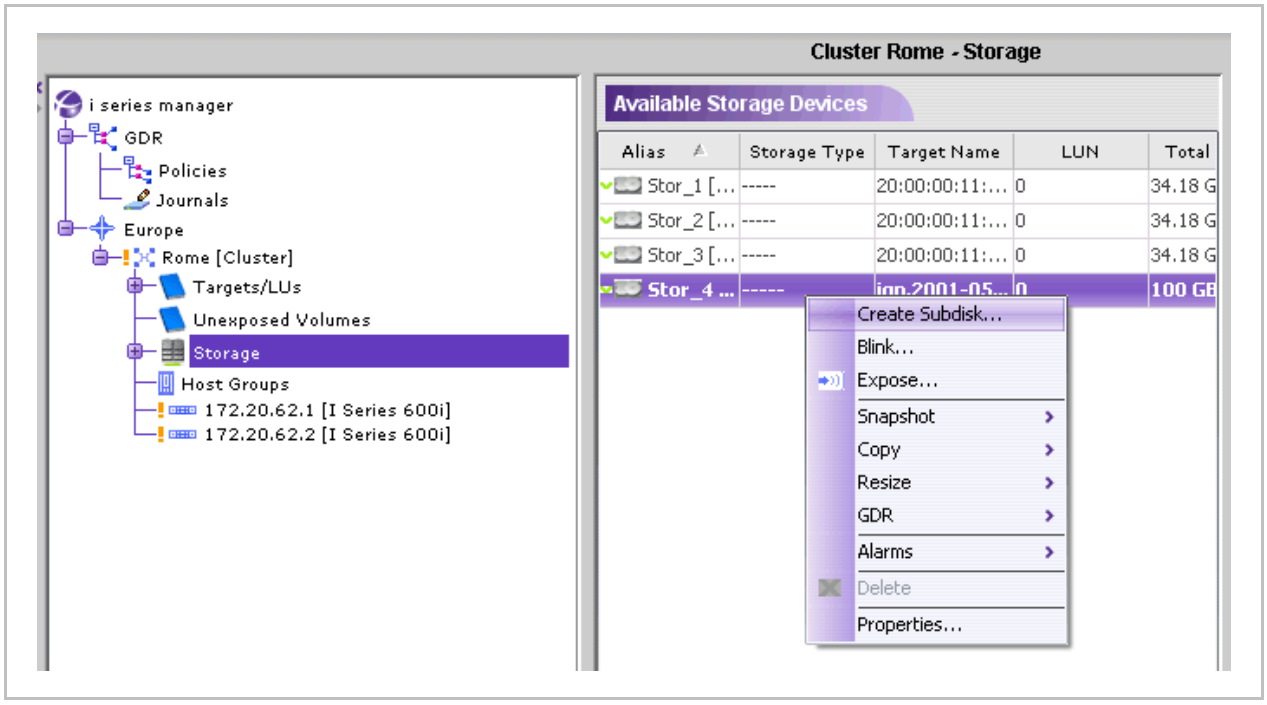



*Figure 4-11. Create Subdisk*

In the **Create Subdisk** dialog box:

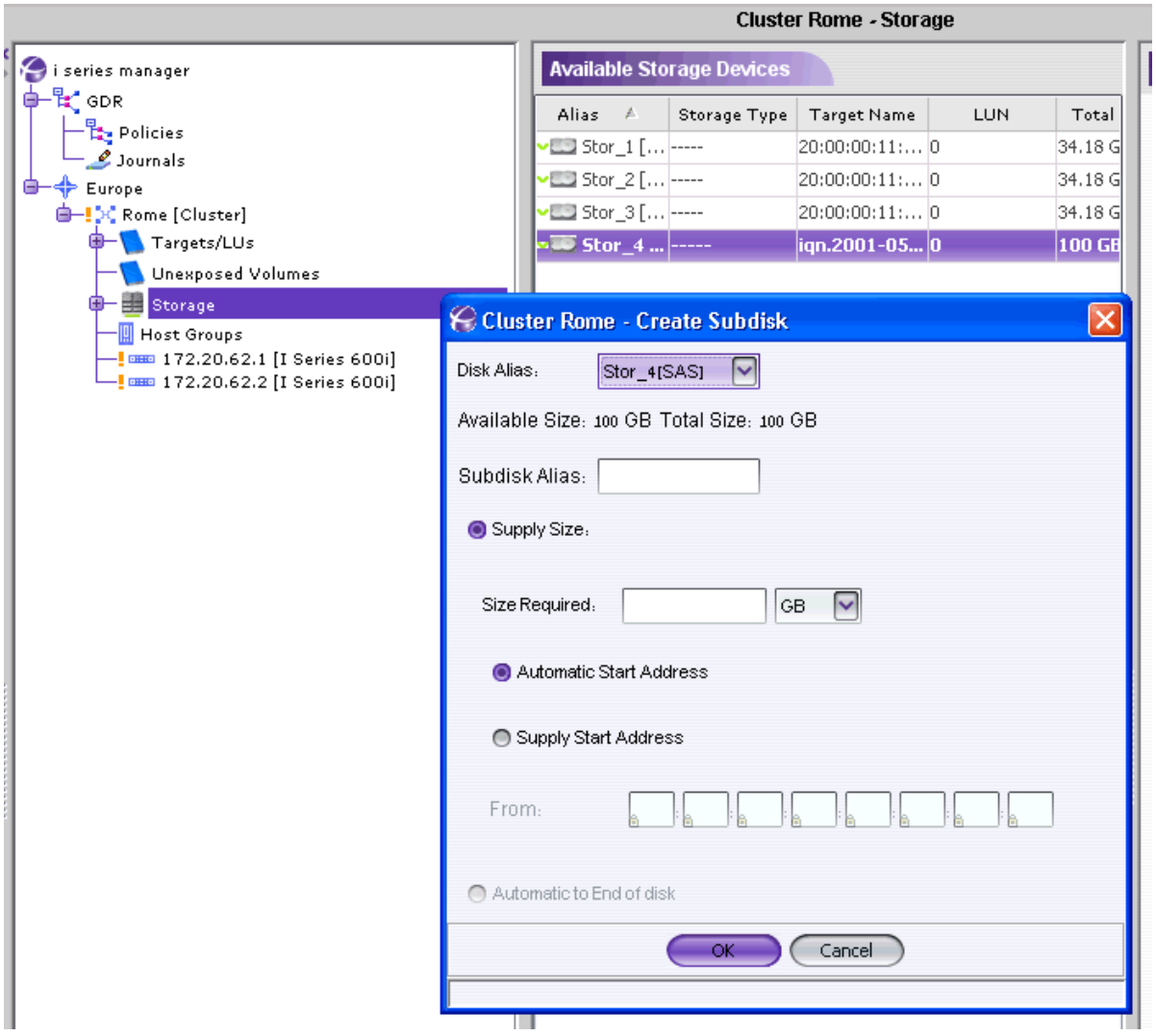
3. Enter the **Subdisk Alias**. If no alias is entered, i series manager will provide a default alias.

4. Enter the **Size Required** for the subdisk required in MB, GB or TB.

   Select the **Starting Address** for the subdisk by checking either **Automatic Start Address** or **Supply Start Address** (and enter starting address).

   By selecting Supply Start Address, you must enter the start address in hexadecimal form in the Start Address field. The next available start address for subdisks side by side is the first subdisk end address plus disk block size.

> **Note:**
> *By selecting **Automatic Start Address**, i series manager will choose the smallest available space to start for your subdisk.*



5. Click **OK**.

   The disk in the Subdisk Details pane is repartitioned to include the new subdisk (Figure 4-12). For each subdisk, the following information is listed (next to the graphical representation of the partition): subdisk alias, size of the subdisk and its relative percentage of the disk.

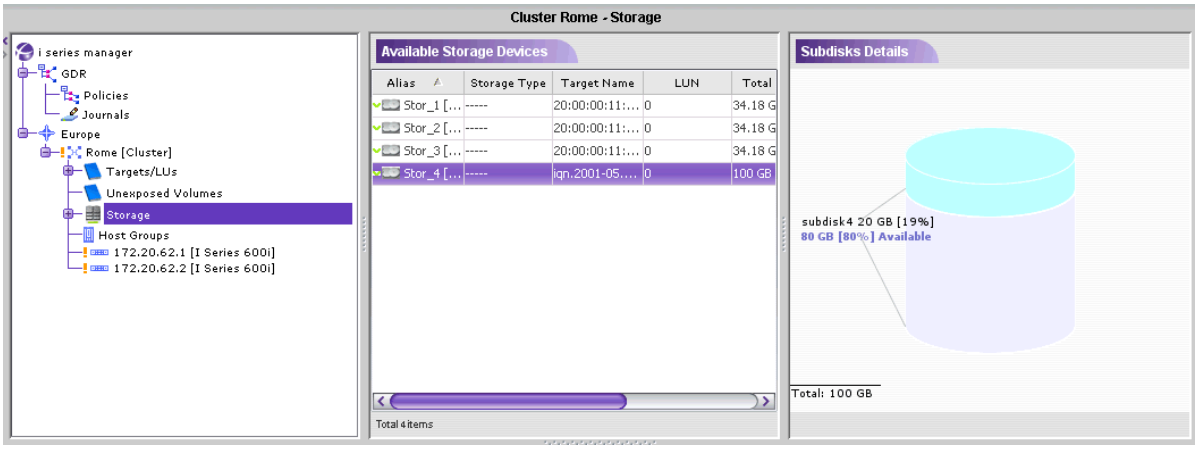



*Figure 4-12. New Subdisk (Subdisks Details Pane)*

## Volume Exposure & Targets

Every volume that is exposed is connected to a target. When exposing volumes, you can create a new target or use an existing one. Basically there are two things you can do:

- Expose a volume by creating a new target for it.
- Expose a volume by using an existing target.

### *Exposing Volumes and Creating a New Target*

***To expose a volume and create a new target:***

1. From the Create Volume window, select the volume to expose.
2. Click Expose .

   The Expose Volume dialog box opens.

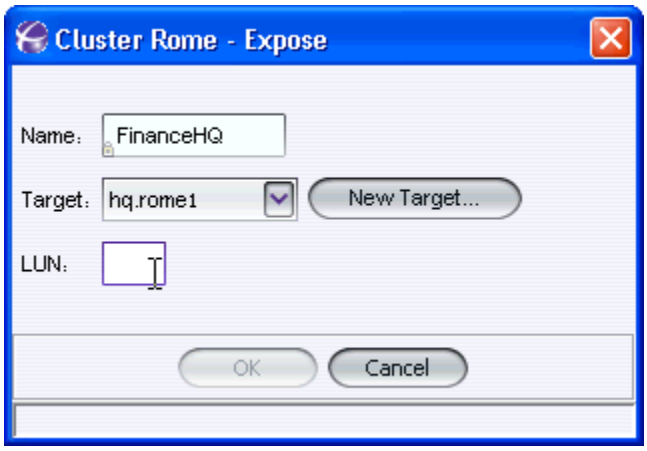



*Figure 4-13. Expose Volume*

3. From the Expose Volume dialog box, click New Target.

   The New Target dialog box opens.


*Figure 4-14. New Target*

4. Enter the Target Alias and Target Name (target WWUI).
5. Select value for i series Exposed on (the i series on which to expose the target).
6. Select the Default Access rights for the target. Choose from Read/Write (RW), Read Only (RO) or Not Available (N/A). The default is RW.

**Note:**
*A target alias is an internal identifier and can be modified later.*

- A target name is the WWUI of the target and for external use when connecting to an initiator and cannot be modified.
- A target name must be in lower case letters.
- A target alias and name can be the same.

7. Click **OK**.

   The New Target dialog box closes and the new target appears in the Expose Volume dialog box (Figure 4-15).

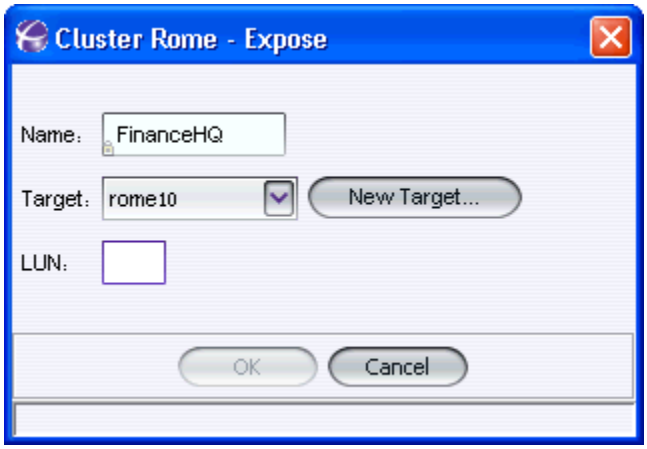



*Figure 4-15. New Target Listed in Expose Volume Dialog Box*

8. Assign a LUN and click **OK**. The LUN can be any value between 0 and 255.

   The exposed volume disappears from the Create Volume window and appears under Targets/LUs in the navigation pane (Figure 4-16). The attached volume is now exposed on the target to all initiators as a read-write volume. To Restrict refer to ***Volume Security***.

9. Targets without attached volumes are indicated by a blue exclamation mark on the left of the target name.
10. Targets with an attached volume are indicated by a green check mark on the left of the target name.

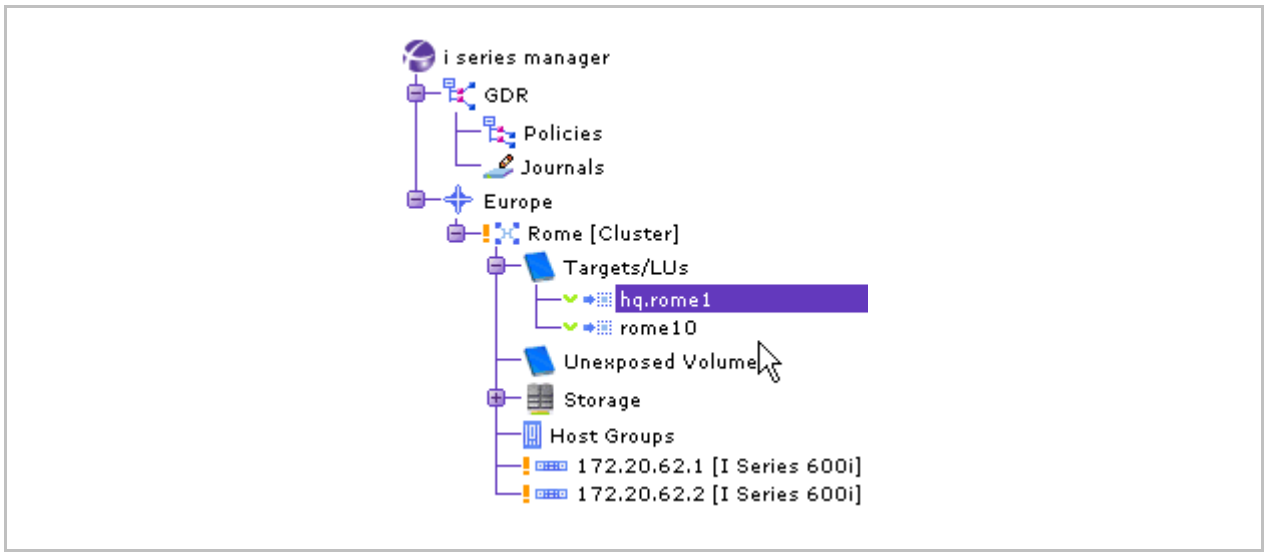



*Figure 4-16. New Target Listed in Navigation Pane*

## Creating a New Stand-Alone Target

**Note:**

*Targets can be created without a volume associated with it. These targets will have no initial associated LUNs and will not be exposed to hosts when first created.*

***To create a new stand-alone target:***

1. From the Navigation pane, right click the desired Cluster and select **New** > **Target…**

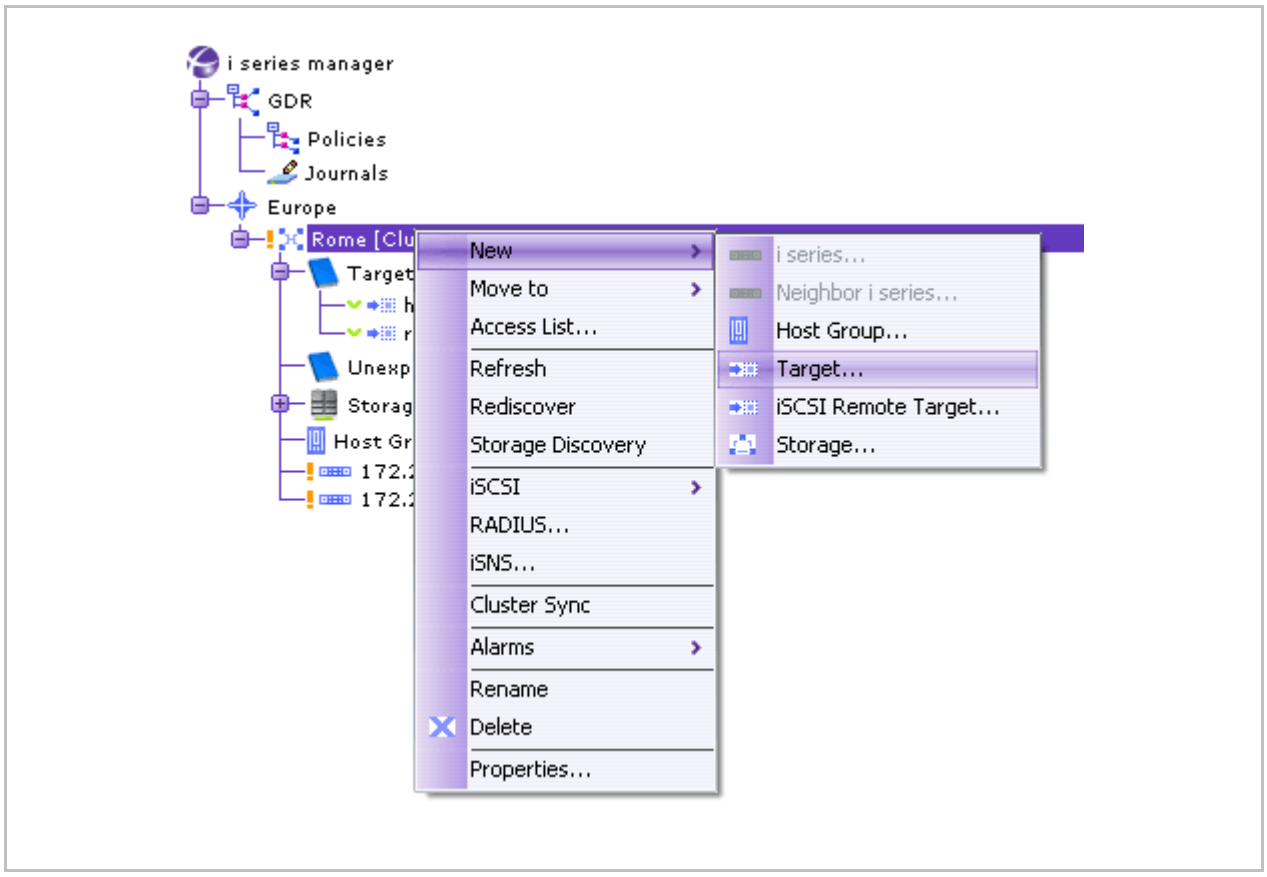



*Figure 4-17. Create New Target*

2. Enter the Target Alias and Target Name (target WWUI).
3. Select value for i series Exposed on (the i series on which to expose the target).
4. Select the Default Access rights for the target. Choose from Read/Write (RW), Read Only (RO) or Not Available (N/A). The default is RW.

**Note:**

- A target alias is an internal identifier and can be modified later.
- A target name is the WWUI of the target and for external use when connecting to an initiator and cannot be modified.
- A target name must be in lower case letters.
- A target alias and name can be the same.


*Figure 4-18. New Target Alias and Name*

5. Click **OK**.

   The new target is listed under Exposed Volumes in the Navigation pane. The target is displayed by its alias. Move the mouse over the alias to display the target name and exposing i series.

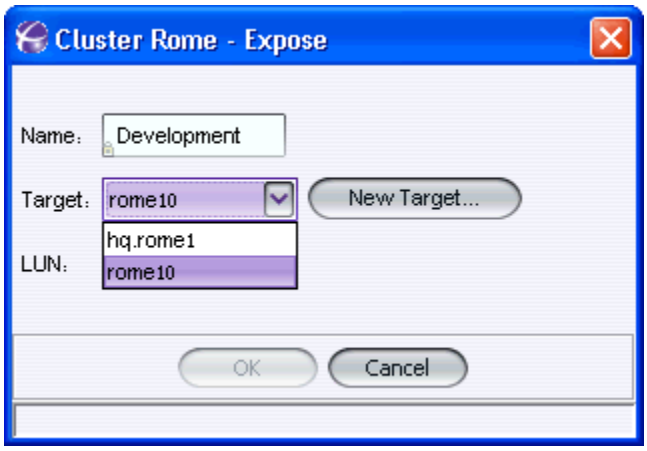



*Figure 4-19. New Target in Navigation Pane*

## Exposing Volumes on Existing Targets

***To expose a volume on existing targets:***

1. From the Create Volume window (Figure 4-10), select the volume to expose, and click Expose .

   The Expose Volume dialog box opens.

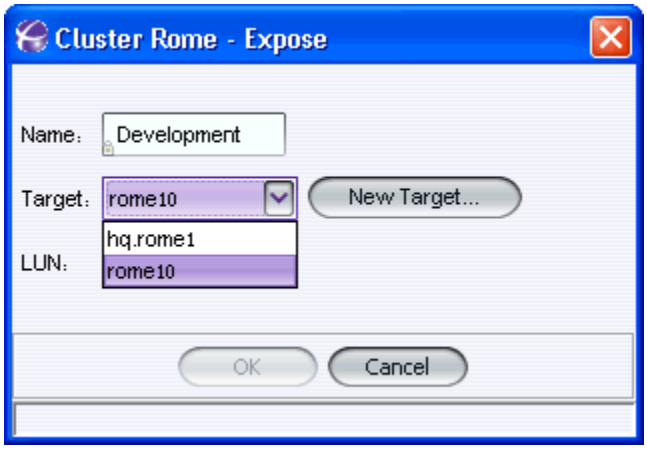



*Figure 4-20. Expose Volume*

2. Select an existing Target from the list.
3. Assign a LUN for the target. The LUN should be unique for a specific target.
4. Click **OK**.

**Note:**

- A LUN value is any number between 0 and 255.
- A snapshot volume must be exposed on the same i series as the source volume.

## *Modifying & Displaying Target Properties*

You can modify/display some target properties.

### *To modify or display target properties*

1. In the Navigation pane, select the target.
2. Right click on the target and select **Properties...**

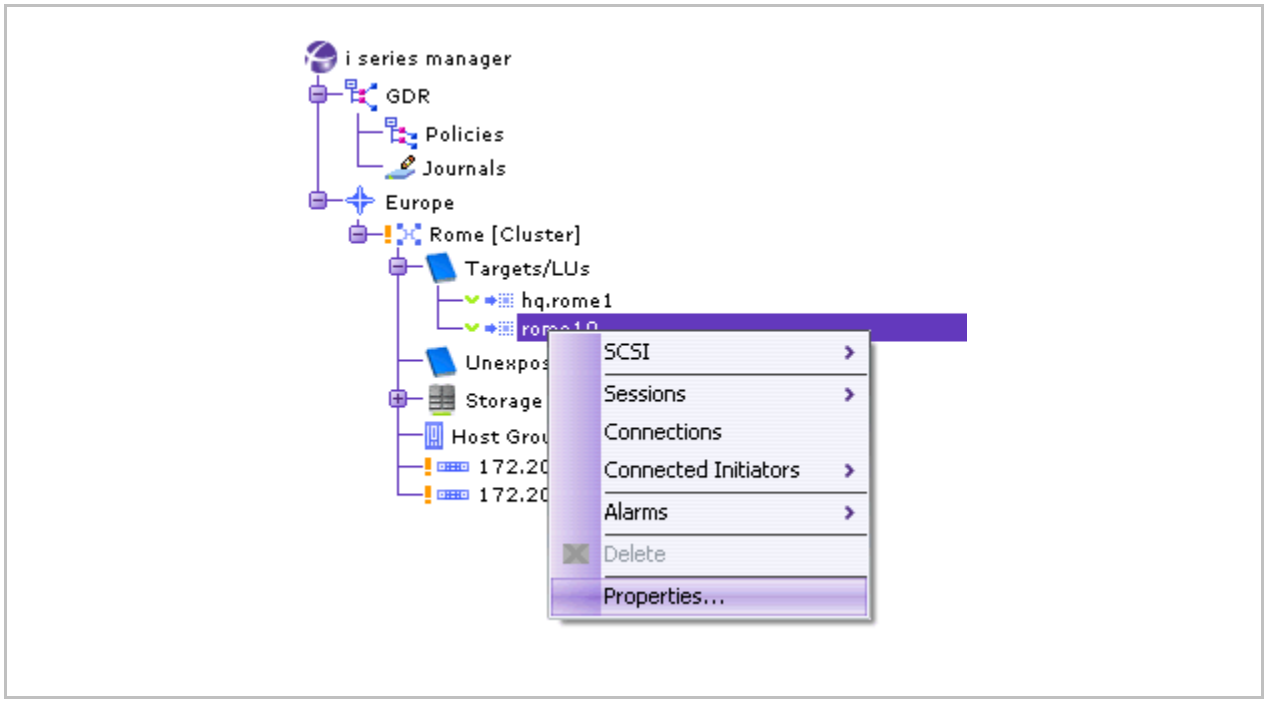



*Figure 4-21. Target Properties*

The Target Properties dialog box opens (Figure 4-22).

You may edit the following target properties.

- **Target Alias,** i series **Exposed**, **Default Access** (General tab)
- **User Name, Password** (Authentication tab)

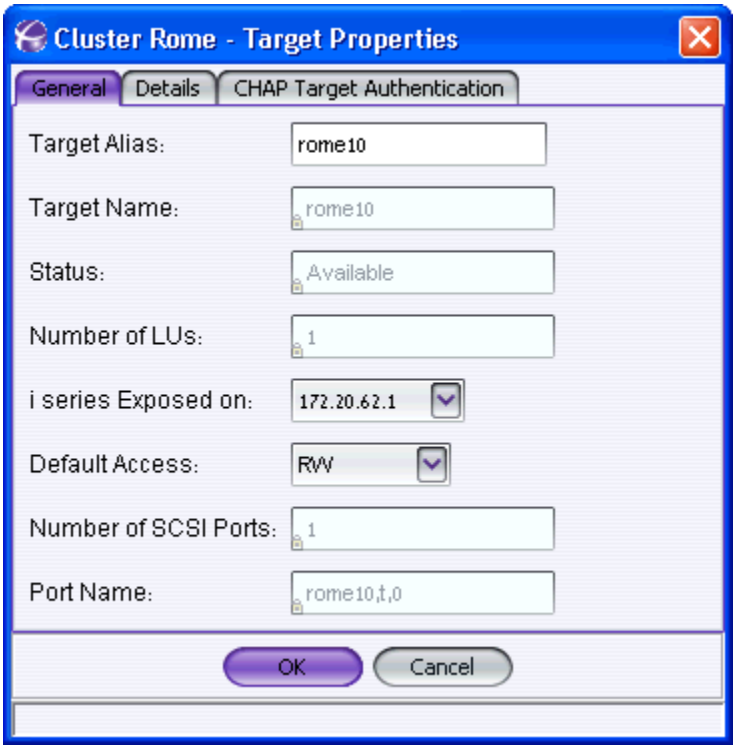



*Figure 4-22. Target Properties – General Tab*

*Table 4-1. General Target Properties*

| Parameter | Description |
|---|---|
| Target **Alias** | User-given alias for target |
| Target Name | WWUI of target |
| Status | Status of target |
| Number of LUs | Number of LUs associated with the target |
| i series Exposed On | i series on which the target and its attached LUs are exposed |
| Default Access | Default Access to the target<br>RW – read-write<br>RO – read only<br>NA – no access |
| Number of SCSI ports | Number of SCSI ports on i series |
| Port Name | target port name |

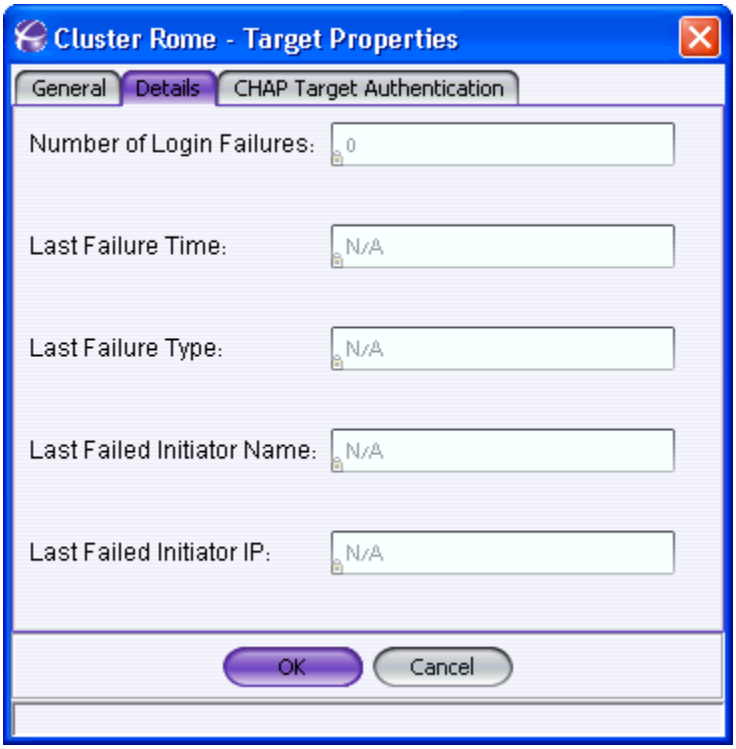



*Figure 4-23. Target Properties – Details Tab*

*Table 4-2. Target Details*

| Parameter | Description |
|---|---|
| Number of Login Failures | Number of Login attempts that failed |
| Last Failure Time | Time of last failed login attempt |
| Last Failure Type | Type of login failure<br>options: other; redirect; authorize; authenticate; negotiate |
| Last Failed Initiator Name | Name of last initiator that failed to login |
| Last Failed Initiator IP | IP address of last initiator that failed to login |

***To configure target authentication parameters for iSCSI initiators:***

1. In the Navigation pane, right click on the target and select Properties (Figure 4-21).

   The Target Properties dialog box appears.

2. Select the authentication tab (Figure 4-24).
3. Enter the desired User Name and Password.
4. Click **OK**.

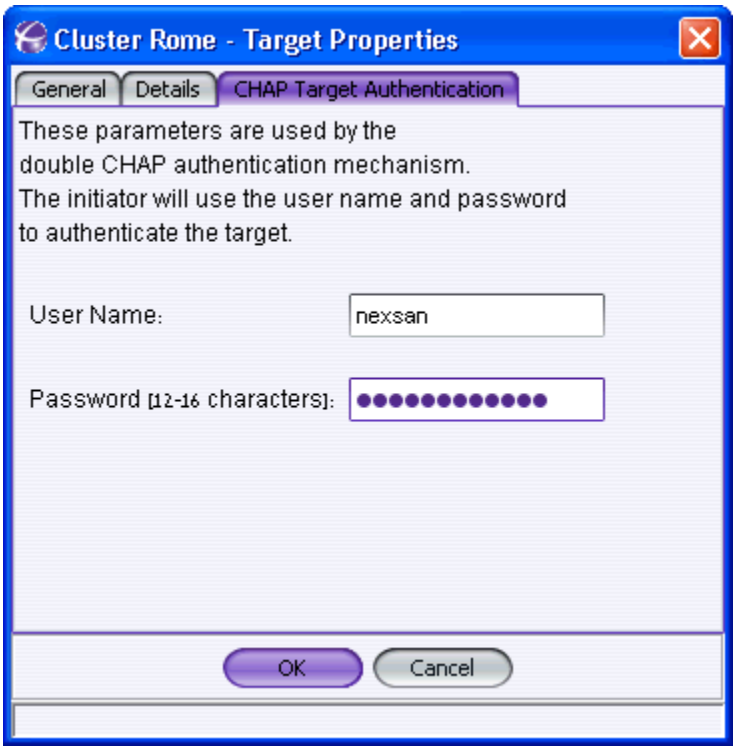



*Figure 4-24. Target Properties – Authentication Tab*

**Note:**
*If no password is provided, no target authentication properties are applied. Passwords must be 12-16 character in length.*

## Advanced Volume Creation

Advanced volume operations are performed from the Advanced Volume Creation window (Figure 4-26).

***Access the Advanced Volume Operations window as follows:***

1. From the i series manager menubar:
   **Configure > Advanced Volume Operations**

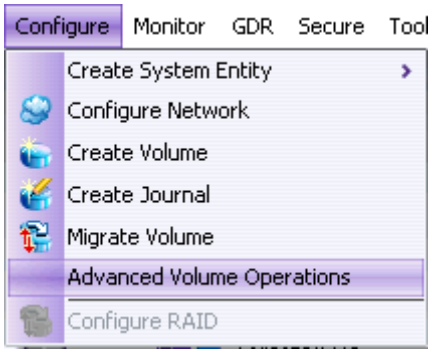



*Figure 4-25. Accessing Advanced Volume Operations*

The Advanced Volume Creation window appears.

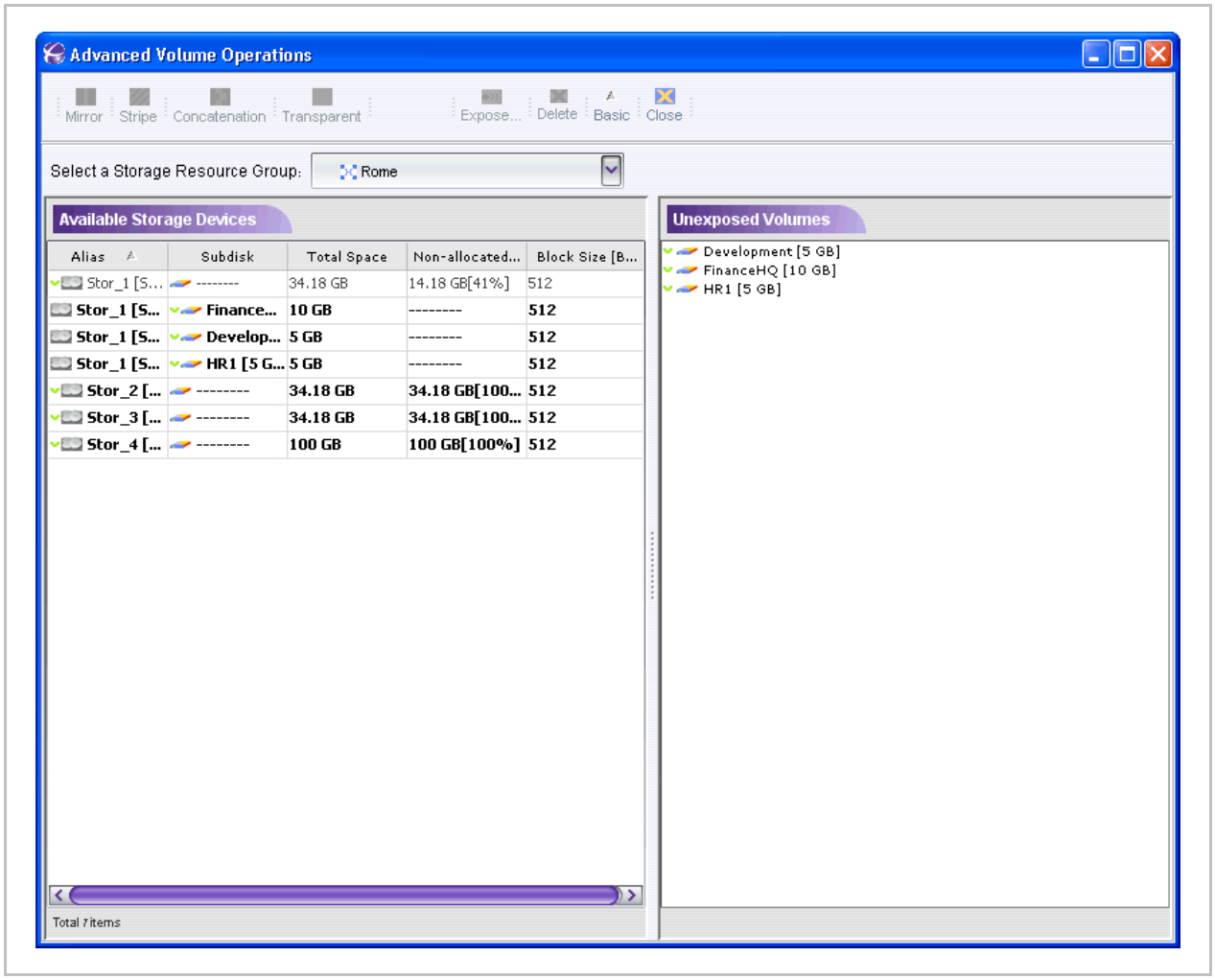



*Figure 4-26. Advanced Volume Creation*

## Creating Concatenated Volumes

You can concatenate volumes across storage devices to create larger virtual volumes. Concatenated volume can be created from any two (or more) disks or subdisks of equal block size.

### To concatenate volumes:

1. Navigate to the Advanced Volume Creation window (Figure 4-26).
2. Using the Ctrl key select all the subdisks (children) to use for the concatenated volume (Figure 4-27).

**Note:**
*The disks/subdisks must be of the same block size.*

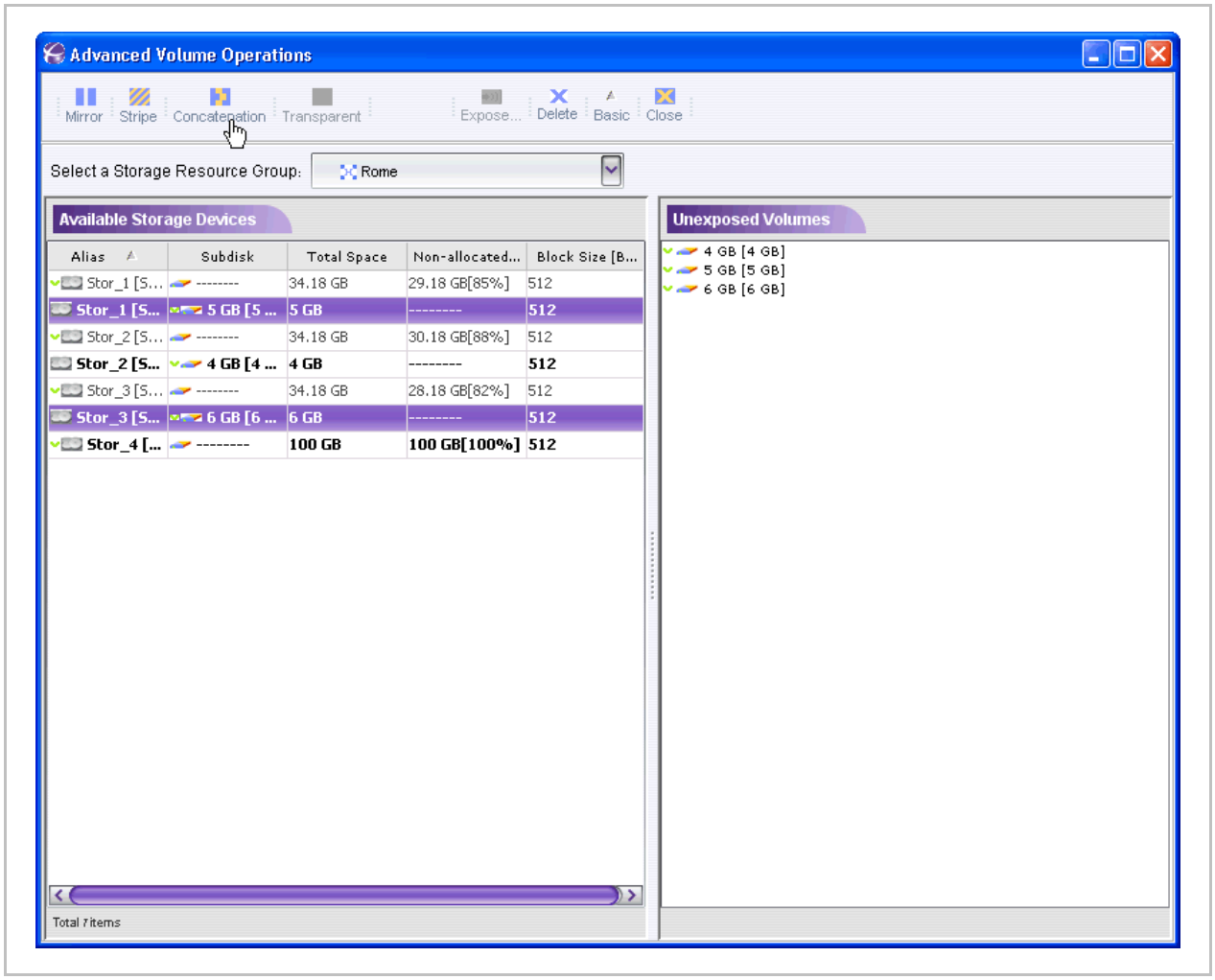



*Figure 4-27. Subdisks Selected*

3. Click Concatenation icon to create the concatenated volume.

   The New Volume dialog box opens (Figure 4-28).

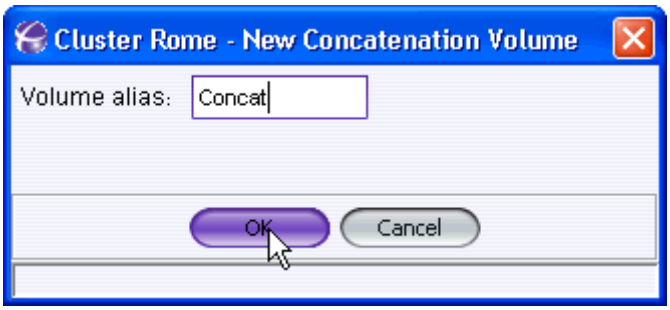



*Figure 4-28. New Volume*

4. Enter the Volume Alias of the concatenated volume. If no alias is entered, a default alias will be assigned.
5. Click **OK**.

   The concatenated volume appears in the right pane of the Create Volume window (Figure 4-29). The blue exclamation mark signifies that the volume is internal (not exposed to hosts).

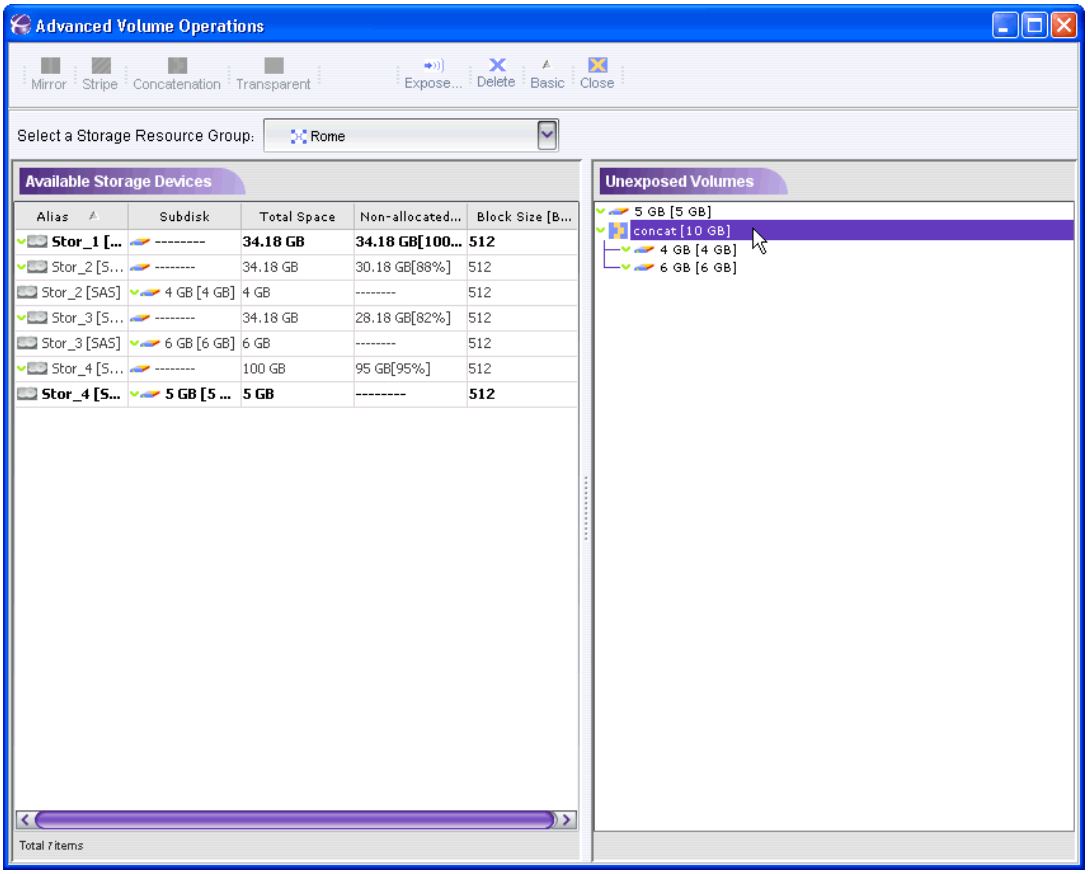



*Figure 4-29. Concatenated Volume*

## Creating Mirrored Volumes

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

> **Note:**
> *Mirrored volumes should be located on different physical disks.*

### To create a mirrored volume:

1. Navigate to the Advanced Volume Creation window (Figure 4-26).
2. Using the Ctrl key select the subdisks (children) (Figure 4-30) to use for the mirrored volume.

**Note:**
*The disks/subdisks/volumes must be of the same block size.*

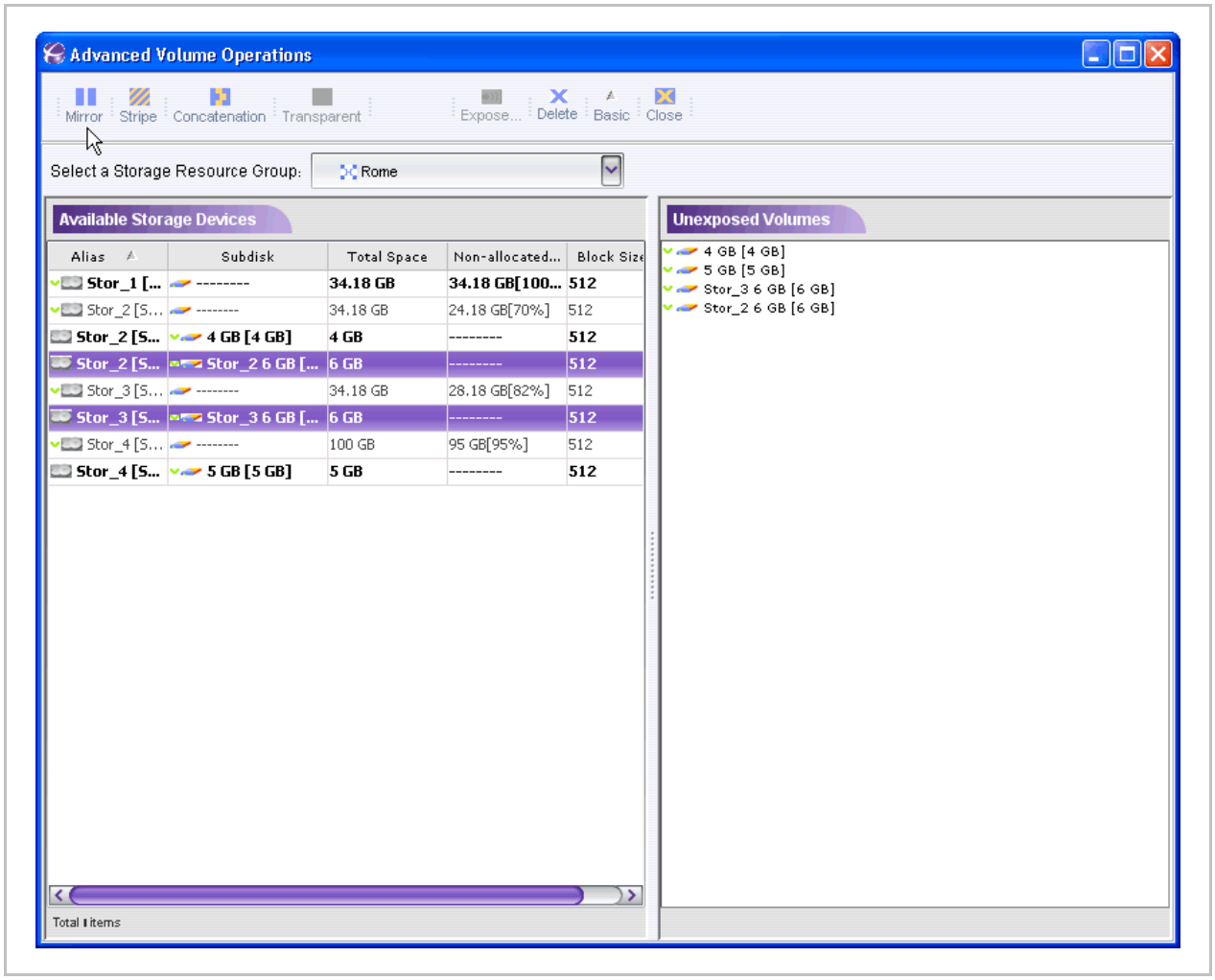



*Figure 4-30. Subdisks Selected for Mirror*

3. Click the Mirror icon to create the mirrored volume.

   The New Mirror Volume dialog box opens.


*Figure 4-31. New Mirror*

4. Enter the **volume alias** of the mirrored volume. If no alias is entered, a default alias will be assigned.
5. Click **OK**.

   The mirrored volume appears in the right pane of the Create Volume window (Figure 4-29). The blue exclamation mark next to the mirror icon signifies that the volume is internal (not exposed to hosts).

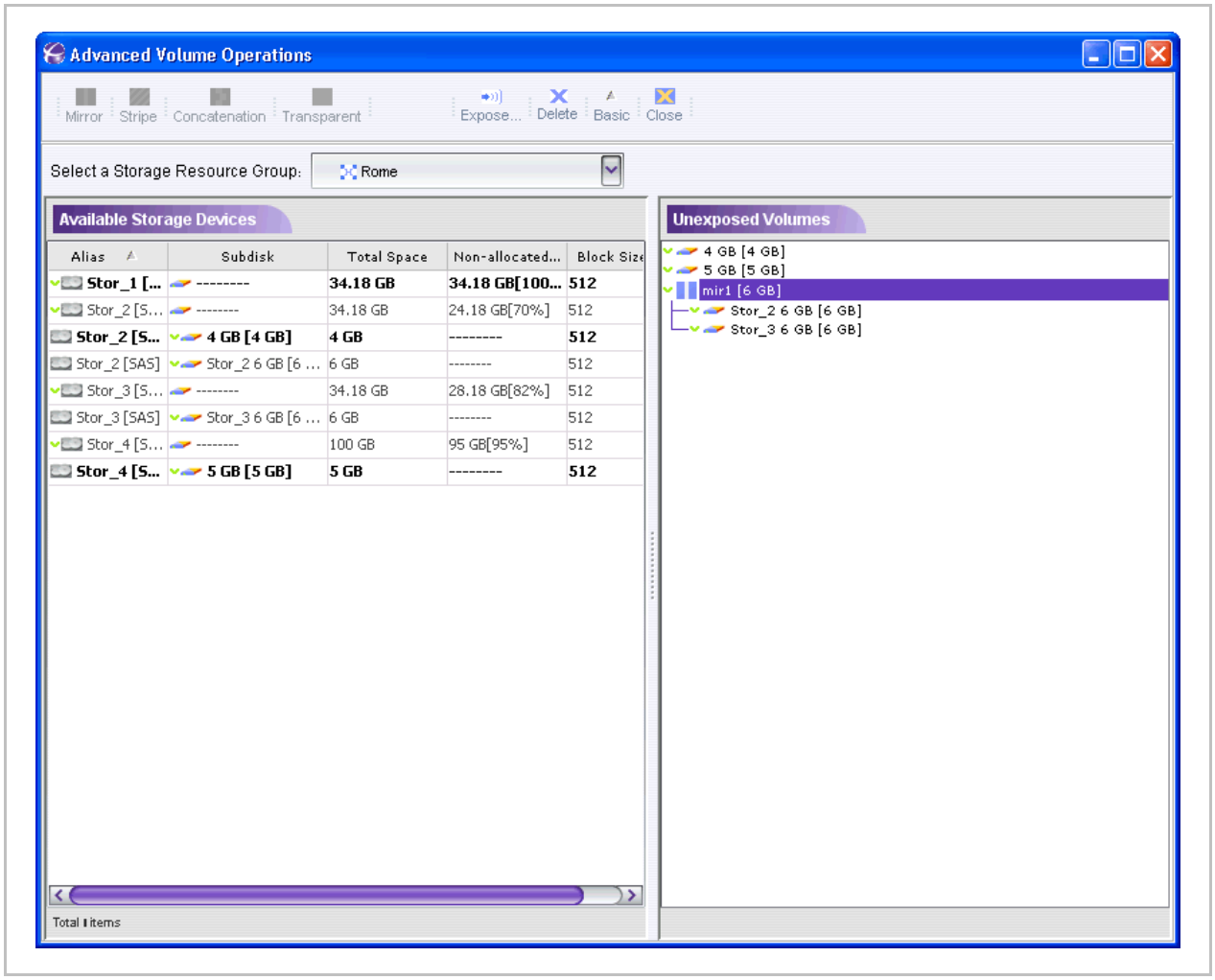



*Figure 4-32. Mirrored Volume*

## Creating Striped Volumes

A striped volume has data written equitably across two or more disks to provide higher read/write rates. Throughput increases with the number of disks within a striped volume.

> **Note:**
> *Children volumes within a striped volume need to be on different disks/RAID sets to realize the benefits of striping.*

Create a striped volume using two or more disks/subdisks/volumes of the same size and block size. A striped volume has a ***stripe unit size.*** The stripe unit size is the size of the data chunk read/written on each of the stripe's children.

### *To create a striped volume:*

1. Navigate to the Advanced Volume Creation window (Figure 4-26).
2. Using the Ctrl key select the subdisks (children) (Figure 4-33) to use for the striped volume.

> **Note:**
> *The disks/subdisks must be of the same block size.*

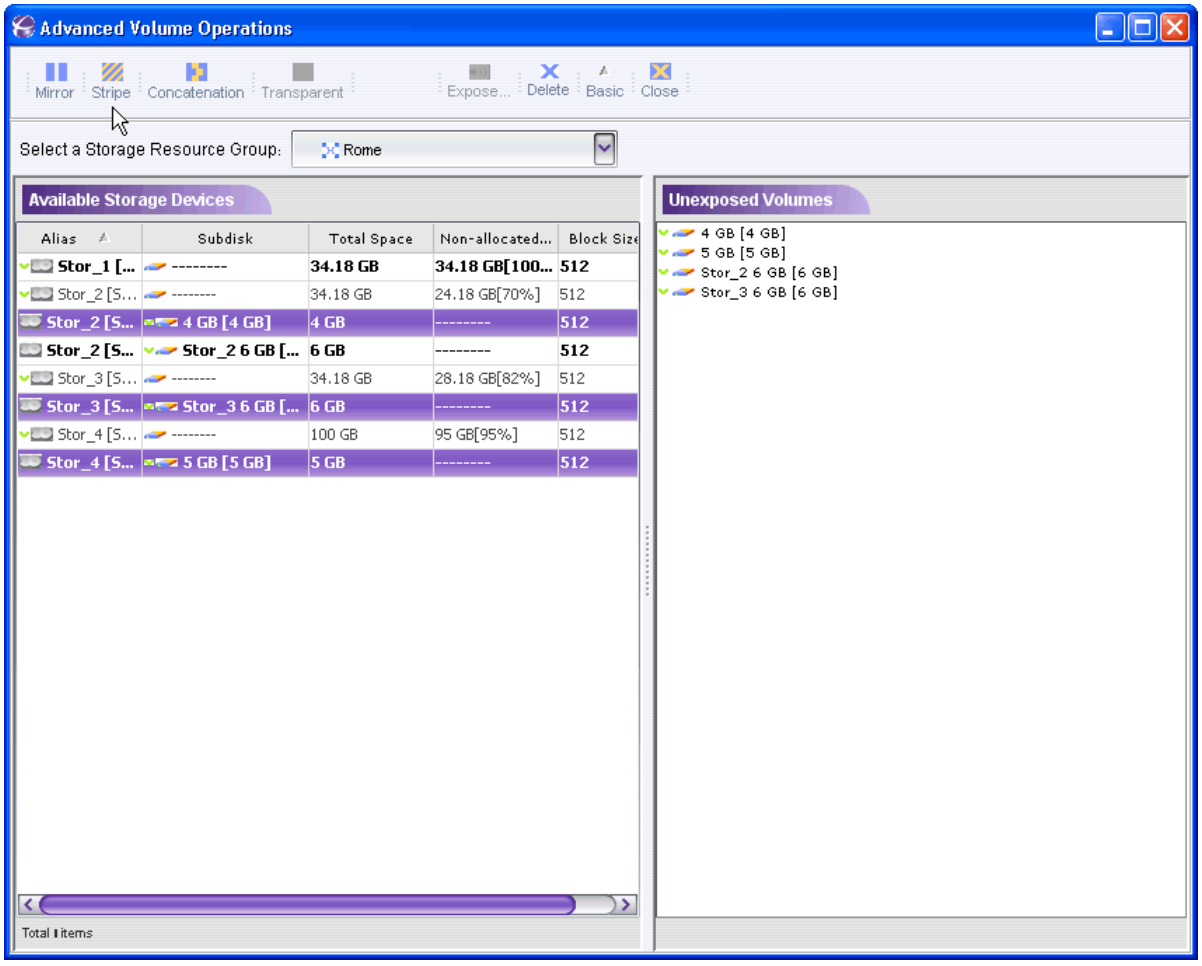



*Figure 4-33. Subdisks Selected for Stripe*

3. Click the Stripe icon to create the striped volume.

   The New Stripe Volume dialog box opens (Figure 4-34).


*Figure 4-34. New Stripe*

4. Enter the Stripe Unit Size to use in creating the striped volume.
5. Enter the Volume Alias of the striped volume. If no alias is entered, a default alias will be assigned.
6. Click **OK**.

   The striped volume appears in the right pane of the Create Volume window (Figure 4-35). The blue exclamation mark next to the striped volume icon signifies that the volume is internal (not exposed to hosts). As the subdisks are incorporated into the striped volume, the green check marks to the left of the subdisk name change to blue exclamation marks.

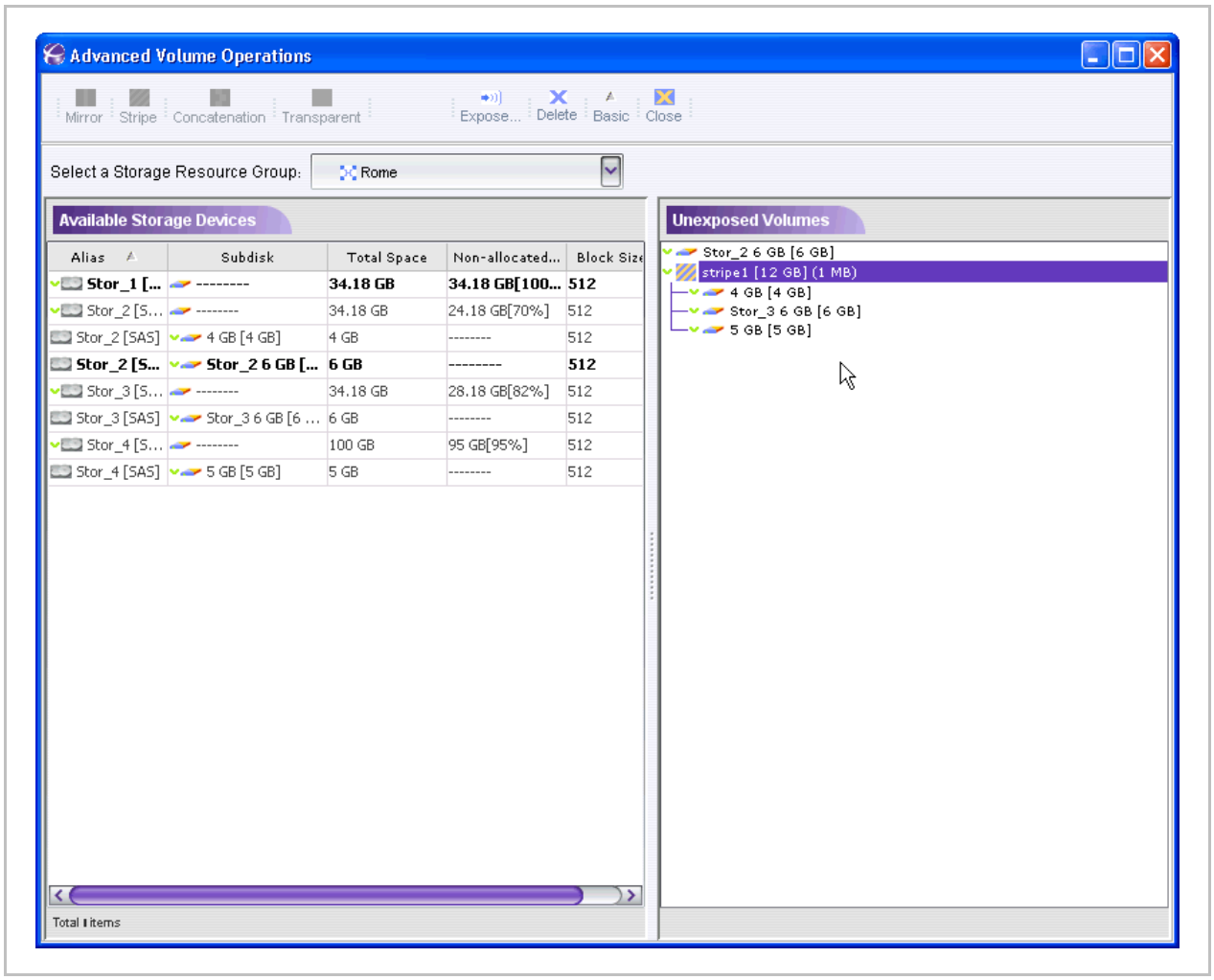



*Figure 4-35. Striped Volume*

## *Transparent Volumes*

You can create a transparent volume from a disk/tape resource for direct exposure.

**Note:**
*Transparent volumes are mainly used for connecting tape devices to the i series.*

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

**Notes:**

- Only a full, not partitioned disk can be used to create a transparent volume.
- Unlike all other types of volumes, Transparent volumes cannot be used in further volume hierarchies.
- Transparent volume must maintain the physical LUN number of the physical disk it was configured on.
- You cannot define ACL for transparent volumes. It is always R/W.
- Unexposing a transparent volume (deleting LU) will automatically delete the volume.

***To create a transparent volume:***

1. Navigate to the Advanced Volume Creation window (Figure 4-26).
2. Select the disk to use for the transparent volume.

   The Transparent icon is now available.
3. Click the Transparent icon to create new transparent volume.

   The New Transparent Volume dialog box opens.

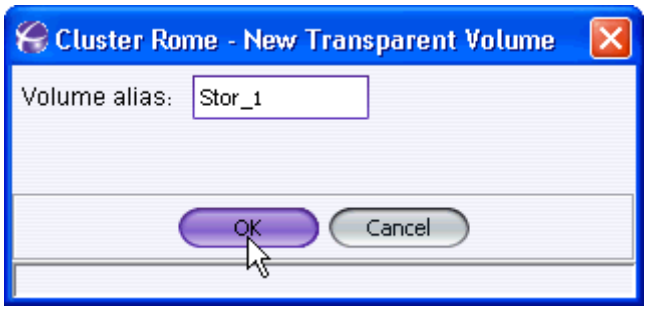



*Figure 4-36. New Transparent Volume Dialog Box*

4. Enter the Volume Alias of the transparent volume. Note: If you leave the alias blank, the system will assign the disk alias.
5. Click **OK**.

   The transparent volume appears in the right pane of the Create Volume window. The blue exclamation mark next to the transparent icon signifies that the volume is internal (not exposed to hosts).

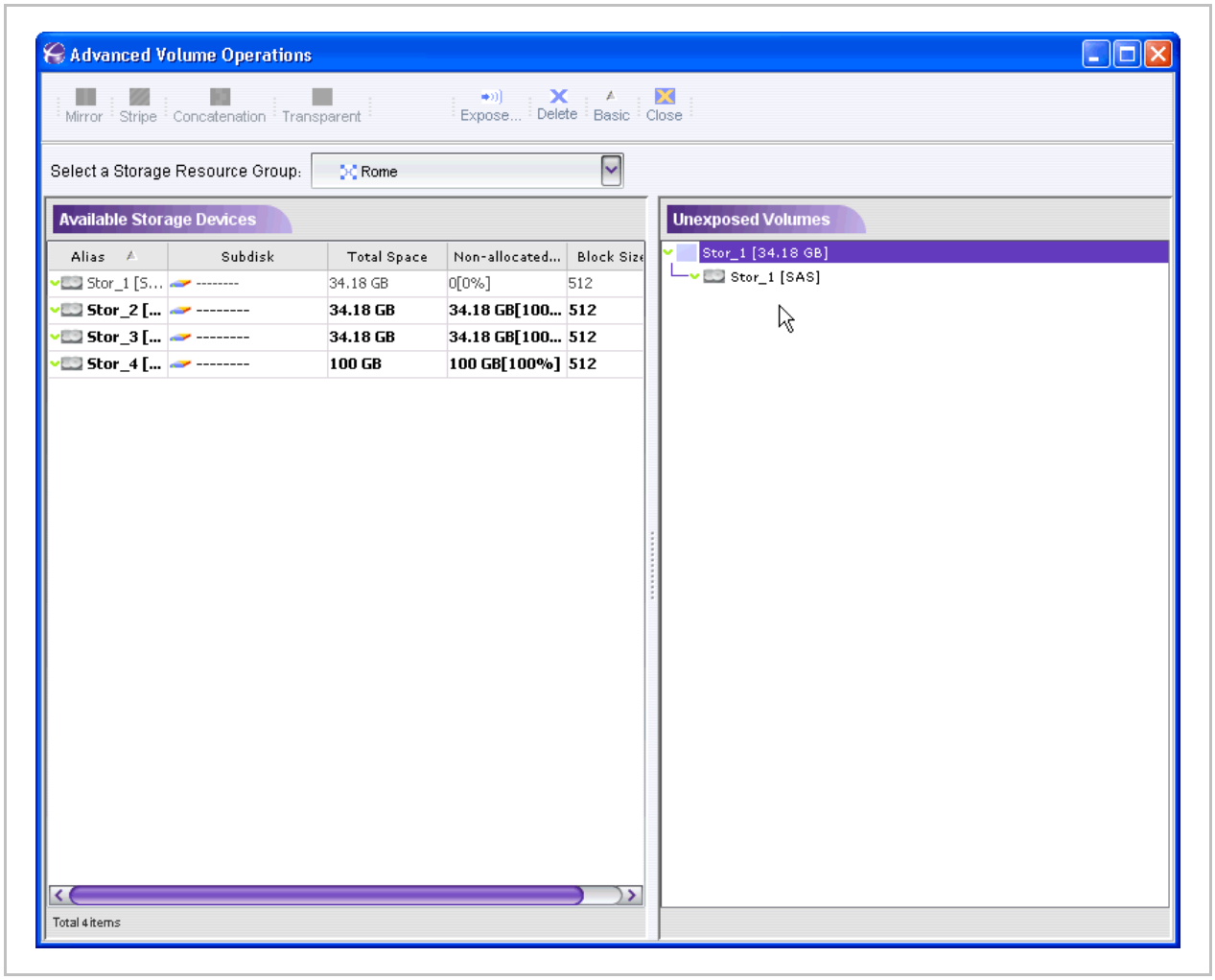



*Figure 4-37. Transparent Volume*

## Creating a Mirror over Striped Volumes

**Note:**

- All striped or mirrored volumes in the ground level hierarchy must be the same size.
- All volumes in a hierarchy must have the same block size.

### To create a mirror over striped volume:

1. Select the Stripe children (Figure 4-38).

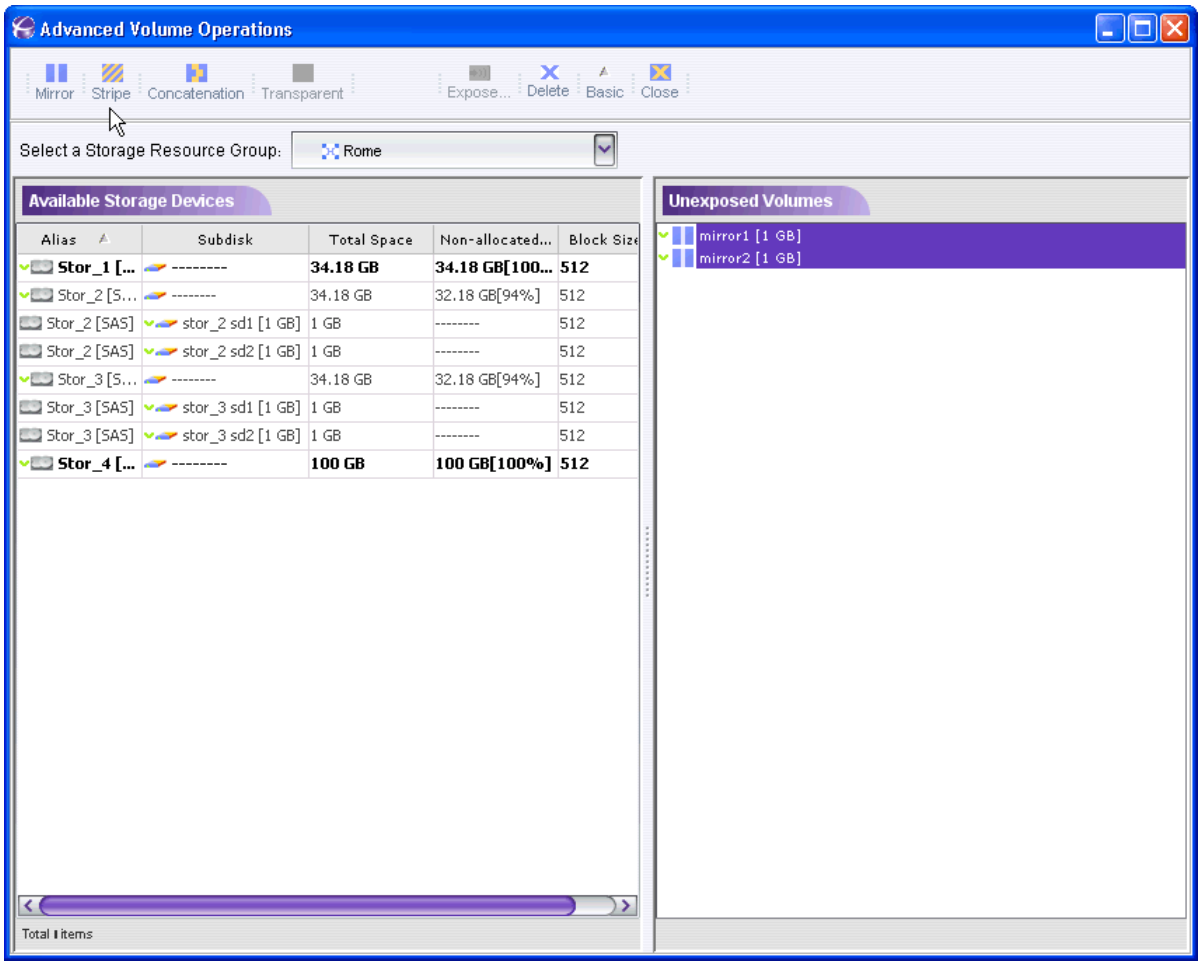



*Figure 4-38. Striped Volumes Selected*

2. Click the Mirror icon to create the mirrored volume.

The New Mirror Volume dialog box opens.

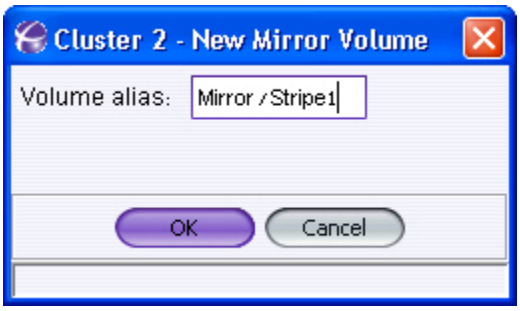



*Figure 4-39. New Mirror Volume*

3. Enter the Volume Alias for the mirrored volume. If no alias is entered, a default alias will be assigned.
4. Click **OK**.

   The new mirrored volume appears in the Unexposed Volumes pane (Figure 4-40).

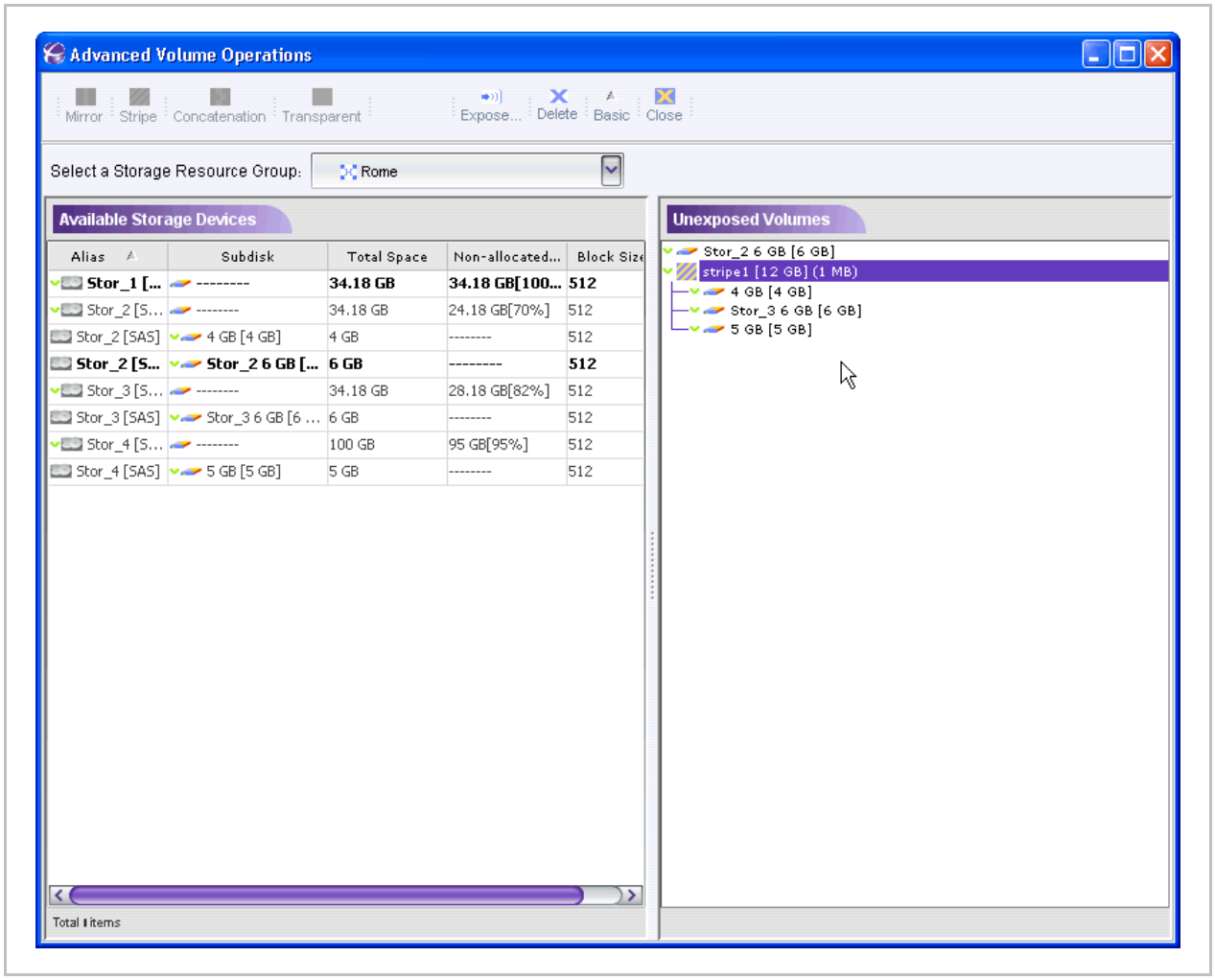



*Figure 4-40. Mirror over Stripe*

## Creating a Stripe over Mirrored Volumes

**Notes:**

- All striped or mirrored volumes in the ground level hierarchy must be the same size.
- All volumes in a hierarchy must have the same block size.

### To create a stripe over mirrored volume:

1. Select the Mirror children (Figure 4-41).

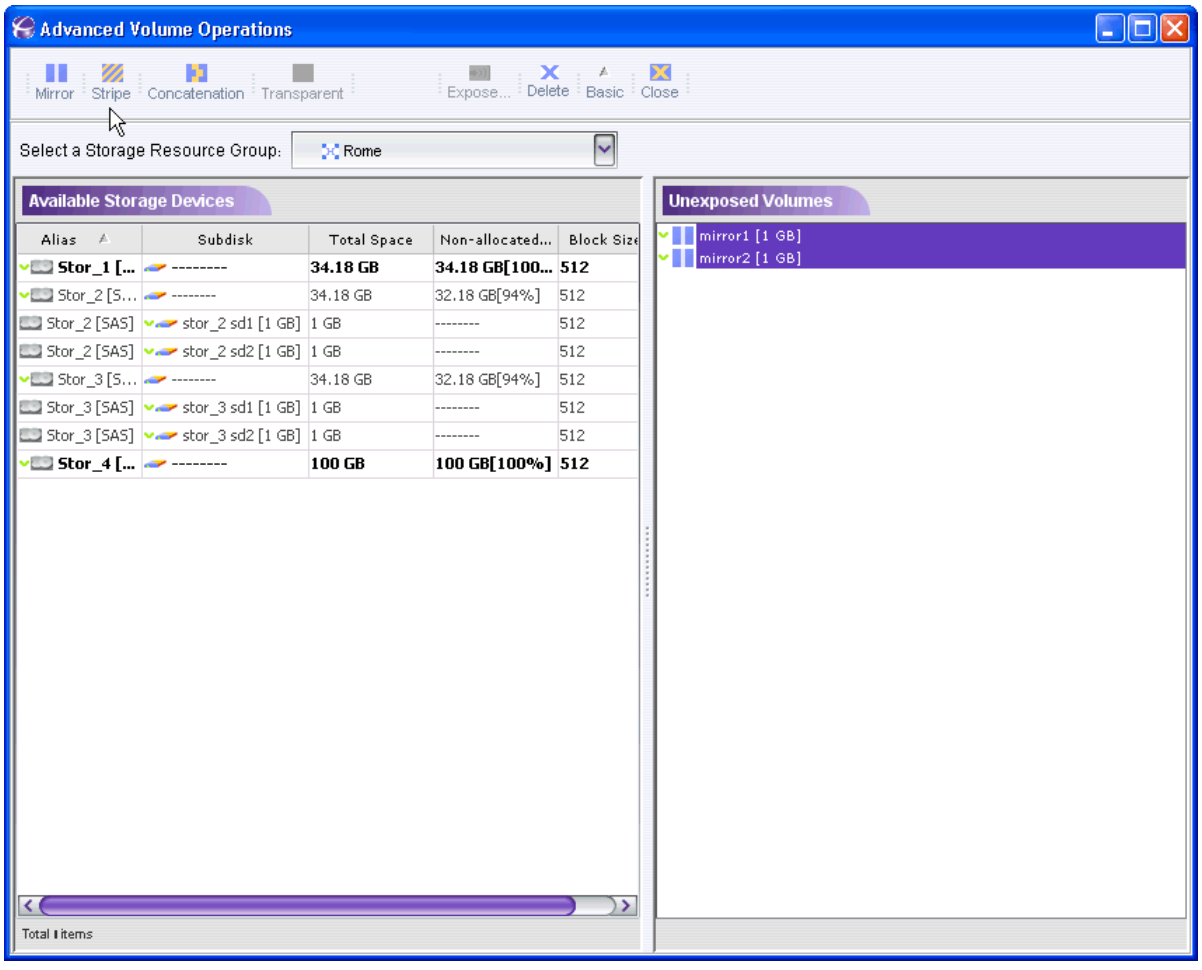



*Figure 4-41. Mirrored Volumes Selected*

2. Click the Stripe icon to create the mirrored volume.

   The New Stripe Volume dialog box opens.

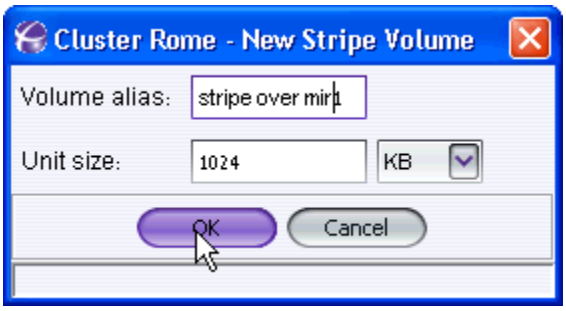



*Figure 4-42. New Stripe Volume*

3. Enter the Volume Alias of the striped volume. If no alias is entered, a default alias will be assigned.
4. Click **OK**.

   The new striped volume appears in the Unexposed Volumes pane (Figure 4-43).

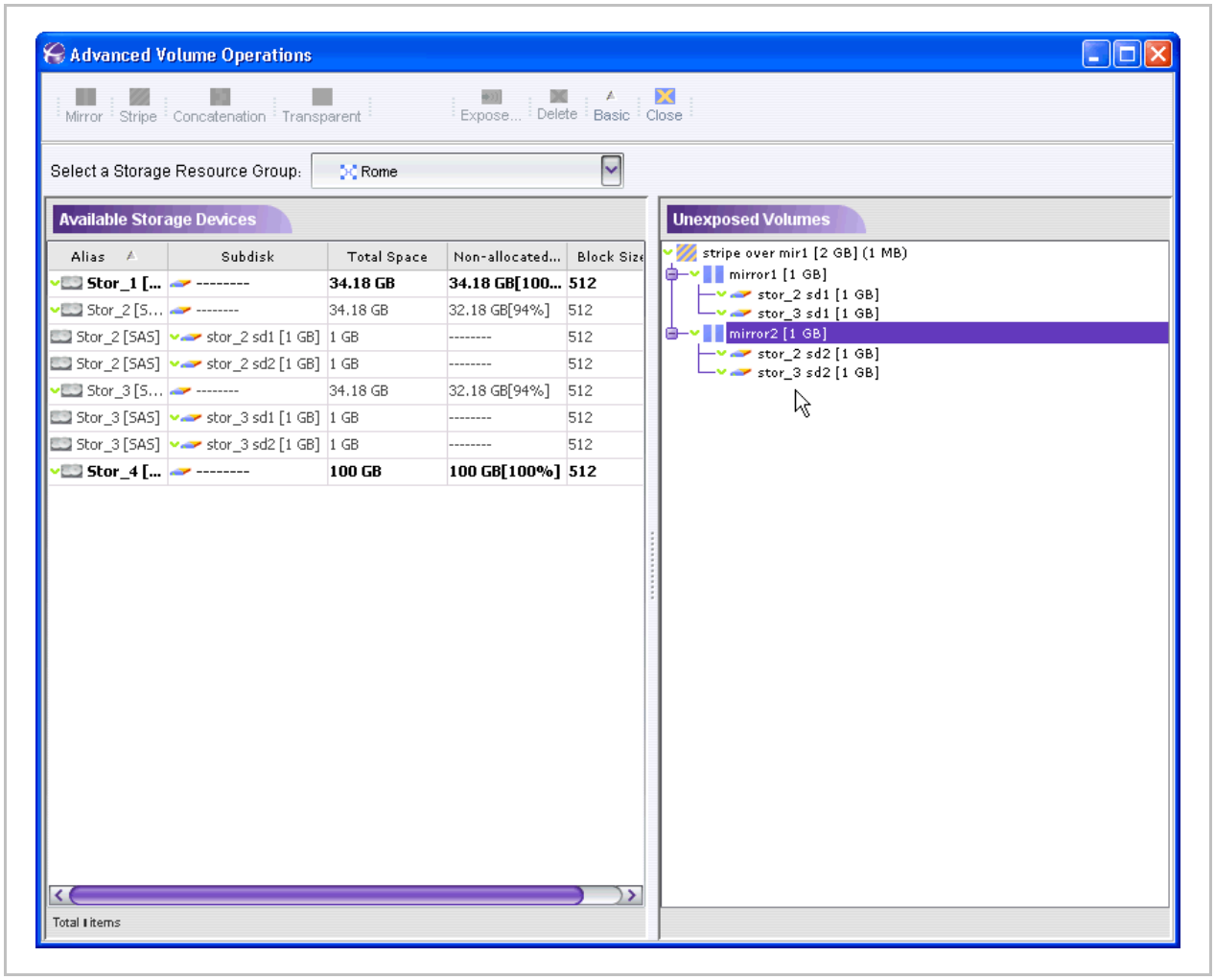



*Figure 4-43. Stripe over Mirror*

## Displaying Volume Hierarchies

You can display exposed and unexposed volume hierarchies. The hierarchy levels are displayed from the volume children down to the storage device level.

### To display a volume hierarchy:

1. Navigate to the Advanced Volume Creation window (Figure 4-26).
2. Double click on the selected volume.

   The first level opens under the top level volume.

3. To view subsequent layers, double click on the volume children until the desired hierarchy level. The hierarchy can be opened to the storage device or subdisk level.

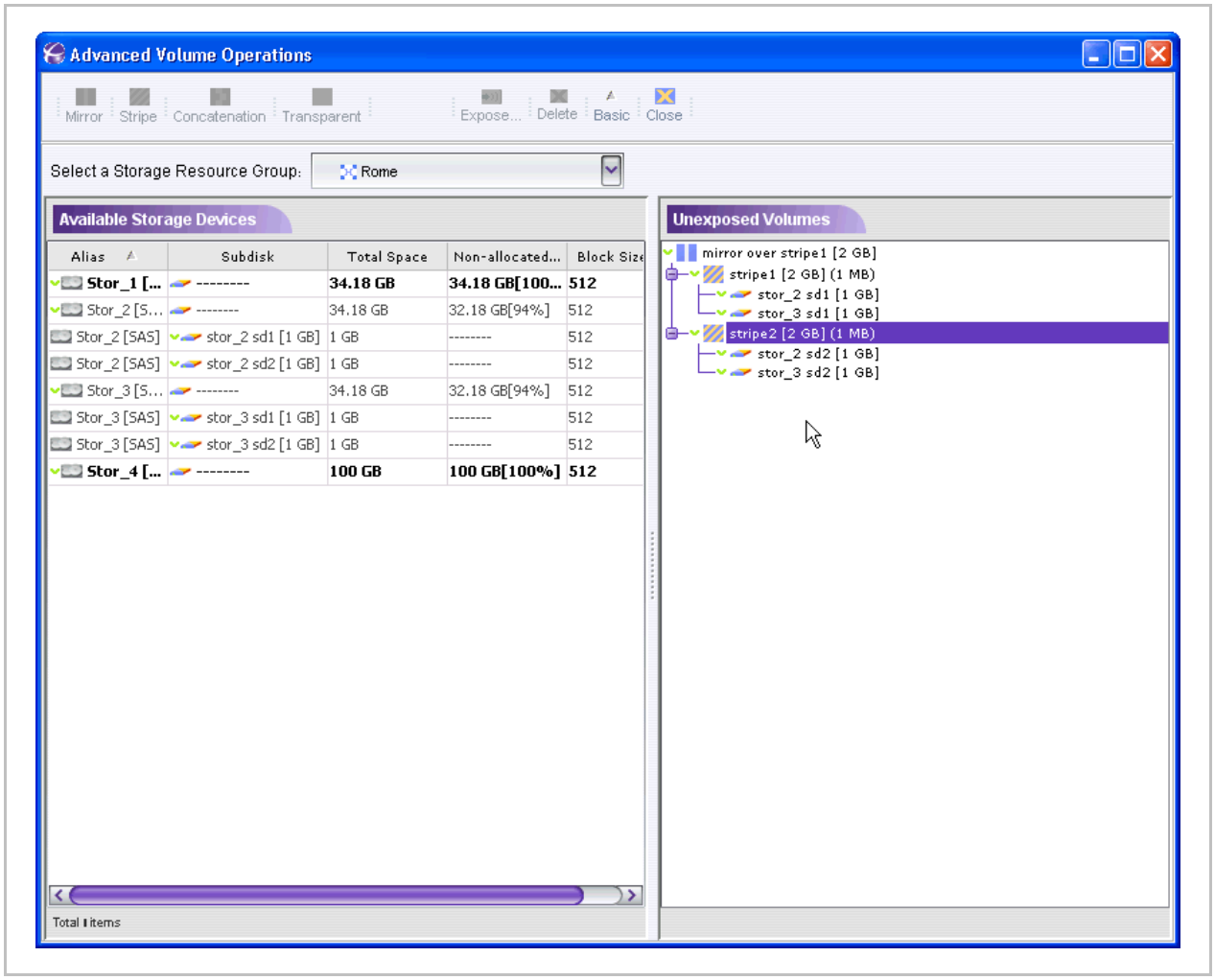



*Figure 4-44. Expanded Hierarchy*

# Volume Security

## Target Authentication

The i series supports the authentication methods CHAP and SRP for the iSCSI initiator.

## Host Groups

Host Groups are collections of iSCSI hosts, i.e. iSCSI initiators. A Host Group can contain several initiators, with each initiator having a unique WWUI. If a host has more than one iSCSI initiator installed, all the initiators can be included in the host group.

**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 add or modify access control on a target after its volumes have been exposed, the access rights will take effect only at the next login for each iSCSI initiator.

### *Creating Host Groups*

If you want to limit host (iSCSI initiator) access to targets, you must create a host group that will define exactly the allowed initiator(s). For a more detailed explanation refer to ***Concept of iSCSI***.

**Note:**

*When creating host groups, keep in mind that:*

- Each host group can contain one or more iSCSI initiators.
- Each host group can be assigned one or both login authentication methods.
- Each host group can be attached to more than one target.
- Each target is not accessible to any initiator by default.

### *To create host groups:*

1. In the Navigation pane, right click on **Hosts Groups** and select **New Host Group…**

   The New Host Group dialog box opens (Figure 4-47).

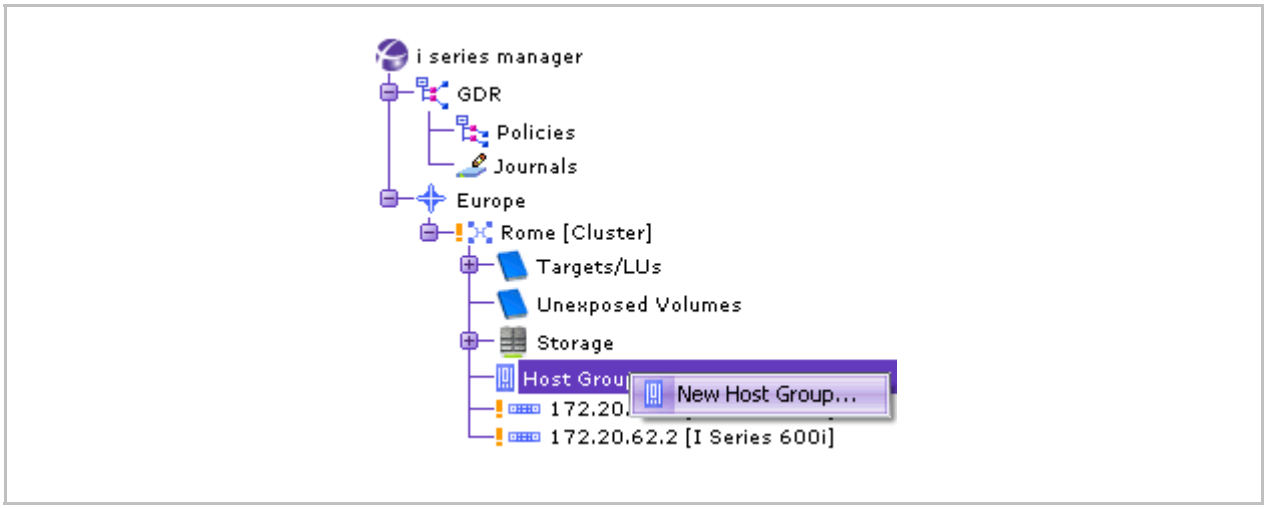



*Figure 4-46. New Hosts Group*

2. Enter an Alias and Description for the host group.

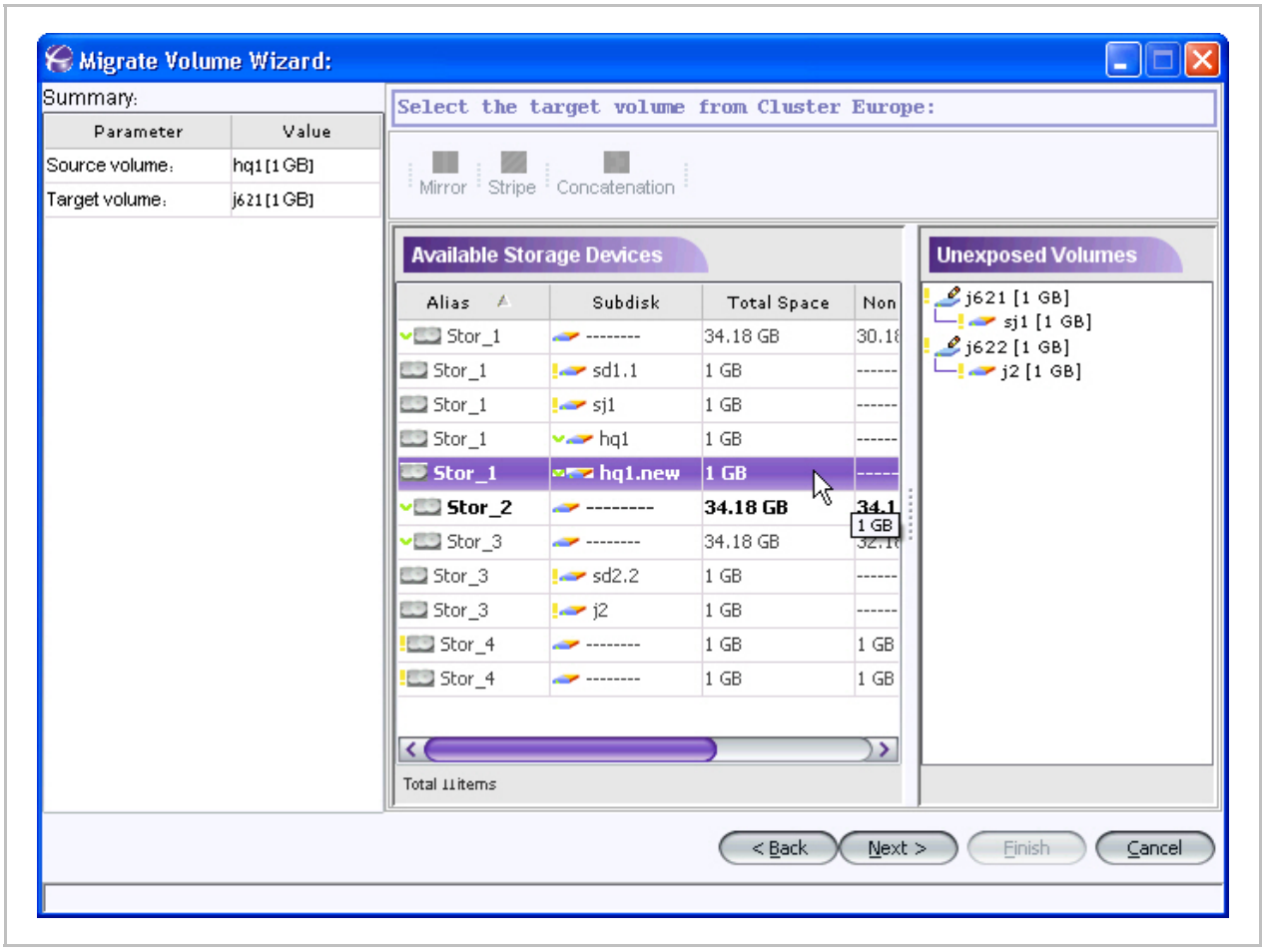



*Figure 4-47. New Host group Parameters*

3. Click **OK**.

## Adding Initiators to a Host group

After creating a host group, you can begin adding hosts to the group by their iSCSI initiator WWUIs.

### To add initiators to a host group:

1. From the Hosts Groups List, select the host group, right click and select **Properties**.

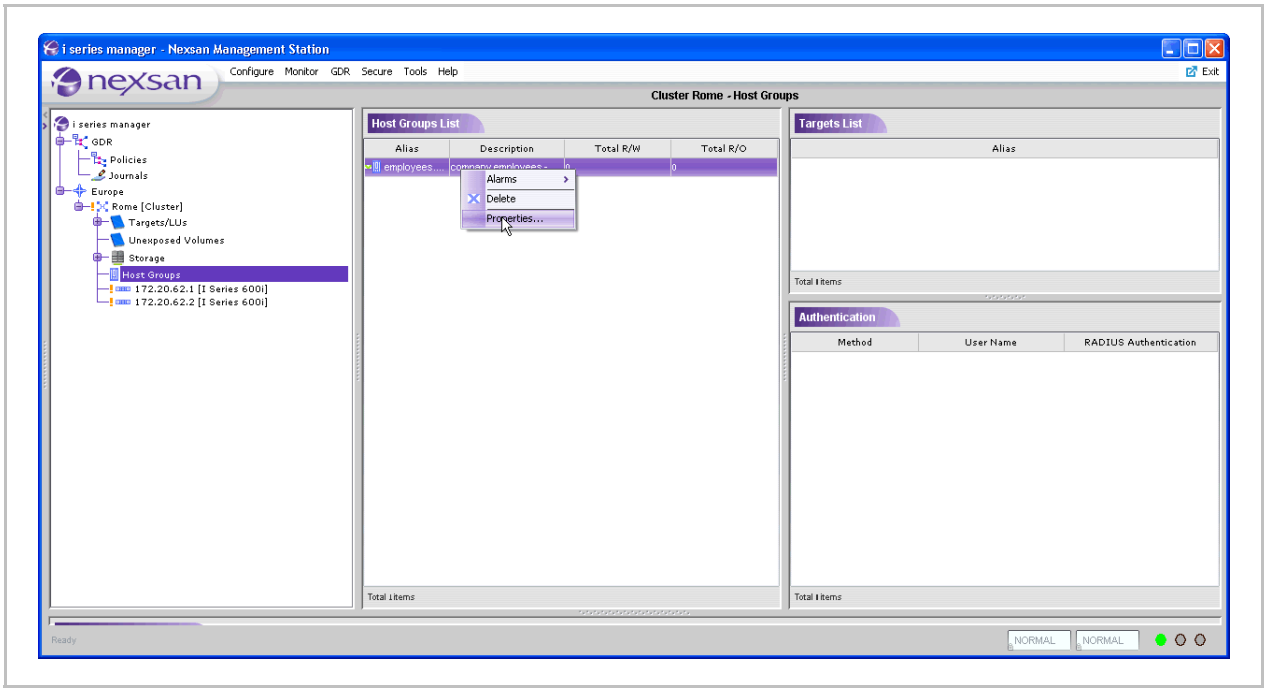
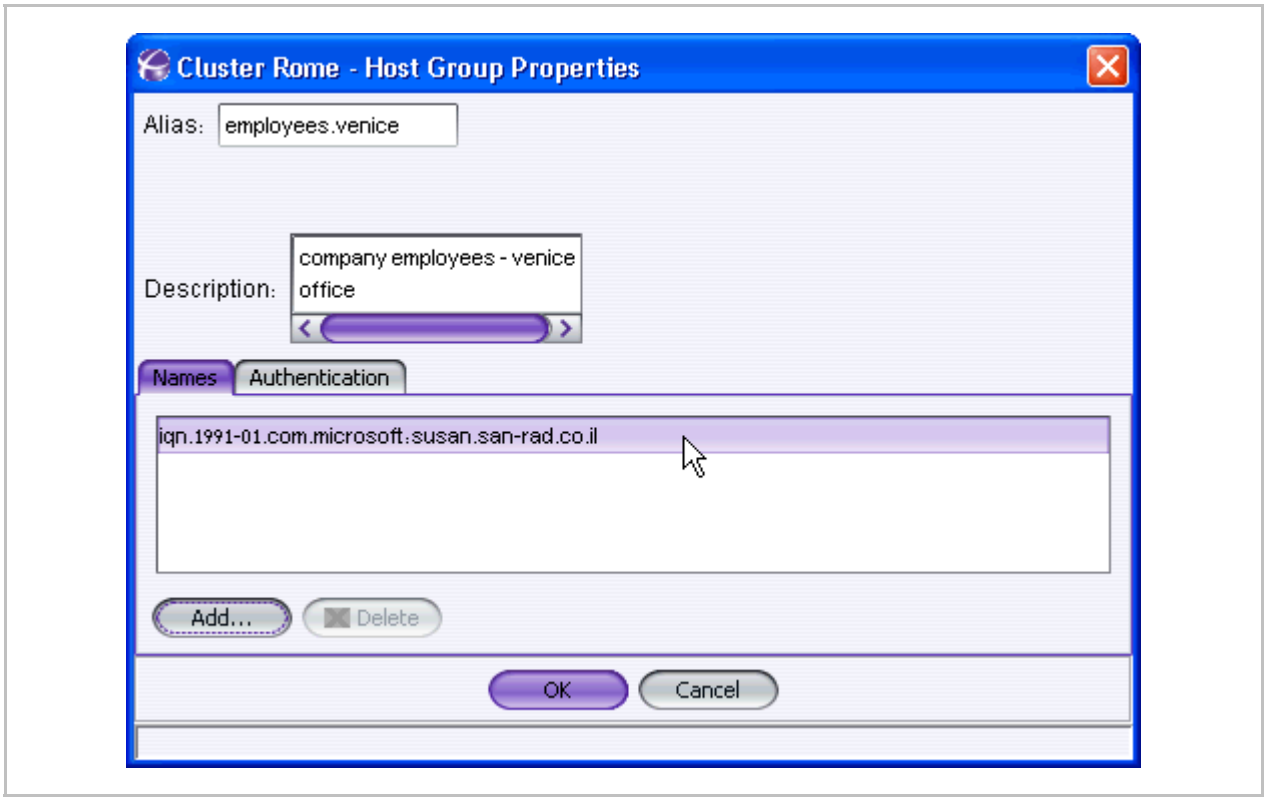



*Figure 4-48. Host Group Selected*

2. The Host group Properties dialog box opens (Figure 4-49).


Cluster Rome - Host Group Properties
Alias:
employees.venice
Description:
company employees - venice office
Names
Authentication
iqn.1991-01.com.microsoft:susan.san-rad.co.il
Add...
Delete
OK
Cancel

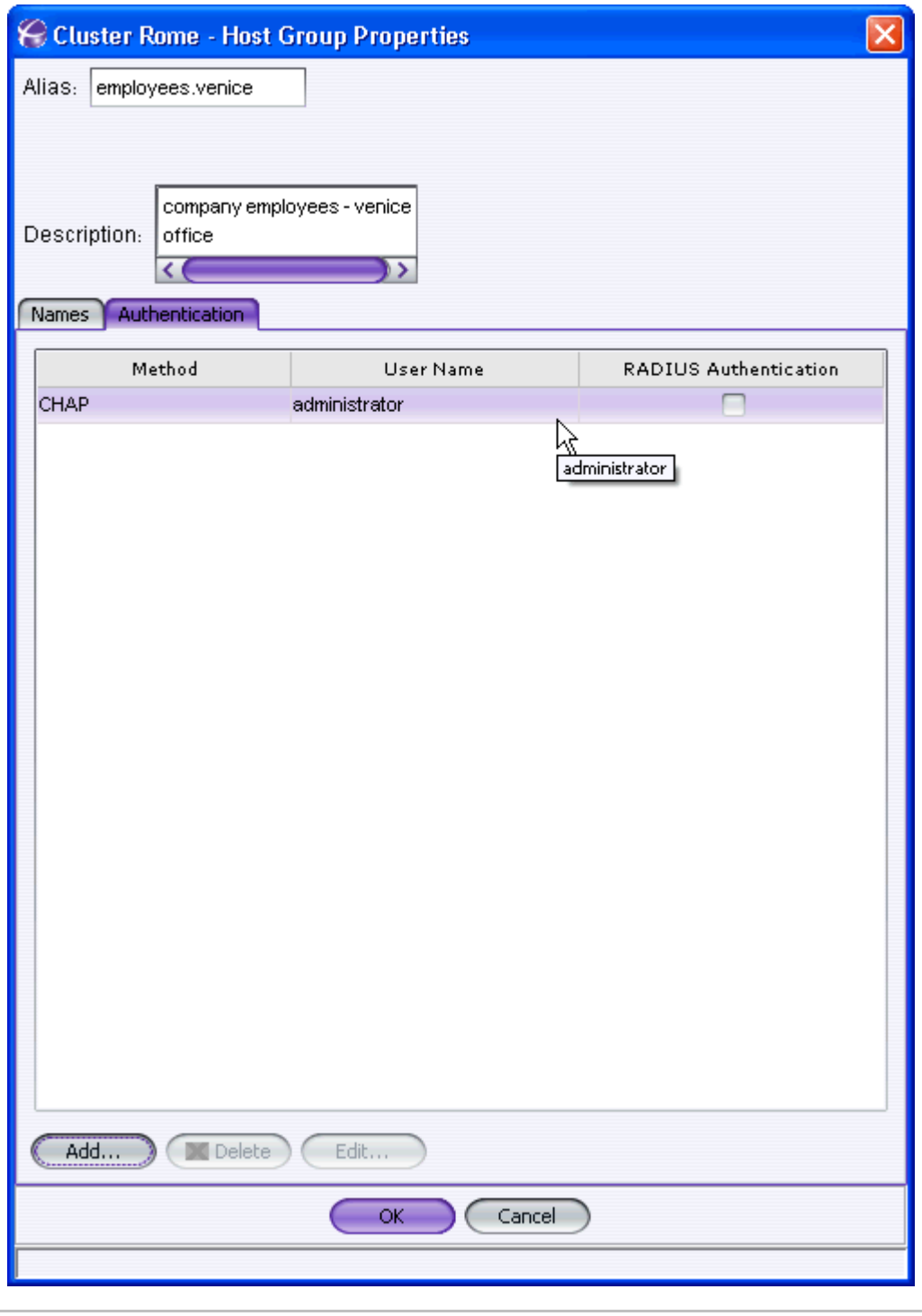



*Figure 4-49. Host group Properties Dialog Box*

3. Click Add.
4. Enter the Initiator Name (WWUI) of the initiator and click **OK**.
5. The new initiator appears in the Names tab of the Properties dialog box (Figure 4-50).

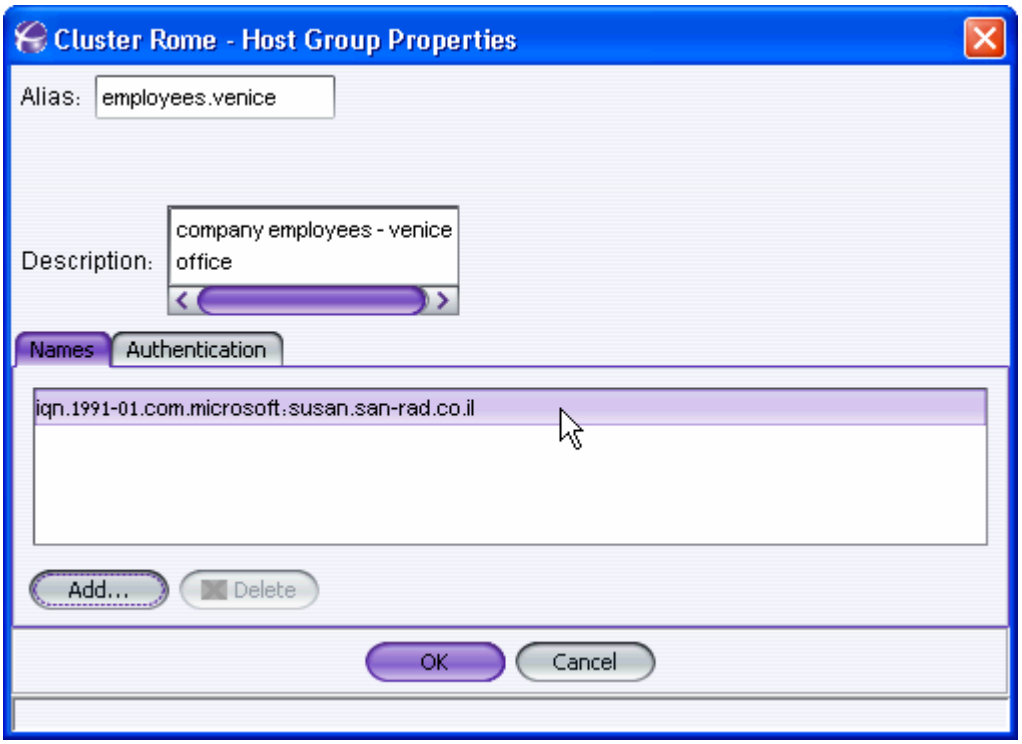



*Figure 4-50. Initiator Added*

## Assigning Credentials (Initiator Authentication)

You can require initiator authentication before allowing access to a target and its underlying volume(s). The i series supports CHAP and SRP authentication methods.

**Note:**

- When working with a Microsoft initiator and configuring target authentication: Do not configure initiator passwords with a zero as the final character (since the i series exchanges the final character in the password with a zero).
- CHAP passwords must be between twelve to sixteen characters in length.
- If a host has more than one iSCSI initiator installed, both initiators can

be included in the host group and given authentication methods.

- The user name and password do not need to be the same for different initiators on the same host.

### *To assign authentication to a host group:*

1. From the Host Group List pane, select the host group, right click and select **Properties**.

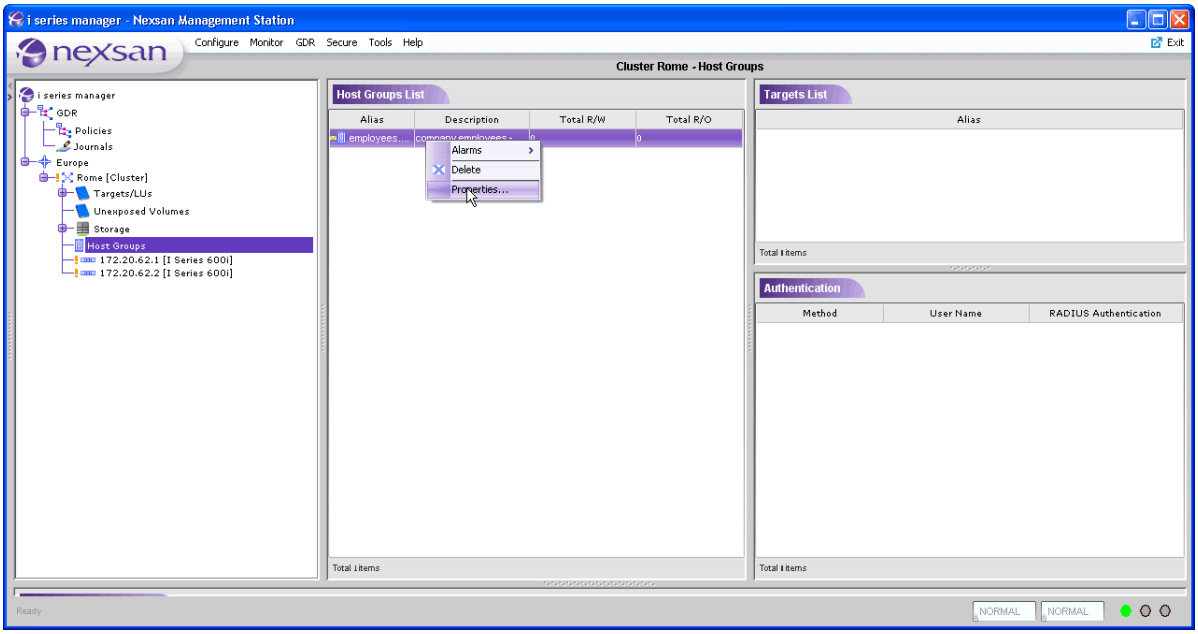
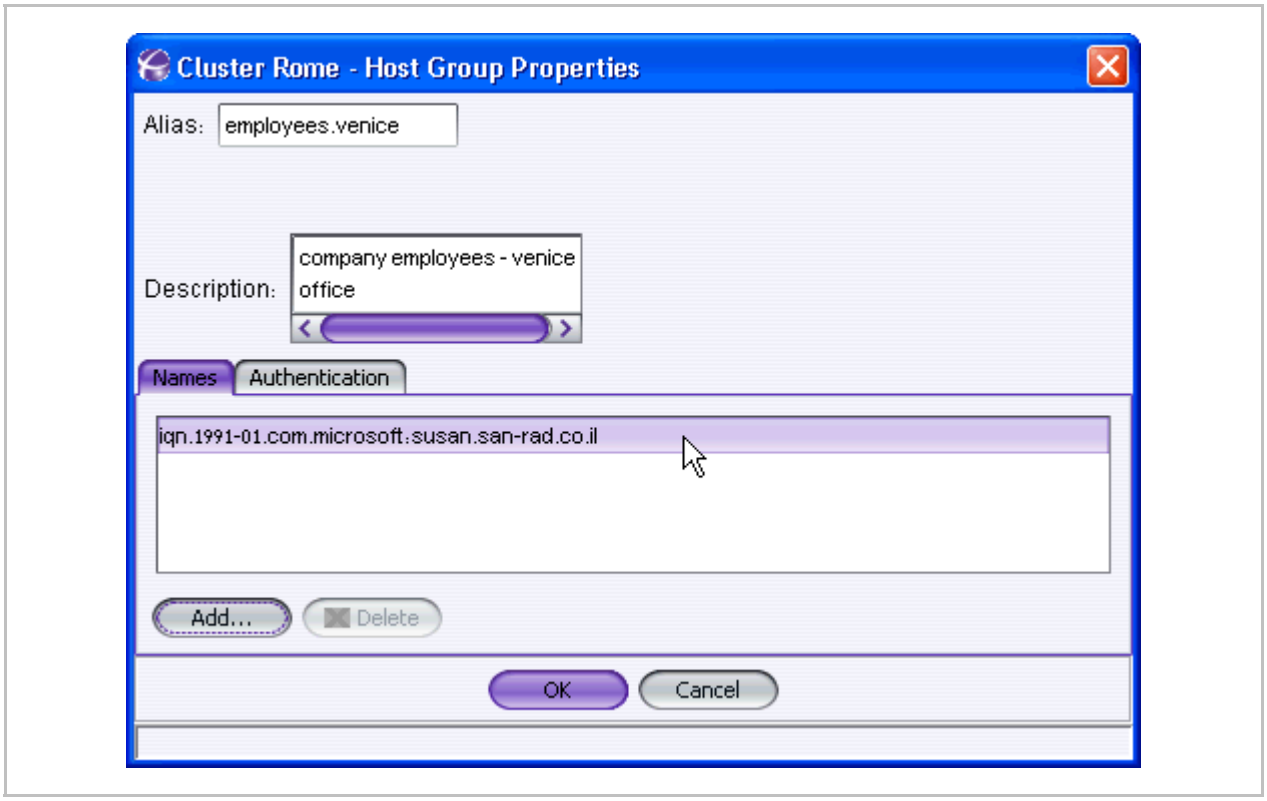



*Figure 4-51. Properties Selected*

The Properties dialog box opens (see Figure 4-50).

2. Toggle to the Authentication tab.
3. Click **Add**. Enter the authentication method parameters (Figure 4-52).



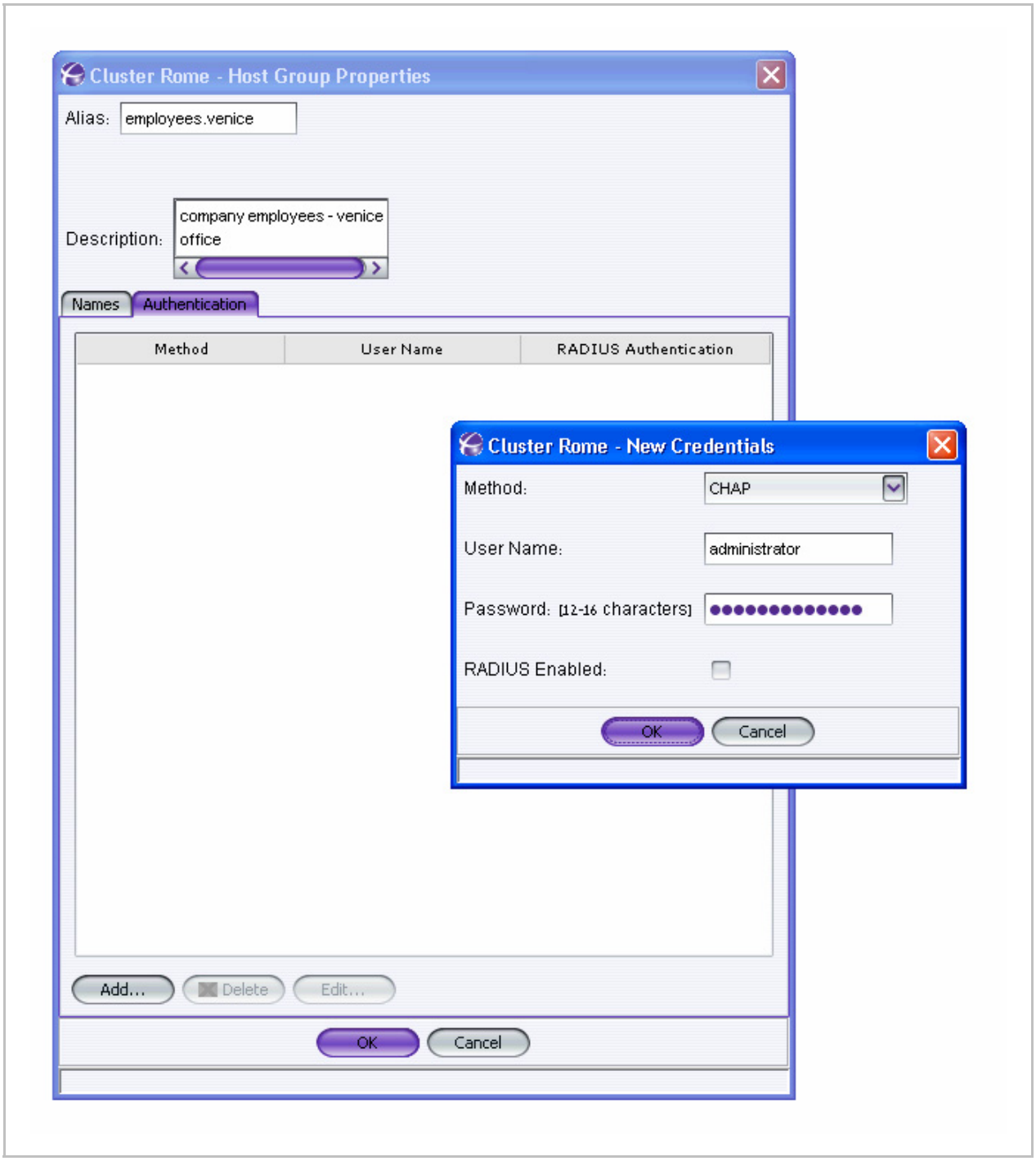



*Figure 4-52. Authentication Method Parameters*

4. Click **OK**. The added authentication method appears in the authentication table (Figure 4-53).

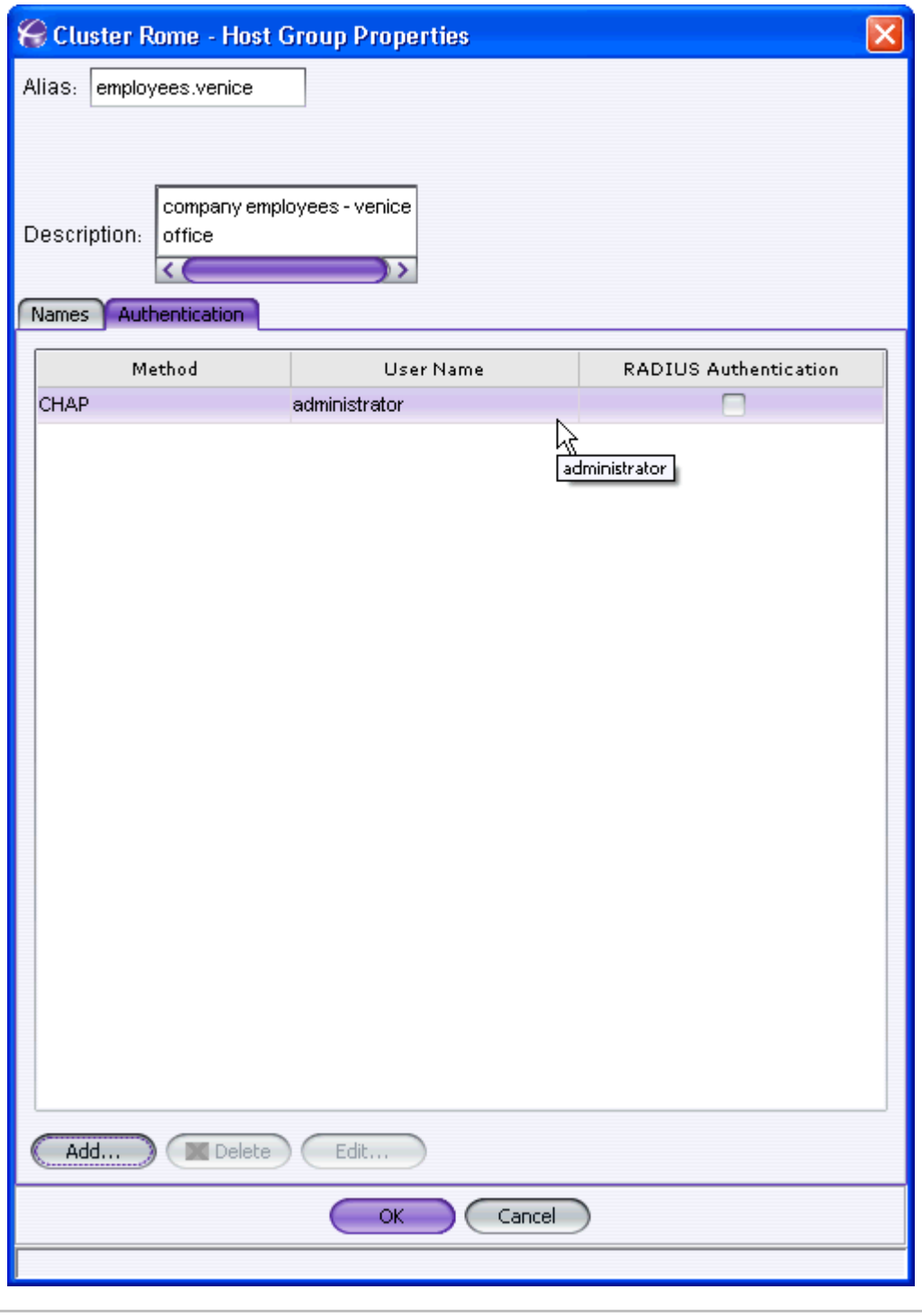



*Figure 4-53. Added Authentication Method*

## Attaching Host Groups to Targets

Once created, a host group must be attached to a target to provide it with access control. This attachment specifies which access rights the iSCSI initiators within the Host Group have to the target.

> **Note:**
> *If you add or modify Host Group attachment on a target after its volumes have been exposed, the access rights will take effect only at the next login for each iSCSI initiator.*

When a Host Group is attached to a target, it is also given a *position* in the target host group list. The position determines its place in the i series access rights evaluation.

- The first host group in the list is the first host group evaluated when an initiator tries to access a volume.
  If the initiator meets the profile of the host group, it is granted that host group's access rights. If not, the i series continues to the next position. The i series does not scan all host groups to determine which most specifically fits the host.
- Host Groups must be positioned in decreasing specificity to function correctly. The i series scans for the first fit and not the best fit.
- The default access rights are evaluated last.
- A host group can be connected to more than one target to provide the same pre-defined list of initiators for each target.

### *To attach a Host Group to a target:*

1. From the Navigation pane, select the target.

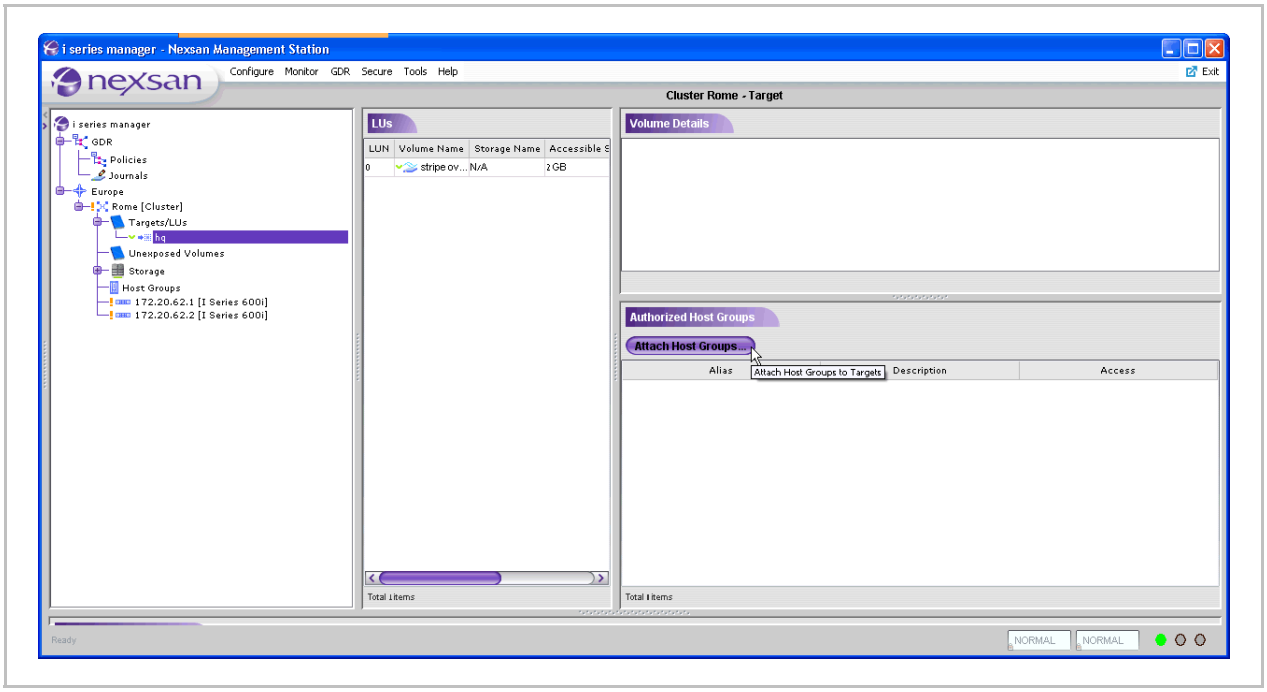



*Figure 4-54. Attaching Host Groups to Targets*

2. Click **Attach Host Groups…** from the Authorized Host Groups pane (Figure 4-54).

   The Attach Host Groups to Target window opens (Figure 4-55). Available Host Groups are listed in the bottom pane.

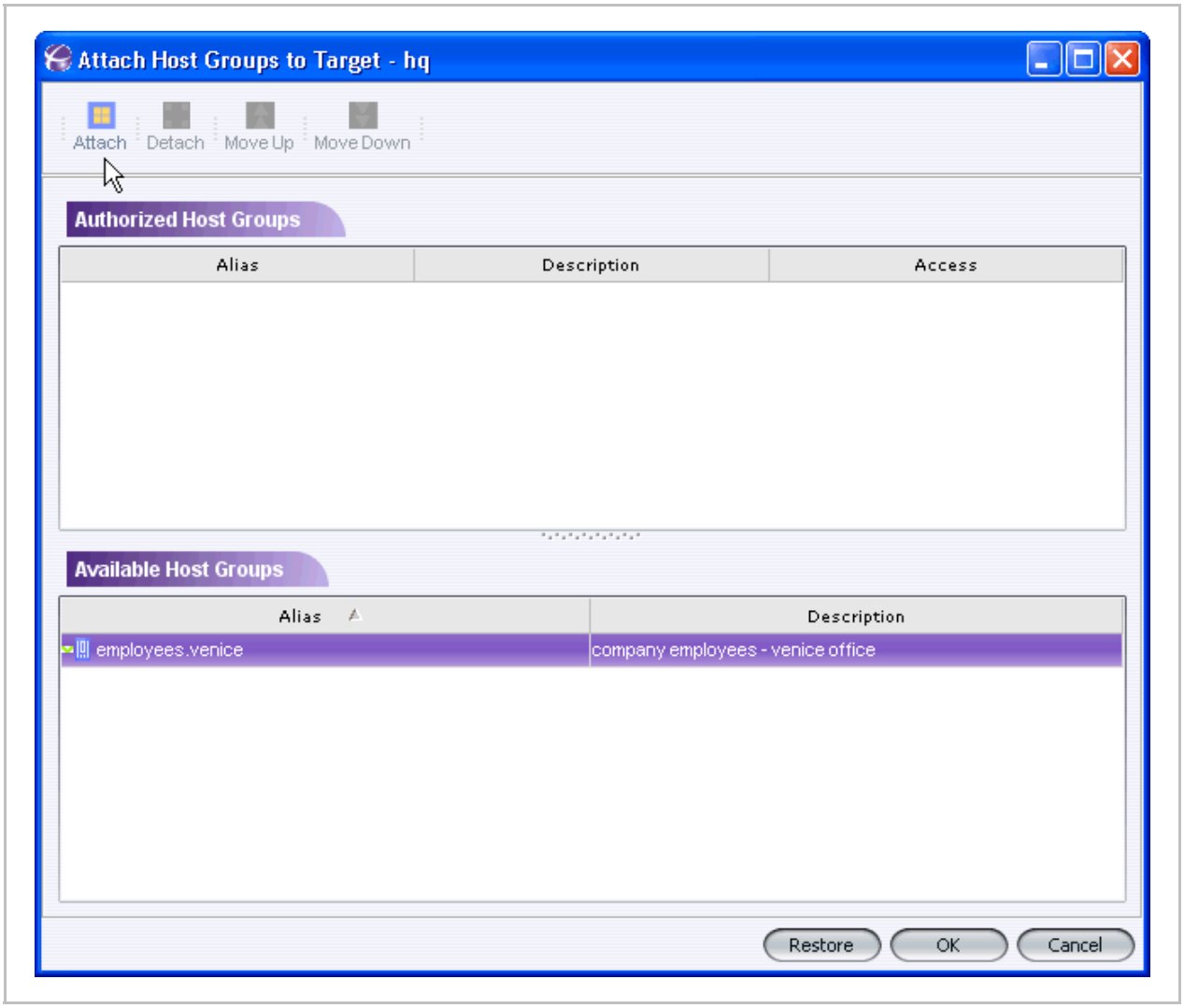



*Figure 4-55. Attach Host Group to Target Window*

3. Select the host group to attach.
4. Click Attach .

   The host group is attached to the target.

5. Click the access rights for the host group and select the access rights from the list (Figure 4-56).
6. Click **OK**.

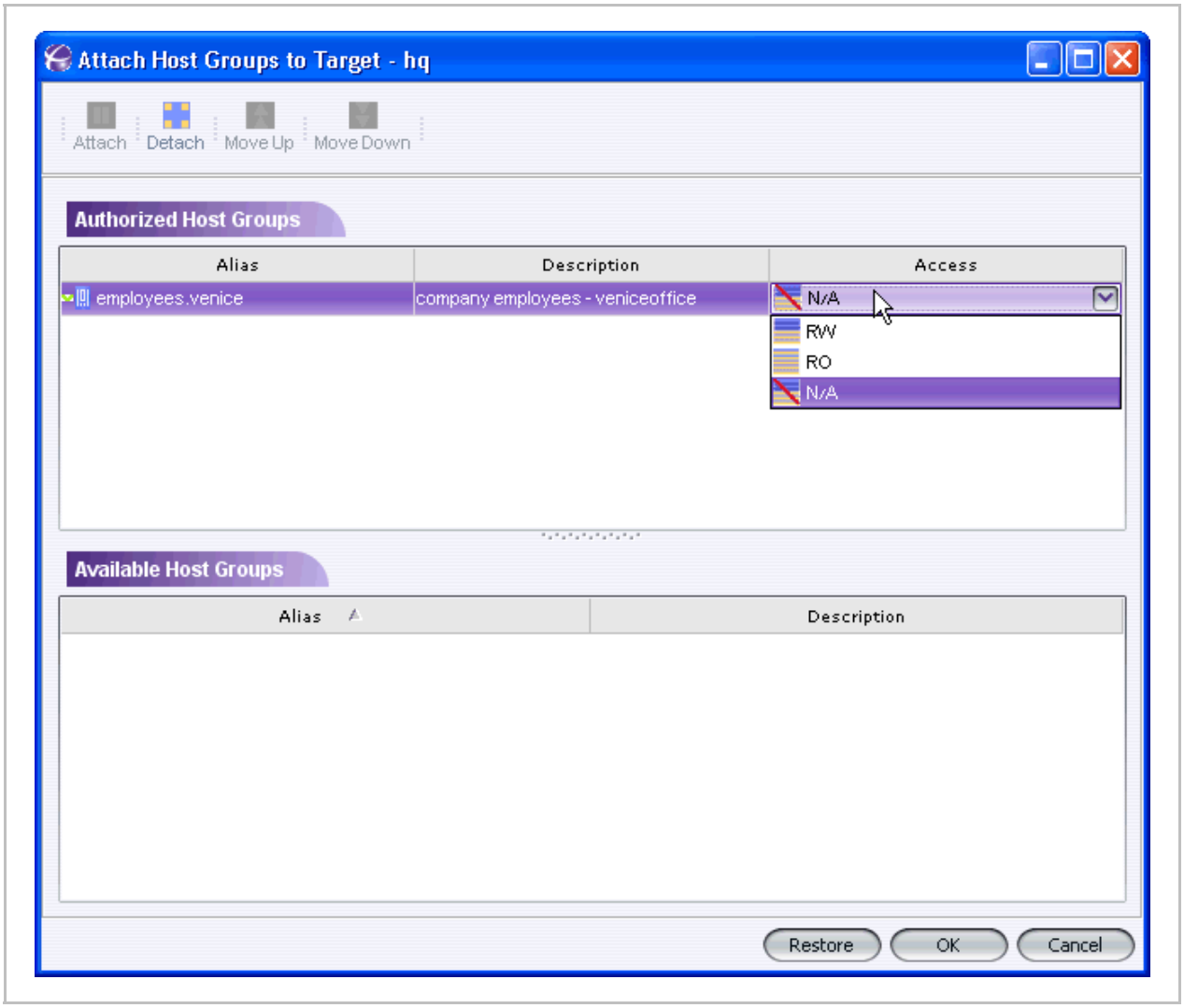



*Figure 4-56. Access Rights for an attachment*

**Note:**

*You can attach/detach host groups, change access rights and position as much as needed. The configuration will be downloaded to the i serieses only after clicking on OK.*

*Clicking **Restore** will restore the screen to reflect the actual configuration in the i series.*

# Volume 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.

***To perform an offline volume copy:***

1. Click on **Unexposed Volumes** in the Navigation pane.
2. From the Volume Details pane, select the volume and right click. Open the Copy menu and select Copy.

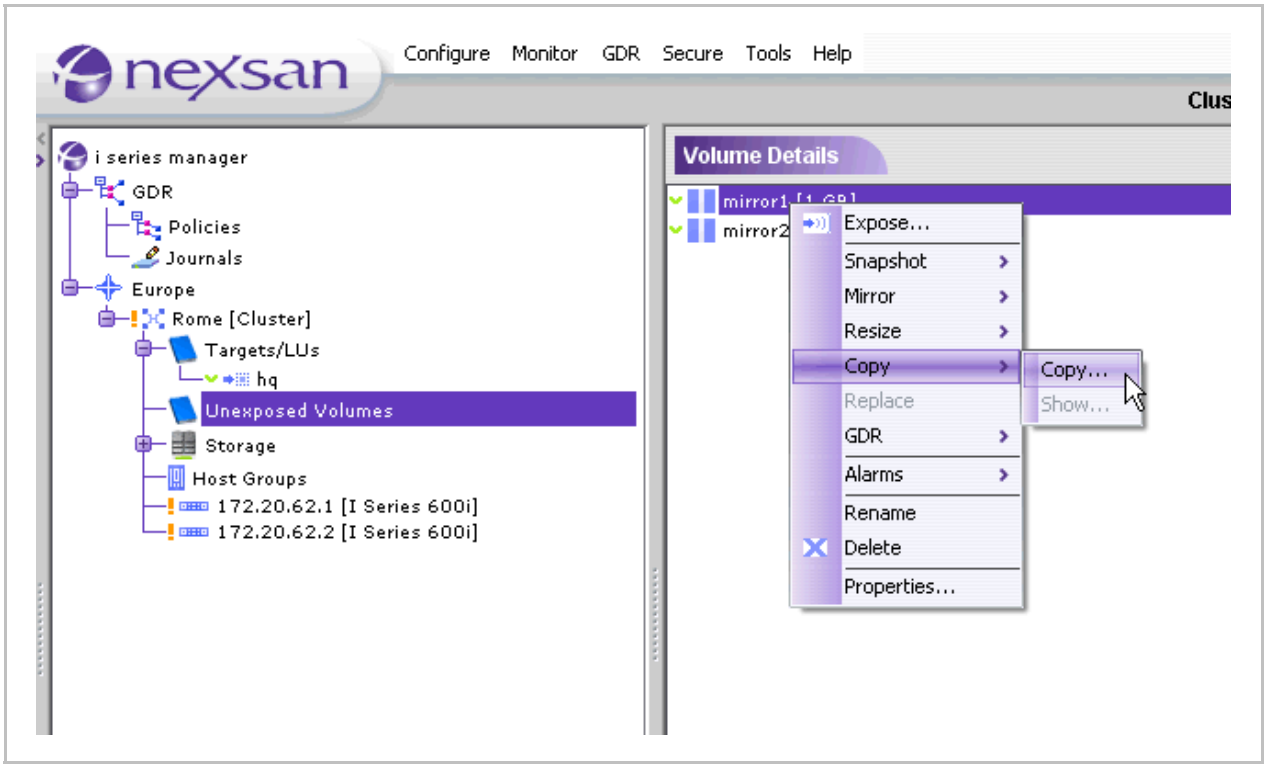



*Figure 4-57. Copy Volume*

The Offline Copy window opens with all available resources.

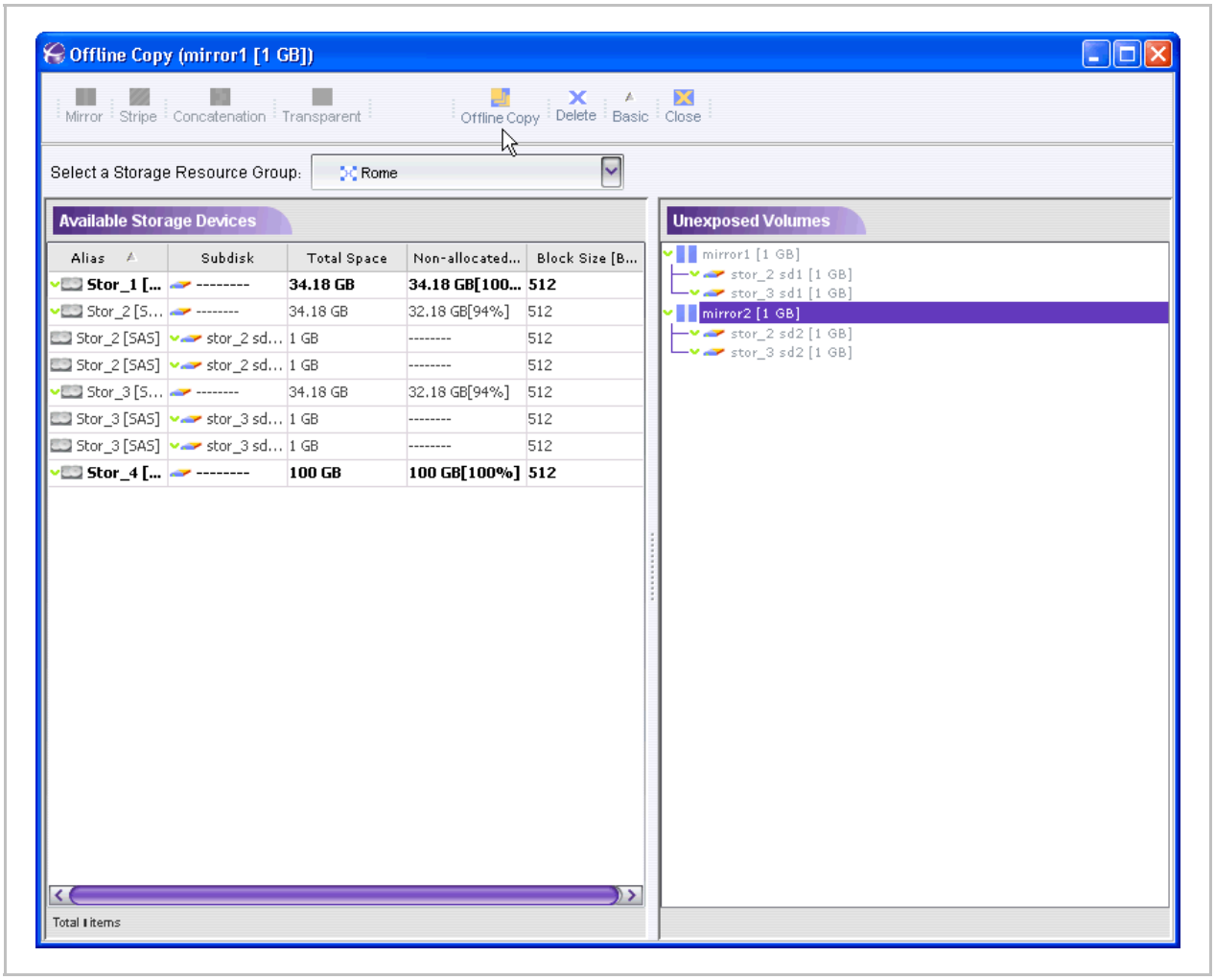
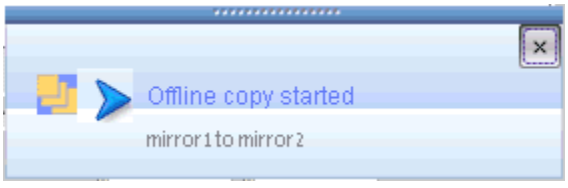



*Figure 4-58. Offline Copy Window*

3. Select a resource the same size or greater than the volume to copy.
4. Click Offline Copy . The source volume begins being copied to the destination volume.




5. To view the status of the volume copy, from the *Quick Launch:* **Monitor > Offline Copy**


*Figure 4-59. Show Offline Copy*

The Offline Copy Operations window opens.

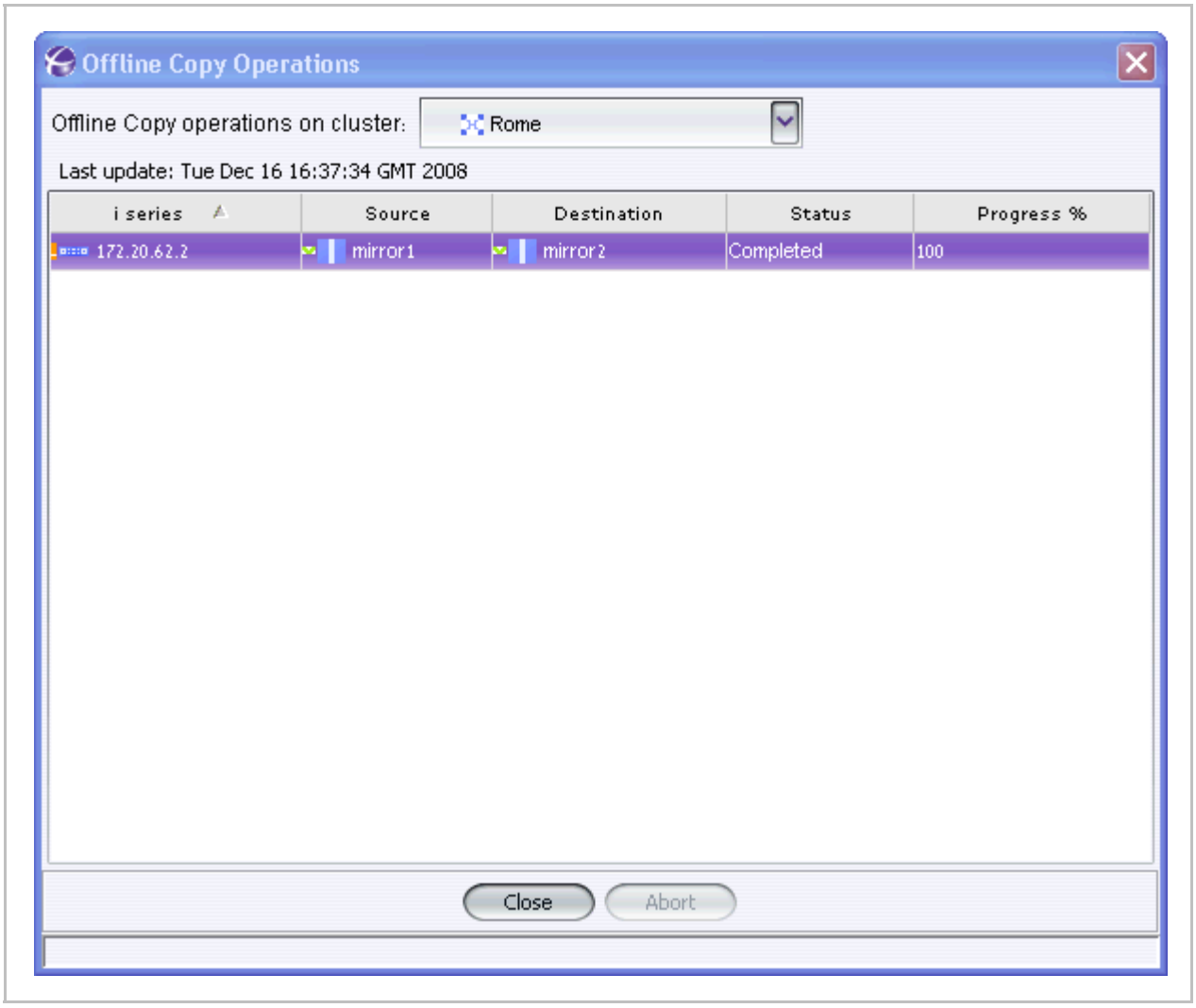
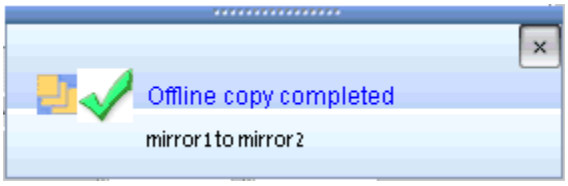



*Figure 4-60. Offline Copy Operations Window*




**Note:**

After the offline copy has finished (progress indicates 100%), in order to perform any operation on the destination volume, you must delete this line from the table.

***To delete the entry from the offline copy table:***

1. Select the entry.
2. Right click and select Delete.

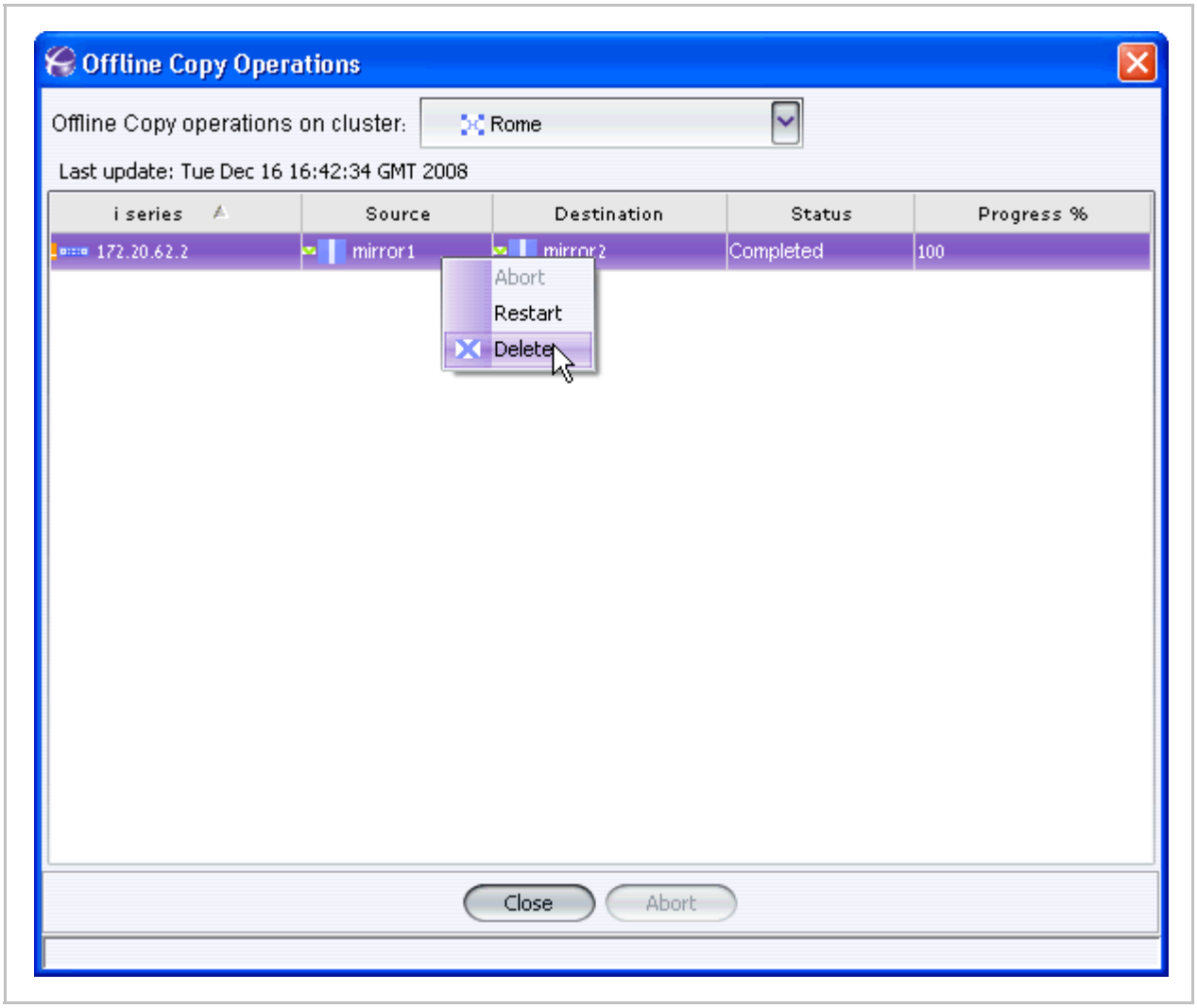



*Figure 4-61. Delete Offline Copy Entry*

## Online Copy

Online data replication allows the source volume to remain online with no interruption of service to the volume host(s).

**Notes:**

- Online copy is performed using the mirror synchronization operation.
- You can perform an online copy to any type of volume.

## Adding a Child Mirror to a Volume

### To add a child mirror to a volume:

1. From the Targets/LUs pane, select the volume to add mirror too.
2. From the Volume Details pane, select the volume, right click and select **Mirror > Add Mirror**.

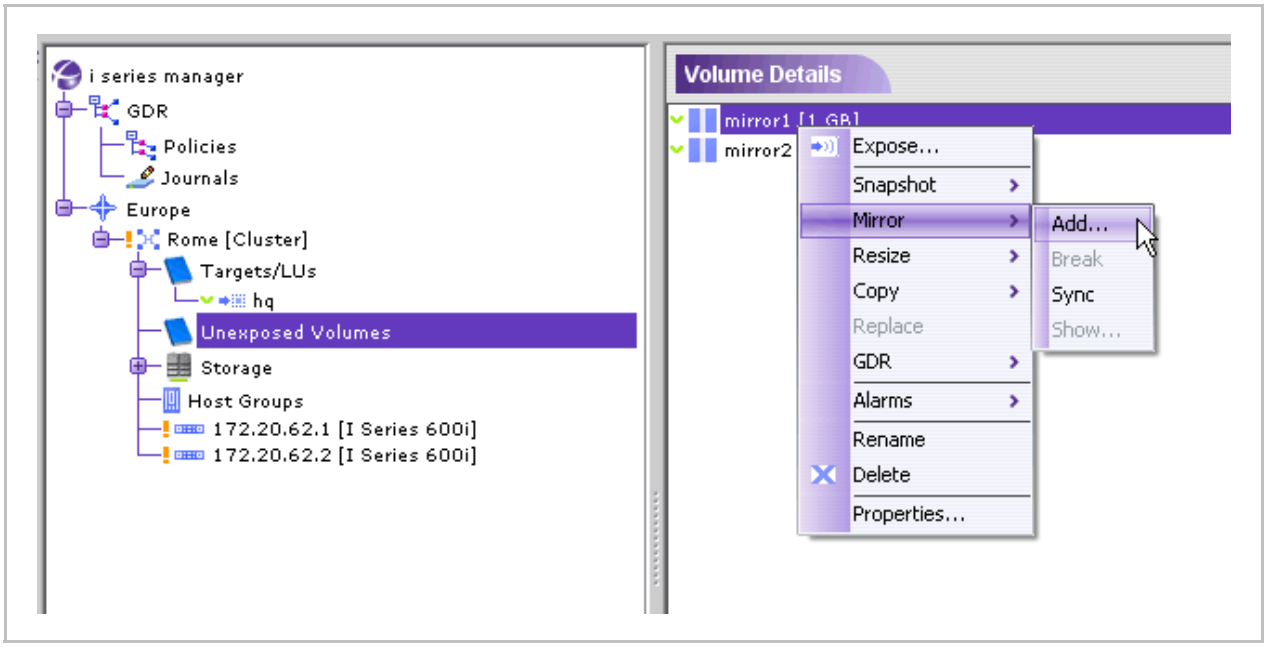



*Figure 4-62. Add Mirror Menu*

The Add Mirror window opens with all available resources.

3. Select a resource the same size or bigger than the volume to copy.

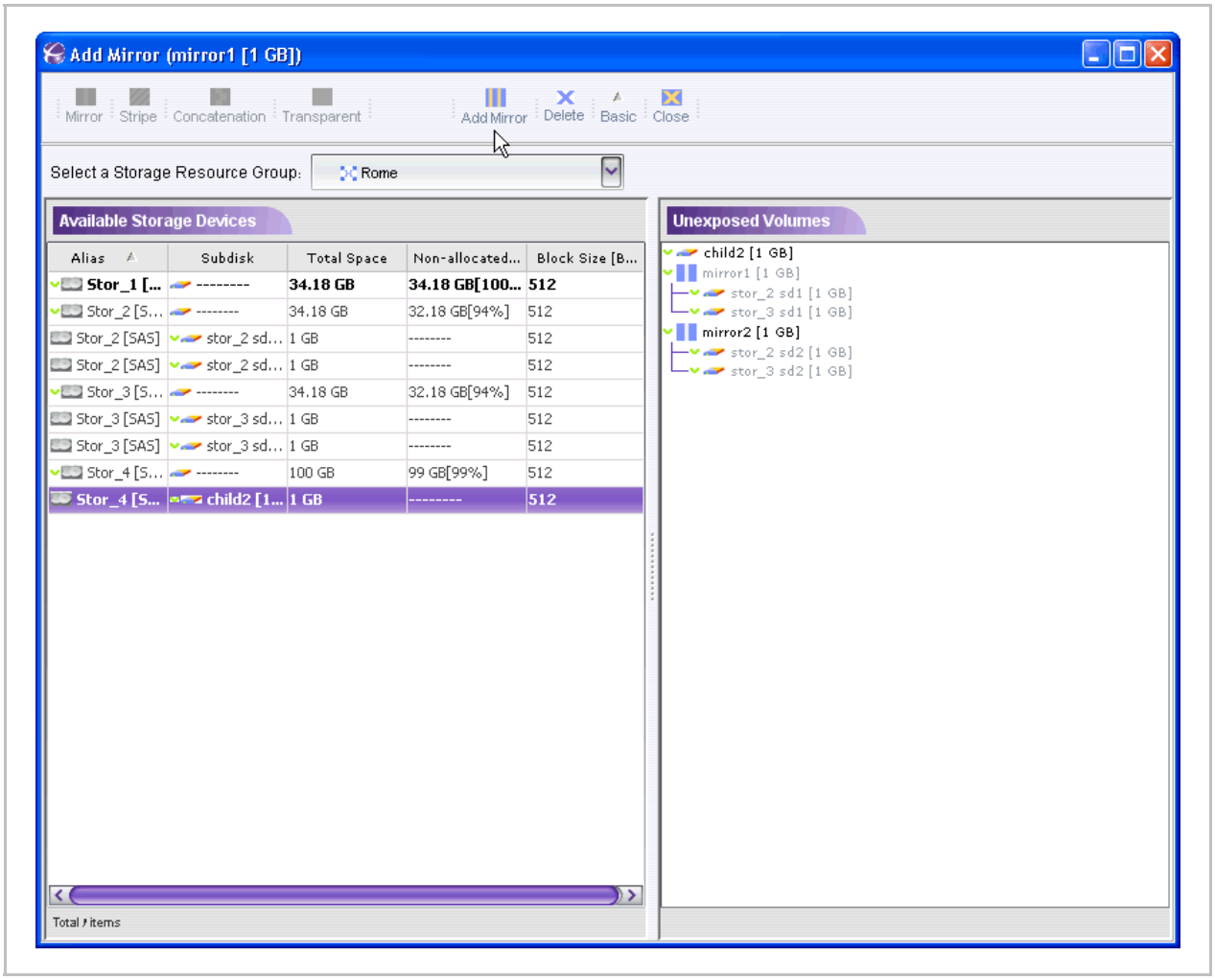



*Figure 4-63. Resource Selected in Add Mirror Window*

4. Click Add Mirror .

   The Mirror Volume New Children confirmation dialog box opens (Figure 4-64).

5. Check box to automatically synchronize the new child with the source volume or do it at a later time.

6. Click **OK**.


*Figure 4-64. Mirror Volume New Children Synch*

## Viewing Mirror Synchronization Status

You can **view all** synchronizing mirror volumes, the exposing i series, the source volume and destination volume, the status and the process of the synchronization.

1. From the *Quick Launch:*
   **Configure > Mirror Syncs**

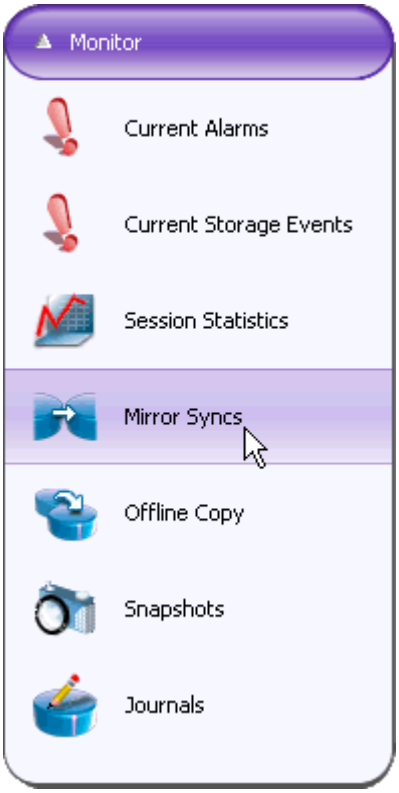



*Figure 4-65. Quick Launch - Migrate Volume*

The Mirror Sync Operations window opens.

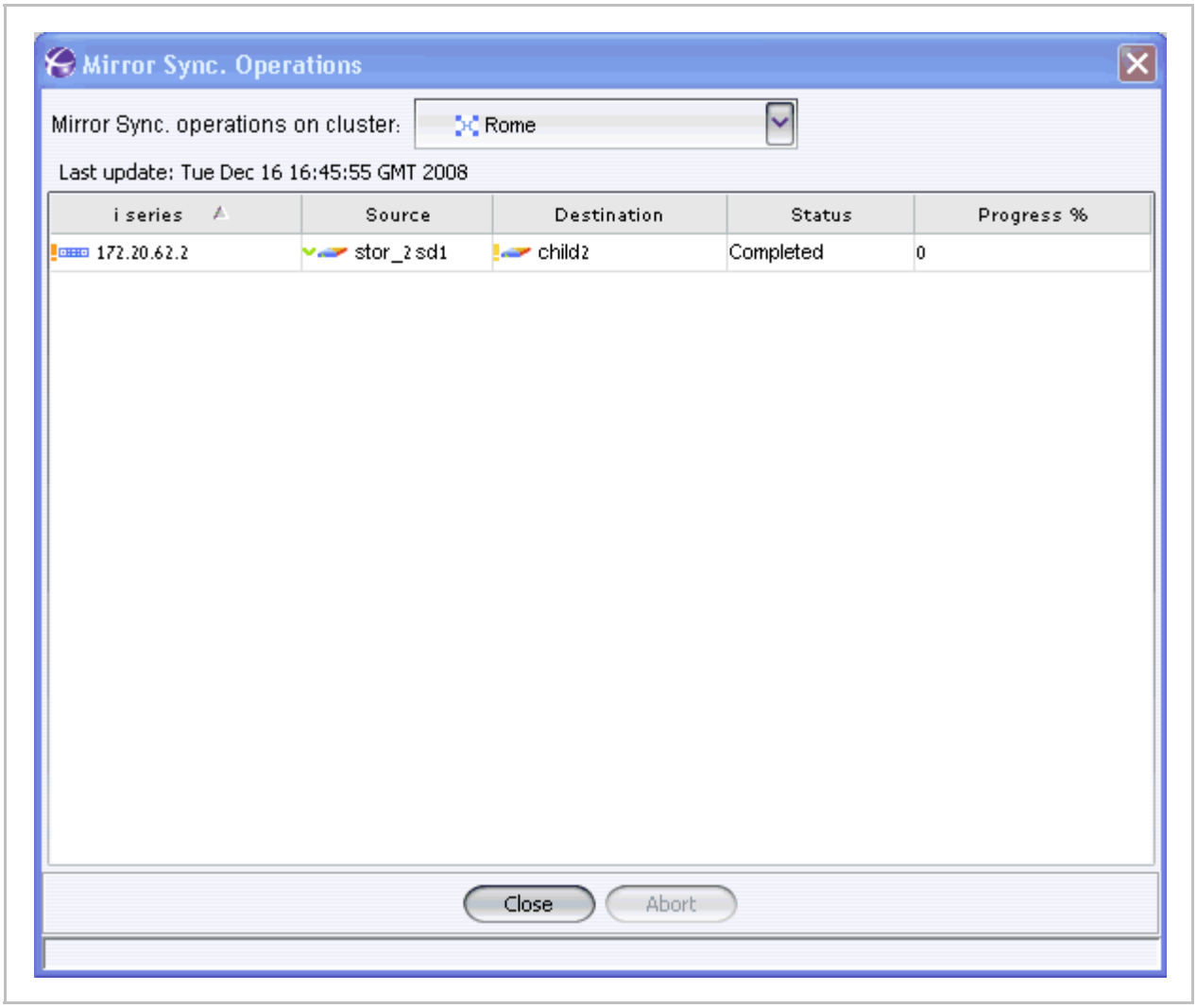



*Figure 4-66. Mirror Sync Operations Window*

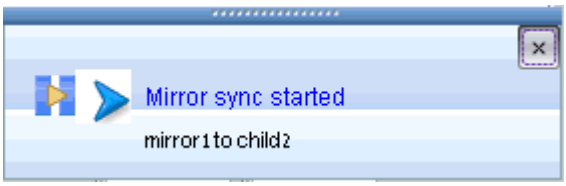



*Figure 4-67. Mirror Sync Started*

When the Mirror Sync Operation is completed a confirmation message appears.

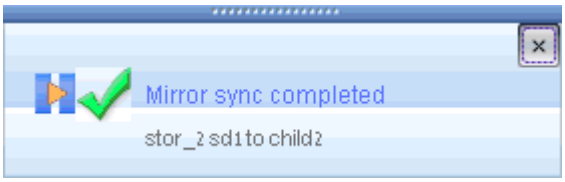



*Figure 4-68. Mirror Sync Completed*

## Breaking a Mirror

***To break a mirror:***

1. In the Navigation pane, click on Target/LUs.
2. Select the volume to break a mirror from. In the Volume Details pane, select the child to break from the mirror (Figure 4-69).
3. Right click and select **Mirror > Break**.

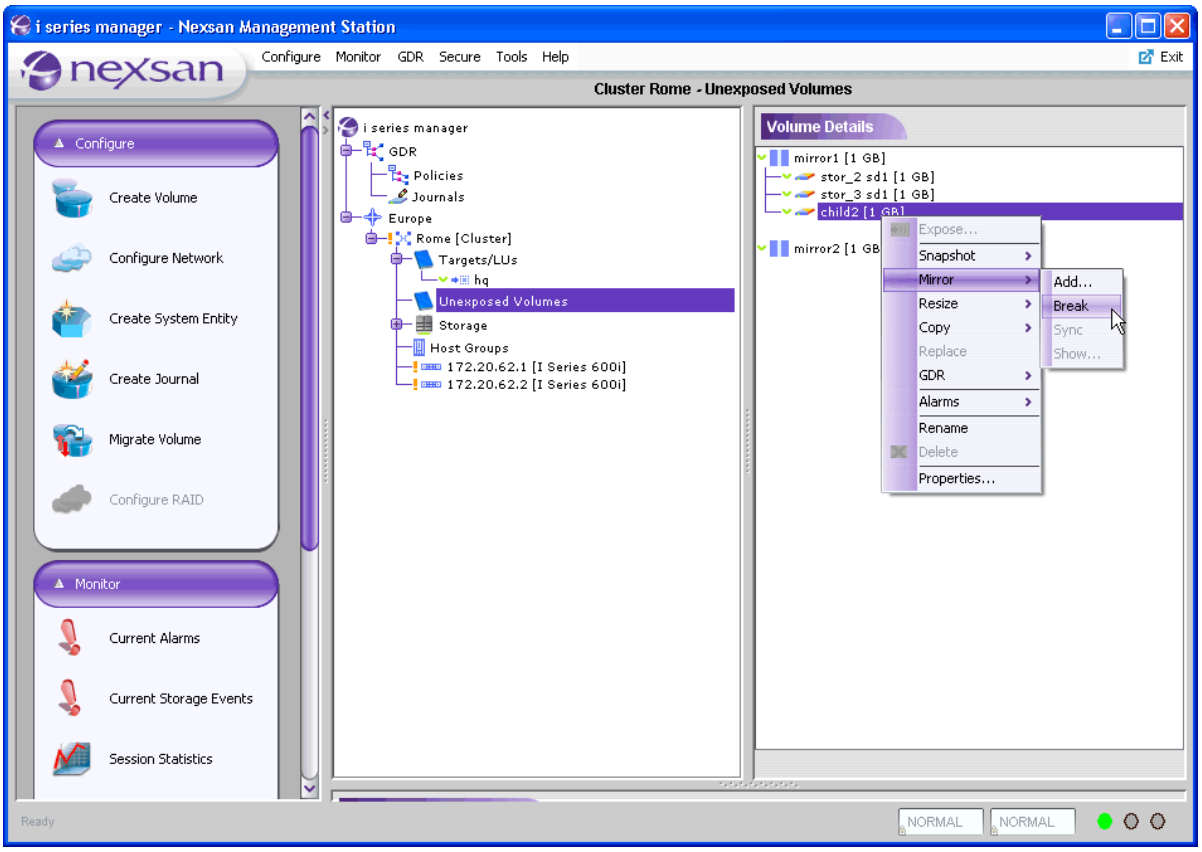



*Figure 4-69. Break Mirror Menu*

The Break Mirror Confirmation dialog box opens.

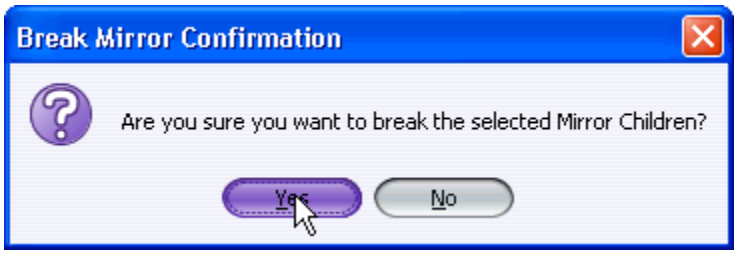



*Figure 4-70. Break Mirror Confirmation Dialog Box*

4. Click **OK**.

   The child is once again an available resource.

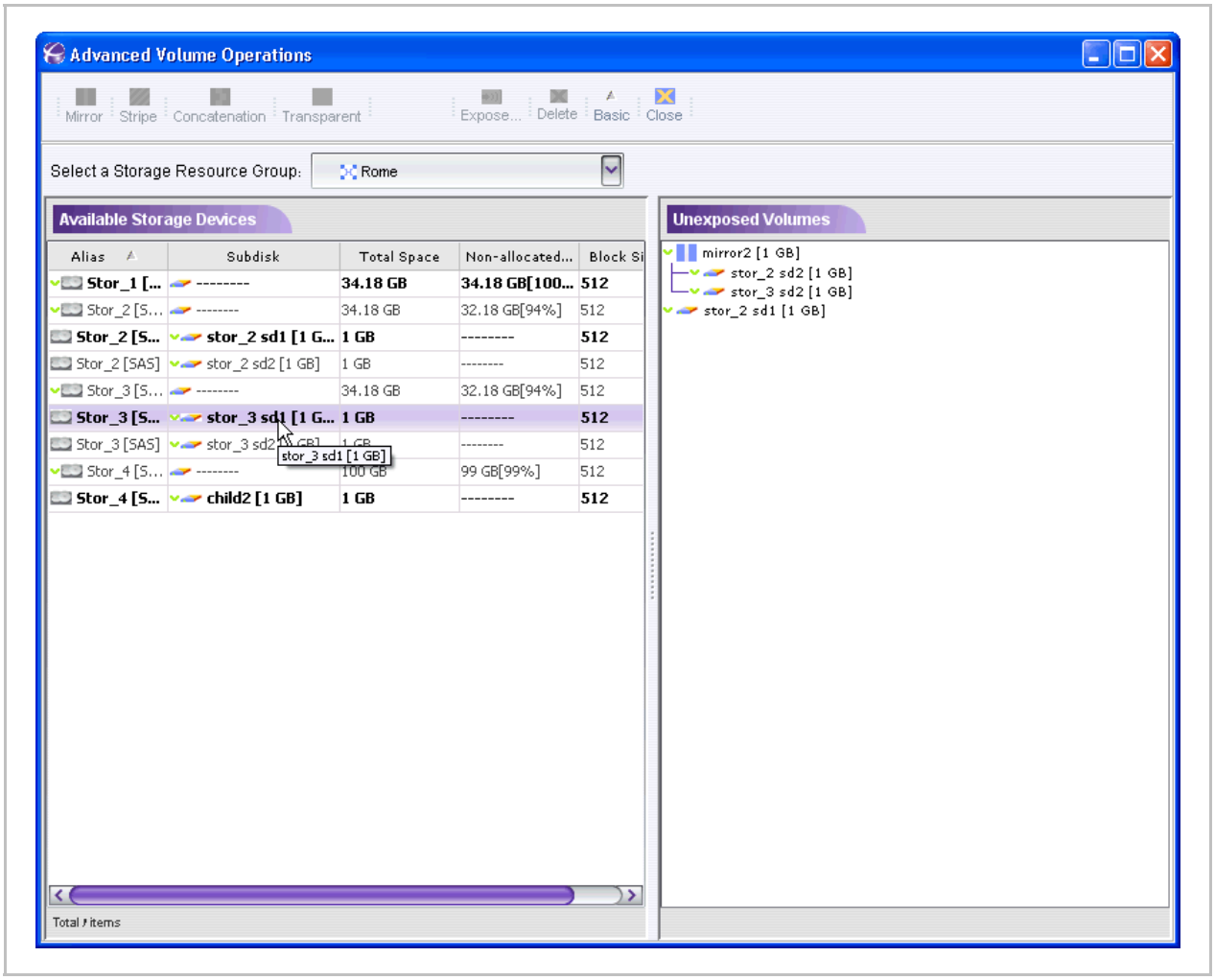



*Figure 4-71. Create Volume Window with Mirror Child Resource Available*

## Migrating Volumes

Data can be migrated (copied) online from one volume to another.

- In order to migrate data online, the volume must be exposed.
- All types of data can be migrated except transparent & journal volumes.

***To migrate volumes:***

1. From the *Quick Launch:*
   **Configure > Migrate Volume**

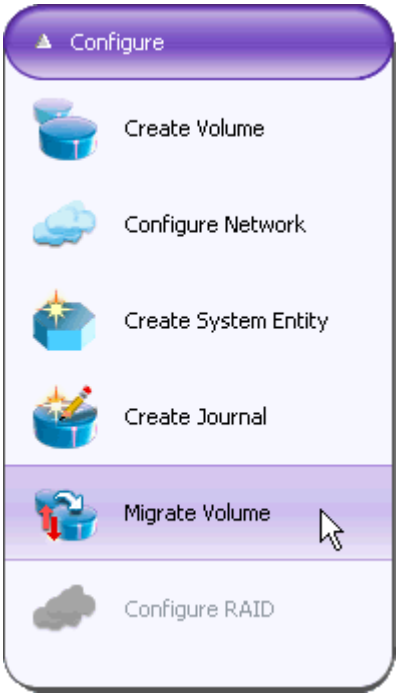



*Figure 4-72. Quick Launch - Migrate Volume*

The Migrate Volume Wizard appears.

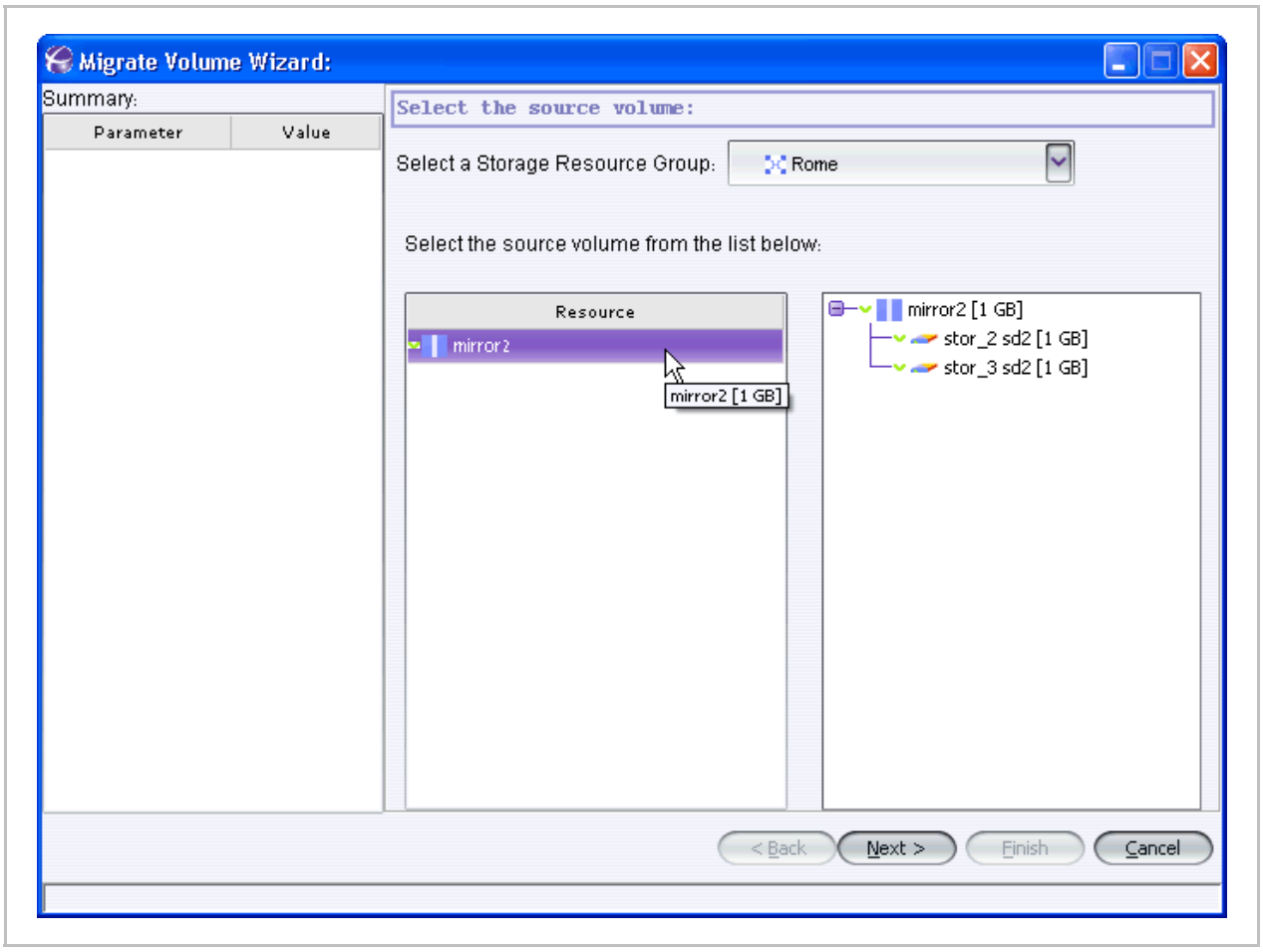



*Figure 4-73. Migrate Volume Wizard – Select Source Volume*

2. Select a source volume from the list and click **Next**.

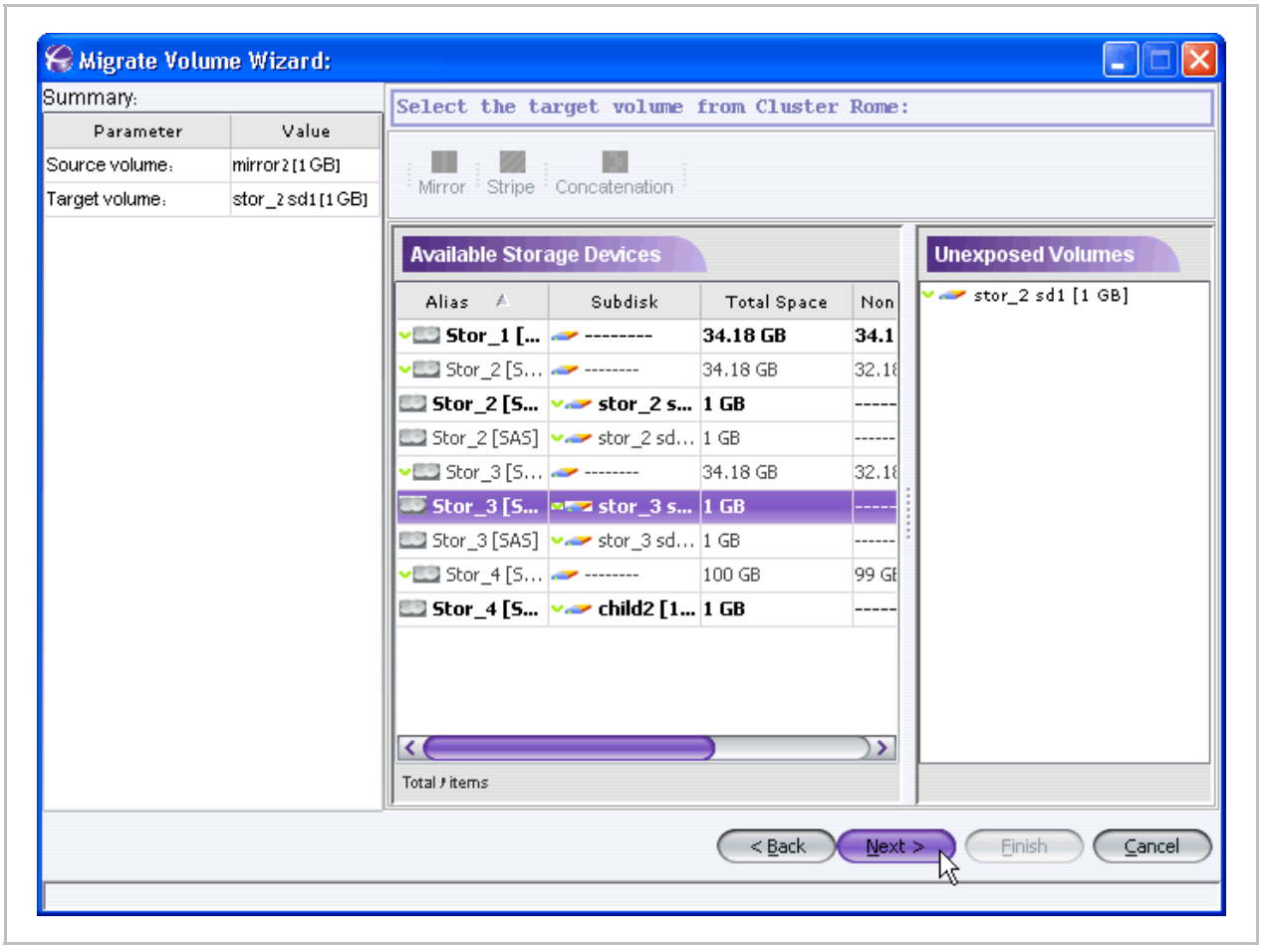



*Figure 4-74. Migrate Volume Wizard – Select Target Volume*

3. Select a target volume to migrate the volume to and click **Next**.

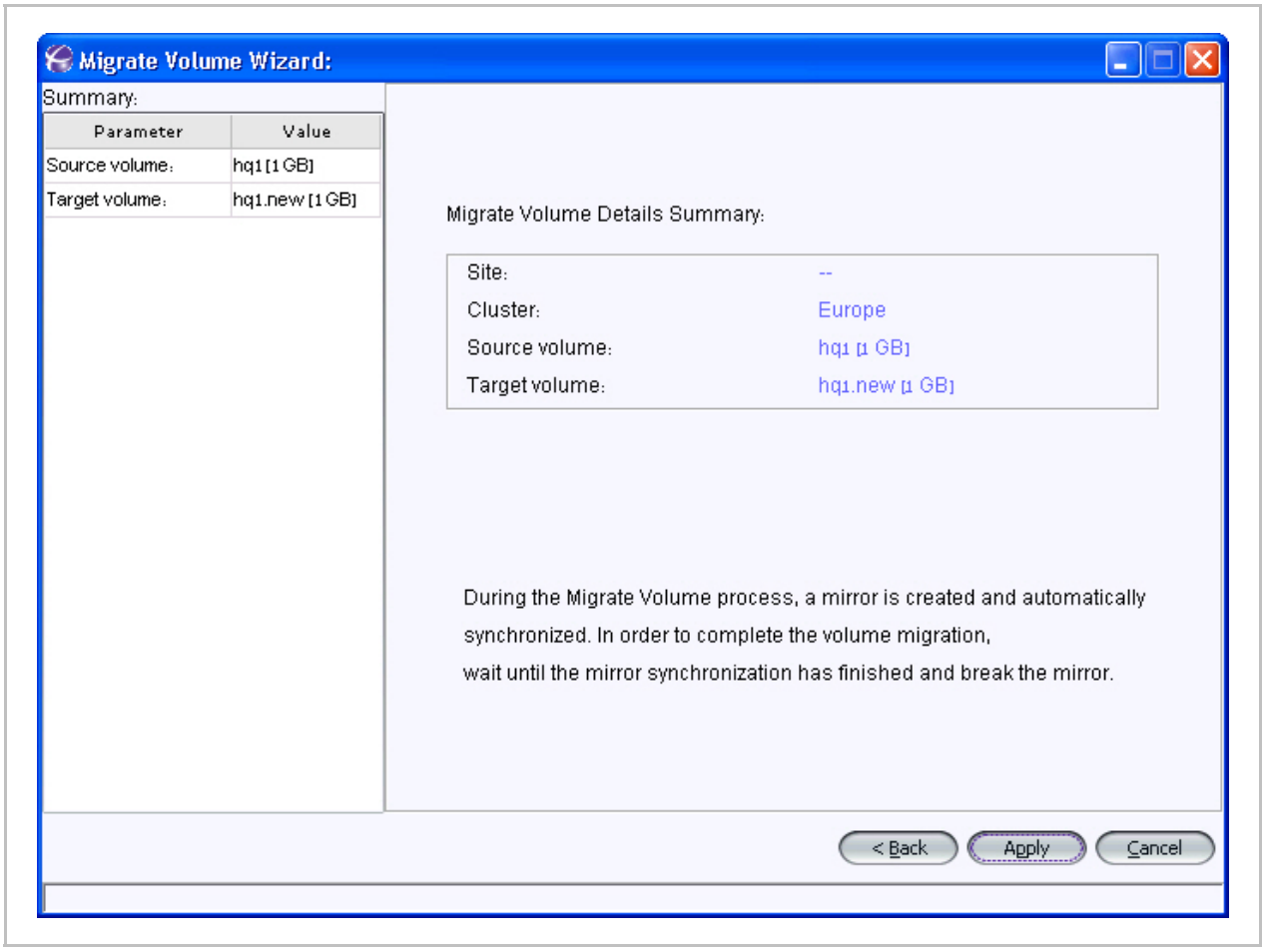



*Figure 4-75. Migrate Volume Wizard – Summary*

4. Verify that the details of the migration are correct and click **Apply**.
5. The Migrate Volume process will start.
6. When the automatic mirror synchronization has finished (add reference) you must break the mirror. Make sure to remove the source that you migrated from the mirror.

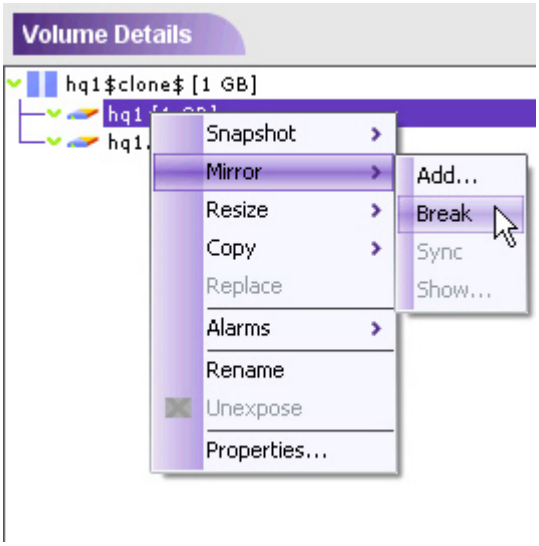



*Figure 4-76. Break Mirror*

# Snapshot Operations

Snapshot can be **active** or **inactive**. Additionally, snapshots can be "rolled back" (see Snapshot Rollback).

> **Note:**
> *A snapshot does not create a full copy of its source volume. A snapshot volume only records the changes to the source volume from the time of the snapshot's creation.*

## Creating a Snapshot

You can create a snapshot, a point-in-time copy, of any volume at the top of a hierarchy.

***To create a snapshot of a volume:***

1. In the Targets/LUs or Unexposed Volumes View screen, from the Details pane, select the volume to create a snapshot of, right click and select **Snapshot > Create**.

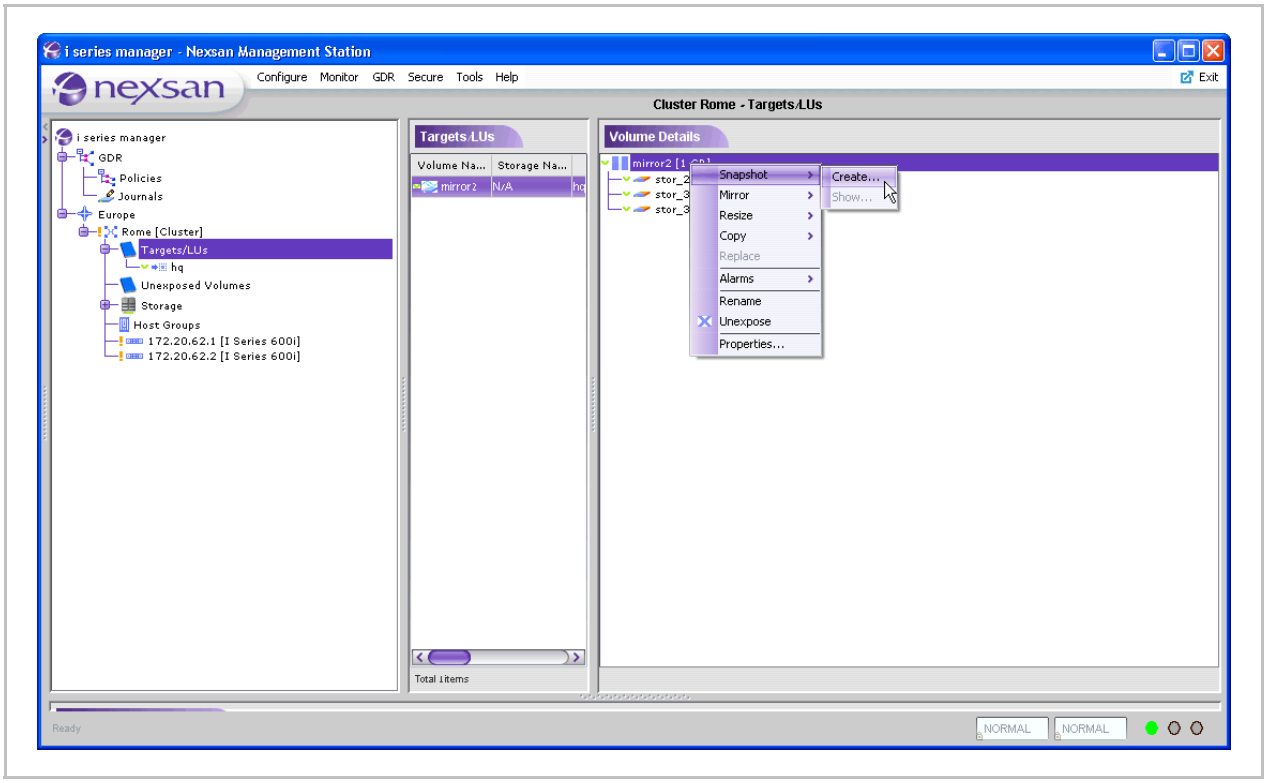



*Figure 4-77. Create Snapshot*

The Create Snapshot Volume window opens with all available resources.

2. Select a resource for the snapshot volume. Snapshot volumes can be resized as needed.

> **Note:**
> *NEXSAN recommends that a snapshot volume should be at least twenty percent of the size of the source volume, depending on projected write activity to the source volume.*

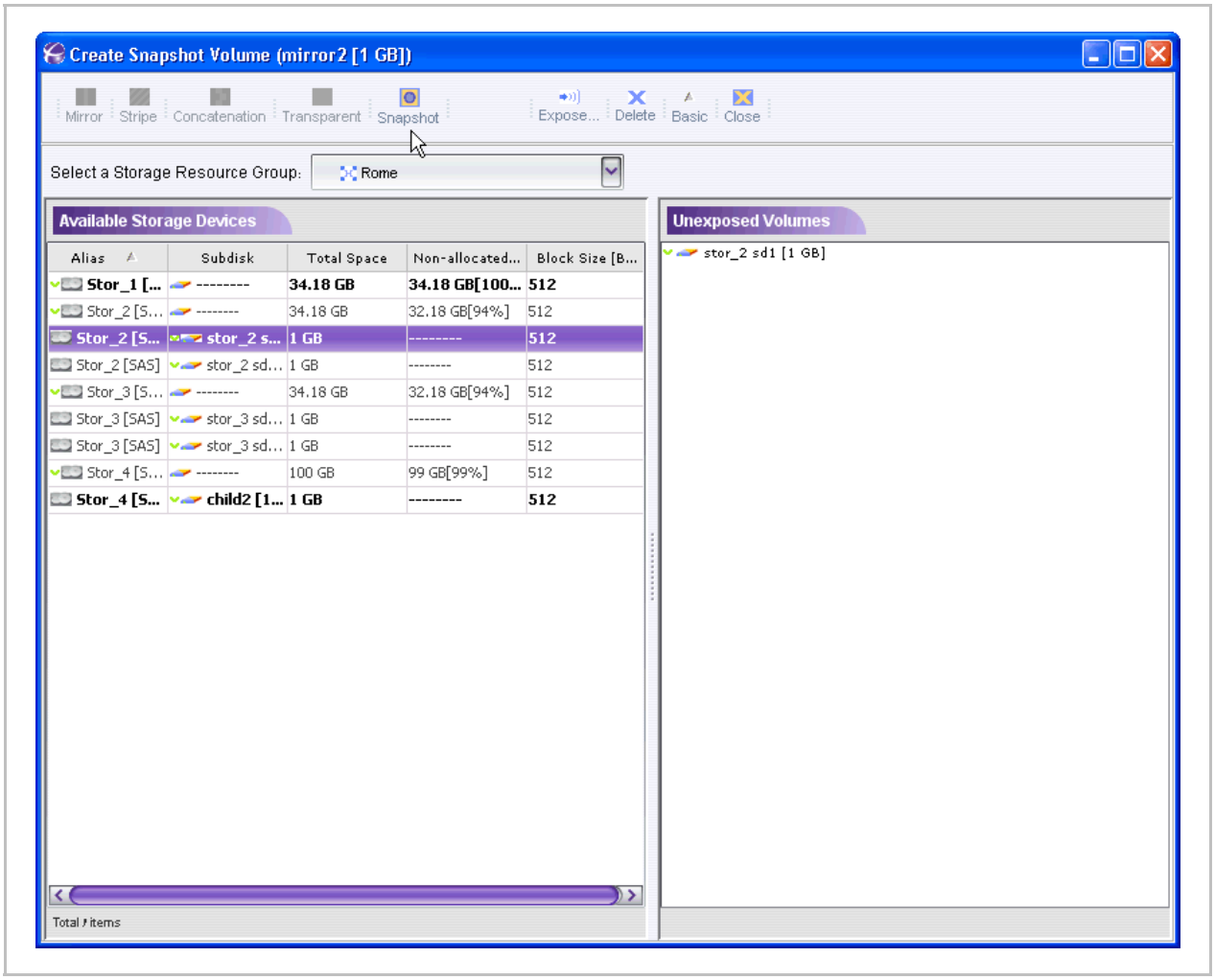



*Figure 4-78. Resource Selected in Create Snapshot Volume Window*

3. Click Snapshot .

   The **New Snapshot Volume** dialog box opens.


*Figure 4-79. New Snapshot Volume*

4. Click **OK**.

   The snapshot is created but inactive.

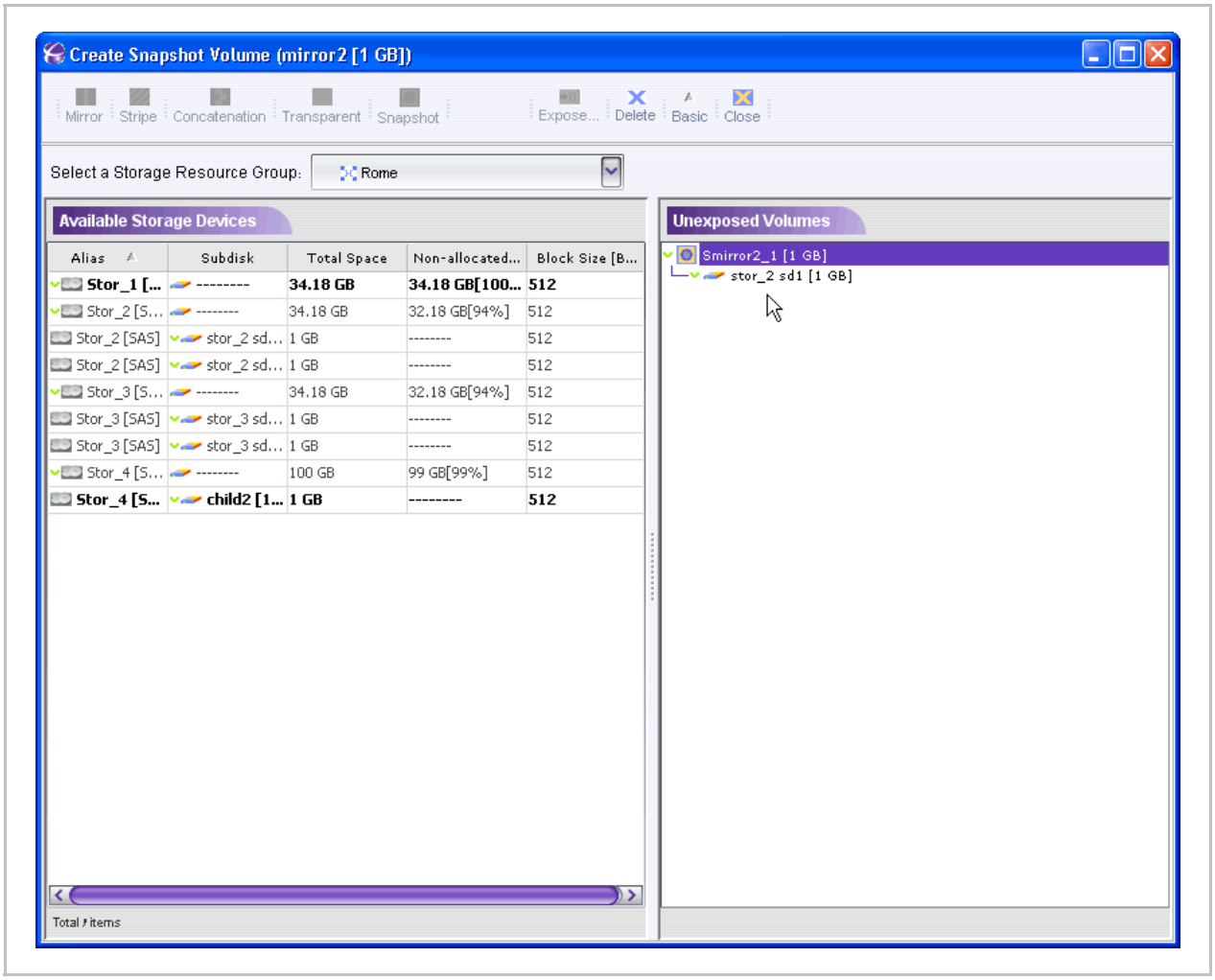



*Figure 4-80. Snapshot Volume*

## Activating a Snapshot

> **Note:**
> *After creating a snapshot, you must activate it so that data can begin to be written to it.*

***To activate a snapshot:***

1. From the *Quick Launch:*
   **Monitor > Snapshots**

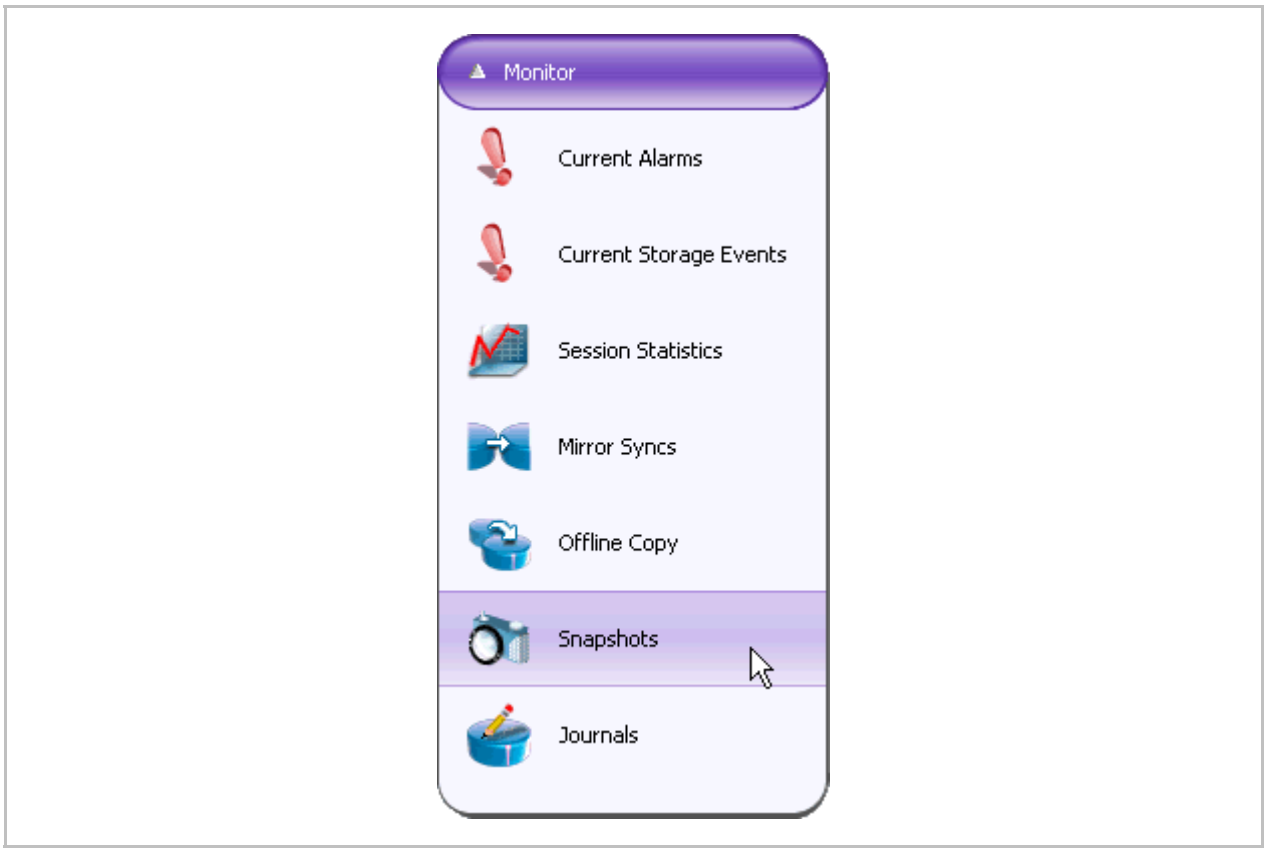



*Figure 4-81. Quick Launch - Create Volume*

The Snapshot Volumes window appears.

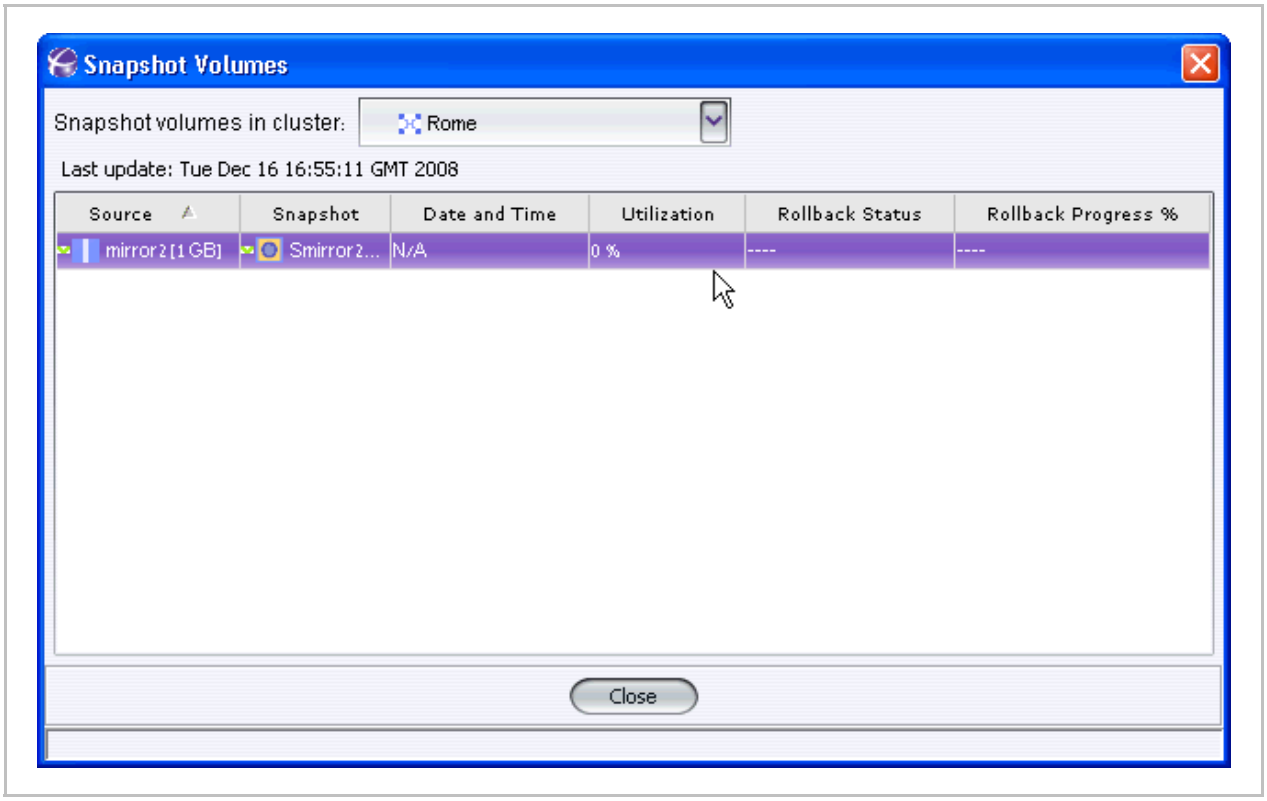



*Figure 4-82. Snapshot Volumes*

1. Select the snapshot volume you want to activate.

   The Snapshot Volumes window appears. When a snapshot is not active its **Date and Time** value will be N/A.

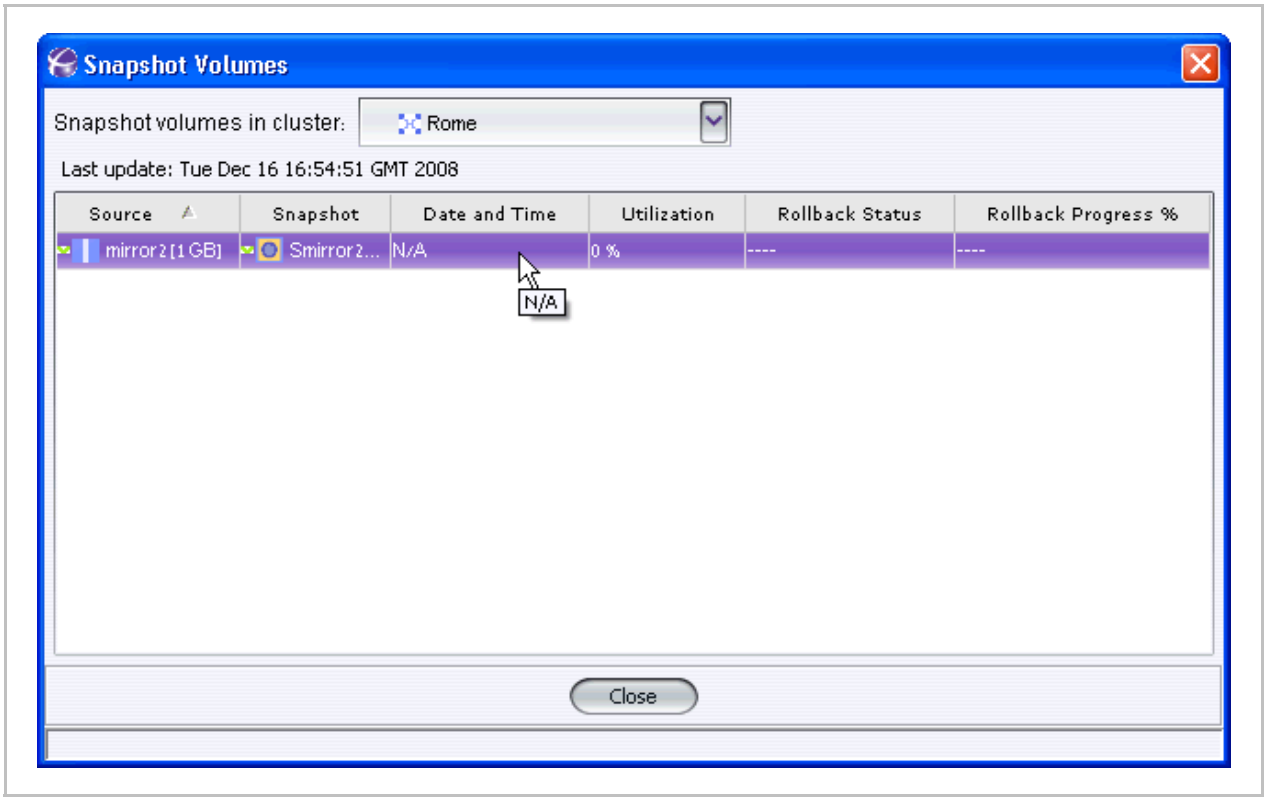



*Figure 4-83. Snapshot Volumes*

2. Right click and select **Activate**.

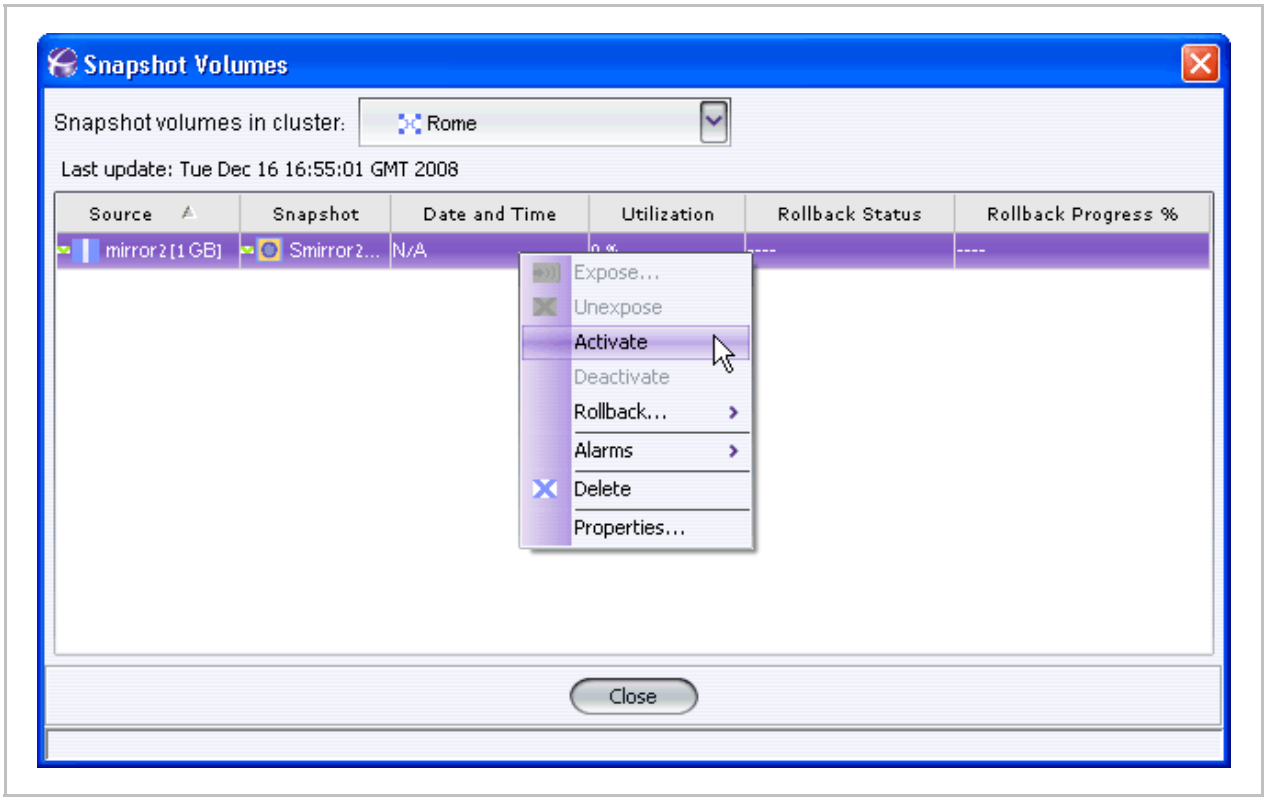



*Figure 4-84. Activating a Snapshot*

The snapshot is now active. Write operations will begin according to the configured time schedule. The snapshot Date and Time property will change from not active (N/A) to the date and time that the snapshot was started.

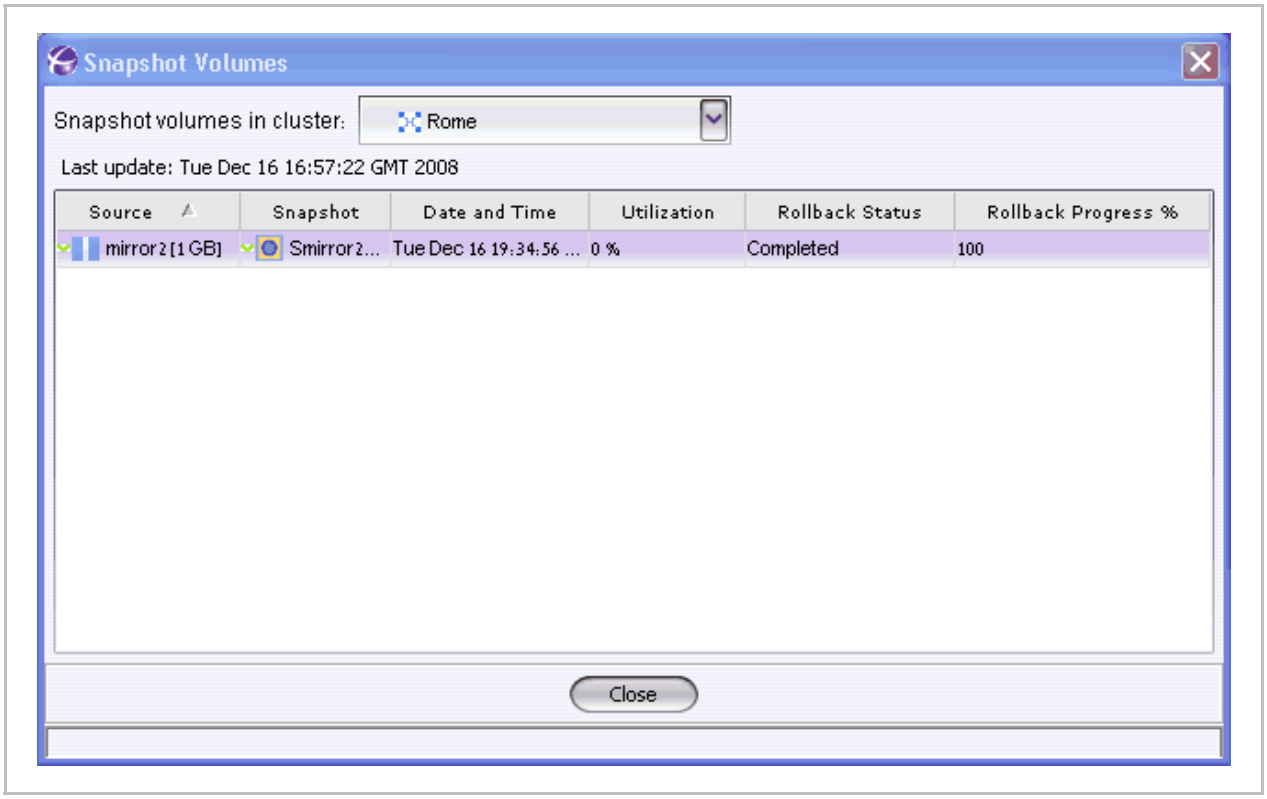



*Figure 4-85. Activated Snapshot*

## Deactivating a Snapshot

> **Note**
> *Deactivating an active snapshot erases all data contained on the snapshot.*

***To deactivate a snapshot:***

1. Select the snapshot volume you want to deactivate.
2. Right click and select **Deactivate**.

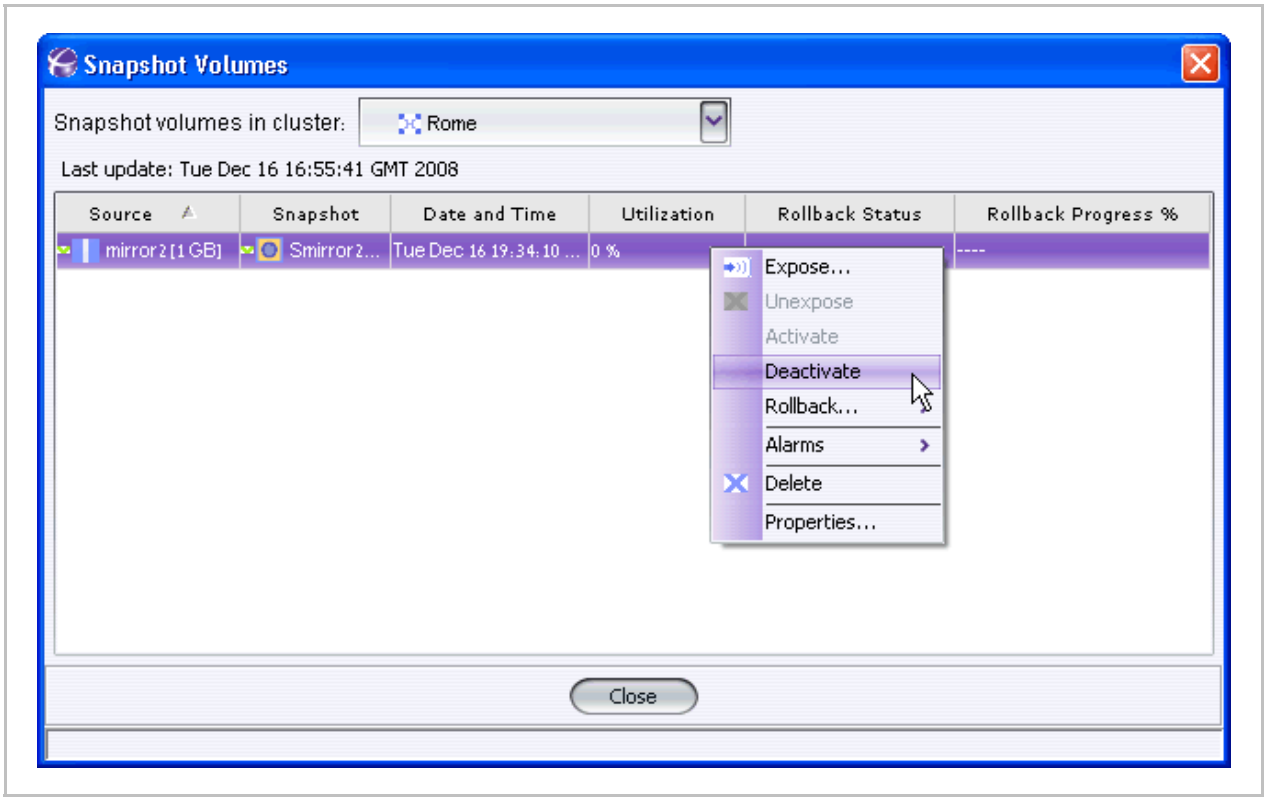



*Figure 4-86. Deactivating a Snapshot*

The snapshot is now deactivated. All data on the snapshot is erased. The snapshot Date and Time property will change from the date and time that the snapshot was started to not active (N/A).

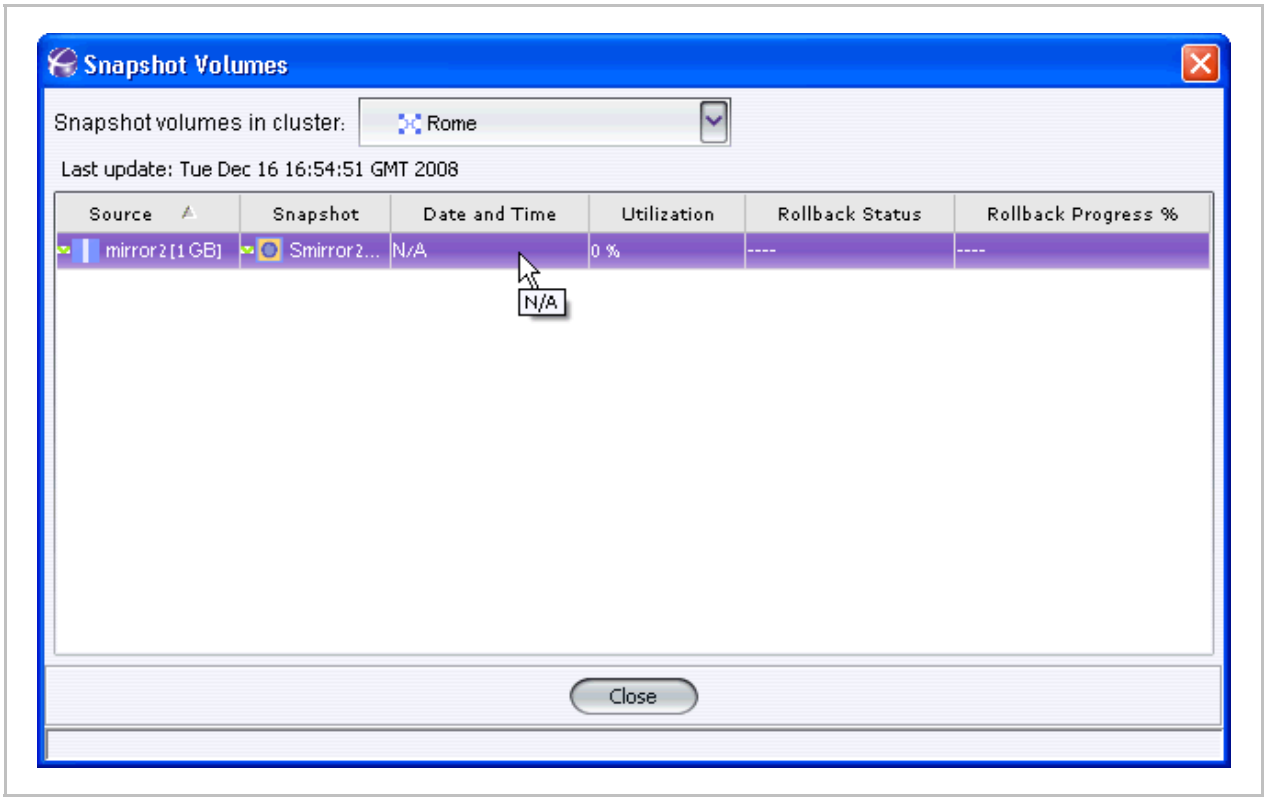



*Figure 4-87. Deactivated Snapshot*

## Viewing Snapshot Volumes

You can view all created snapshot volumes, the exposing i series, the time the snapshot was created and the percent capacity utilization. The default load threshold is eighty (80) percent. When the default threshold is exceeded, a resize snapshot alert is sent.

***To view snapshots:***

1. From the *Quick Launch:*
   **Monitor > Snapshots**

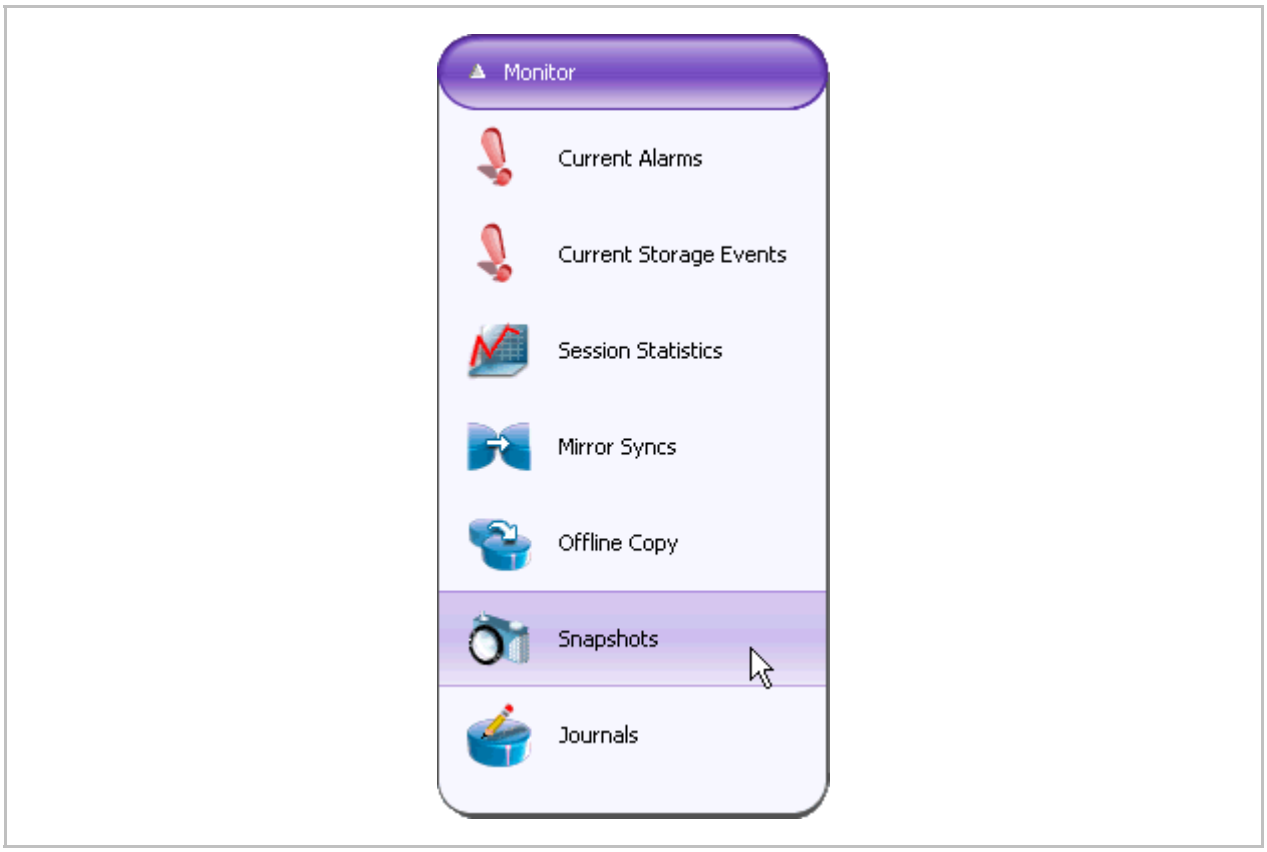



*Figure 4-88. Quick Launch - Create Volume*

The Snapshot Volumes window appears.

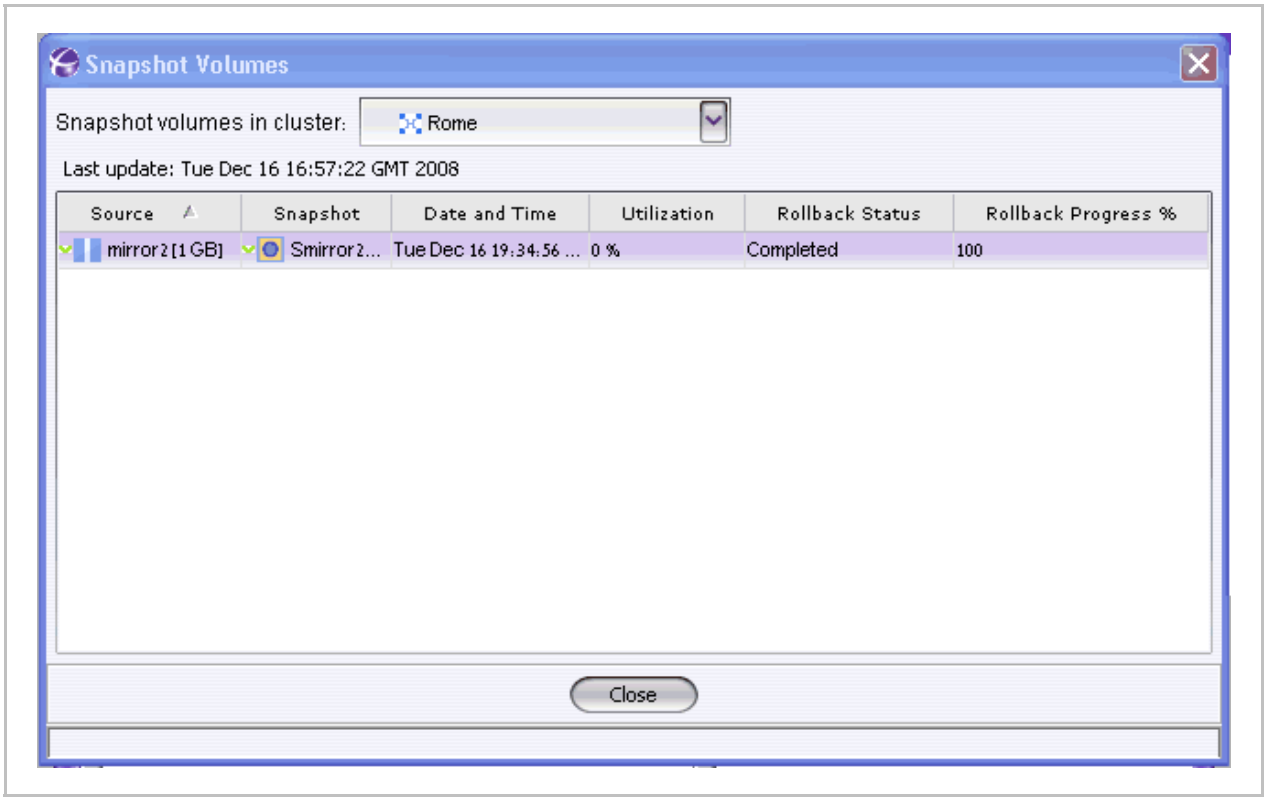



*Figure 4-89. Snapshot Volumes*

## Snapshot Rollback

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

> **Note:**
> *In order to avoid any writes to the volume while snapshot rollback is active, bring down any applications that use the volume.*

***To rollback a snapshot:***

1. From the snapshot volumes window, right click on desired active snapshot and select **Rollback > Start**.

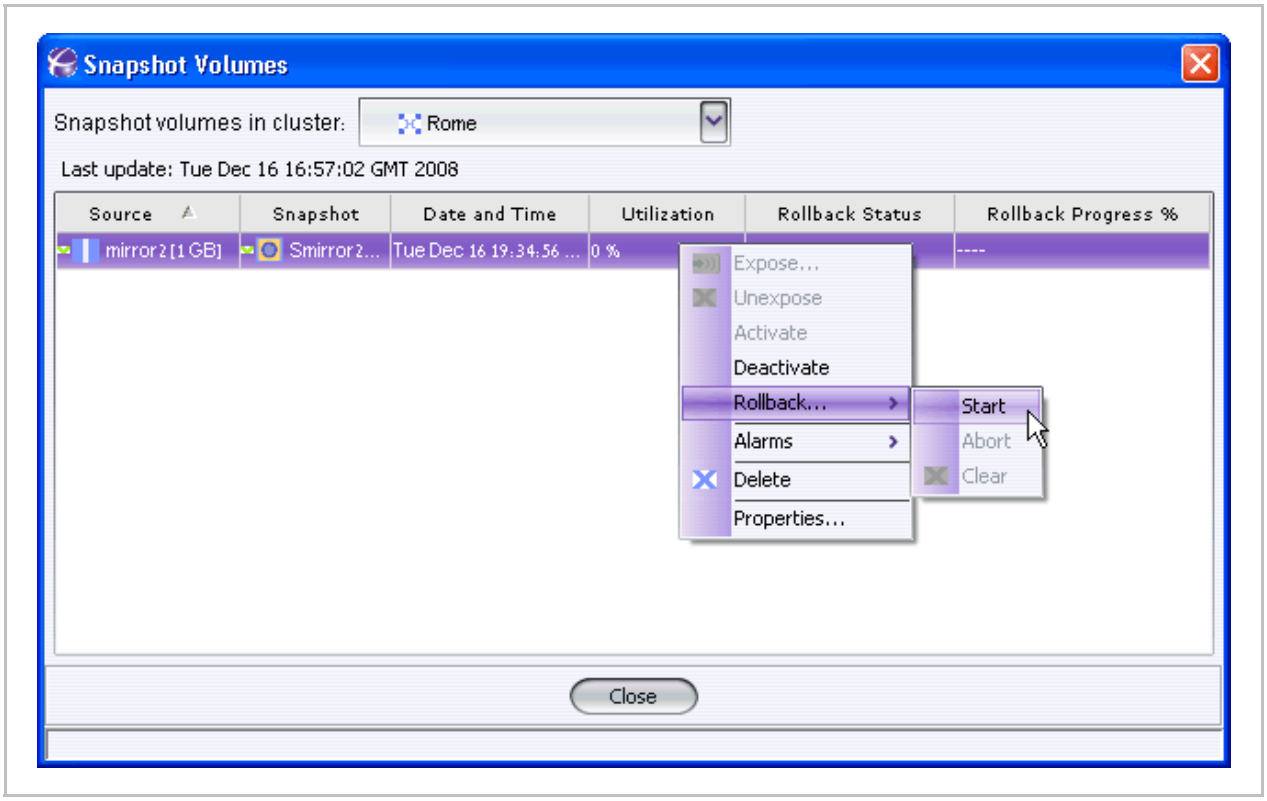



*Figure 4-90. Snapshot Volume Window*

A warning message appears.

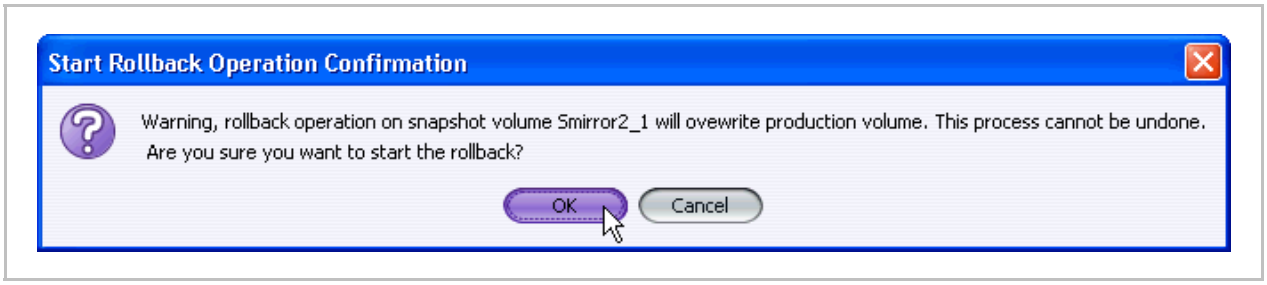



*Figure 4-91. Snapshot Volume Window*

2. Click **OK**.

   The rollback starts. Rollback Progress and Rollback Status are indicated in the Snapshot window.

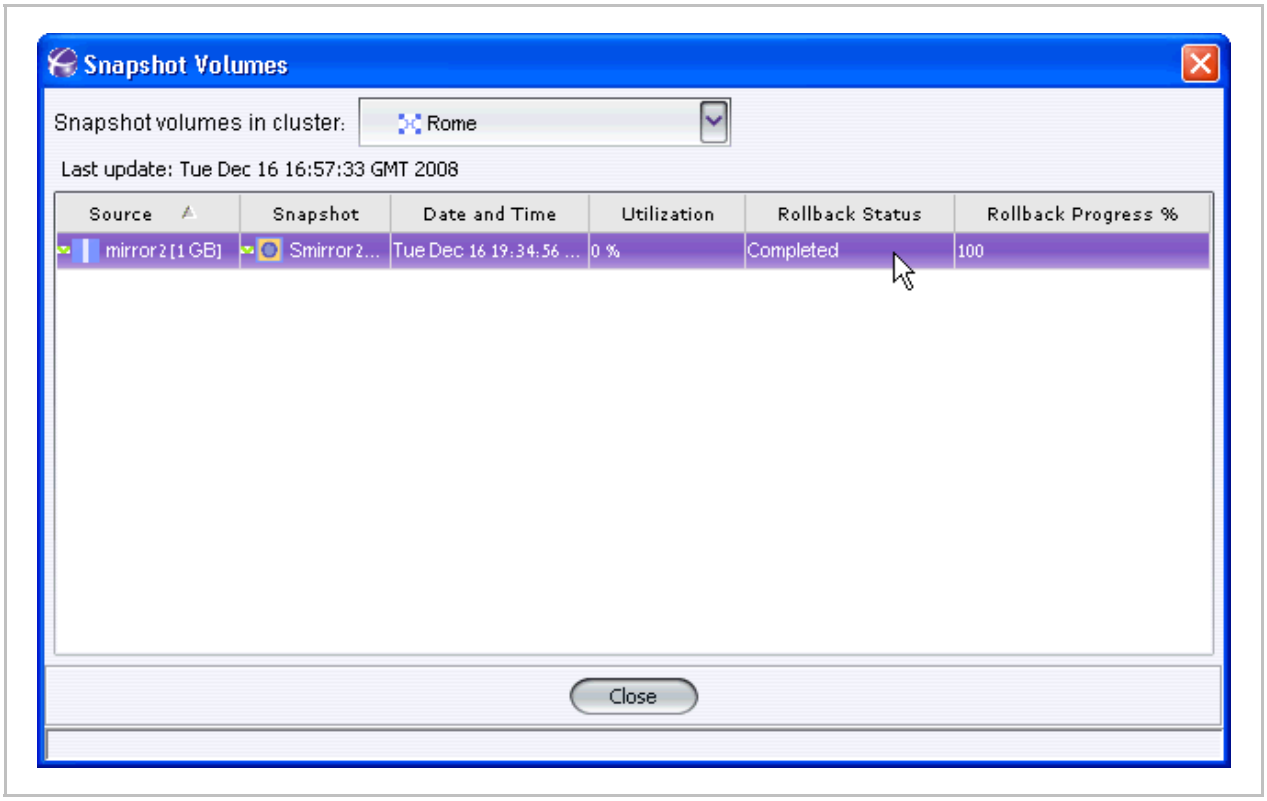



*Figure 4-92. Snapshot Rollback Completed*

## Configuring i series for VSS

The i series can be used as the VSS hardware provider for a Windows Application server.

***To configure Windows Application server to use the i series as the VSS hardware provider:***

1. On the Windows 2003 Application server, double click on the **i series manager**_VSS_Setup.exe file in the **i series manager** folder on the NEXSAN CD shipped with the i series.

   The VSS Wizard opens (Figure 4-93).

2. Click **Next**.

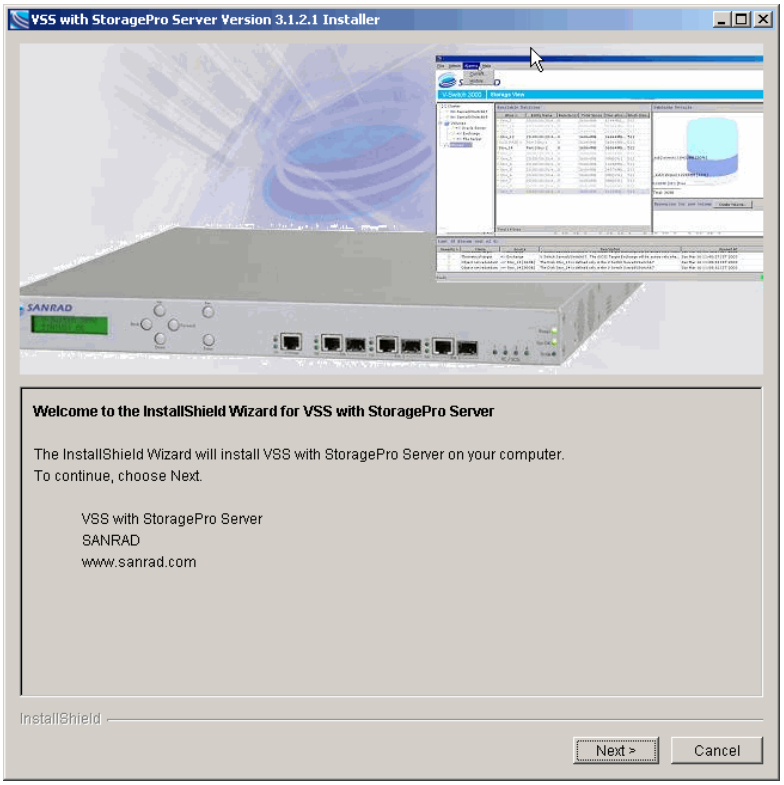



*Figure 4-93. Install NEXSAN VSS driver on the Windows Application server (Change Picture)*

3. Open the **i series manager** GUI and configure disks as "**Allocable**".

***To allocate storage for the snapshots:***

1. Right click the desired storage object and select Properties.

> **Note:**
> *It is recommended to allocate one physical disk in a disk array (or one single disk on a JBOD) to be used as the storage area for the snapshots. The total size of this disk should be at least 20% of all production volumes size (in total) you are planning to backup using VSS.*
> *However, if you can not allocate a dedicated physical disk, you still can use disks that are already in use. The system will take what ever space it can grab from all these disks to create the snapshots.*

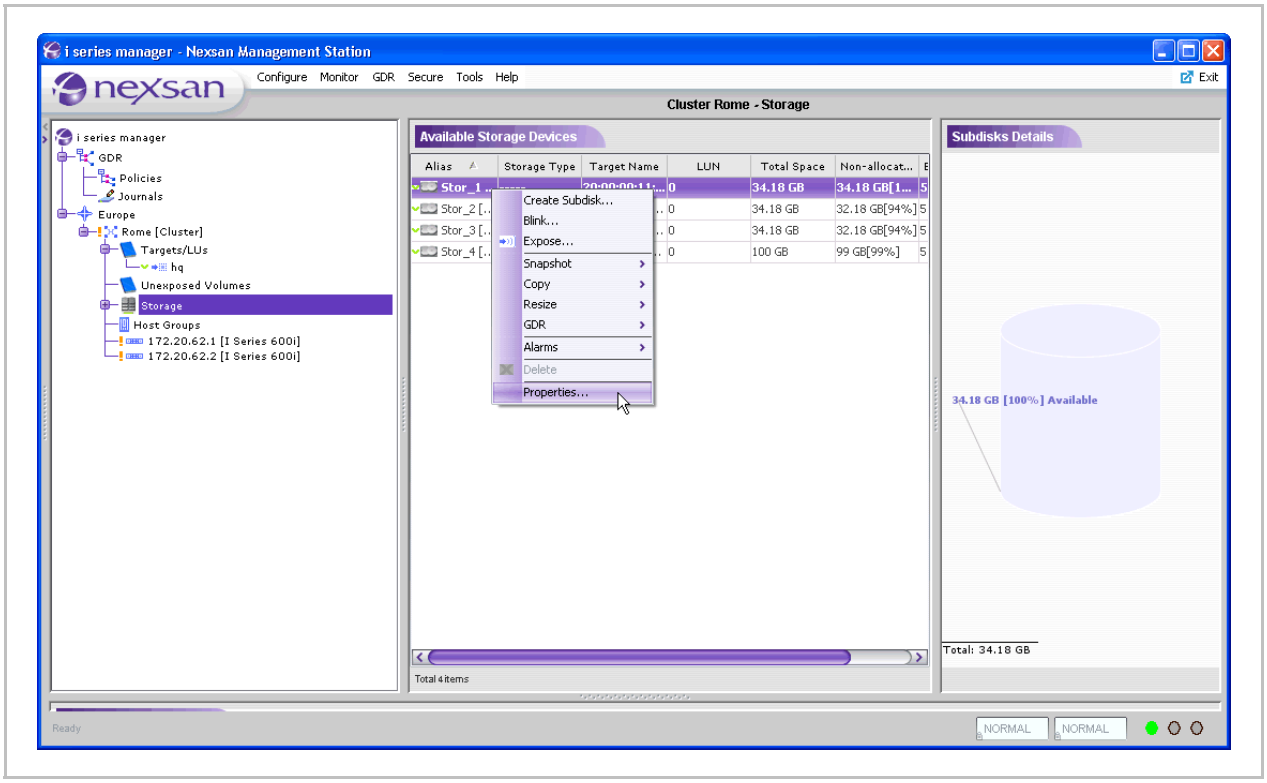



*Figure 4-94. Disk Properties*

The Disk Properties window appears.


*Figure 4-95. "Allocable" in the Disk Properties*

2. Check "**Allocable**" and click **OK**.

# Resizing Volumes

Resizing volumes allows you to add storage easily. Resizing volumes is a two part process. First the volume is resized, second, it is expanded. If for some reason you decide not to expand the volume, you can retract it and remove the added volume(s) used to resize the original volume.

***To resize volumes:***

1. From the Exposed Volumes pane, select the volume.
2. From the Volume Details pane, right click the child to resize and select **Resize**.

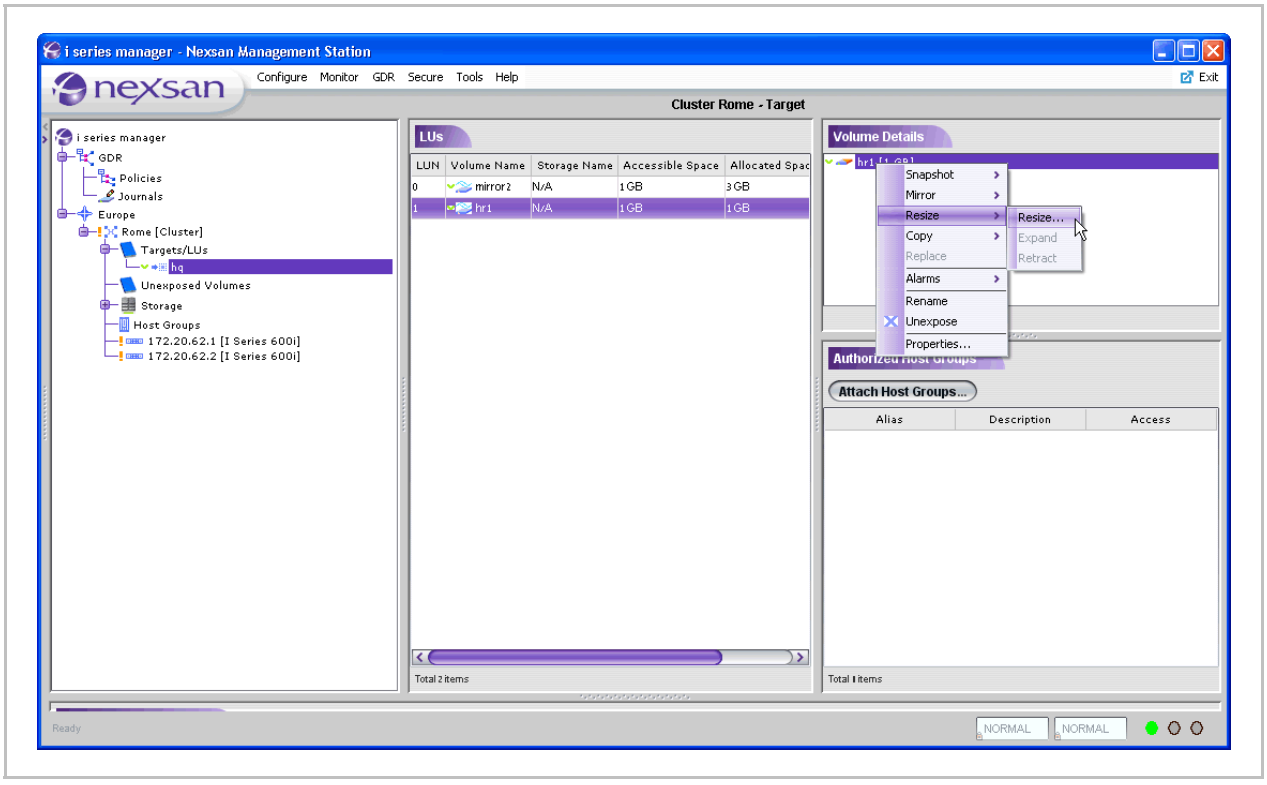



*Figure 4-96. Volume Selected*

The Resize window opens with all available resources.

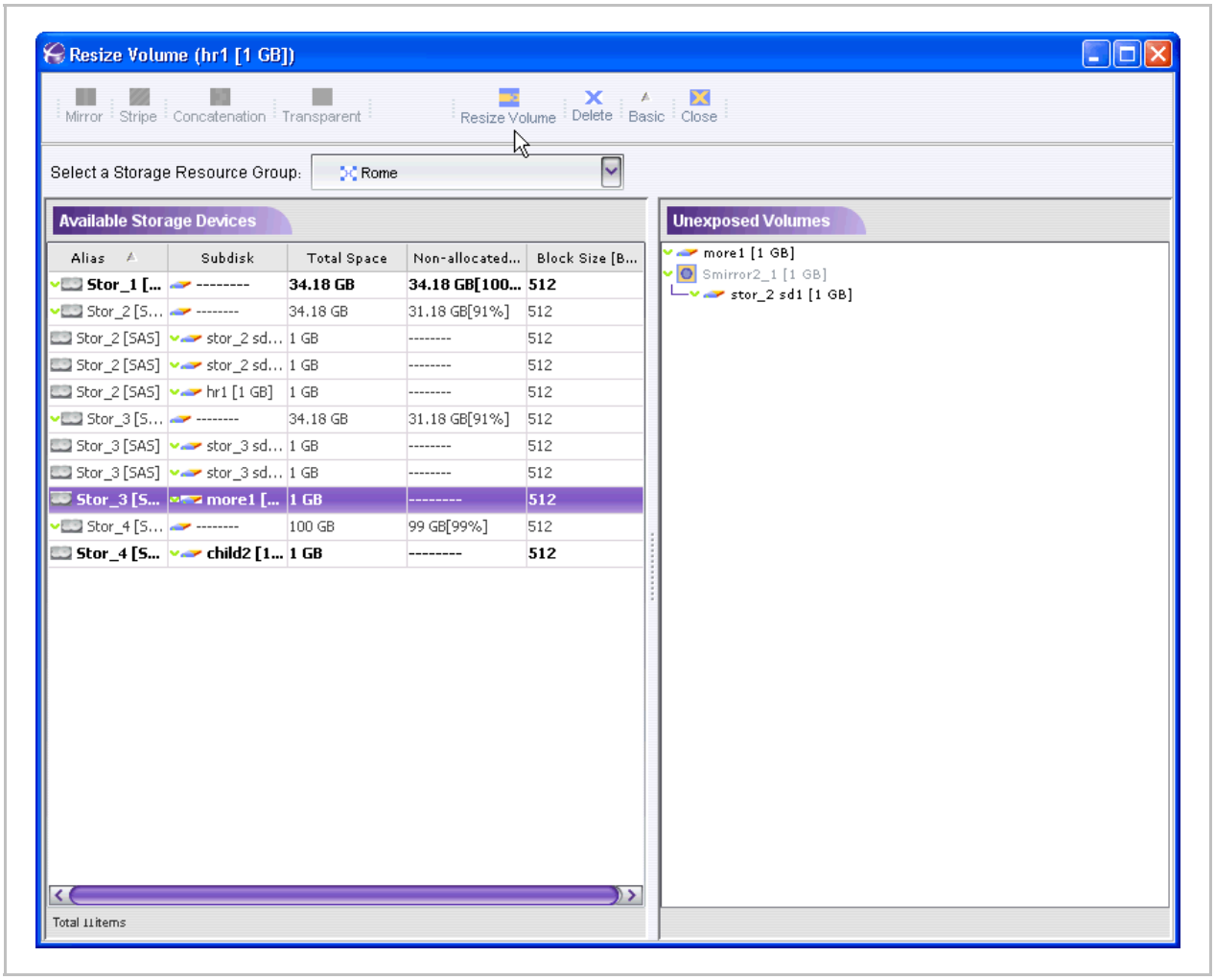



*Figure 4-97. Resource Selected for Resize*

3. Select a resource for resizing the volume and click Resize .

   The New Cube Volume dialog box opens

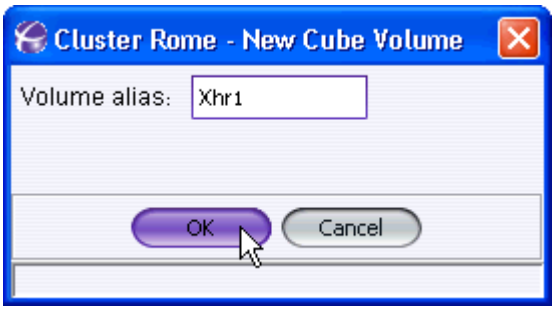



*Figure 4-98. New Cube Volume*

4. Click **OK**.

   The resized volume now appears in the Volume Details pane as a cube .

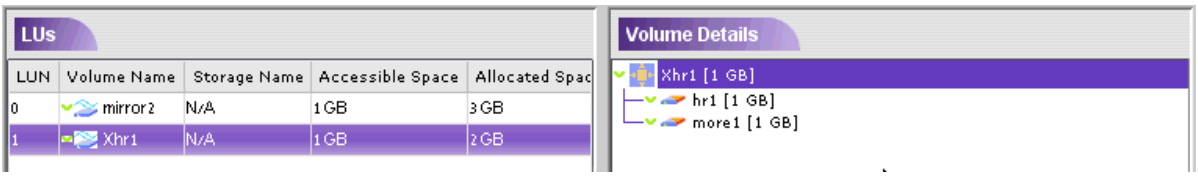



*Figure 4-99. Cube Volume*

**Note:**

- You must Expand the volume before you can use the new added volume.
- Resized volumes can be retracted before being expanded.

### *To expand volume*

- In the Exposed Volumes screen, from the Volume Details pane, right click the volume and select **Resize > Expand**.

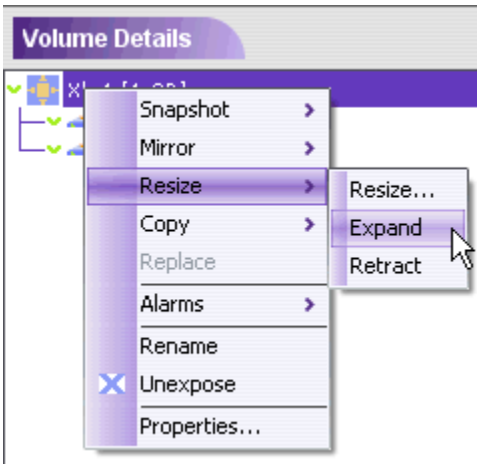



*Figure 4-100. Resize Menu*

The expanded volume now appears in the Details pane.

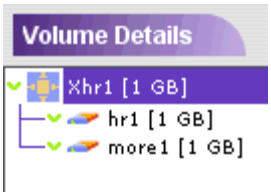



*Figure 4-101. Resized Volume*

***To retract a volume before expanding its hierarchy:***

- From the Details pane, right click the child to resize and select **Retract**.

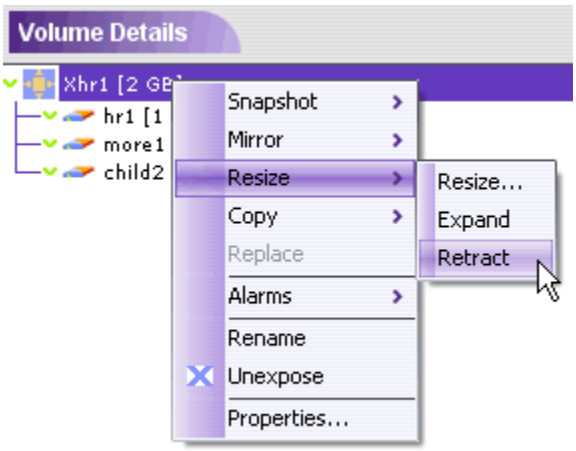



*Figure 4-102. Retract Menu*

The cube volume is dissembled and the volume that was added during the resize is removed.

# Renaming Volumes

You can rename disks, subdisks and exposed/unexposed volumes.

***To rename a disk:***

1. From the list of Available Storage Devices (Figure 4-103), double click on the name of the disk that you want to rename.

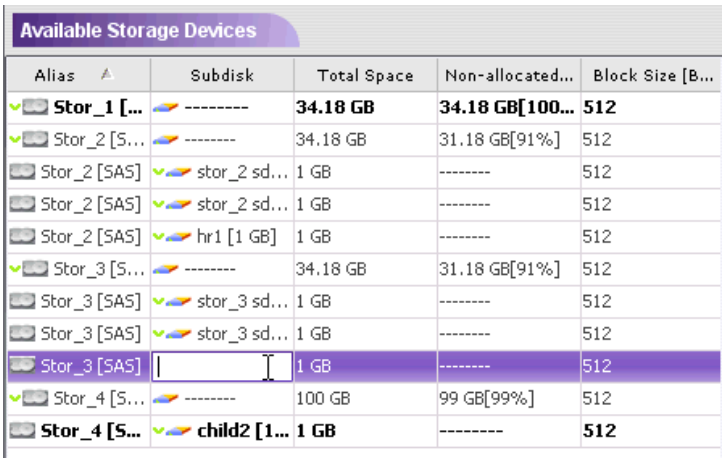



*Figure 4-103. Rename Disk*

2. Enter the new name in the Alias field.

   The new name appears in the list.

### *To rename a subdisk:*

1. From the list of Available Storage Devices (Figure 4-104), double click on the name of the subdisk that you want to rename.

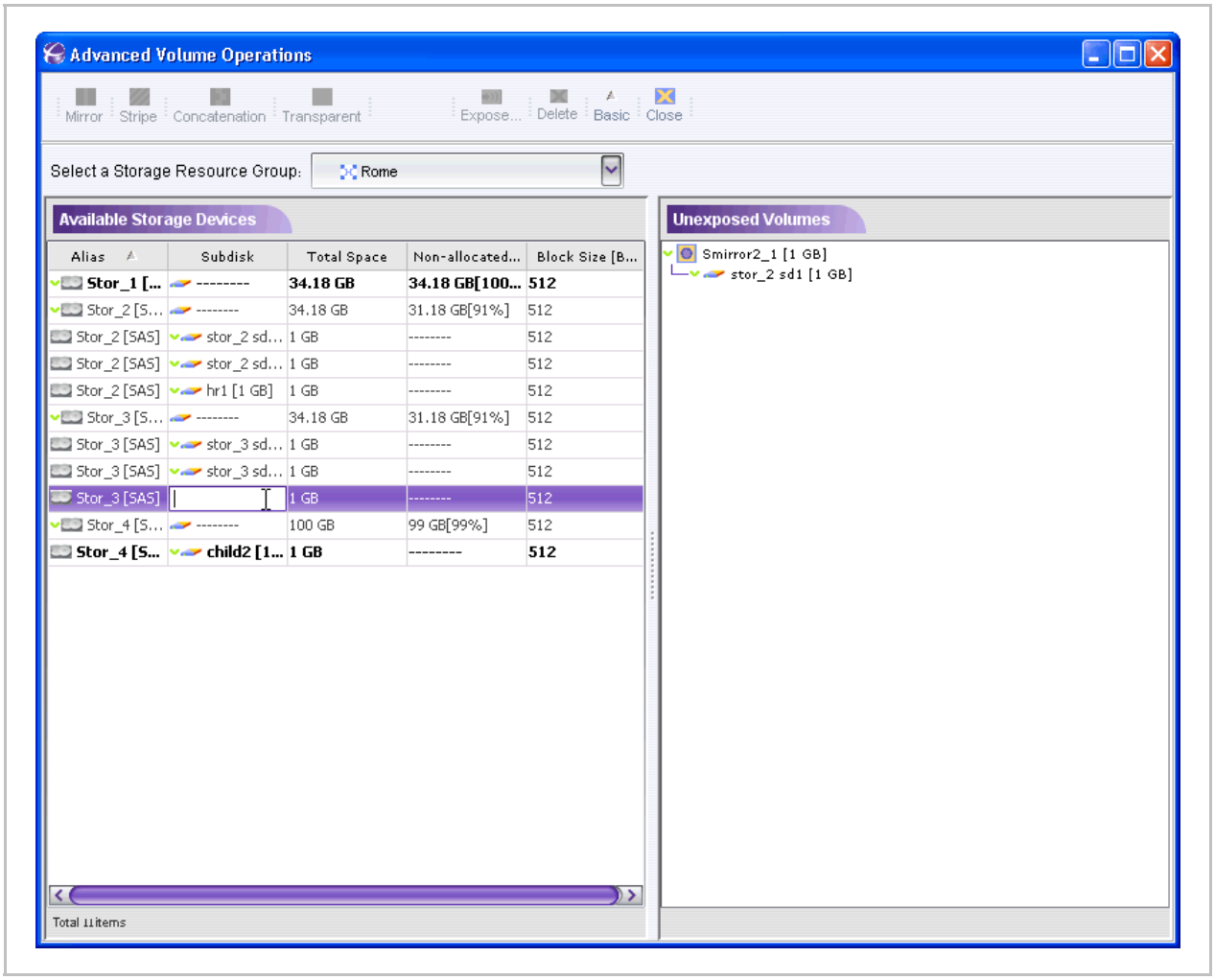



*Figure 4-104. Renaming Subdisk*

2. Enter the new name.

   The new name appears in the list.

### *To rename volumes:*

1. From the Volume Details pane, select the volume to rename.

2. Right click and select **Rename**.

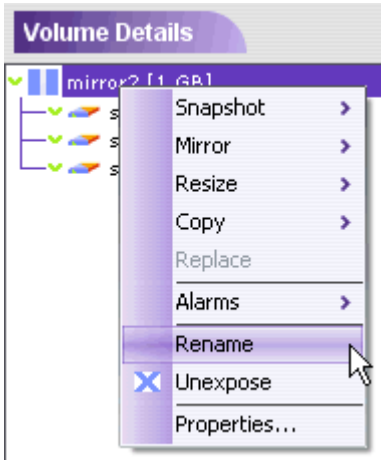



*Figure 4-105. Rename Volume*

The Volume Details window appears.

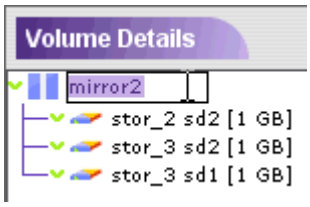



*Figure 4-106. Renaming Volume*

3. Click on the volume name and enter the new name.
4. Click Enter.

# Unexposing Volumes (Deleting LUNs)

When you unexpose a volume, its LUN is deleted.

***To unexpose a volume:***

1. Select the volume
2. In the Exposed Volumes View screen, from the Exposed Volumes or Volume Details pane, select the volume, right click and select **Unexpose**.

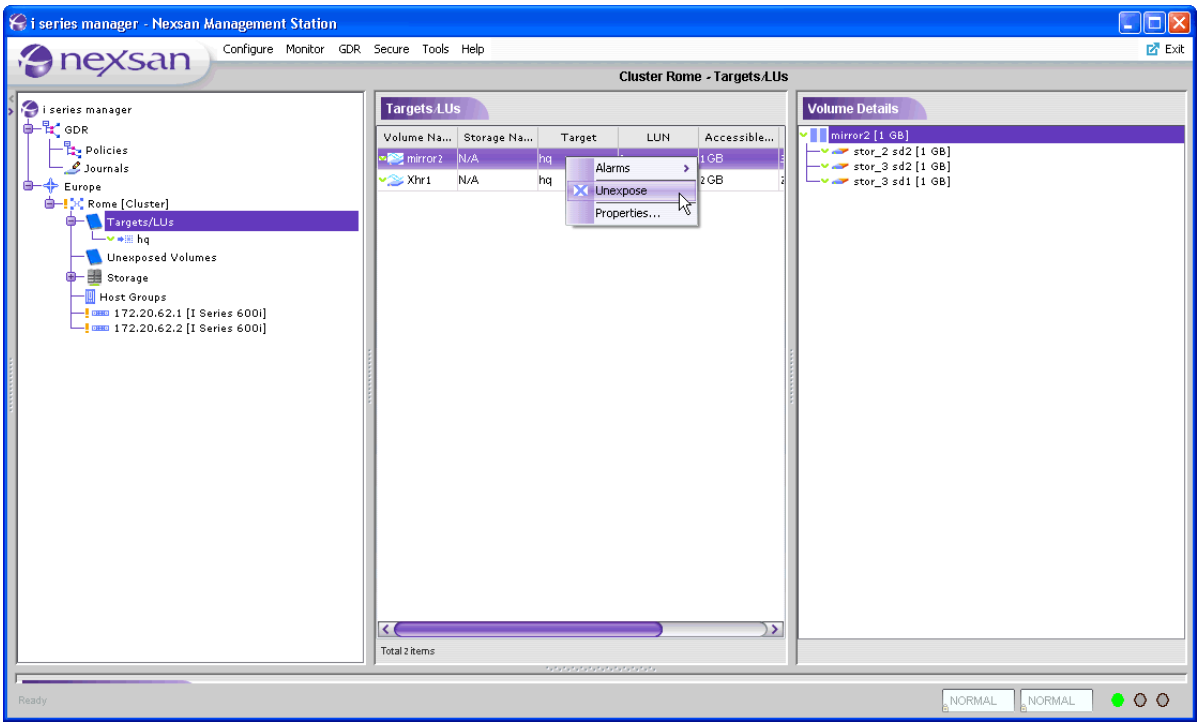



*Figure 4-107. Volume Selected to Unexpose*

The Unexpose confirmation box opens.

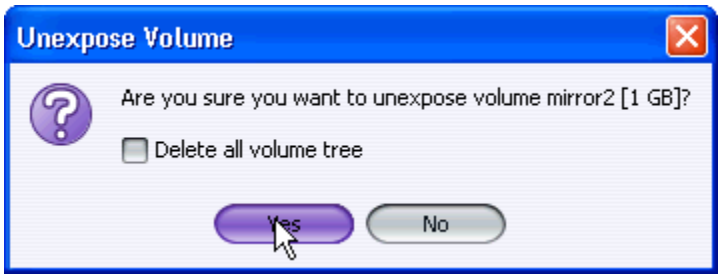



*Figure 4-108. Delete LU Confirmation Box*

3. Click **Yes**.

   The unexposed volume now appears in the Create Volume window.

# Deleting Volumes

**Notes:**

- Only unexposed volumes can be deleted.
- When deleting the top level on a hierarchy comprised of virtual components, only the top level is deleted and not the underlying volumes hierarchies which can subsequently be removed.

***To delete unexposed volumes:***

1. In the Unexposed Volumes View screen, right click the volume and select **Delete**.

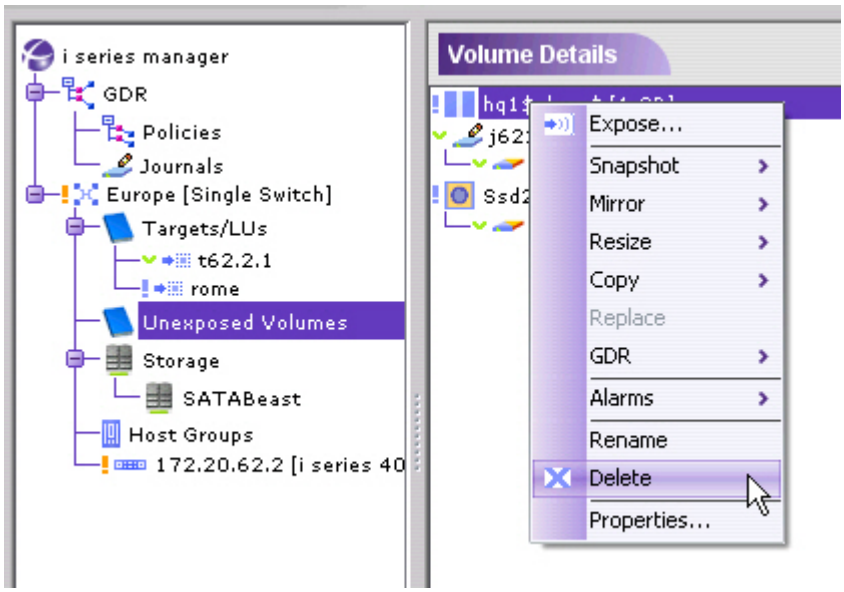



*Figure 4-109. Delete Unexposed Volume*

The Delete Volume confirmation box appears.

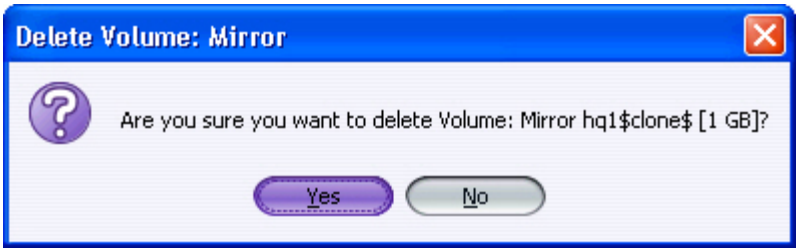



*Figure 4-110. Delete Volume Confirmation*

2. Click **Yes** to confirm the delete.

   Deleted component volumes are now available in the Create Volumes window.

***To delete a subdisk:***

1. In the Subdisks Details pane (Figure 4-111), click on the subdisk to delete.

   The selected subdisk is outlined in red.

2. Right click and select **Delete**.

   The subdisk is deleted.

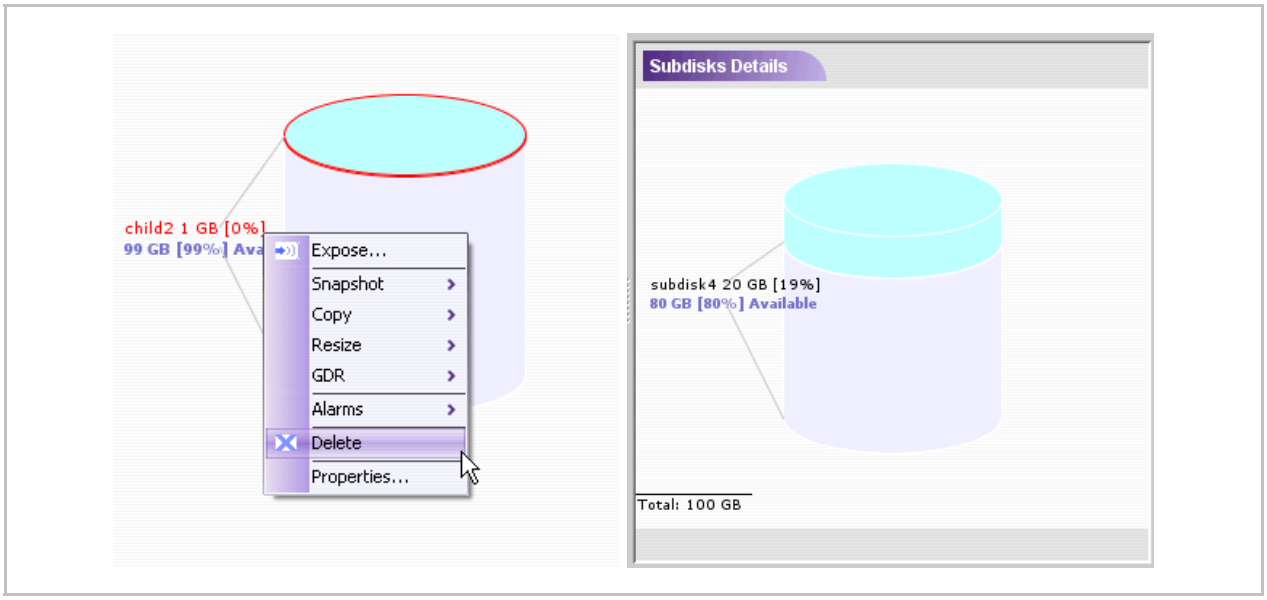



*Figure 4-111. Deleting Subdisks*

**Note:**
*You can't delete a subdisk that is part of a volume (exposed or unexposed).*

# Chapter 5

# Monitoring & Statistics

The i series enables RFC standards compliant health, interface and session monitoring and statistics reporting of all interfaces. For specific details on a monitoring or statistic parameter, consult RFC 2863.

## Health Monitoring

You can monitor the status of i series hardware.

***To view i series hardware status:***

- In the Navigation pane, right click on the i series and select **Hardware**.

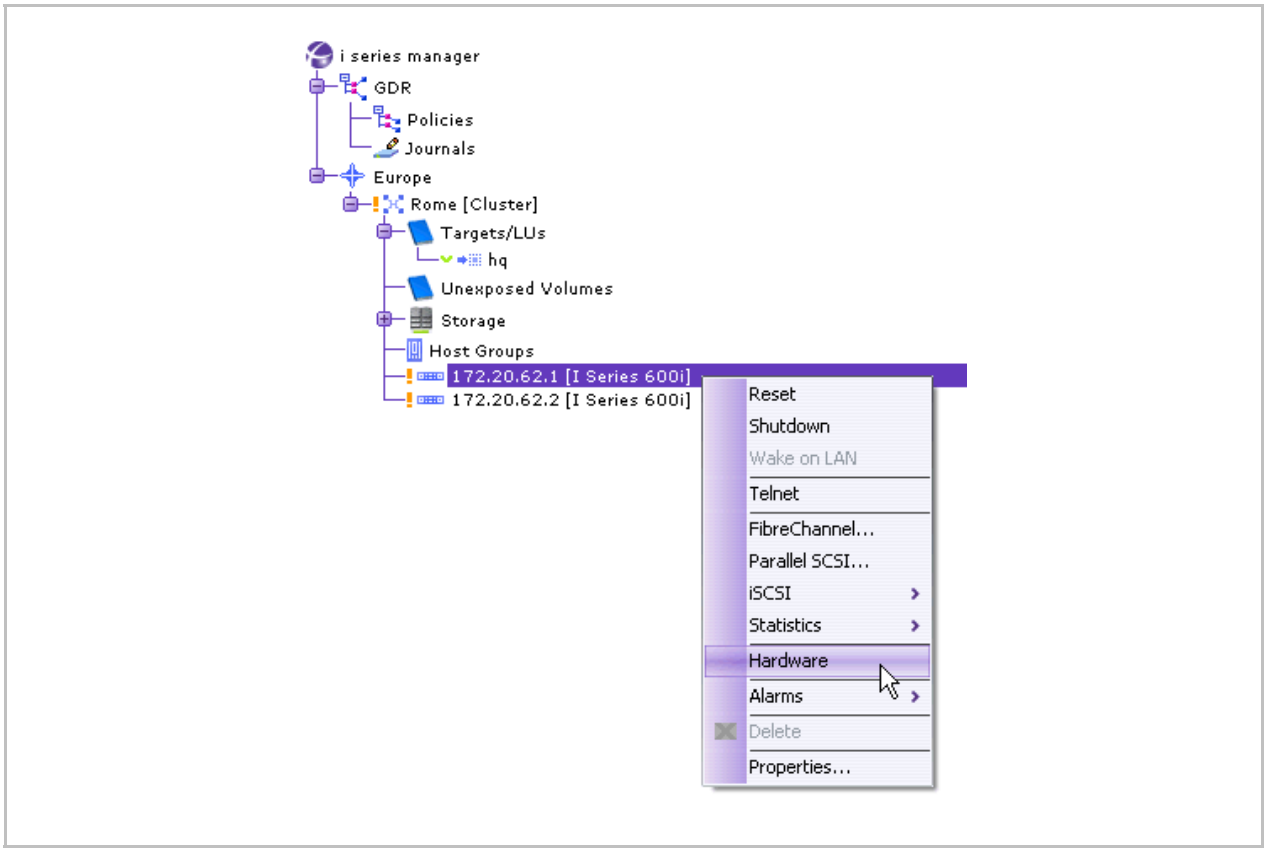



*Figure 5-1. Hardware Selected from i series Menu*

The i series Hardware Status window opens.

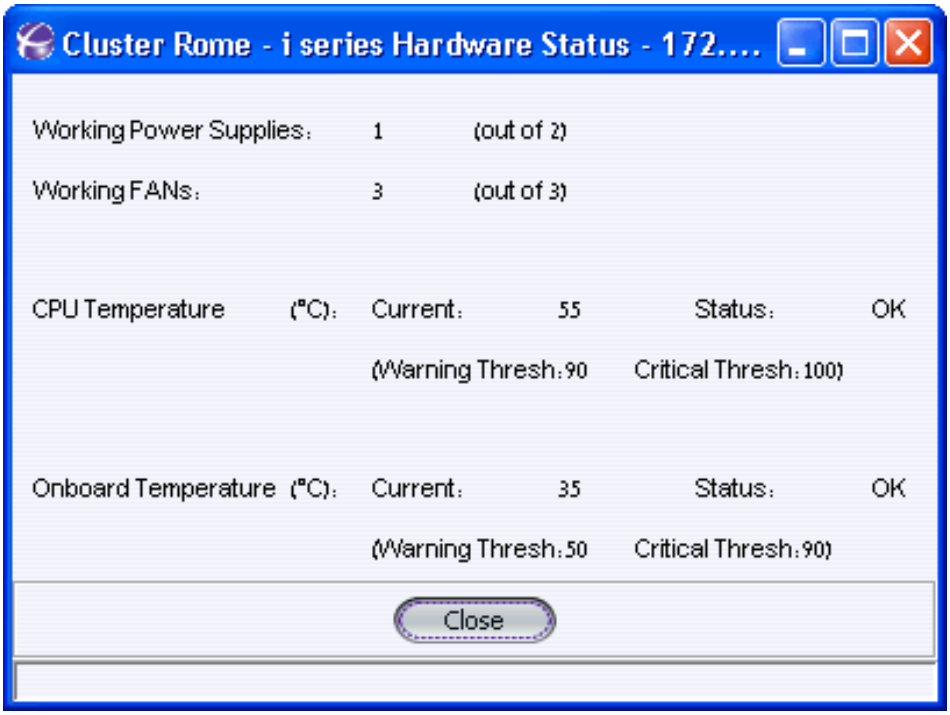



*Figure 5-2. i series Hardware Status Window*

# Scroll and Zoom Functions

The performance statistics graphs include both scroll and zoom functions. These functions are accessed via the different Statistics menus detailed below.

***To scroll within a window:***

1. Click the scroll icon 

in the top right corner of the graph.

   The cursor becomes a hand when placed inside the graph.

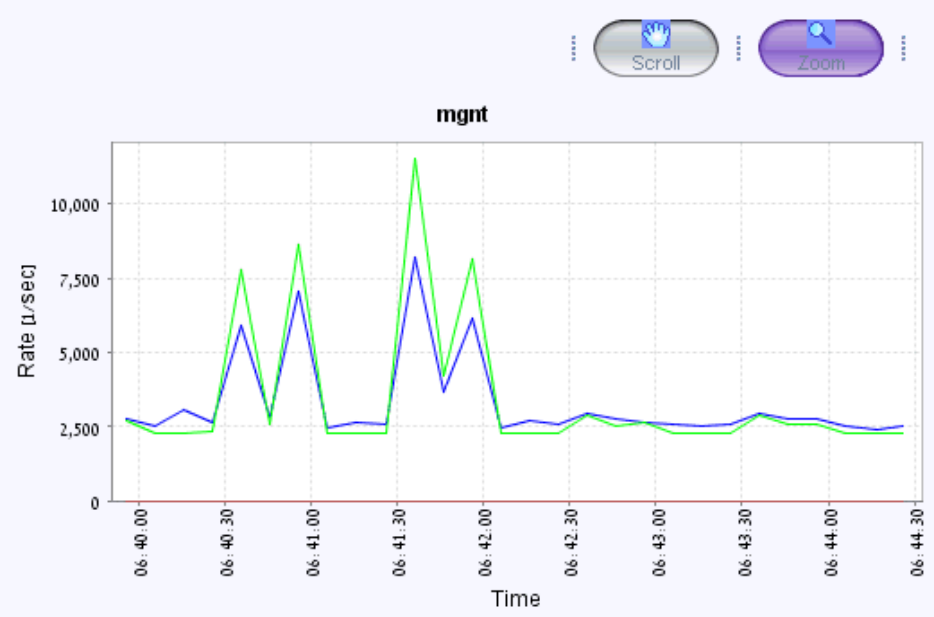



*Figure 5-3. Scrolling within Graph*

2. Holding down the left mouse button move the scroll hand in the direction you want to scroll.

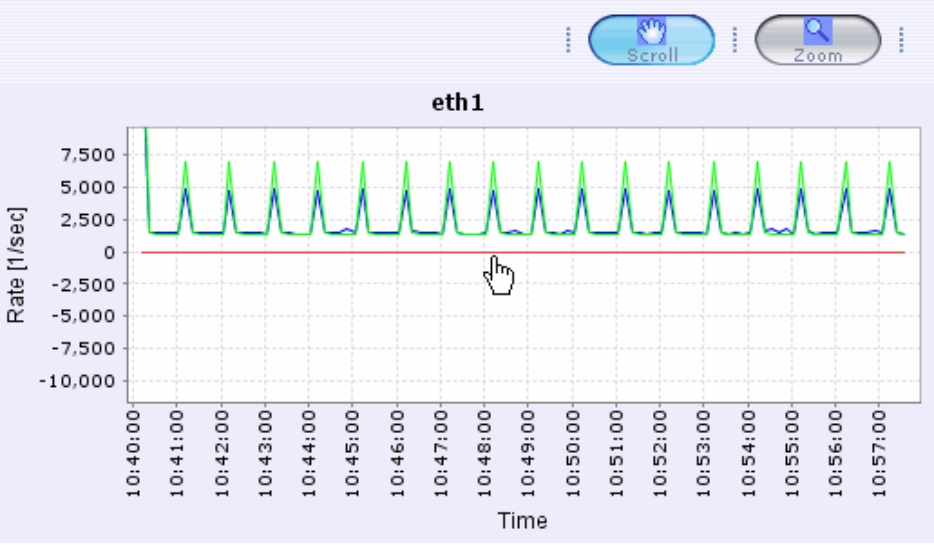



*Figure 5-4. Graph Scrolled*

***To quick zoom an icon:***

1. Click the zoom icon 

in the top right corner of the graph.
2. Hold down the left mouse button and select the area to zoom in on.


*Figure 5-5. Graph Area Selected*

3. After the area is selected, release the mouse button.

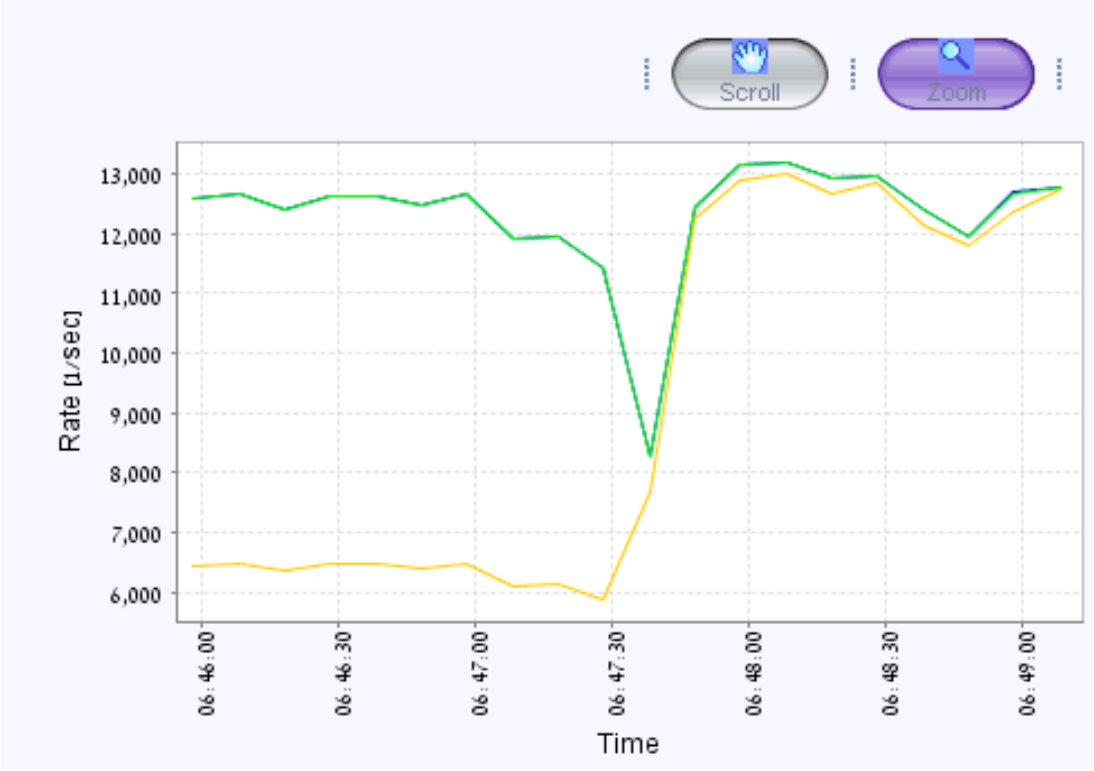



*Figure 5-6. Area Zoomed In*

***To zoom in/out on a specific range:***

1. Click the zoom icon 

in the top right corner of the graph.
2. Place the cursor in the graph. Right click and open the context menu.
3. Select to zoom in or out and along which axes.

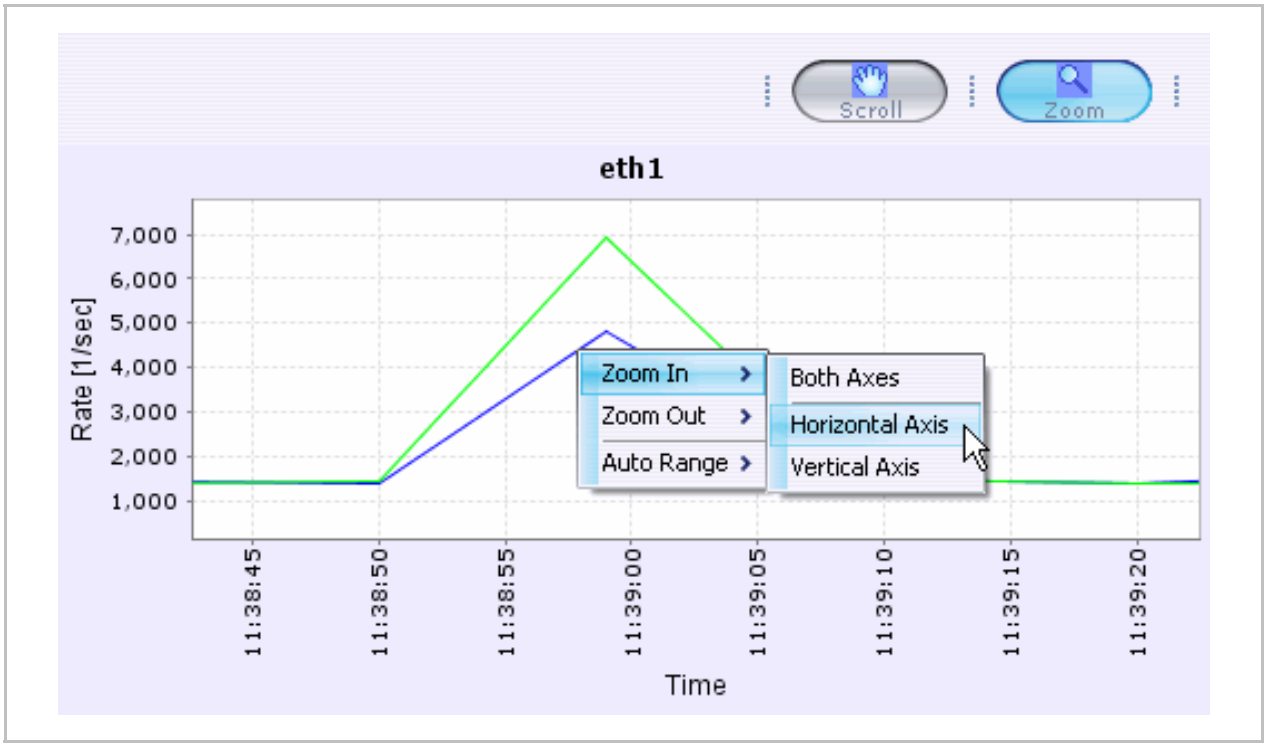



*Figure 5-7. Zoom Context Menu*

# Interface Statistics and Counters

You can view interface traffic statistics and errors for each i series interface to aid in system diagnostics

***To view interface statistics:***

- In the Navigation pane, select the i series, right click and select **Statistics > Interfaces**.

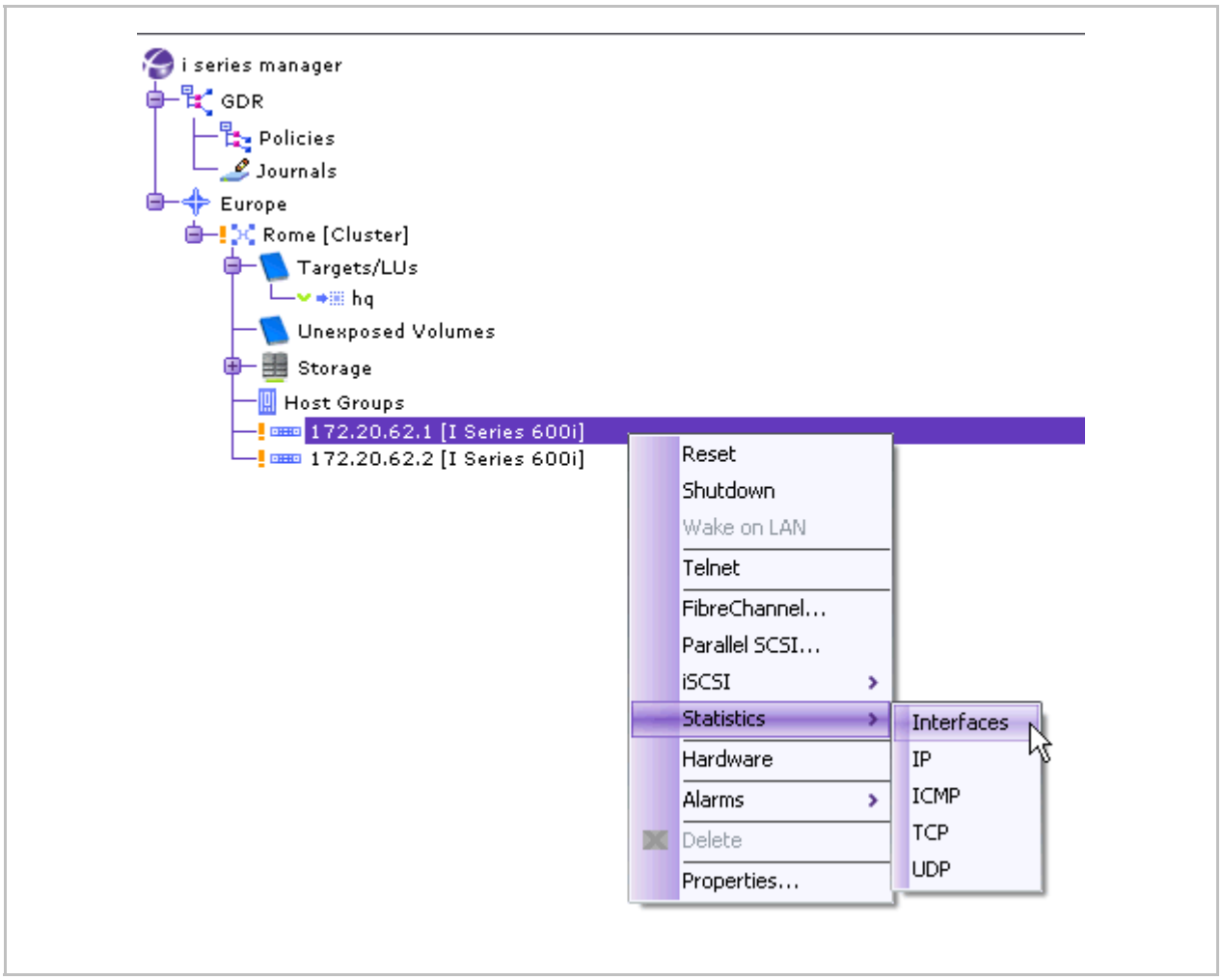



*Figure 5-8. Interface Statistics Selected from i series Menu*

The Interface Statistics window opens.

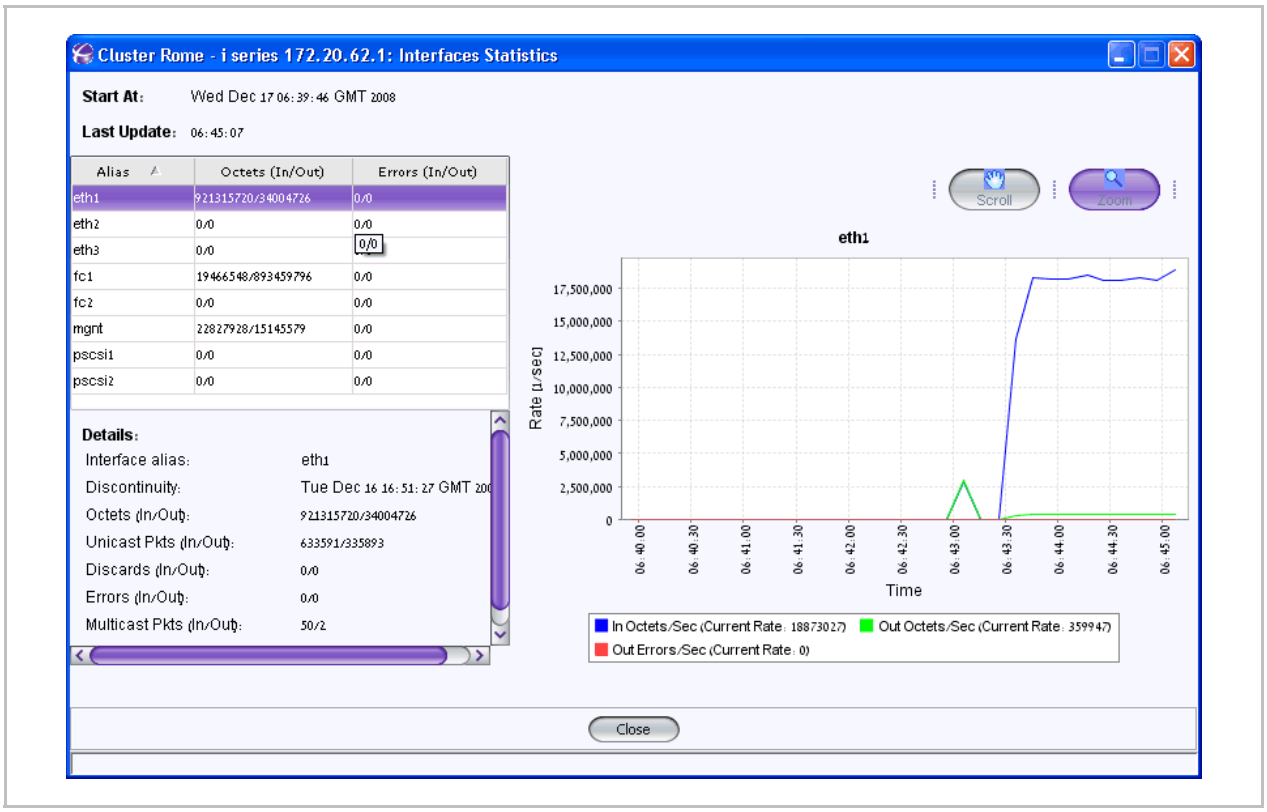



*Figure 5-9. i series Interface Statistics*

## IP

### *To Viewing TCP/IP Counters:*

- In the Navigation pane, select the i series, right click and select **Statistics > IP**.

  The IP Statistics window opens.

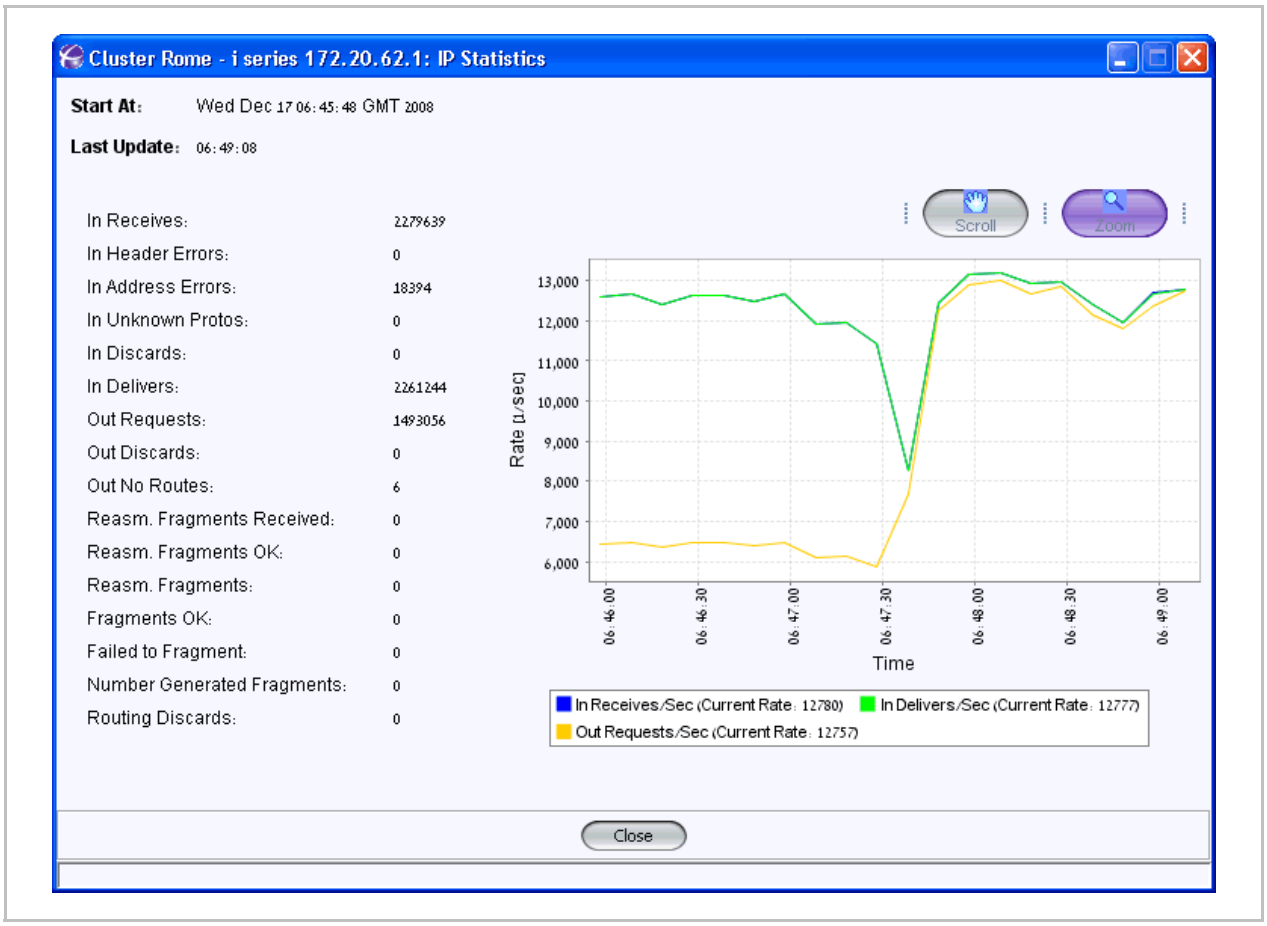



*Figure 5-10. IP Statistics*

## ICMP

### *To View ICMP Statistics:*

- In the Navigation pane, select the i series, right click and select **Statistics > ICMP**. The ICMP Statistics window opens.

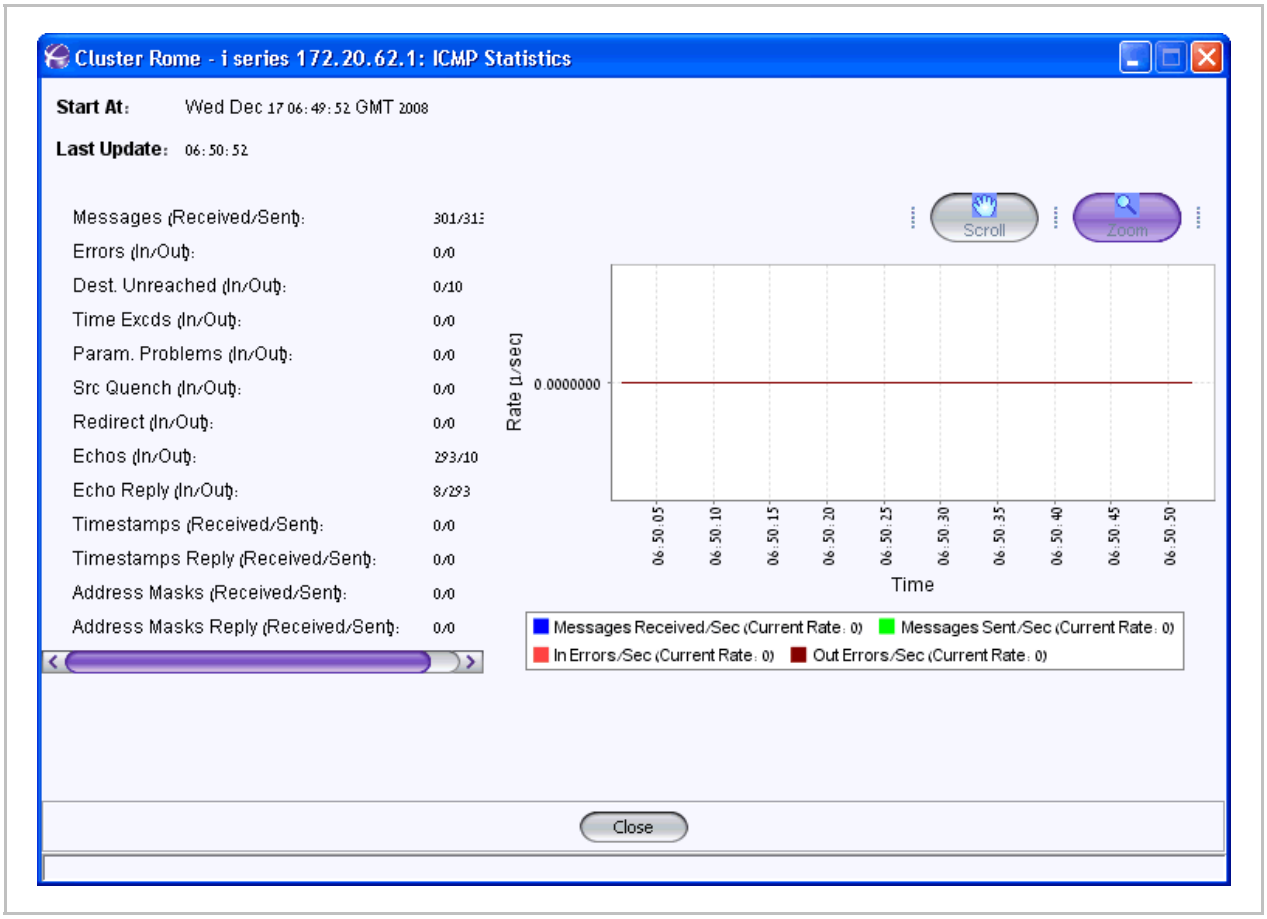



*Figure 5-11. ICMP Statistics Window*

## TCP

***To view TCP Statistics:***

- In the Navigation pane, select the i series, right click and select **Statistics** > **TCP**.

  The TCP Statistics window opens.

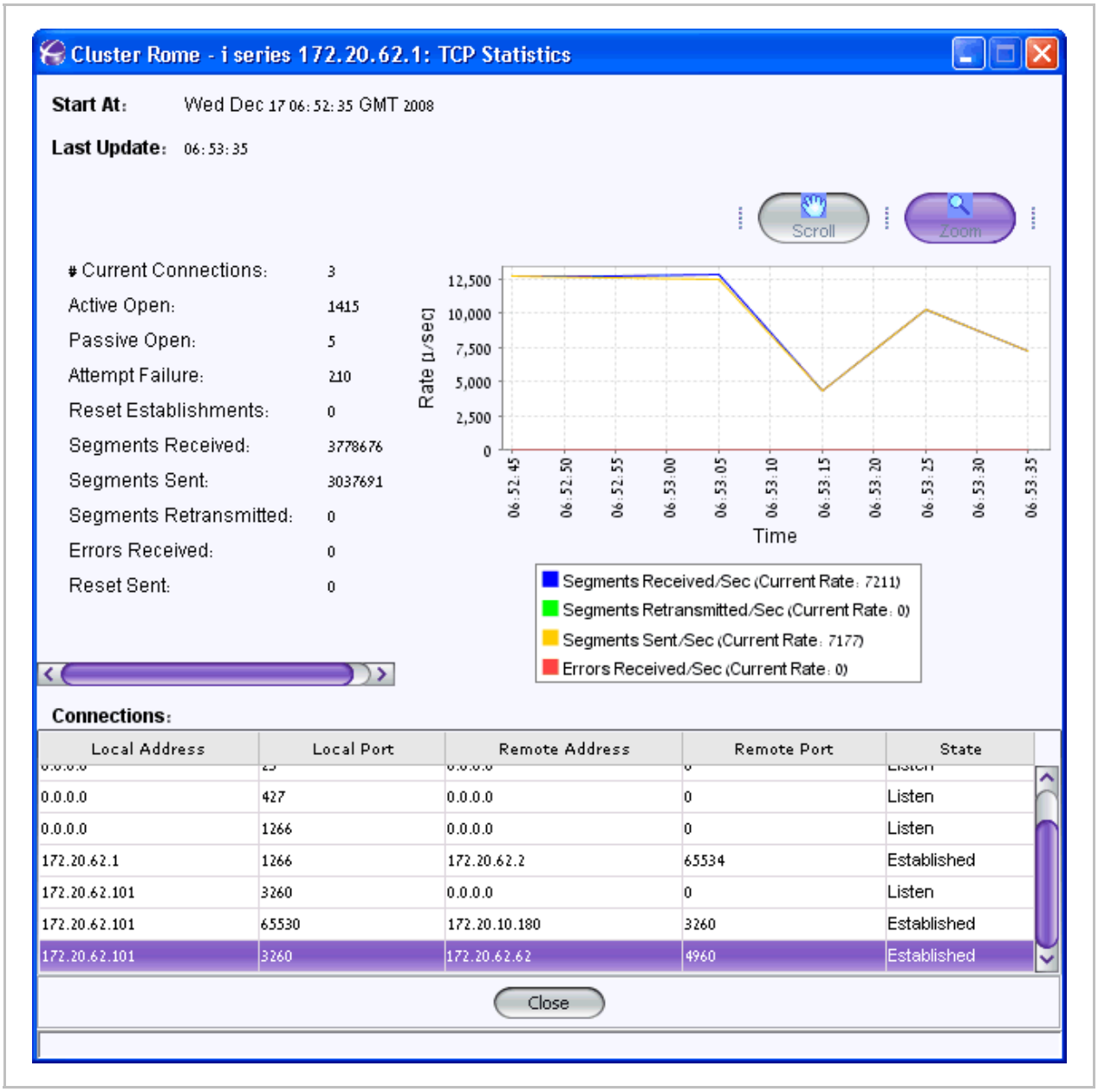



*Figure 5-12. TCP Statistics Window*

## UDP

### *To view Viewing UDP Statistics:*

- In the Navigation pane, select the i series, right click and select **Statistics > UDP**.

  The UPD Statistics window opens.

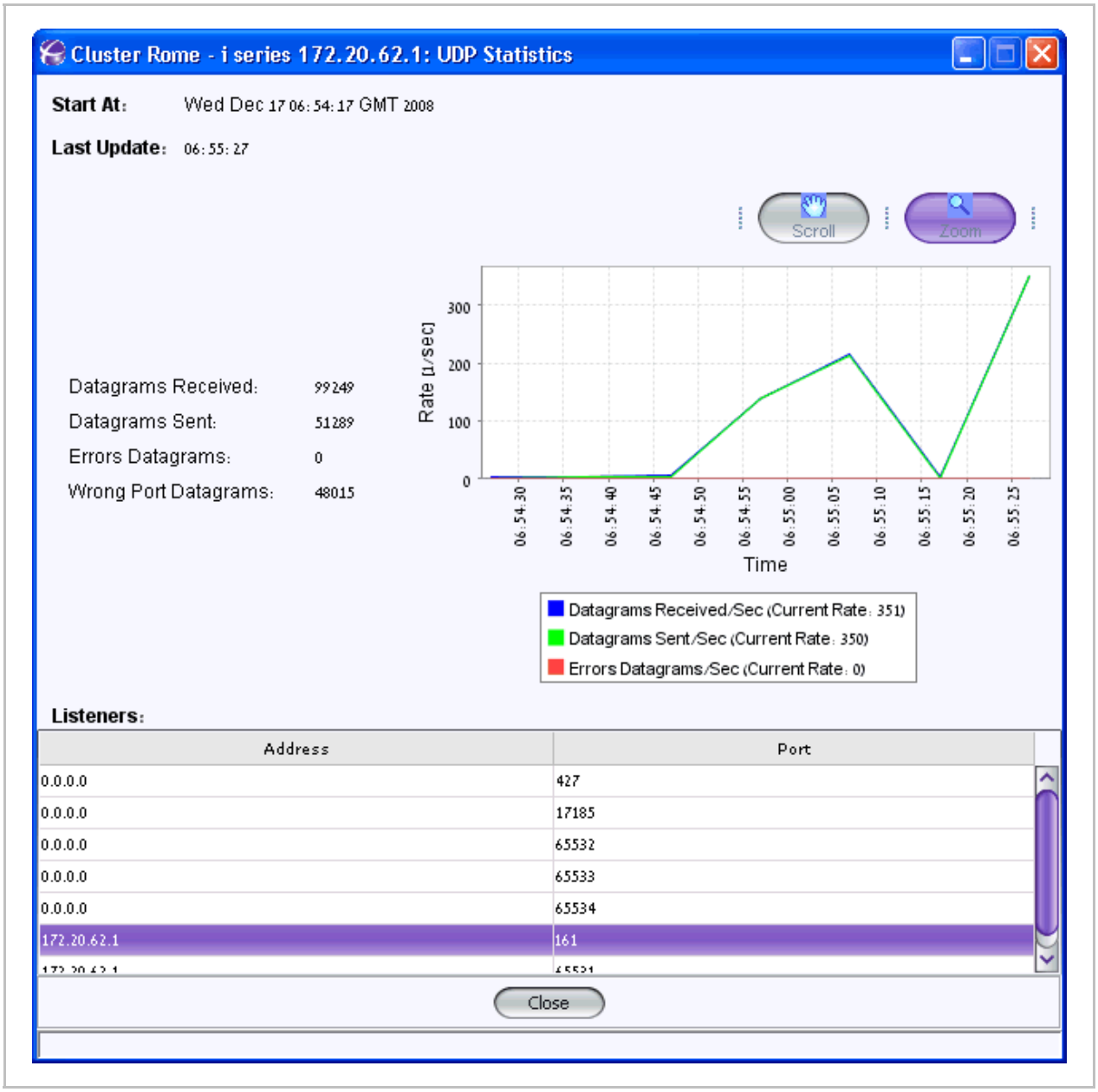



*Figure 5-13. UDP Statistics Window*

# iSCSI 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.

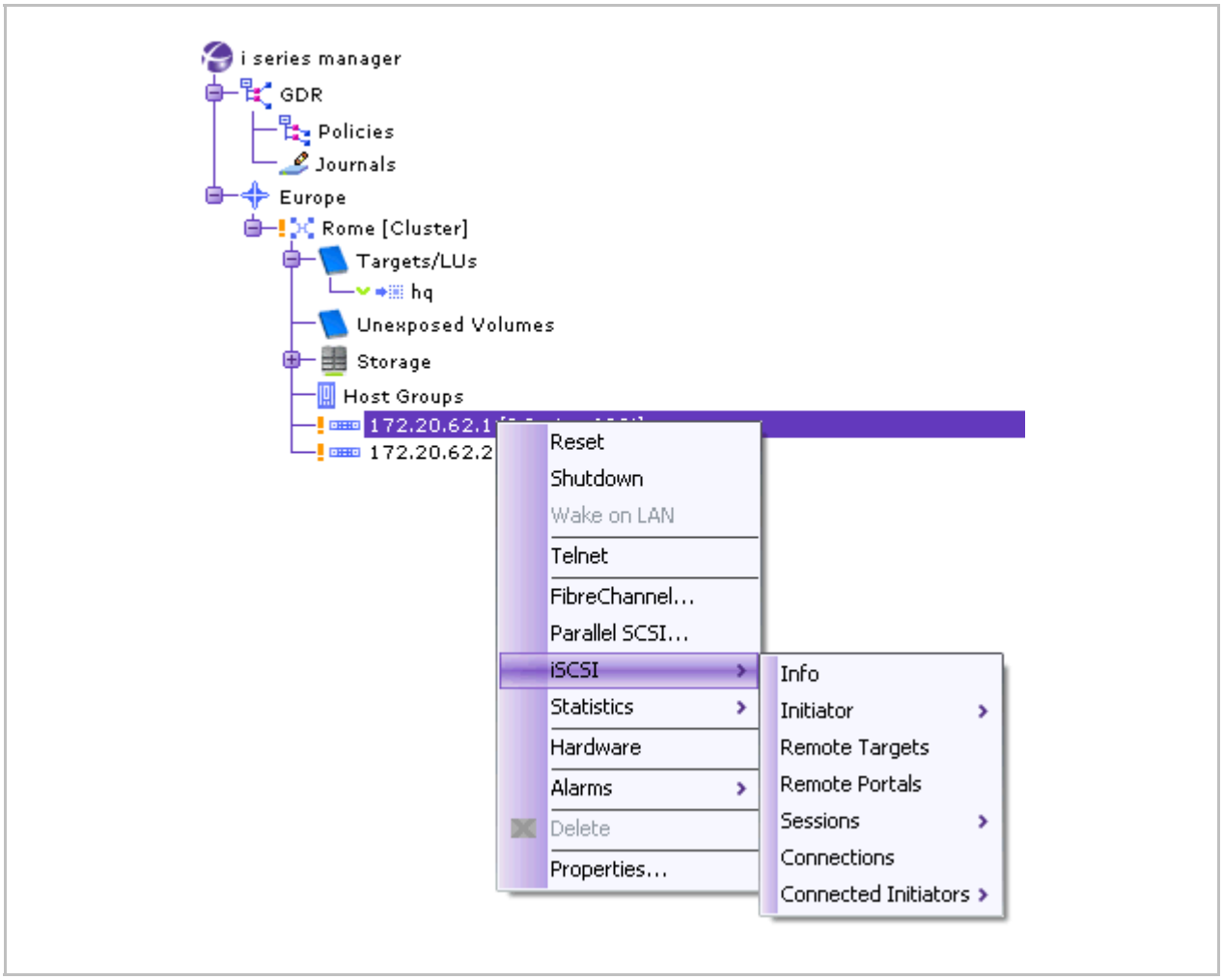



*Figure 5-14. iSCSI Menu*

## Viewing iSCSI Information

***To view iSCSI Information:***

- In the Navigation pane, select the i series, right click and select **iSCSI** > **Info** (Figure 5-14).

  The iSCSI Info window opens.

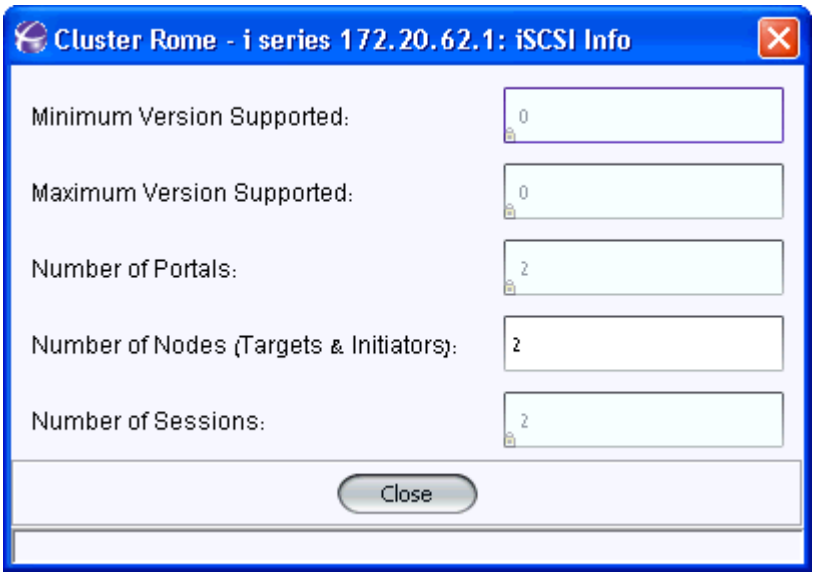



*Figure 5-15. iSCSI Information Window*

## Viewing iSCSI Initiator Properties

You can configure the initiator's CHAP secret.

***To modify or view iSCSI initiator properties:***

1. In the Navigation pane, select the i series, right click and select **iSCSI > Initiator > Properties** (Figure 5-14).

   The iSCSI Initiator Properties window opens.

2. If desired, enter a CHAP User name and password and click **OK**.

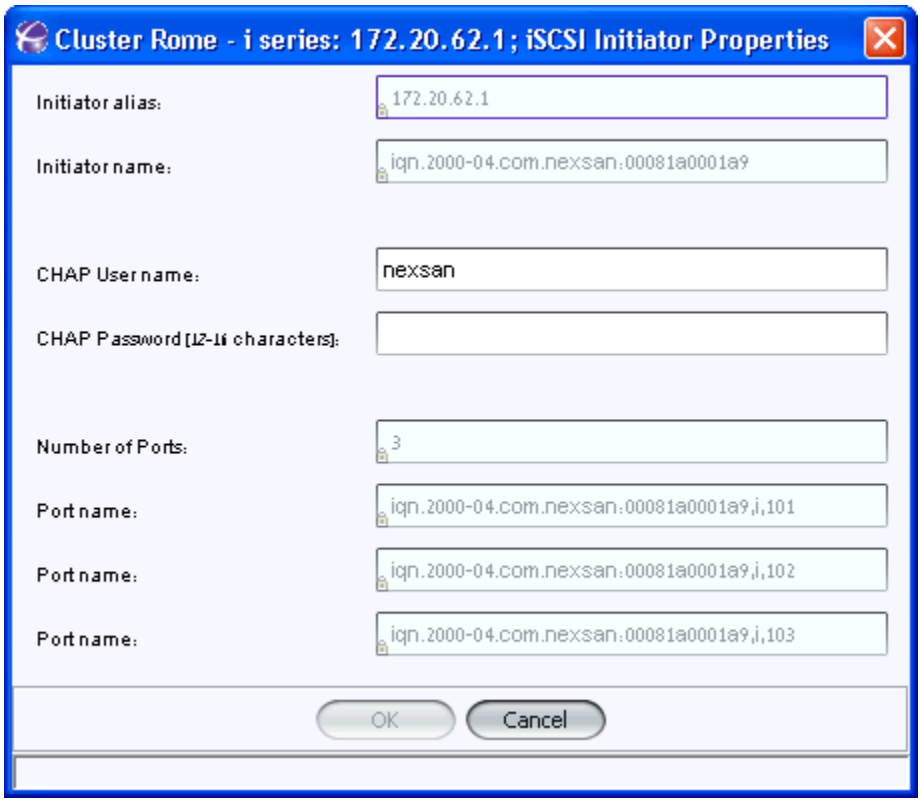



*Figure 5-16. iSCSI Initiator Properties*

***To view iSCSI initiator counters:***

- In the Navigation pane, select the i series, right click and select **iSCSI** > **Initiator > Statistics** (Figure 5-14).

  The iSCSI Initiator Counters window opens.

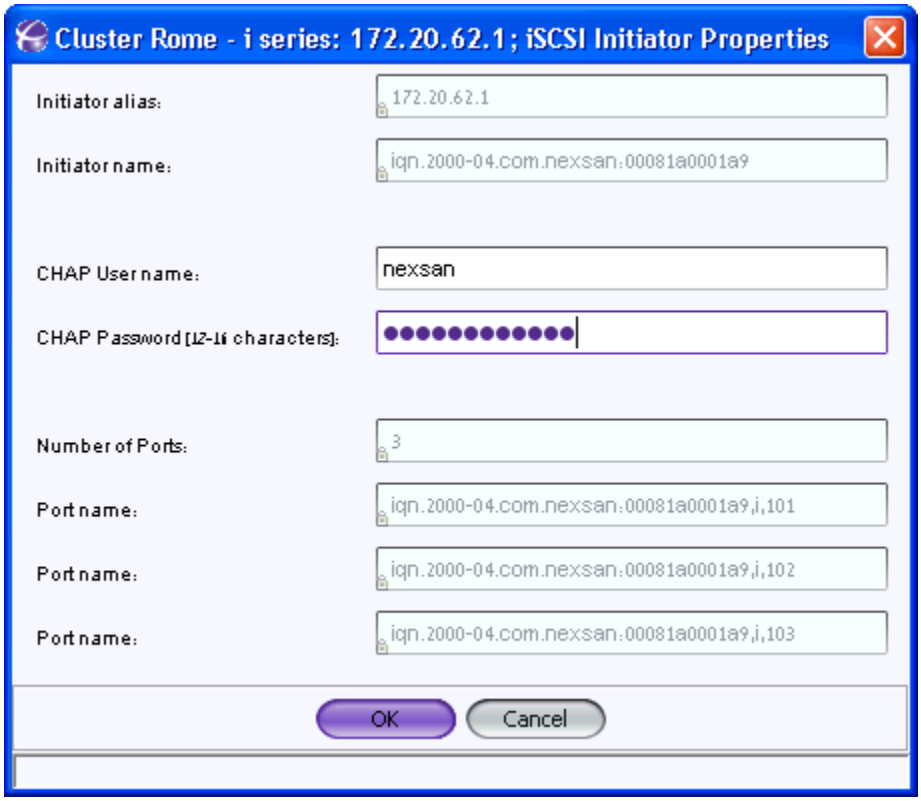



*Figure 5-17. iSCSI Initiator Counters*

## Viewing iSCSI Sessions

***To view iSCSI Sessions:***

- In the Navigation pane, select the i series, right click and select **iSCSI** > **Sessions** > **Show** (Figure 5-14).

  The iSCSI Sessions window opens.

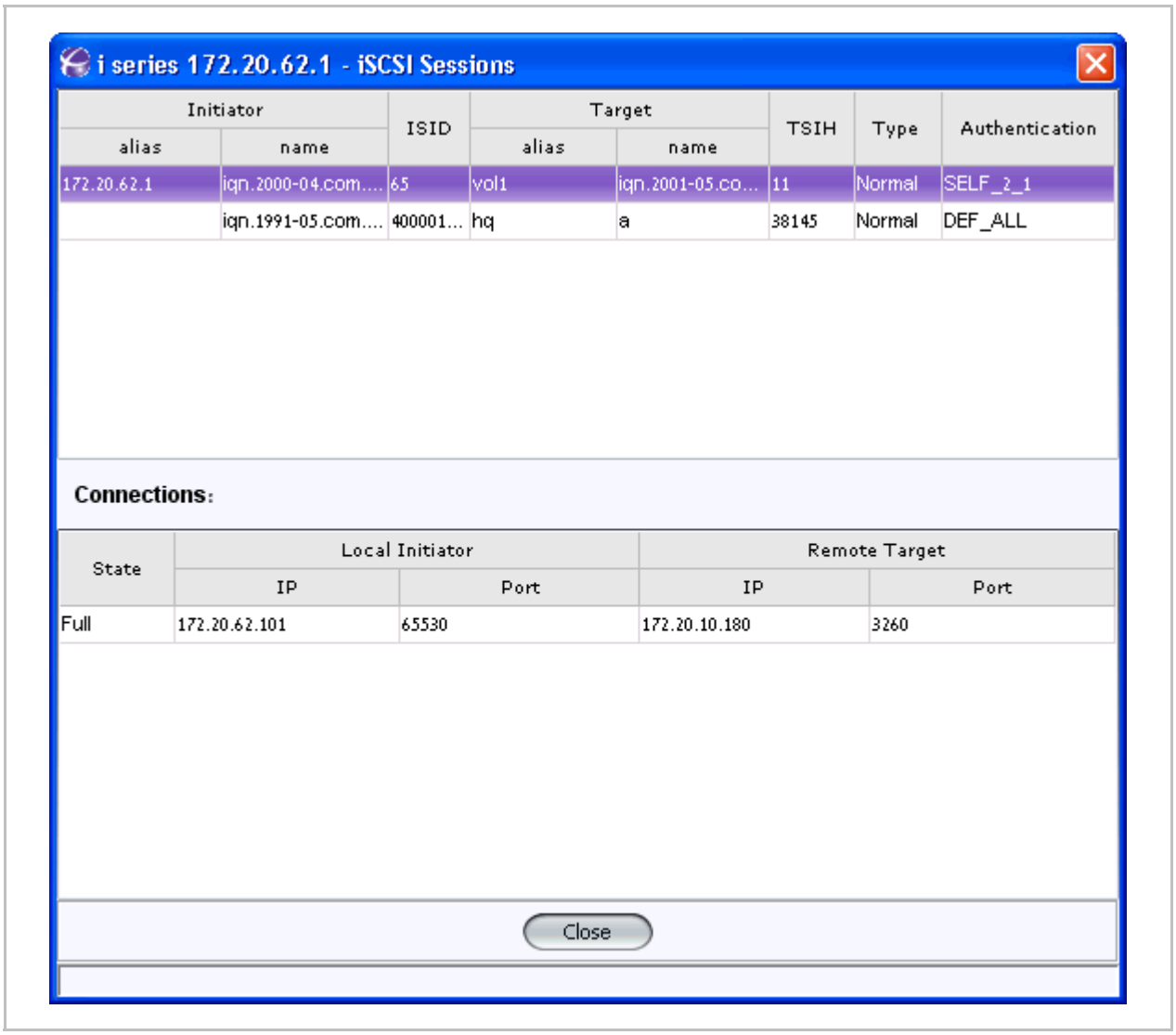



*Figure 5-18. iSCSI Sessions Window*

## Viewing iSCSI Session Statistics

***To view iSCSI Session Statistics:***

1. From the *Quick Launch:*
   **Monitor > Session Statistics**

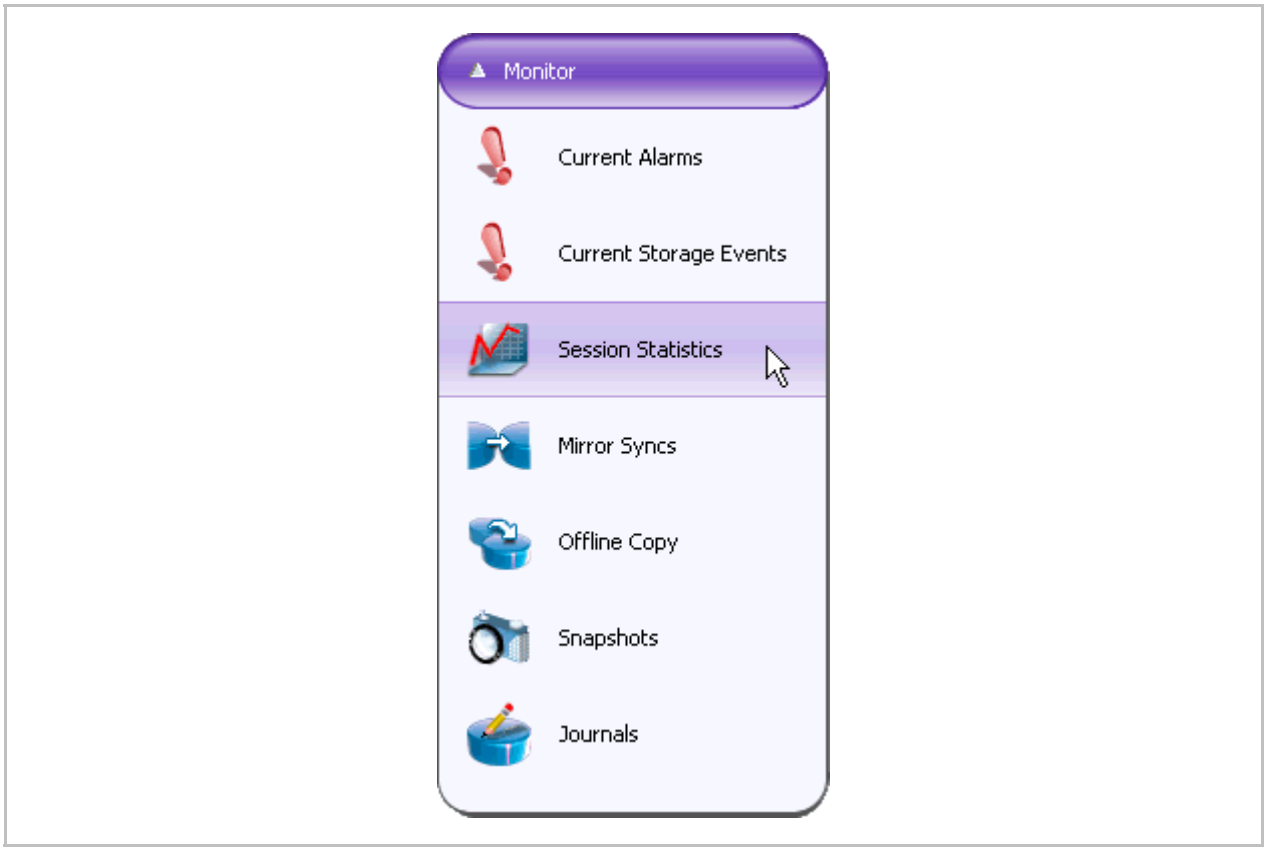



*Figure 5-19. Session Statistics*

The iSCSI Sessions Statistics window opens.

2. Select the cluster and specific i series.

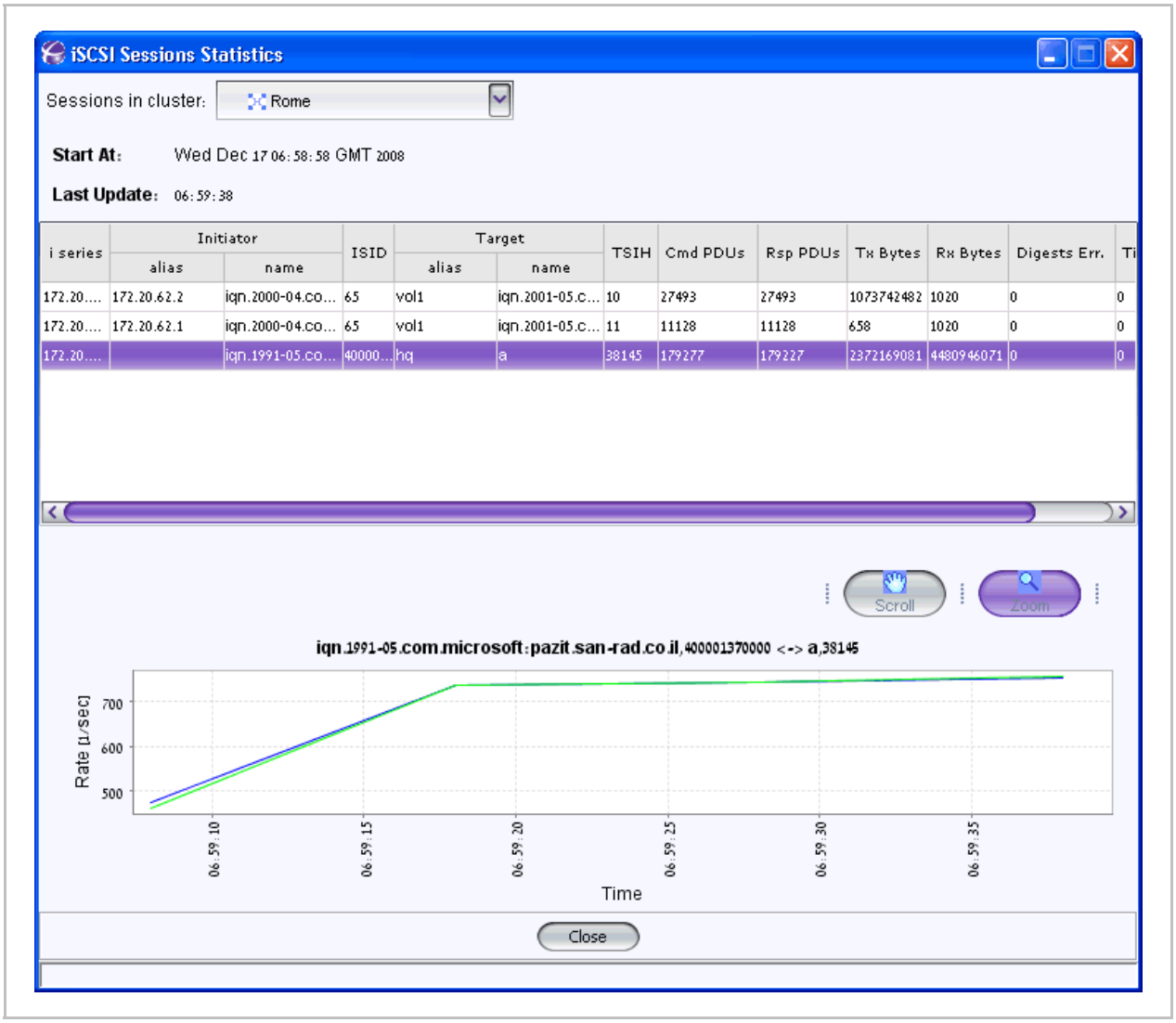



*Figure 5-20. iSCSI Sessions Statistics*

# 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.

## Viewing iSCSI Connections

***To view iSCSI connections for specific targets:***

- In the Navigation pane, select the i series, right click and select **iSCSI > Connections**.

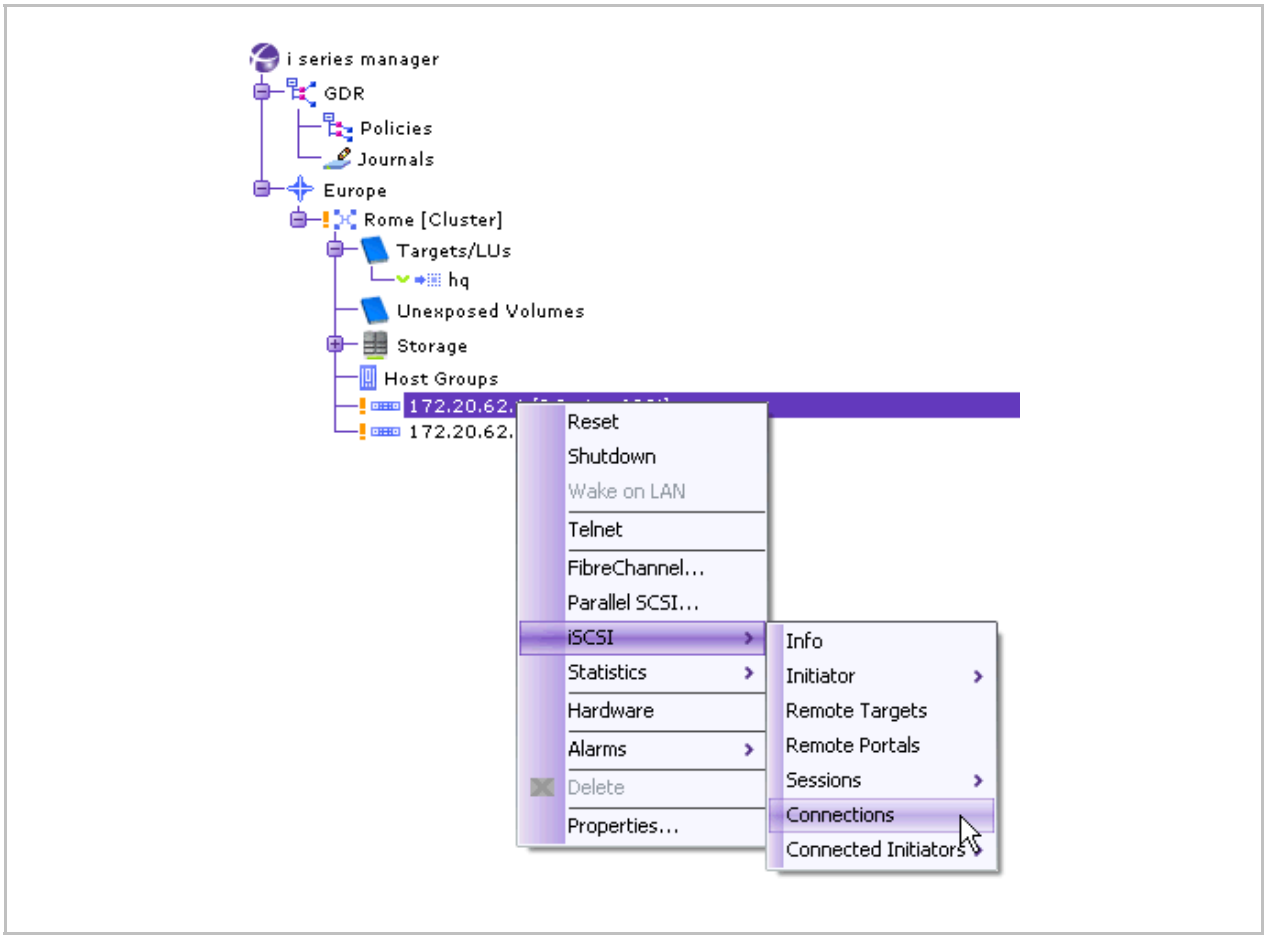



*Figure 5-21. Connections Selected from Target Menu*

The iSCSI Connections window opens.

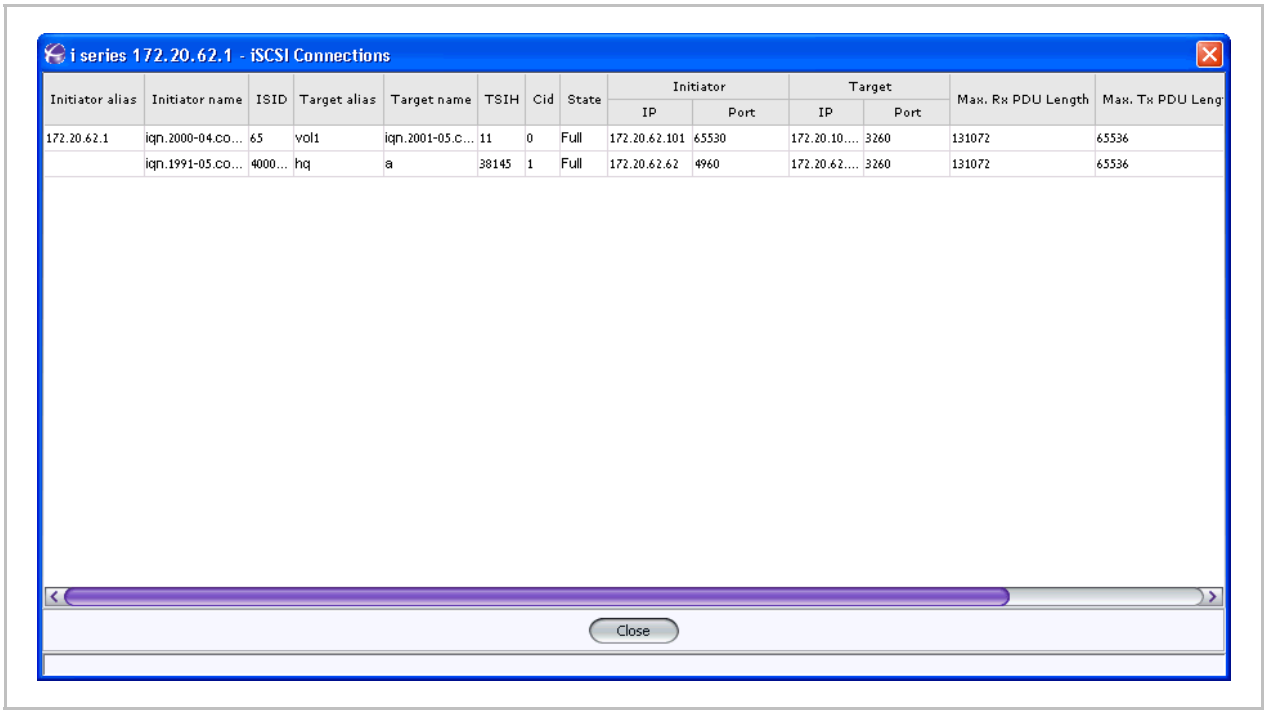



*Figure 5-22. iSCSI Target Connections Window*

## Viewing Connected iSCSI Initiators

***To view connected iSCSI Initiators:***

- In the Navigation pane, select the i series, right click and select **Connected Initiators** > **Show**.

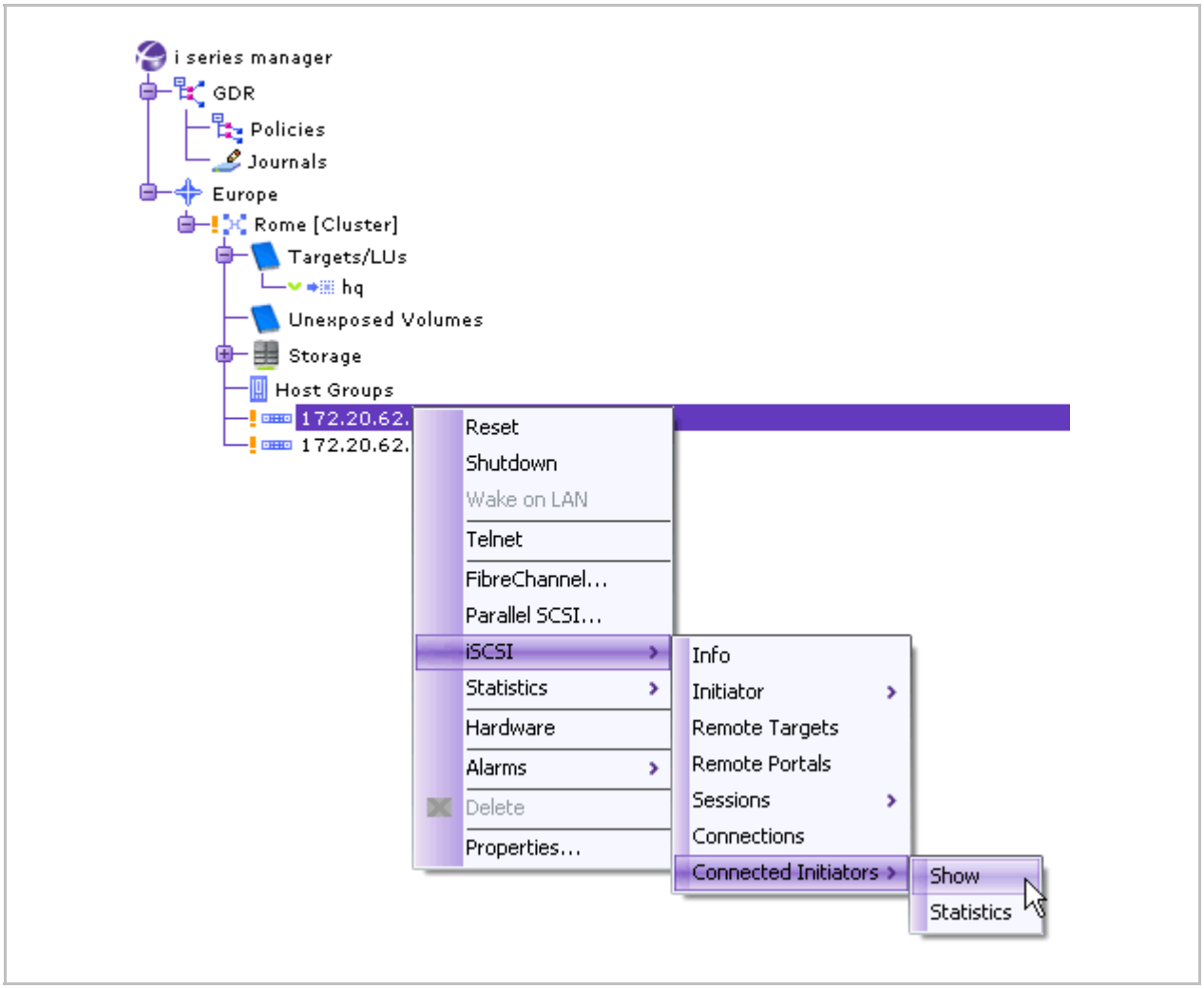



*Figure 5-23. Show Selected from the Connected Initiators Menu*

The iSCSI Connected Initiators window opens.

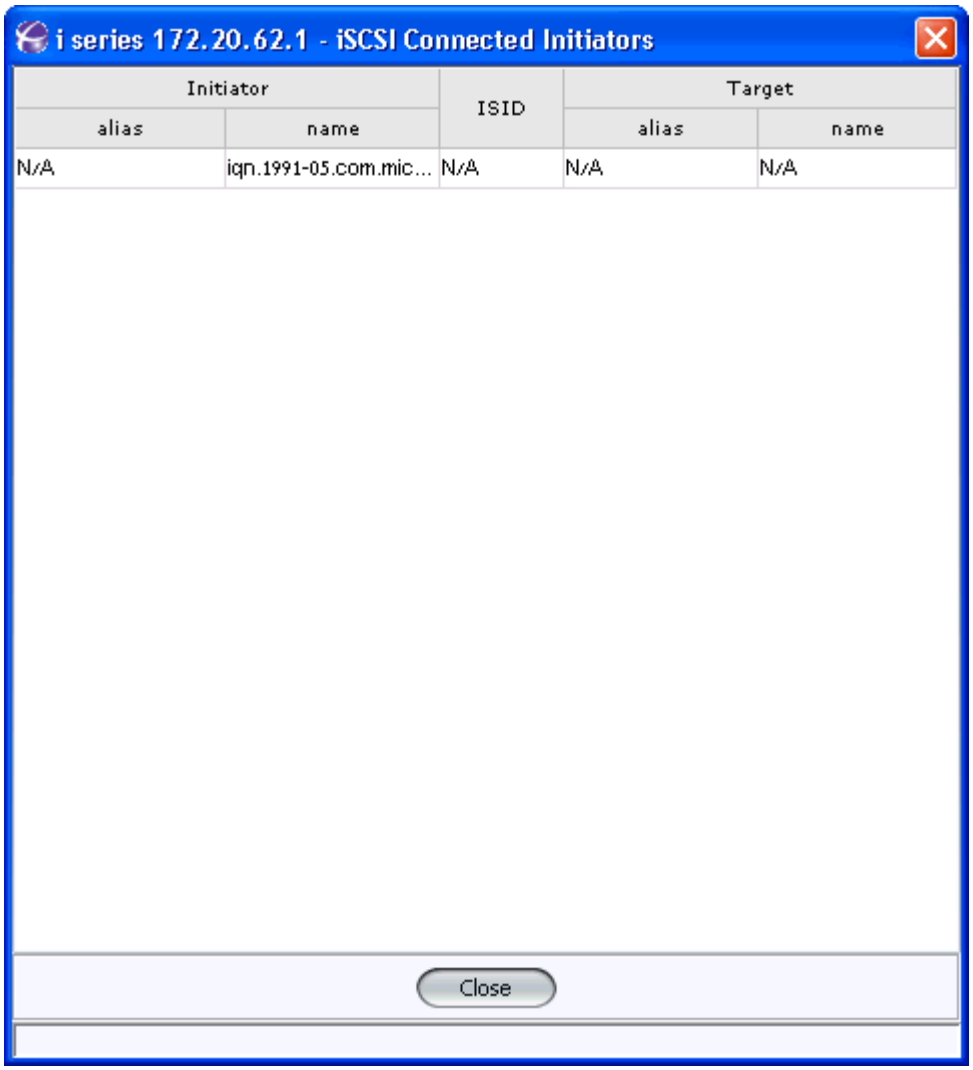



*Figure 5-24. iSCSI Connected Initiators*

## Viewing iSCSI Initiator Statistics

***To view iSCSI Initiator statistics:***

- In the Navigation pane, select the i series, right click and select **Connected Initiators > Statistics**.

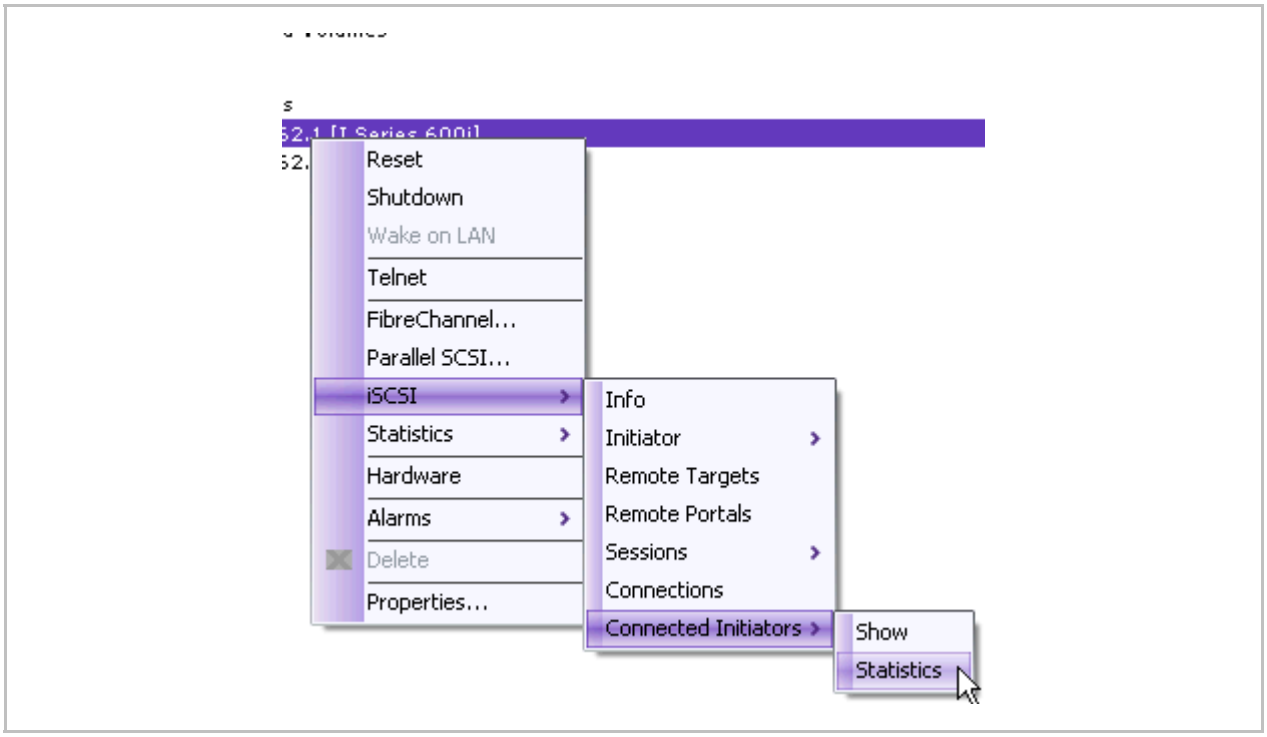



*Figure 5-25. Statistics Selected from the Connected Initiators Menu*

The Connected Initiators Statistics window opens.

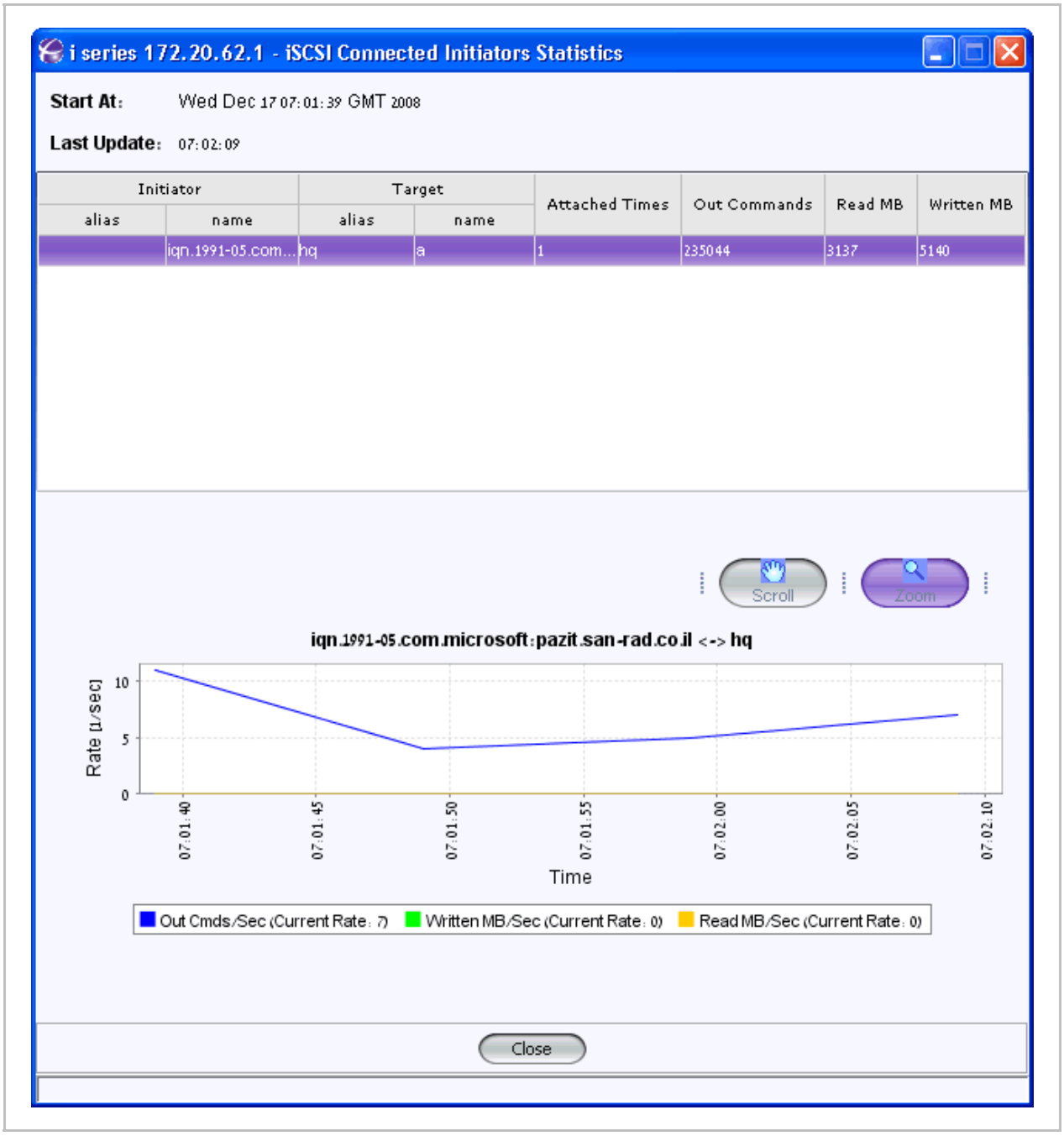



*Figure 5-26. iSCSI Connected Initiators Statistics Window*

# SCSI Target Statistics

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

***To view SCSI target statistics:***

- Select a target, right click and select **SCSI > Statistics**.

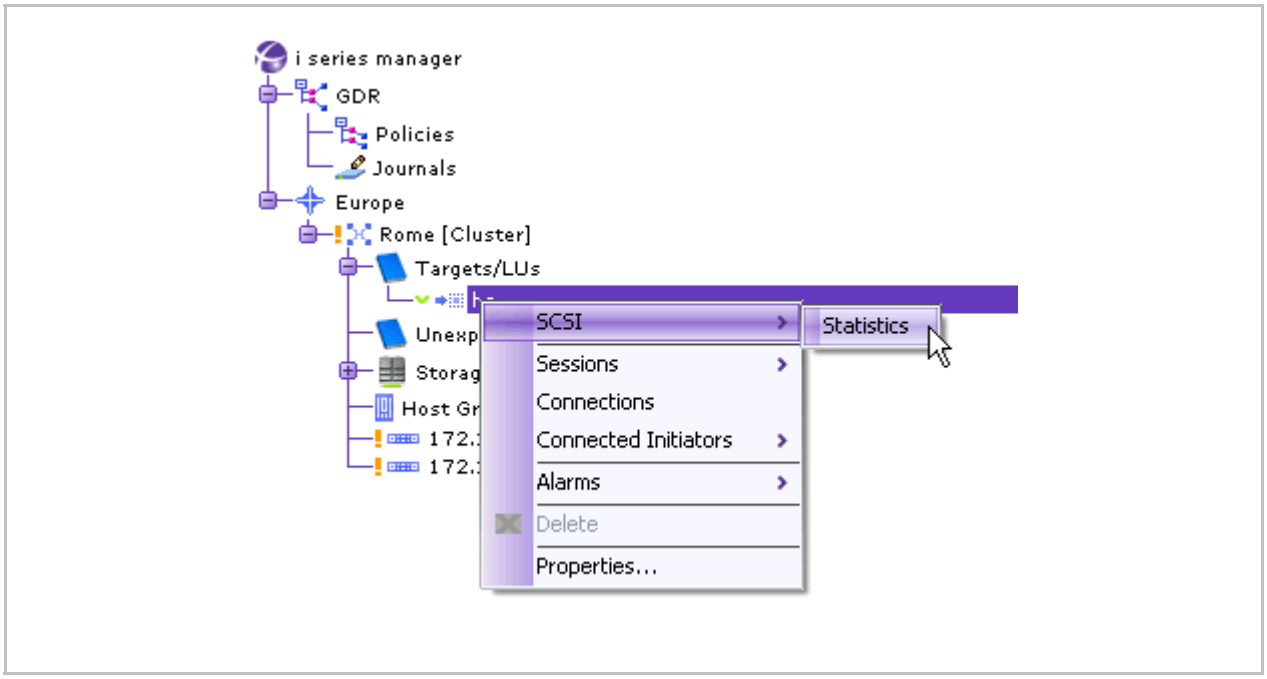



*Figure 5-27. SCSI Menu*

The SCSI Statistics window opens.

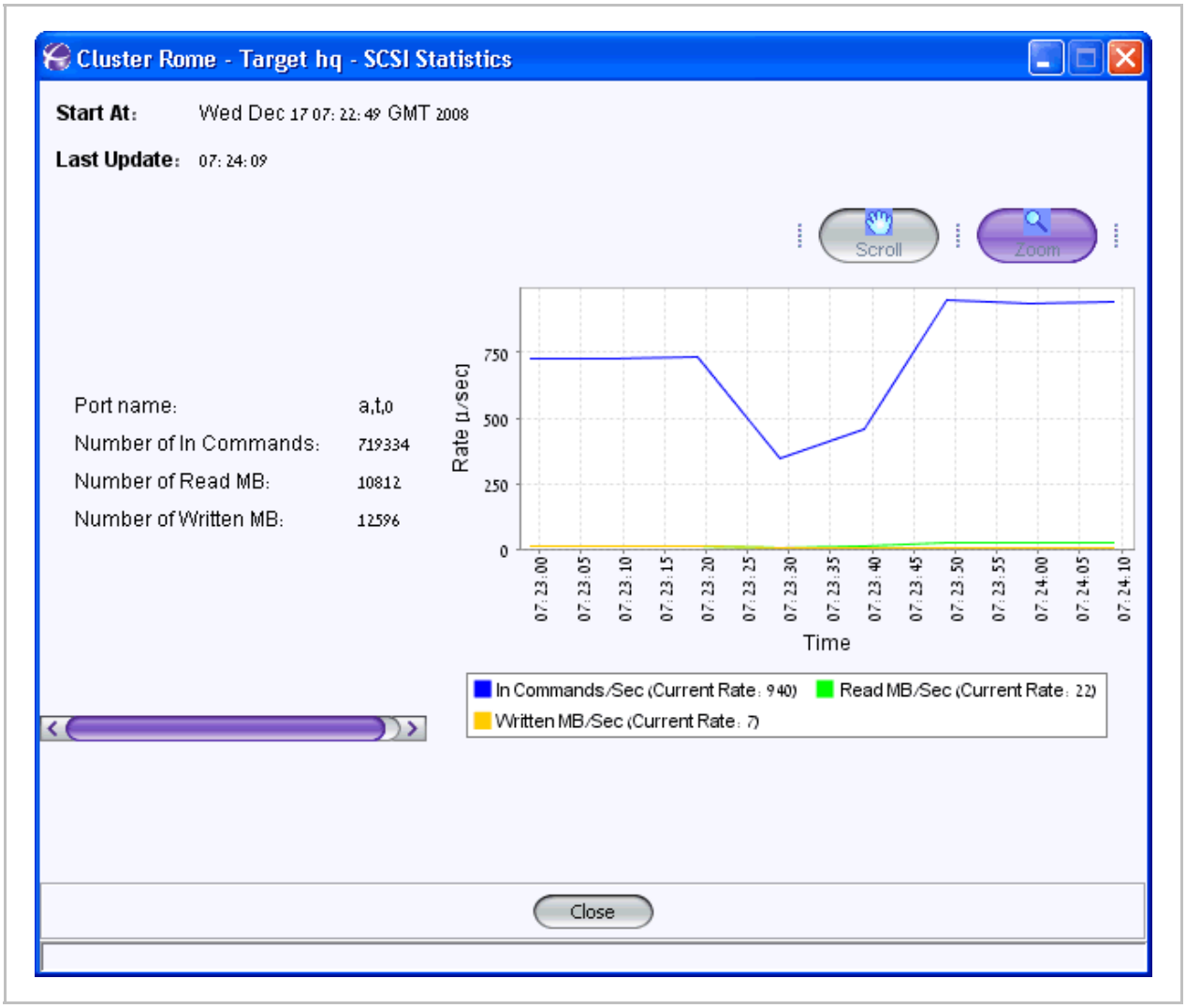



*Figure 5-28. SCSI Target Statistics*

# Chapter 6
# Troubleshooting

i series manager identifies error conditions and generates alarms accordingly.

The alarms are viewable and can be sorted. The last ten unacknowledged alarms generated are displayed in the bottom pane of the i series manager GUI.

## Alarm Operations

i series manager supports alarm messages for real-time tracking and monitoring of both i series manager and i series configurations and activity. Alarms are time-stamped according to the i series manager server date and time.

### Configuring Email Alarm Notification

You can send an email when an alarm is opened for off-site alarm monitoring. The administrator should configure the alarms which will trigger the Email notification using i series manager Alarms Notification Configuration list.

A user profile must be configured on the SMTP server for sending Email notifications received from i series manager. The profile must include a user name and password for authentication. The SMTP server parameters are:

- Mail Server: Name or IP address of SMTP server
- From Address: Address that Email appears to be sent from
- User Name: User authentication name
- Password: User authentication password

### *To configure the alarm notification list:*

1. From the i series manager menu bar, select **Alarm Notifications > Email Setup…**

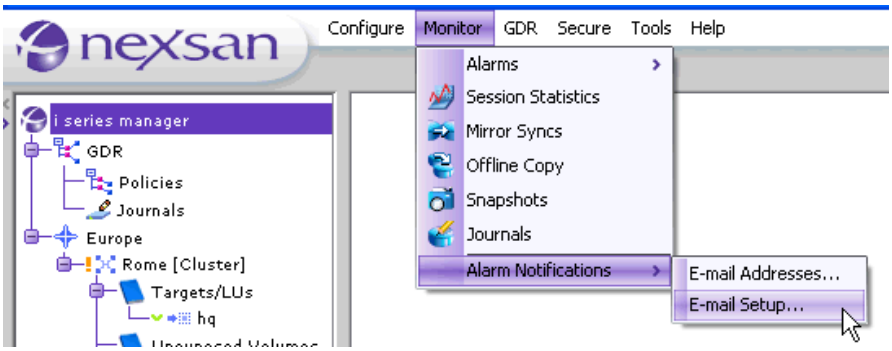



*Figure 6-1. Alarms Menu*

The Alarms Notification Configuration window opens.

2. Select each alarm for which you want to receive email notification.
3. Click **OK**.

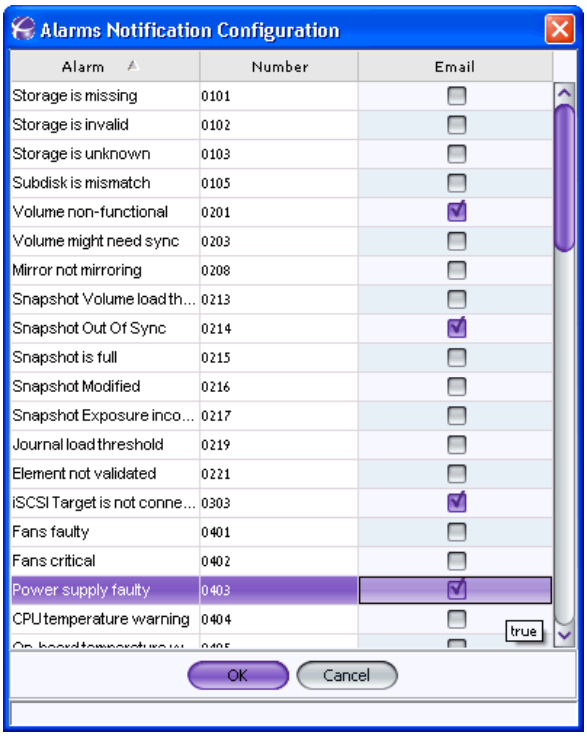



*Figure 6-2. Selected Alarms for Email Notification*

### *To configure the email address for alarm notification:*

1. From the i series manager menu bar, select **Alarms Notifications > E-mail Addresses…**

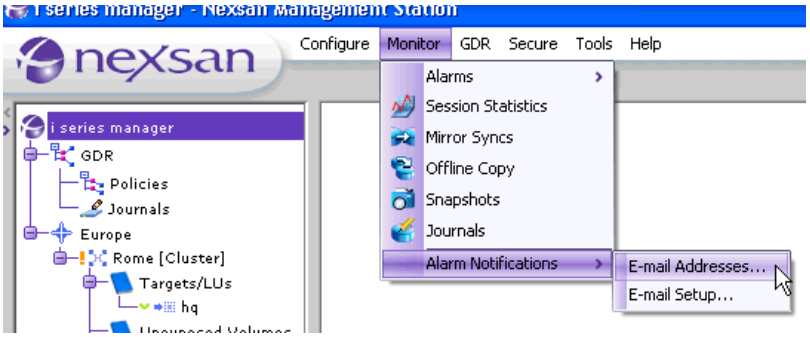



*Figure 6-3. Configure Menu*

The **Email Configuration** dialog box opens.

2. Enter the name or IP address of the SMTP server.
3. Enter the email address for the outgoing email notification.
4. Enter the User Name and Password for user authentication.

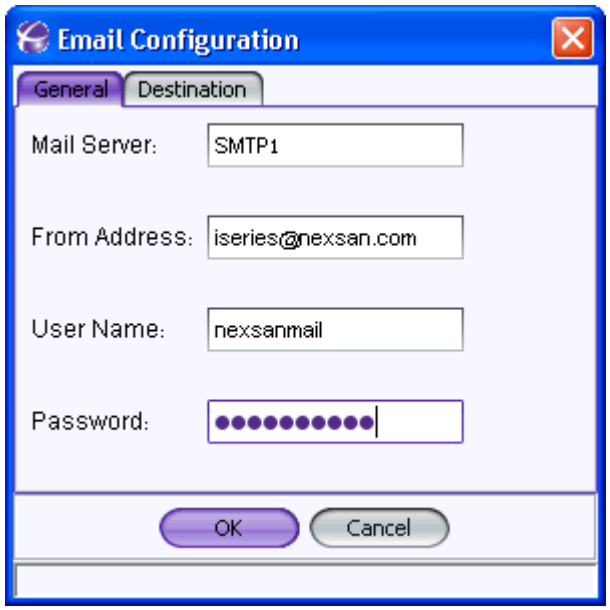



*Figure 6-4. SMTP Server Configuration*

5. Toggle to the **Destination** tab and click **Add…**

The **Add Address** dialog box opens.

6. Enter the Email address to send alarm notifications to and click **OK**.

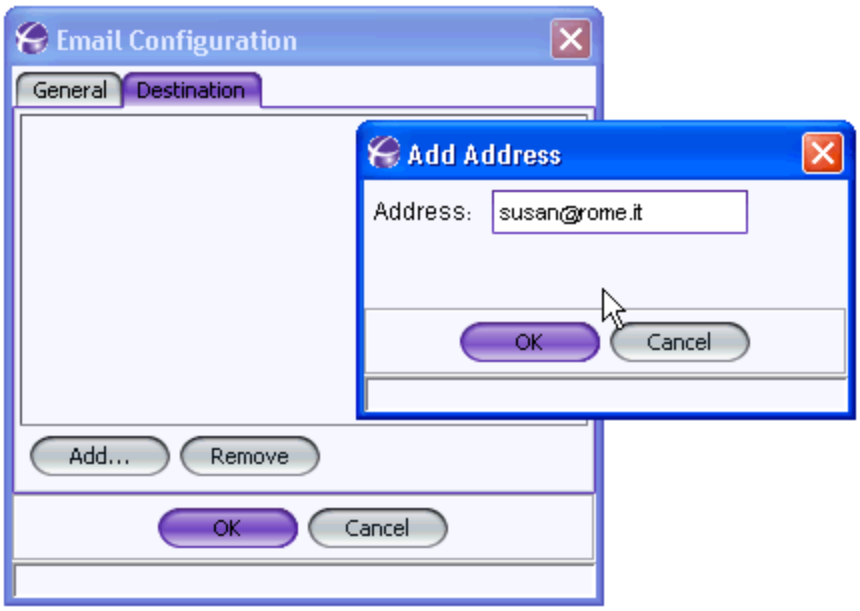



*Figure 6-5. Email to Send Alarm Notification to*

The Email notification format is shown in Figure 6-6.

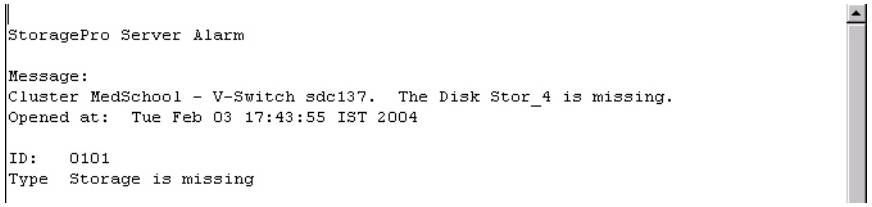



*Figure 6-6. Alarm Email*

**Note:**
*Email is sent only at the time when an alarm is generated. If an alarm entry already exists during the Email notification configuration, an Email notification will not be sent.*

## Viewing Specific Alarms

Every alarm can be associated with a specific i series manager element, e.g. cluster, i series, disk, volume or target.

***To view specific alarms:***

Select the element.

- Right click and select **Alarms** > **Specific**.

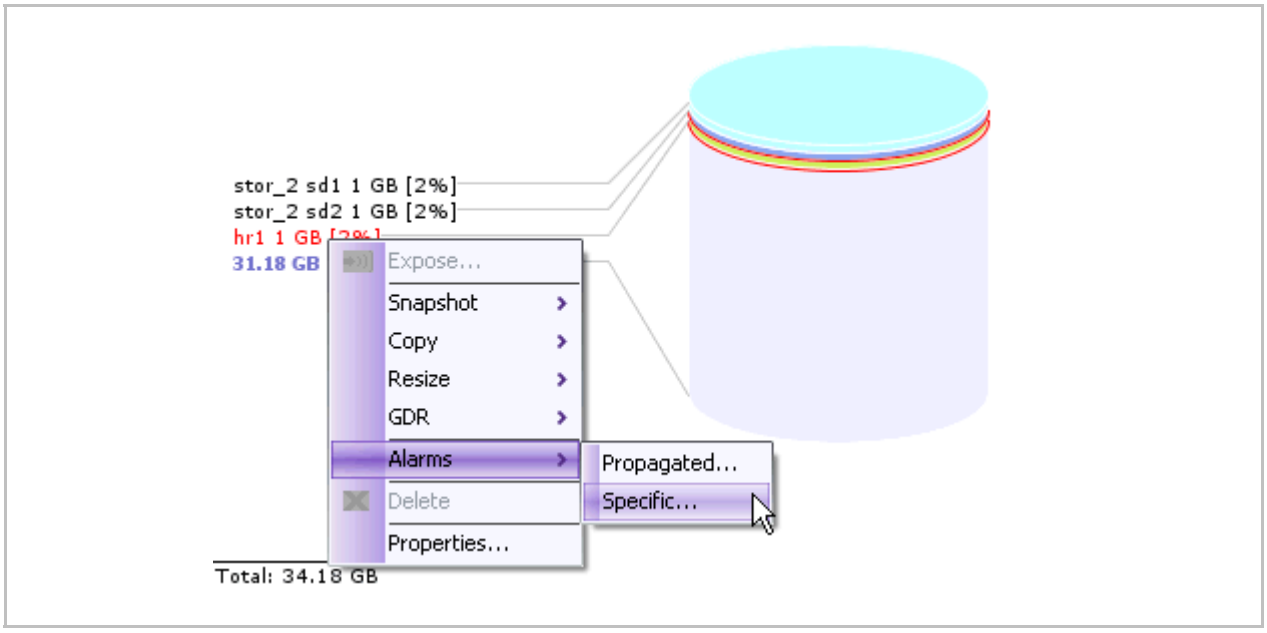



*Figure 6-7. Specific Alarms Selected*

The **Specific Alarms** window opens.

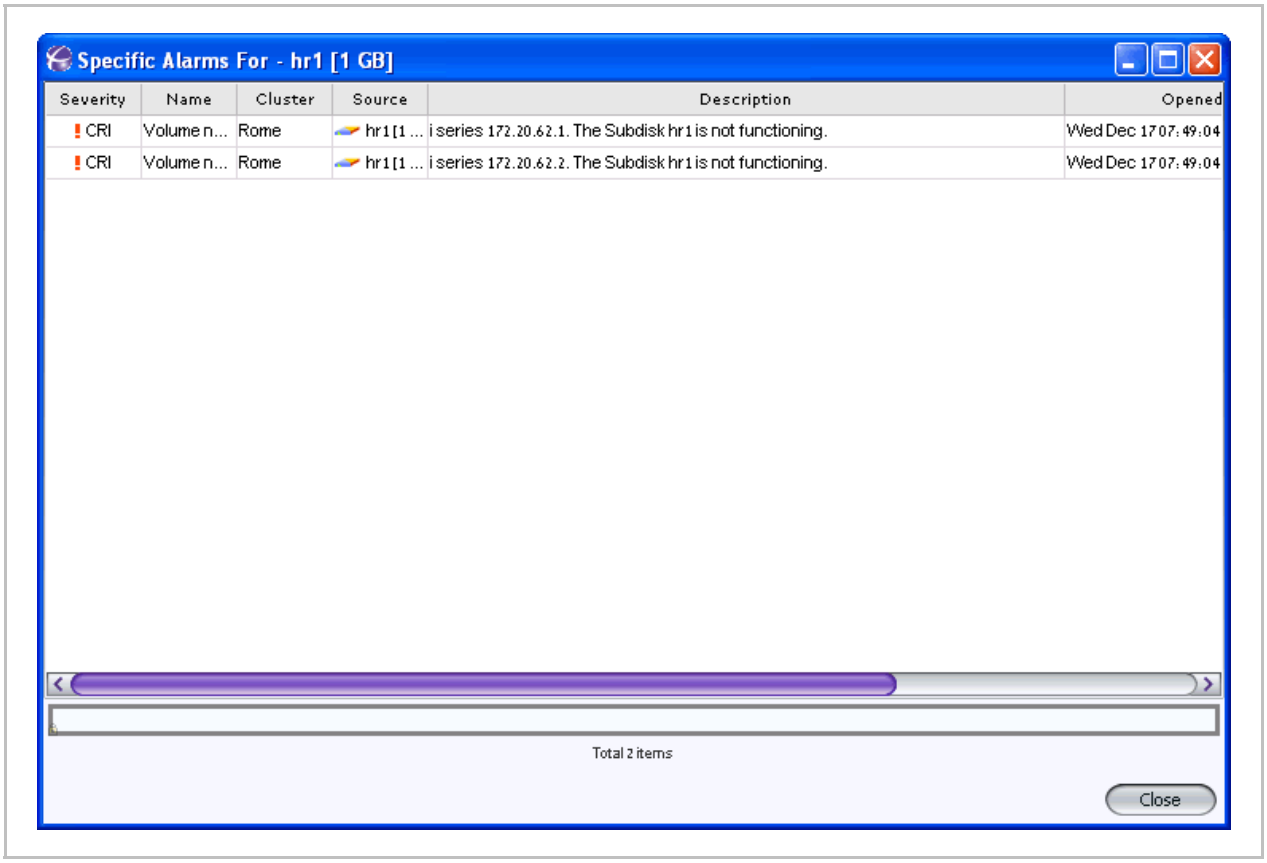



*Figure 6-8. Specific Alarms Window*

From the Specific Alarms window, you can select an alarm and view its source and properties. You can also close an alarm. This will remove the closed alarm from the Current Alarms list and move it to the Closed Alarms list.

## Viewing Propagated Alarms

A propagated alarm is generated by a source which is a logical member of a selected element.

The Propagated Alarms window lists all the specific alarms of a selected element as well as all the selected element derived alarms.

There are two propagation hierarchies:

- Cluster > Target > LU > Volume > Subdisk > Disk
- Cluster > i series > Management Parameters and Configurations

***To view propagated alarms:***

- Select the element whose propagated alarms you want to view. Right click and select **Alarms** > **Propagated**.

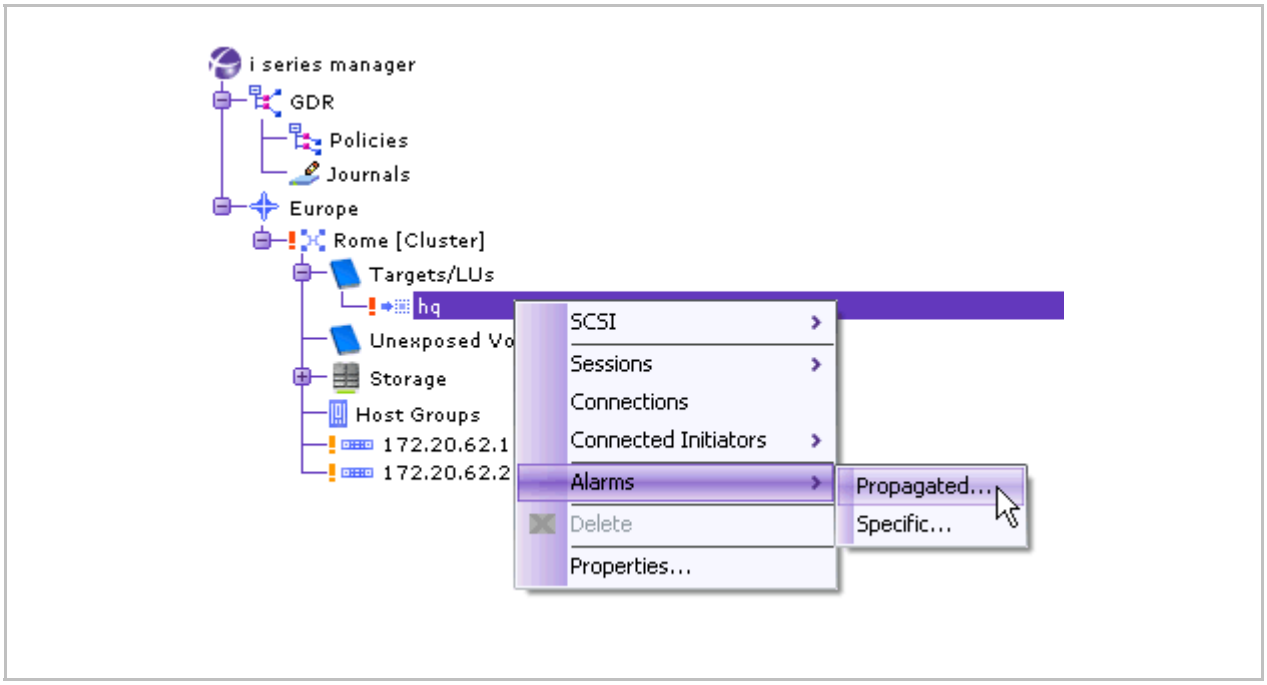



*Figure 6-9. Propagated Alarms Selected*

The **Propagated Alarms** window opens with all propagated alarms for the element.

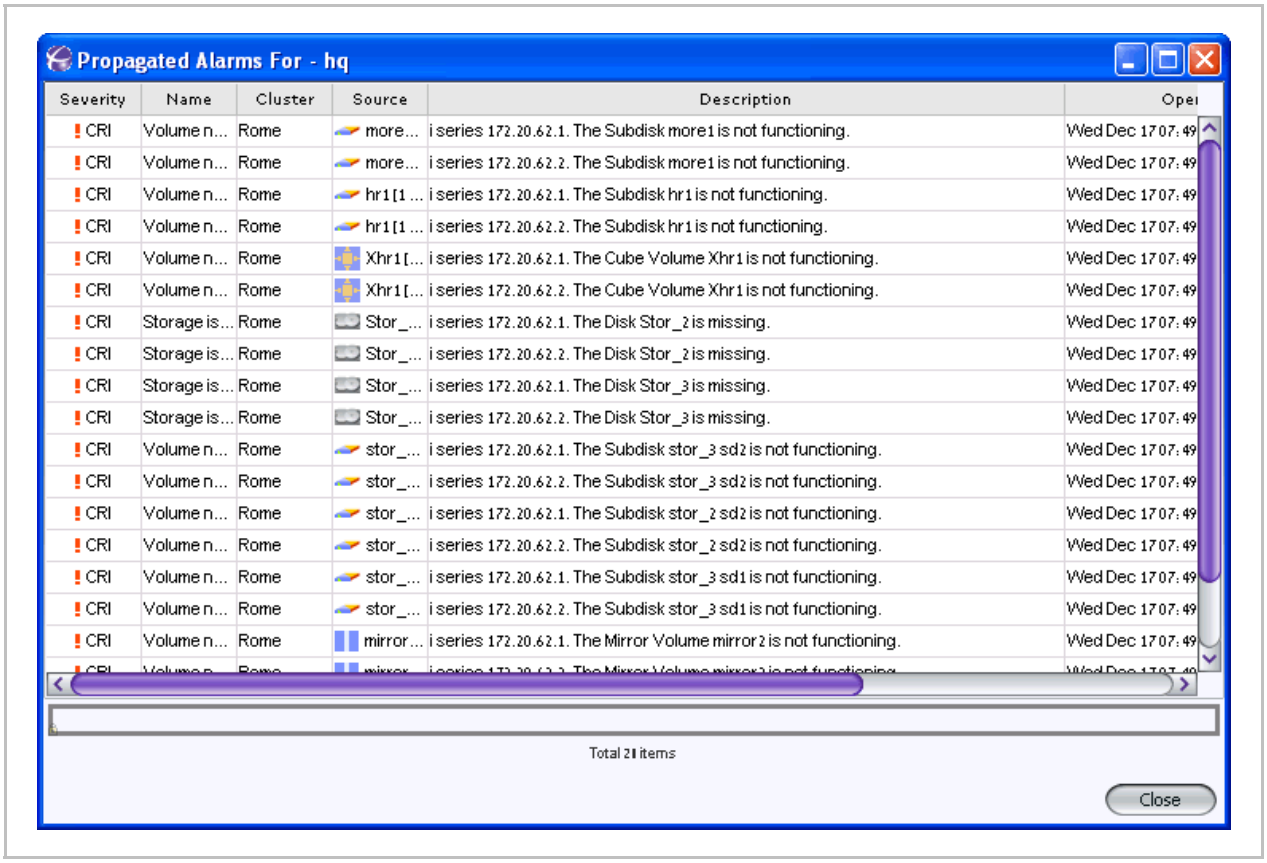



*Figure 6-10. Propagated Alarms Window*

From the Propagated Alarms window, you can select an alarm in order to view its source and properties. You can also close an alarm. This deletes it from the Current Alarms list and moves it to the Closed Alarms list.

## Viewing Alarms History

You can view the list of all acknowledged (previous) alarms.

***To view previous alarms:***

- From the standard i series manager toolbar, click **Alarms > History** or click the History button
  
  .

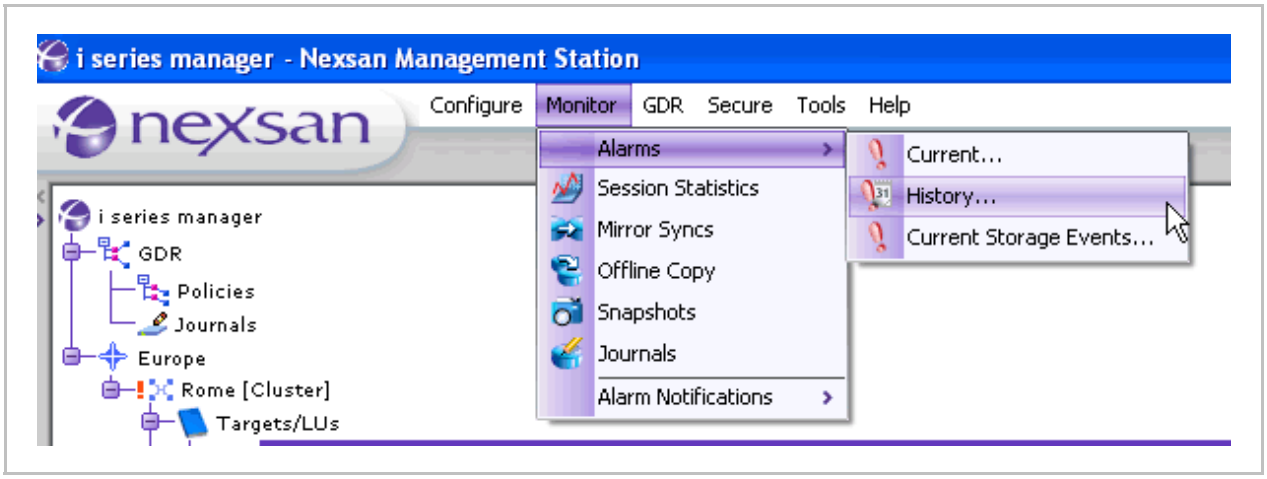



*Figure 6-11. Alarms Menu*

The **Alarms History** window opens.

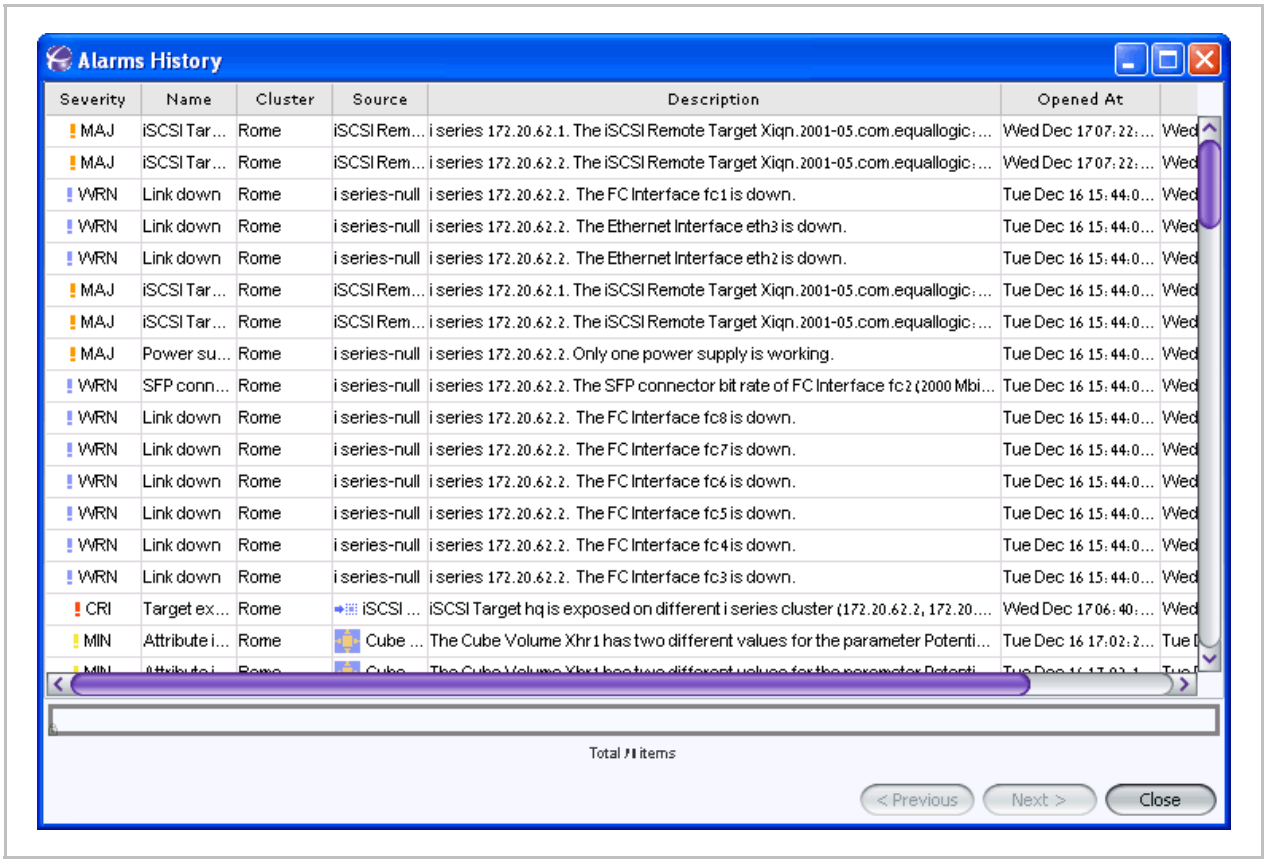


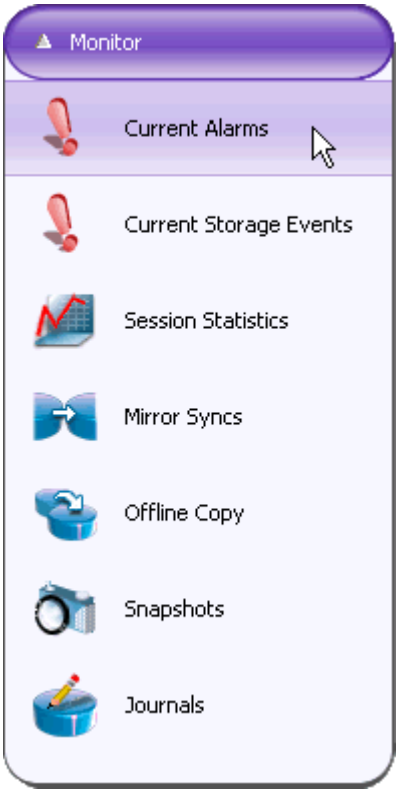

*Figure 6-12. Alarms History Window*

## Viewing Current Alarms

You can view all current open alarms for all the i series manager elements.

***To view current alarms:***

1. From the *Quick Launch:*
   **Monitor > Current Alarms**




The **Current Alarms** window opens.

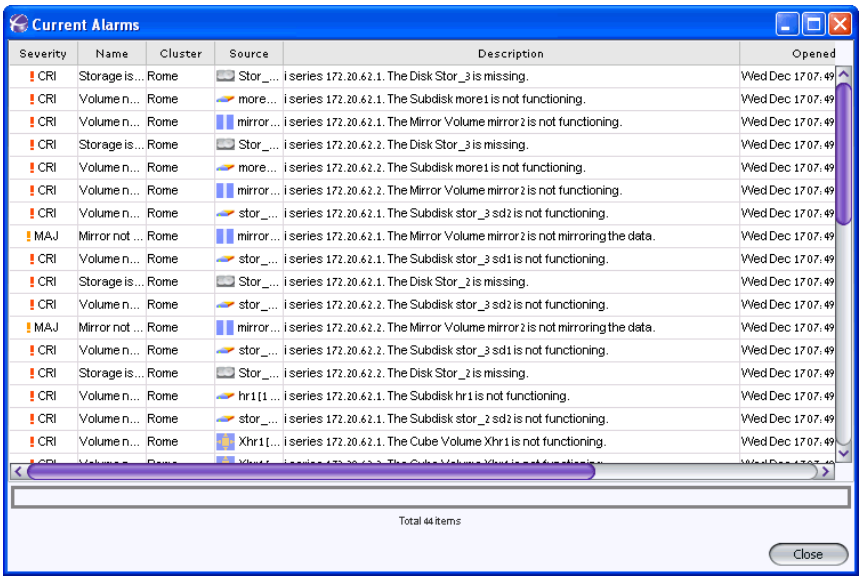



*Figure 6-13. Current Alarms Window*

## Acknowledging an Alarm

An *acknowledged* alarm still exists but its severity will not propagate to higher levels. However, the alarm will still be listed in the Current Alarms window, along with the name of the user who acknowledged the alarm.

***Note:***
*If an alarm is listed in the Last 10 Alarms pane, after being acknowledged it is removed from the pane.*

***To acknowledge an alarm:***

Select the alarm to acknowledge.

Do one of the following:

- Right click and select **Acknowledge**

OR

- Check the Ack checkbox from any alarm pane.

If the alarm was in the **Last 10 Alarms** pane, it is removed.

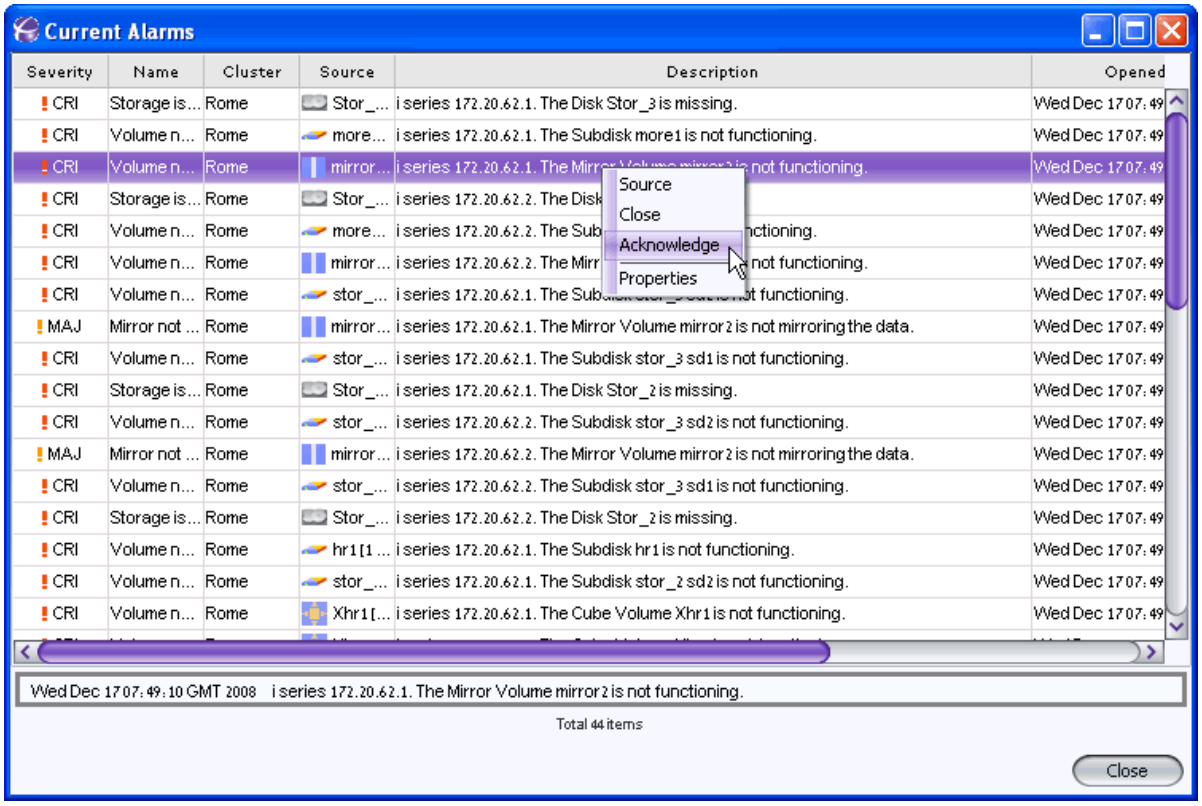



*Figure 6-14. Acknowledge Alarm*

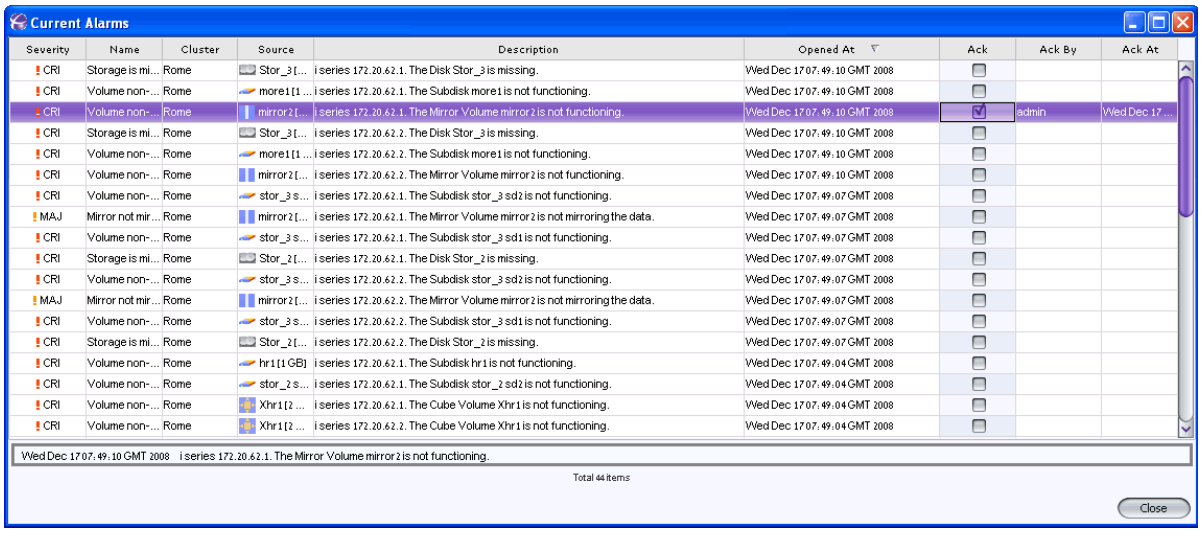



*Figure 6-15. Ack Checkbox*

## Closing an Alarm

Once an alarm occurs, it remains in the current alarm list till the situation that caused it ceases. However, it can be closed manually.

If the event that generated the alarms occurs again, another alarm will be generated and added to the current alarm list.

***To close an alarm:***

1. Select the alarm to close. Right click and select **Close**.

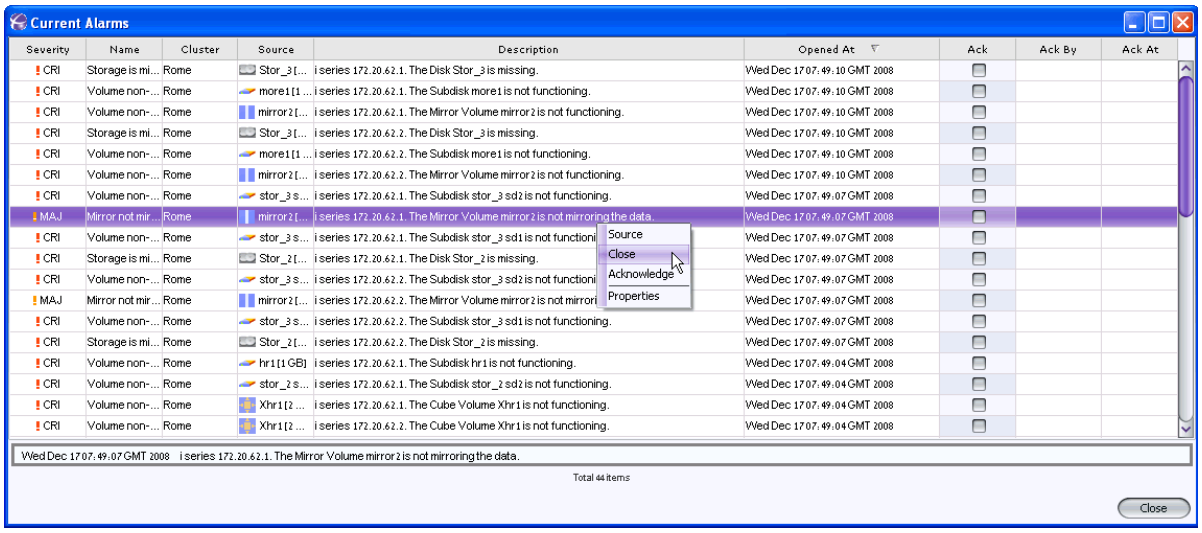



*Figure 6-16. Close Alarm*

The **Close Alarm** dialog box opens.

2. Click **Yes** to reconfirm the alarm closure.

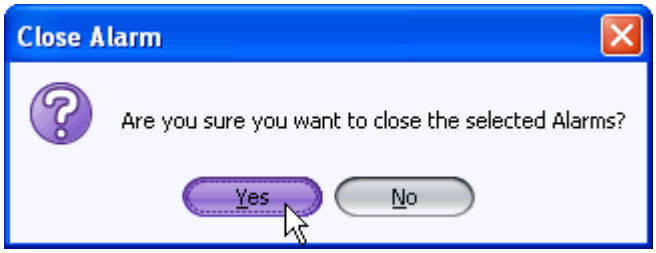



*Figure 6-17. Close Alarm Confirmation Dialog Box*

The alarm will be closed and removed from the pane. You can view the closed alarm in the Alarms History window (Figure 6-12).

## Viewing Alarm Properties

You can view the properties of an alarm, including:

- Alarm Severity
- Alarm Name
- Source Name
- Source Type
- Date Opened
- Category
- Probable Cause
- Alarm Text
- Troubleshooting

Use the alarm properties to help solve the alarm issue.

***To display alarm properties:***

From any of the alarm windows, select the alarm whose properties you want to view.

- Right click and select **Properties.**

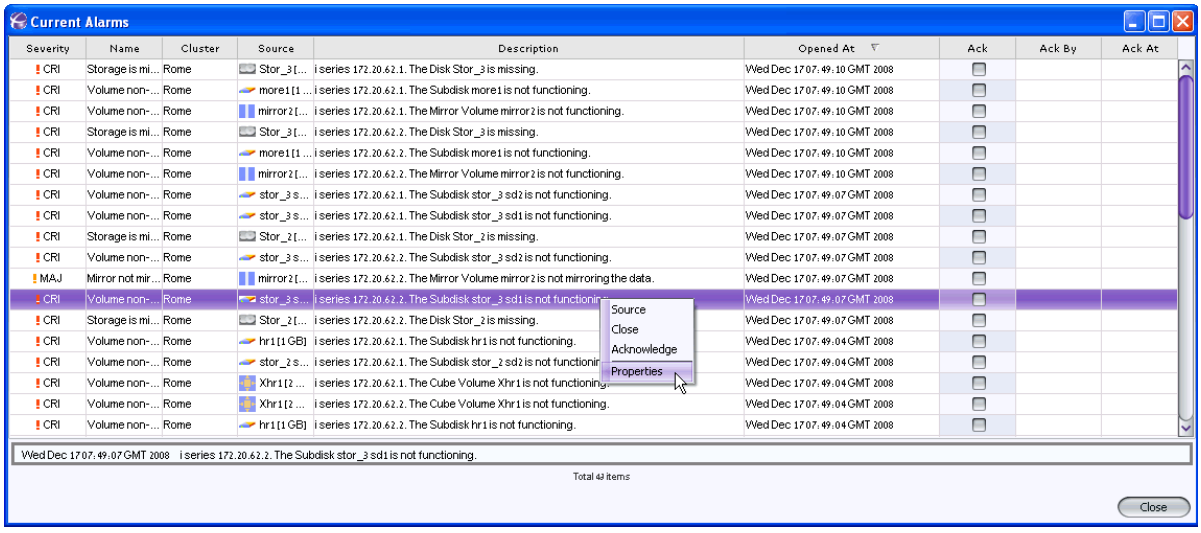



*Figure 6-18. Properties*

The **Properties** window opens.

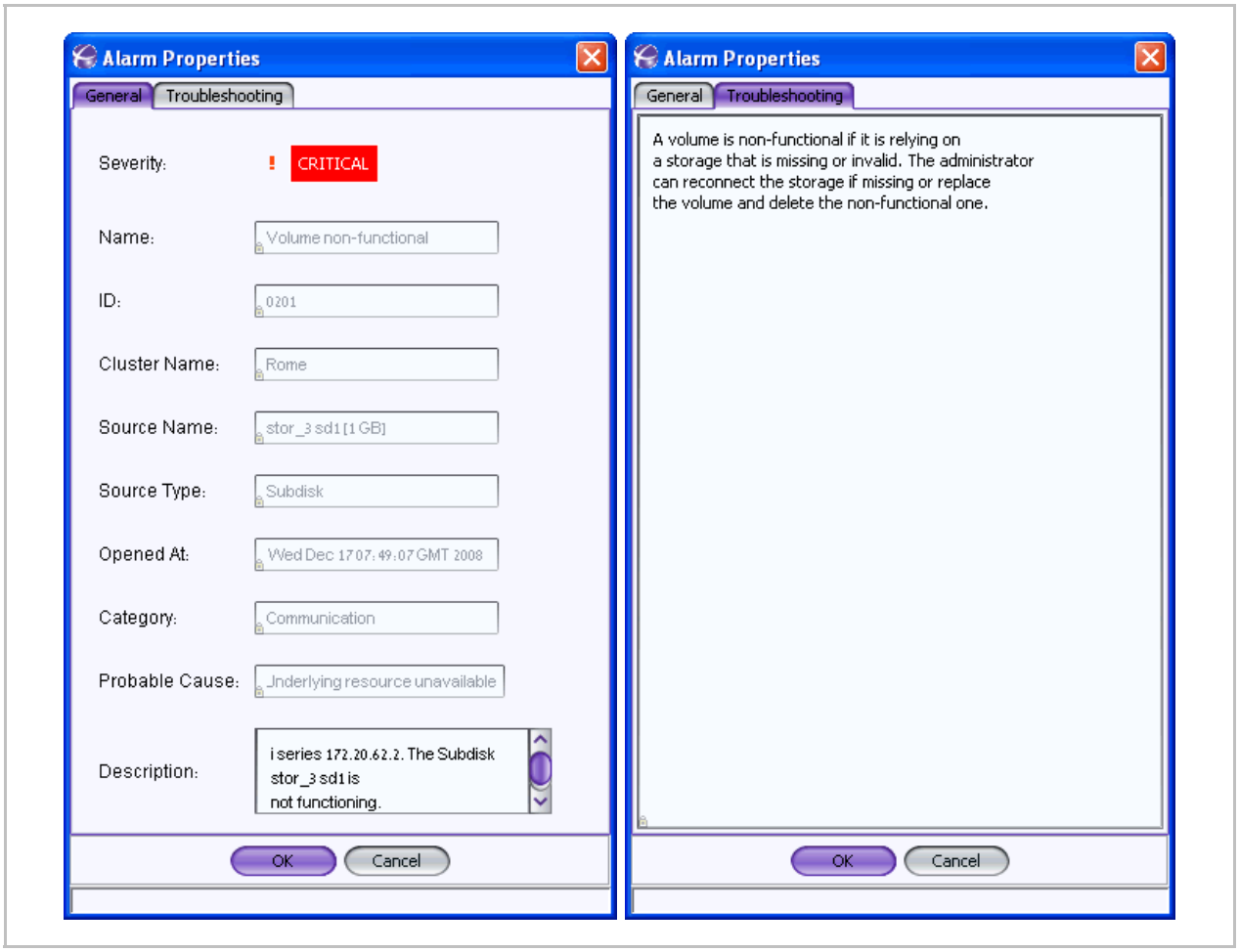



*Figure 6-19. Alarm Properties Window*

## Alarm Severity

i series manager supports four types of alarm severity:

- **Warning alarms:** may be temporary but the administrator should be notified of. Warning alarms are marked with a blue exclamation mark.
- **Minor alarms:** may cause service interruption or have an administrative reason. Minor alarms are marked with a yellow exclamation mark.
- **Major alarms:** may cause service interruption and clearly indicated problems in the system operation. Major alarms are marked with an orange exclamation mark.
- **Critical alarms:** represent service interruption. Critical alarms are marked with a red exclamation mark.

*Table 6-1: i series manager Alarms*

| | Name | ID | Troubleshooting | Action |
|---|---|---|---|---|
| | Mirror sync | -- | Mirror is synchronizing. | |
| | Theoretical target | -- | Target will only be operational with LUN 0. | |
| | Storage is missing | 0101 | Storage has been disconnected.<br>The administrator can reconnect the storage or replace it by a new one and then replace volume and delete the faulty storage | Reconnect or Delete. |
| | Storage Invalid | 0102 | A storage known by the system is configured differently.<br>The administrator can delete the storage. | Delete. |
| | Storage Unknown | 0103 | V Switch doesn't know the state of the storage. Select cluster and then the option Storage Discovery. | Storage Discovery. |
| | Storage Provisioned | 0104 | A storage has been configured by the user but never has been discovered by the V Switch. Select cluster and then the option Storage Discovery. | Storage Discovery. |
| | Subdisk Mismatch | 0105 | A subdisk has been provisioned by the user but after having been connected, its characteristics are different from those configured. | Delete. |
| | Volume non-functional | 0201 | A volume is non-functional if it is relying on a storage that is missing or invalid.<br>The administrator can reconnect the storage if missing or replace the volume and delete the non-functional one. | Replace and Delete. |
| | Volume internal | 0202 | Volume is not exposed. | |
| | Volume needs sync | 0203 | Volume needs to be synchronized. | Synchronize. |
| | Vol Need Sync | 0203 | A volume needs synchronization when it is not synchronized with the other children of a mirror. Activating mirror synchronize will close the alarm when synchronization is finished. | Mirror Synchronize. |
| | Mirror not Mirror | 0208 | A mirror volume is not mirroring because the other leg(s) of the mirror are non-functional. | Replace defective volume. |

| | Name | ID | Troubleshooting | Action |
|---|---|---|---|---|
| | Expandable | 0212 | The administrator has resized a volume hasn't yet expanded them. After expanding the volume, it will be the whole potential size attributed to it. | Expand. |
| | Over Used Snapshot | 0213 | A snapshot is approaching to the limit of its full capacity. | Resize. |
| | Snapshot Out of Sync | 0214 | A snapshot is no longer synchronized with its source. | Delete Snapshot. |
| | Snapshot Full | 0215 | A snapshot is full and no more synchronized with its source. Nothing can be done. Only delete the snapshot volume. | Delete Snapshot. |
| | Snapshot Modified | 0216 | A snapshot has been exposed with read-write access and was modified. | Delete Snapshot. |
| | Snapshot Expose Inconsistency | 0217 | A snapshot is exposed on a target exposed on a switch different from the one exposing the source. | Configuration. |
| | Volume Mismatch | 0220 | A volume has been provisioned by the user but after having been connected, its characteristics are different from those configured. | Delete. |
| | Not Validated | 0221 | A Volume has been configured and its size and block size haven't been validated. | Connect Storage. |
| | Theoretical Target | 0301 | A target has no LUN exposed on it. | Expose LU. |
| | Incomplete Definition | 0302 | There is no portal defined for it remote target. | Add Portal. |
| | Target not Connected | 0303 | The initiator of the V switch couldn't connect to the remote target. | Check IP and ACL. |
| | Fans faulty | 0401 | One FAN (and only one) doesn't work. Call support to replace the FAN. | i series X. Only two fans are working. |
| | Fans critical | 0402 | Both FANs don't work. Call support to replace the FANs. | Call Tech Support. |
| | Power supplies faulty | 0403 | One of the power supplies doesn't work. Call support to replace the power supply. | Call Tech Support. |
| | CPU temperature warning | 0404 | The temperature of the CPU is above the tolerable threshold. Turn off the switch and call support. | Turn off i series. |
| | On-board temperature warning | 0405 | The on-board temperature is above the tolerable threshold. Turn off the switch and call support. | Turn off i series. |
| | No fans | 0406 | No FANs are working. Turn off the i series and call support. | Turn off i series. |

| | Name | ID | Troubleshooting | Action |
|---|---|---|---|---|
| | CPU temperature critical | 0407 | The temperature of the CPU is above the critical threshold. Turn off the switch and call support. | Turn off i series. |
| | On-board temperature critical | 0408 | The on-board temperature is above the critical threshold. Turn off the switch and call support. | Turn off i series. |
| | Inconsistent Database | 0409 | The i series database is corrupted. Call technical support | Call technical support. |
| | Low Memory | 0410 | The device is under heavy load. Redistribute your resources. | Restart the i series. |
| | Cluster Inc | 0501 | At least one V Switch missing from the cluster in order to provide full redundancy. | Add V Switch. |
| | Neighbor dead | 0502 | i series lost connection with one of its neighbors. Check the network. Reconnecting the i series will close the alarm | Reconnect. |
| | Neighbor unknown | 0504 | i series doesn't know the state of one of its neighbors. After few seconds this alarm will be closed. | Wait. |
| | Object not redundant | 0505 | An object doesn't exist in the database of one of the i series of the cluster. Synchronizing the object will solve the problem. | Synchronize the cluster. |
| | Alias inconsistency | 0506 | Inconsistent Alias.<br>By giving a new alias to the object, the administrator will remove the alarm condition | Configure. |
| | LU number inconsistency | 0507 | A volume is exposed on a different LUN on the same target on two i series of the cluster.<br>Delete one of the LU and synchronize the other one. | Delete and synchronize. |
| | Data Attributes inconsistency | 0508 | Some parameters of an object are different according the i series; if the parameters are writable, re-writing them should solve the problem. | Configure. |
| | Illegal Subdisk | 0510 | There is a subdisk on one V Switch while there is a volume on the whole disk on another V Switch. | Delete subdisk. |
| | Illegal Volume | 0511 | The volume is inconsistent in the cluster: its structure is different on each V Switch. | Delete Volume. |
| | LU volume inconsistency | 0512 | A specific LUN is pointing to two different volumes within the cluster. Deleting the virtual LU will solve the problem. | Delete. |

| | Name | ID | Troubleshooting | Action |
|---|---|---|---|---|
| | Target volume inconsistency | 0513 | A volume is exposed on a different target on two i series of the cluster.<br>Delete one of the LU and synchronize the other one. | Delete. |
| | i series takeover | 0514 | i series has taken over its neighbor.<br>Reconnecting the second i series will solve this alarm condition. | Wait. |
| | Inconsistent ACL | 0515 | The ACL configuration is different within the cluster. | Reconfigure ACL. |
| | Inconsistent Volume | 0516 | The volume does not have the same number of children in the cluster | Synchronize volumes. |
| | Inconsistent Size | 0517 | The volume does not have the same actual size in all the V Switches in the cluster. | Expand. |
| | i serieses are not neighbors | 0518 | The switches are not configured as being neighbors. Try to rediscover your cluster.<br>Select cluster, right click and select Rediscover. | Configure. |
| | Target exposed inconsistency | 0519 | A target is inconsistently exposed among the cluster.<br>The administrator should change the exposure of the target. | Configuration. |
| | Illegal LUN serial number | 0523 | The serial number of a specific logical unit is different within the i series of the cluster. The administrator should delete one of the LU and then activate cluster synchronization. | Configuration. |
| | Portal Inconsistency | 0524 | A remote portal for a remote target is not defined in all the switches of the cluster. | Configure. |
| | ACL Entry not Redundant | 0525 | An ACL entry is not defined at the same target in all the switches of the cluster. | Configure. |
| | Incompatible License | 0526 | The devices in the cluster have incompatible licenses. | Configure. Ask your supplier to provide you with an upgraded license. |
| | Synchronizing | 0527 | One of the switches is synchronizing its states with that of its neighbor. | Wait. |
| | Standing | 0528 | Some incompatibility was found. | Check the configuration and correct it. |
| | Neighbor Removed | 0531 | The i series were inconsistently configured from the cluster's point of view, therefore the i series was removed. | Add the neighbor i series in the New i series dialog box. |

| | Name | ID | Troubleshooting | Action |
|---|---|---|---|---|
| ! | i series disconnected | 0901 | i series manager lost connection with a i series. Check the network.<br>Reconnecting the i series will close the alarm.<br>You can check also that the server's IP address is defined in the switch as manager by using the CLI command: snmp manager show. If it is not, please add it by using the CLI command: snmp manager add -ip <IP address> | Reconnect. |
| ! | Trap port in use | 0902 | i series trap port is already in use. Change the trap port via i series ->Properties ->SNMP to receive traps from this i series.<br>This trap port is where i series manager listens from.<br>The trap port must also be changed in the CLI.<br>This trap port is where the i series sends from. | Configuration. |
| ! | i series manager inconsistent with the i series | 0903 | There is total incompatibility between i series manager and the i series. The administrator should exit i series manager and then run it again. | Reset i series manager. |
| ! | LinkDown | 1001 | An interface stopped functioning. | Reconnect. |

*Table 6-2: Disaster Recovery Alarms*

| | Name | ID | Troubleshooting | Action |
|---|---|---|---|---|
| | Journal Internal | 0218 | The journal is not used. | Connect a pair. |
| | Overused Journal | 0219 | A journal is approaching to the limit of its full capacity. | Resize journal. |
| | Illegal Volume Pair | 0521 | The primary or the secondary volume of a pair in a switch is part of another pair in another switch of the cluster. | Select one of the pair as the "good" one and delete the other one. Activate Cluster Sync to synchronize the cluster (or the pair only). |
| | Illegal Pair Consistency Group | 0522 | The pair of a CG in a switch is part of another CG in another switch of the cluster. | Set the problematic pair to appropriate consistency group. |
| | Journal out of sync | 1201 | A journal is no longer synchronized with one of the replicating production volumes. User should abort replication, and restart it including initial synchronization. | Restart DR Process. |
| | Journal Full | 1202 | A journal is no longer synchronized with one of the replicating production volumes because it was full. User should abort replication, and restart it including initial synchronization. | Restart DR Process. |
| | Pair Error | 1203 | One of the volumes essential to the replication is not functioning including a journal volume. | Check that all the volumes: primary, secondary and Journal are well configured and well connected to the switch. |
| | Need Synchronization | 1204 | A pair or a group can be in this state if the remote volume was disconnected. Reconnect and reinitialize the initial synchronization. | Activate Replicate. |
| | Initial Sync in Progress | 1205 | The pair or the group is actually synchronizing its data. | Wait patiently. |
| | Switched | 1206 | Either a disaster occurred or the administrator initiated a planned failover. After fallback, the mode of those objects will switch back to normal. | Fallback. |

| | Name | ID | Troubleshooting | Action |
|---|---|---|---|---|
| | Consistency Group DR Unknown | 1207 | This group has simultaneously, at least one pair in normal mode and at least one pair in switched mode. The only way to correct the problem is to restart everything from the beginning. The administrator should activate the option "Abort Replication" from the pull down menu and then restart initial synchronization. | Restart DR Process. |
| | Replication Inactive | 1208 | The group/pair is well configured but wasn't activated yet. The administrator should activate the option "Start Initial Synchronization or Start Replication" from the pull down menu. | Start DR Process. |
| | Replicate Merge | 1209 | The group/pair is actually merging. | Wait. |
| | Replicate Transfer | 1210 | The group/pair is actually transferring | Wait. |
| | CG Empty | 1211 | The group is empty. Configure a pair to it. | Complete configuration. |
| | PFailover | 1212 | The group/pair started a process of planned failover which has not yet completed. | After waiting a while, you can try:<br>1. Rediscover<br>2. Reset switch |
| | Fallback | 1213 | The group/pair started a process of Fallback which has not yet completed. | After waiting a while, you can try:<br>1. Rediscover<br>2. Reset switch |
| | CFWaiting | 1214 | The group/pair is waiting for the agreement of the other side in order to perform an action. | Wait a while and reset switch. |
| | CFError | 1215 | The group/pair couldn't get the agreement of the other side in order to perform an action. Reset the switches. | Reset. |
| | Not Symmetric DR | 1301 | The pair is not configured in both sites. | Use wizard in order to complete pair configuration. |
| | Unequivalent Pair | 1302 | A pair is defined on Primary1, Secondary1 in one site and Primary1, Secondary2 in another site. | Delete misconfigured pair and use wizard. |
| | Inverted Pair | 1303 | Pair is defined on Primary1, Secondary1 in one site and Secondary1, Primary1 in another site. Delete one pair and then use wizard in order to complete pair configuration.. | Delete misconfigured pair. |

| | Name | ID | Troubleshooting | Action |
|---|---|---|---|---|
| | Asymmetric Attribute | 1304 | One pair has a different value between the sites. | Open the pair properties and reconfigure the initial sync type. |
| | Inverted Role | 1305 | The consistency group is declared local or remote in the both sites. | Use wizard. |
| | Inconsistent Replication | 1306 | The replication attributes are different within the sites. | Use wizard. |
| | Control Function Failure | 1307 | An action couldn't be performed. The most common reason for this alarm is that the network between a local site and a remote site is unavailable | Configuration. |
| | DiffSize | 1308 | The primary volume is different in size from the secondary one. | Delete and recreate the pair. |
| | Disaster | 1309 | The pair/group is in disaster mode. | Fallback. |

# Index