Alnico iSCSI to SAS/SATA-II RAID Subsystem

Software Operation Manual

V1.1

2009/07/08

Copyright ©2008

Notice

We make no warranties with respect to this documentation either express or implied and provide it "as it". This includes but is not limited to any implied warranties of merchantability and fitness for a particular purpose. The information in this document is subject to change without notice. We assume no responsibility for any errors that may appear in this document.

The manufacturer shall not be liable for any damage, or for the loss of information resulting from the performance or use of the information contained herein

Trademarks

Product names used herein are for identification purposes only and may be the trademarks of their respective companies. All trademarks or registered trademarks are properties of their respective owners.

About This Software Operation Manual

This manual contains all the information you need to initially configuring and monitoring the Alnico RAID.

Task Map

1. Prepare

Refer to Software Operation Manual and Hardware Installation Guide, let yourself know the features, capabilities of Alnico RAID and make sure you have everything on hand.

2. Install Hardware

Install the Alnico RAID Subsystem. Refer to:

Hardware Installation Guide

3. Configuration

To create a RAID set and define a volume set via LCD display front panel, remote utility or 10/100 base-T Ethernet.

4. Make a Record

Be sure to clearly write down every items of the configuration, it will help you to rescue the data back in case of RAID fail up.

Symbols in Text

These symbols may be found throughout this guide. They have the following meanings.

Caution

This icon indicates that failure to follow directions could result in personal injury, damage to your equipment or loss of information.

Note

This icon presents commentary, sidelights, or interesting points of information. .

Important terms, commands and programs are put in **Boldface** font.x.

Contents

Chapter 1. INTRODUCTION

This chapter provides a brief introduction of Array Definition and RAID concept.

1.1 Features

AInico 6 Series iSCSI RAID Subsystem:

AL-6080i: Gigabit LAN (x2) -to- SATA II 8 bay

AL-6120i: Gigabit LAN (x2) -to- SATA II 12 bay

AInico 8 Series iSCSI RAID Subsystem:

AL-8121i: Gigabit LAN (x4) -to- SAS/SATA II 12 bay

AL-8161i: Gigabit LAN (x4) -to- SAS/SATA II 16 bay

AInico iSCSI RAID features:

* RAID 6 / 10 / 30 / 50 / 60
* Snapshot / Rollback / Snapshot Export.
* Remote replication for client
* SAS support with SATA-II backward compatible.
* N-way mirror.
* On-line volume expansion and RAID level migration.
* Global/dedicated cache configuration by volume.
* S.M.A.R.T. enabled.
* Support SES.
* Support Microsoft VSS (Volume Shadow Copy Service, model dependent).
* Disk roaming.
* MPIO ready (initiator driver support is needed).
* MC/S ready (initiator driver support is needed).
* Support iSCSI header and data digest.
* Support CHAP authentication.
* Support Link Aggregation Trunking / LACP.

AInico iSCSI RAID connects to the host system in iSCSI interface. It can be configured to any RAID level, including **RAID 6**, and provides reliable data protection for servers. The RAID 6 function allows two HDD failures without any impact on the existing data. Data can be recovered from the remaining data and parity drives. (Data can be recovered from the rest disks/drives.)

Snapshot is a fully usable copy of a defined collection of data that contains an image of the data as it appeared at the point in time, which means a point-in-time data replication. It provides consistent and instant copies of data volumes without any system downtime. **AL-60801i / AL-6120i / AL-8121i / AL-8161i** can keep up to 512 snapshots. **Rollback** feature is provided for restoring the previously-snapshot data easily while continuously using the volume for further data access. The data access is regular as usual including read/write without any impact to end users. The snapshot function does not require any proprietary agents installed at host side, but is taken at target side and done by **iSCSI** controller inside. It will not consume any host CPU time thus the server is dedicated to the specific or other application. The snapshot copies can be taken manually or by schedule every hour or every day, depends on the modification.

AInico iSCSI RAID is a cost-effective disk array with completely integrated high-performance and data-protection capabilities which meet or exceed the highest industry standards, and **the best data solution for small/medium business (SMB) users.**

1.2 Terminology

The document use the following terms

RAID	RAID is the abbreviation of **"R**edundant **A**rray of **I**ndependent **D**isks**"**. There are different RAID levels with different degree of the data protection, data availability, and performance to host environment.
PD	The **P**hysical **D**isk belongs to the member disk of one specific RAID group.
RG	**R**aid **G**roup is created to decide the RAID Level and the number of hard drives used for that RAID Level. Raid Group must be created prior to the creation of Virtual Disk.
VD	**V**irtual **D**isk is equal to volume disk for the operating system to use. Without RG, VD can't be created.

CM	**C**ache **M**emory. Controller takes the onboard memory for cache memory usage in a smart way that the cache size can be auto adjusted invisibly for the max performance.
LUN	**L**ogical **U**nit **N**umber. A logical unit number (LUN) is a unique identifier which enables it to differentiate among separate devices (each one is a logical unit).
GUI	**G**raphic **U**ser **I**nterface.
RAID width, RAID copy, RAID row (RAID cell in one row)	RAID width, copy and row are used to describe one RG. E.g.: One 4-disk RAID 0 volume: RAID width= 4; RAID copy=1; RAID row=1. One 3-way mirroring volume: RAID width=1; RAID copy=3; RAID row=1. One RAID 10 volume over 3 4-disk RAID 1 volume: RAID width=1; RAID copy=4; RAID row=3 RAID width=1; RAID copy=4; RAID row=3.
WT	Write-Through cache-write policy. A caching technique in which the completion of a write request is not signaled until data is safely stored in non-volatile media. Each data is synchronized in both data cache and accessed physical disks.
WB	Write-Back cache-write policy. A caching technique in which the completion of a write request is signaled as soon as the data is in cache and actual writing to non-volatile media occurs at a later time. It speeds up system write performance but needs to bear the risk where data may be inconsistent between data cache and the physical disks in one short time interval.
RO	Set the volume to be Read-Only.
DS	Dedicated Spare disks. The spare disks are only used by one specific RG. Others could not use these dedicated spare disks for any rebuilding purpose.
GS	Global Spare disks. GS is shared for rebuilding purpose. If some RGs need to use the global spare disks for rebuilding, they could get the spare disks out from the common spare disks pool for such requirement.
DC	Dedicated Cache.
GC	Global Cache.

DG	DeGraded mode. Not all of the array's member disks are functioning, but the array is able to respond to application read and write requests to its virtual disks.
SCSI	Small Computer Systems Interface.
SAS	Serial Attached SCSI.
iSCSI	Internet Small Computer Systems Interface.
SAS	Serial Attached SCSI.
FC	Fibre Channel.
S.M.A.R.T.	Self-Monitoring Analysis and Reporting Technology.
WWN	World Wide Name.
HBA	Host Bus Adapter.
SAF-TE	SCSI Accessed Fault-Tolerant Enclosures.
SES	SCSI Enclosure Services.
NIC	Network Interface Card.
LACP	Link Aggregation Control Protocol.
MPIO	Multi-Path Input/Output.
MC/S	Multiple Connections per Session
MTU	Maximum Transmission Unit.
CHAP	Challenge Handshake Authentication Protocol. An optional security mechanism to control access to an iSCSI storage system over the iSCSI data ports.
iSNS	Internet Storage Name Service.

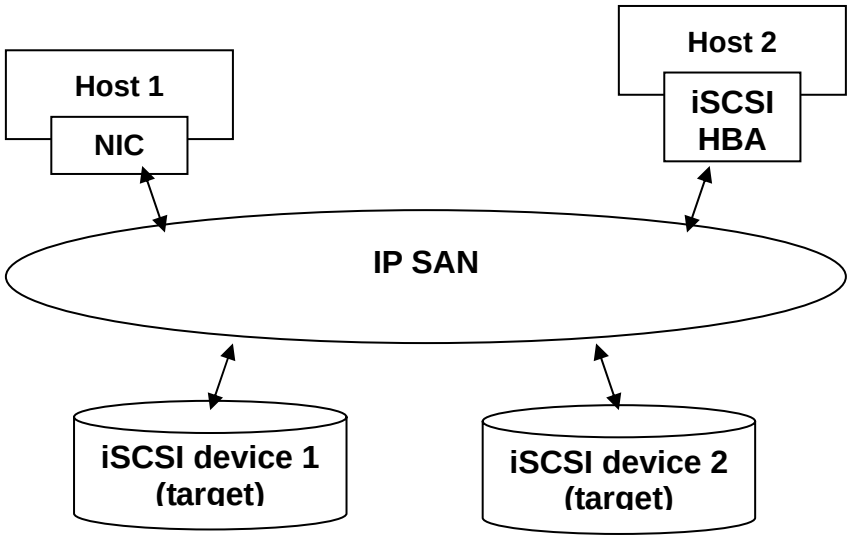
1.3 iSCSI Introduction

iSCSI (Internet SCSI) is a protocol which encapsulates SCSI (Small Computer System Interface) commands and data in TCP/IP packets for linking storage devices with servers over common IP infrastructures. iSCSI provides high performance SANs over standard IP networks like LAN, WAN or the Internet.

IP SANs are true SANs (Storage Area Networks) which allow few of servers to attach to an infinite number of storage volumes by using iSCSI over TCP/IP networks. IP SANs can scale the storage capacity with any type and brand of storage system. In addition, using any type of network (Ethernet, Fast Ethernet, Gigabit Ethernet) and combining operating systems (Microsoft Windows, Linux, Solaris, …etc.) within the SAN network. IP-SANs also include mechanisms for security, data replication, multi-path and high availability.

Storage protocol, such as iSCSI, has “two ends” in the connection. These ends are the initiator and the target. In iSCSI we call them iSCSI initiator and iSCSI target. The iSCSI initiator requests or initiates any iSCSI communication. It requests all SCSI operations like read or write. An initiator is usually located on the host/server side (either an iSCSI HBA or iSCSI SW initiator).

The iSCSI target is the storage device itself or an appliance which controls and serves volumes or virtual volumes. The target is the device which performs SCSI commands or bridges it to an attached storage device. iSCSI targets can be disks, tapes, RAID arrays, tape libraries, and etc.



The host side needs an iSCSI initiator. The initiator is a driver which handles the SCSI traffic over iSCSI. The initiator can be software or hardware (HBA). Please refer to the certification list of iSCSI HBA(s) in Appendix A. OS native initiators or other software initiators use the standard TCP/IP stack and Ethernet hardware, while iSCSI HBA(s) use their own iSCSI and TCP/IP stacks on board.

Hardware iSCSI HBA(s) would provide its initiator tool. Please refer to the vendors' HBA user manual. **Microsoft**, **Linux** and **Mac** provide software iSCSI initiator driver. Below are the available links:

Link to download the Microsoft iSCSI software initiator:

http://www.microsoft.com/downloads/details.aspx?FamilyID=12cb3c1a-15d6-4585-b385-befd1319f825&DisplayLang=en

Please refer to Appendix A & B for Microsoft iSCSI initiator installation procedure.

Linux iSCSI initiator is also available. For different kernels, there are different iSCSI drivers. Please check Appendix A & B for software iSCSI initiator certification list. If user needs the latest Linux iSCSI initiator, please visit Open-iSCSI project for most update information. Linux-iSCSI (sfnet) and Open-iSCSI projects merged in April 11, 2005.

Open-iSCSI website: http://www.open-iscsi.org/

Open-iSCSI README: http://www.open-iscsi.org/docs/README

Features: http://www.open-iscsi.org/cgi-bin/wiki.pl/Roadmap

Support Kernels:

http://www.open-iscsi.org/cgi-bin/wiki.pl/Supported_Kernels

Google groups:

http://groups.google.com/group/open-iscsi/threads?gvc=2

http://groups.google.com/group/open-iscsi/topics

Open-iSCSI Wiki: http://www.open-iscsi.org/cgi-bin/wiki.pl

ATTO iSCSI initiator is available for Mac.

Website: http://www.attotech.com/xtend.html

1.4 RAID Concept

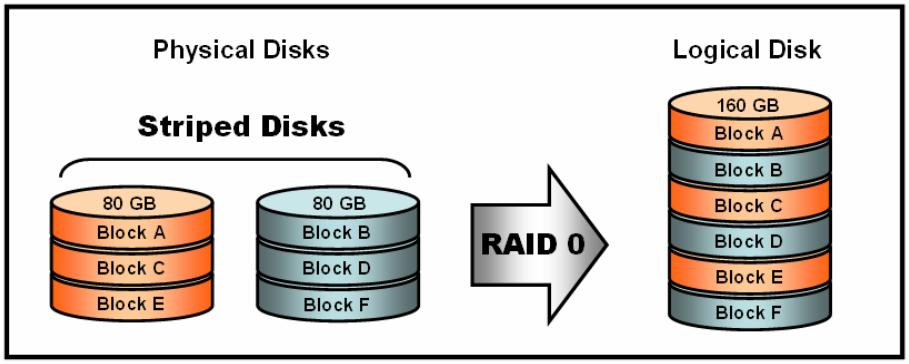
RAID is an acronym for Redundant Array of Independent Disks. It is an array of multiple independent hard disk drives that provide high performance and fault tolerance. The RAID subsystem controller implements several levels of the Berkeley RAID technology. An appropriate RAID level is selected when the

volume sets are defined or created. This decision is based on disk capacity, data availability (fault tolerance or redundancy), and disk performance. The following are the RAID levels which are supported in the RAID subsystem.

The RAID subsystem controller makes the RAID implementation and the disks' physical configuration transparent to the host operating system. This means that the host operating system drivers and software utilities are not affected, regardless of the RAID level selected. Correct installation of the disk array and the controller requires a proper understanding of RAID technology and the concepts.

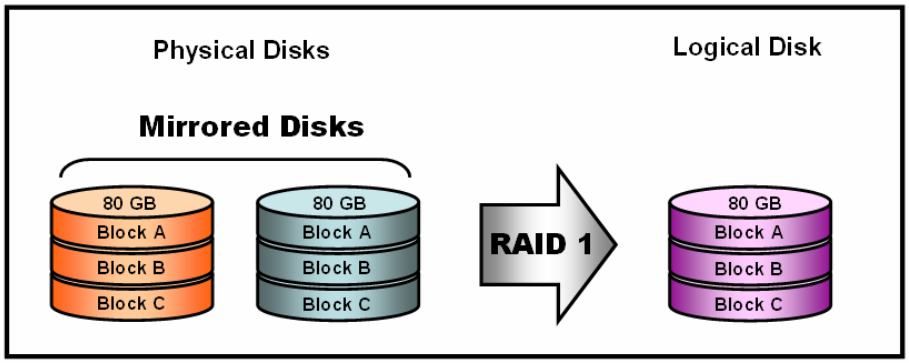
1.2.1 RAID 0

RAID 0, also referred to as striping, writes stripping of data across multiple disk drives instead of just one disk drive. RAID 0 does not provide any data redundancy, but does offer the best high-speed data throughput. RAID 0 breaks up data into smaller blocks and then writes a block to each drive in the array. Disk striping enhances performance because multiple drives are accessed simultaneously; but the reliability of RAID Level 0 is less than any of its member disk drives due to its lack of redundancy.



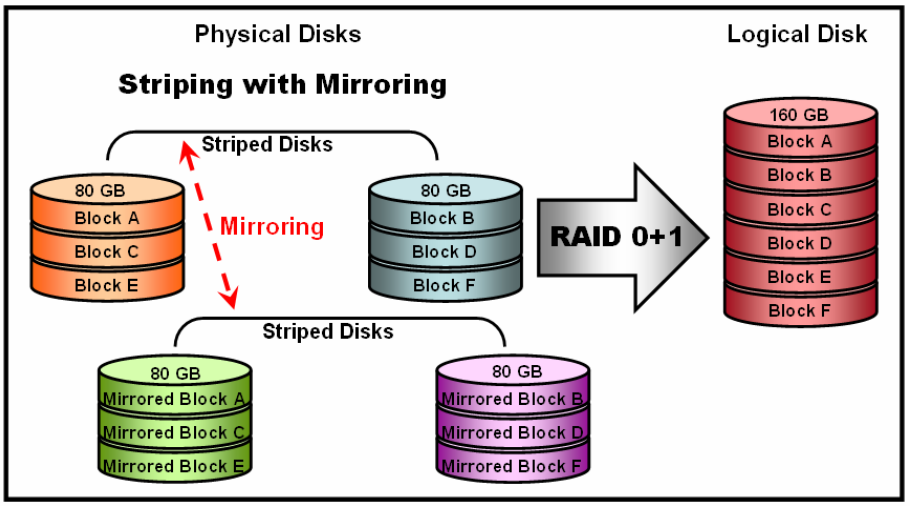
1.2.2 RAID 1

RAID 1 also known as "disk mirroring", data written to one disk drive is simultaneously written to another disk drive. Read performance may be enhanced if the array controller can parallel accesses both members of a mirrored pair. During writes, there will be a minor performance penalty when compared to writing to a single disk. If one drive fails, all data (and software applications) are preserved on the other drive. RAID 1 offers extremely high data reliability, but at the cost is doubling the required data storage capacity.



1.2.3 RAID 0+1

RAID 0+1 is a combination of RAID 0 and RAID 1, combing stripping with disk mirroring. RAID Level 10 combines the fast performance of Level 0 with the data redundancy of Leve1 1. In this configuration, data is distributed across several disk drives, similar to Level 0, which are then duplicated to another set of drive for data protection. RAID 0+1 provides the highest read/write performance of any of the Hybrid RAID levels, but at the cost of doubling the required data storage capacity.



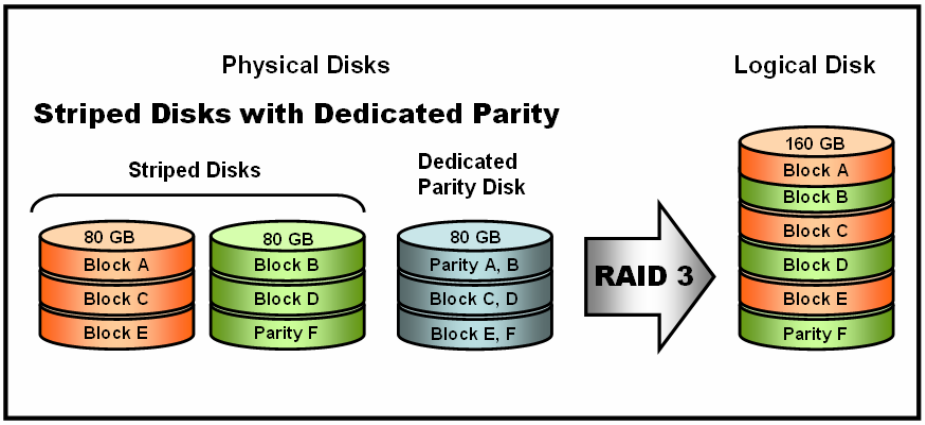
.

1.2.4 N-way mirroring

Extension to RAID 1 level. It has N copies of the disk.

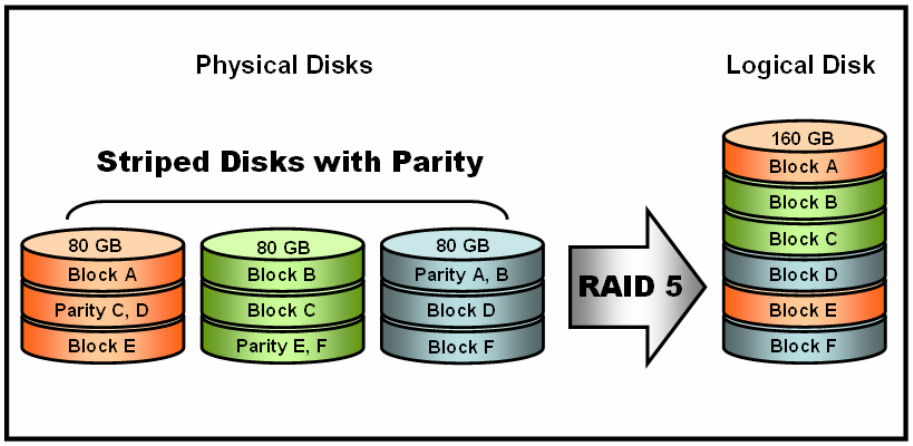
1.2.5 RAID 3

RAID 3 provides disk striping and complete data redundancy through a dedicated parity drive. RAID 3 breaks up data into smaller blocks, calculates parity by performing an exclusive-or on the blocks, and then writes the blocks to all but one drive in the array. The parity data created during the exclusive-or is then written to the last drive in the array. If a single drive fails, data is still available by computing the exclusive-or of the contents in the corresponding strips of the surviving member disk. RAID-3 is best for applications that require very fast data- transfer rates or long data blocks



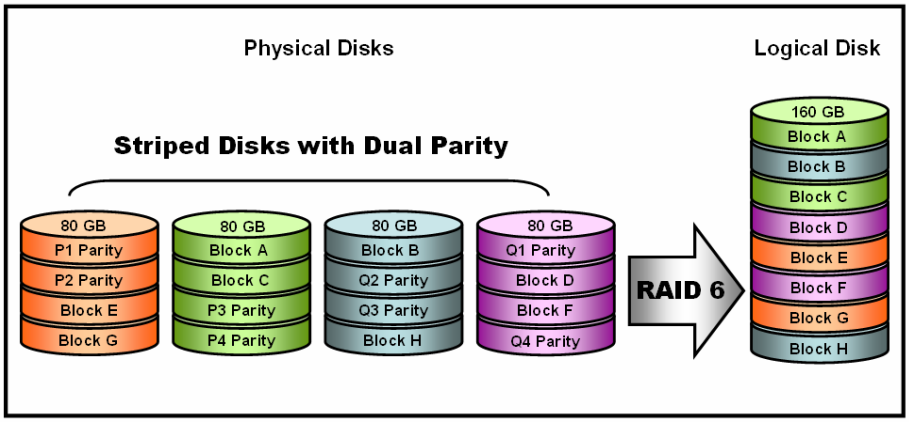
1.2.6 RAID 5

RAID 5 is sometimes called striping with parity at block level. In RAID 5, the parity information is written to all of the drives in the subsystems rather than concentrated on a dedicated parity disk. If one drive in the system fails, the parity information can be used to reconstruct the data from that drive. All drives in the array system can be used to seek operation at the same time, greatly increasing the performance of the RAID system.



1.2.7 RAID 6

A RAID 6 array is essentially an extension of a RAID 5 array with a second independent distributed parity scheme. Data and parity are striped on a block level across multiple array members, just like in RAID 5, and a second set of parity is calculated and written across all the drives. As larger disk arrays are considered, it is desirable to use stronger codes that can tolerate multiple disk failure. When a disk fails in a parity protected disk array, recovering the contents of the failed disk requires successful reading on the contents of all no-failed disks. RAID 6 provides an extremely high fault tolerance, and can sustain two simultaneous drive failures without downtime or data loss. This is a perfect solution when data is mission-critical.

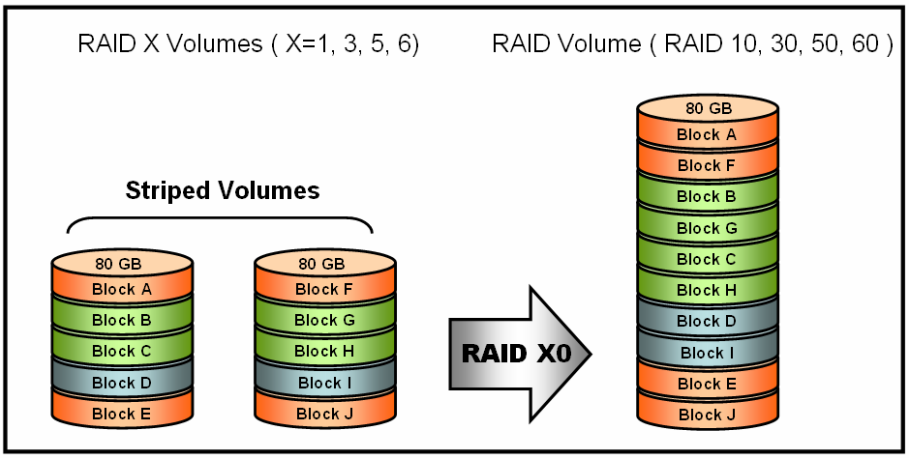


1.2.8 RAID X0

RAID level-X0 (available only on Alnico 8 Series) refers to RAID level- 10, 30,

50 and 60. RAID X0 is a combination of multiple RAID x volume sets with RAID 0 (striping). Striping helps to increase capacity and performance without adding disks to each RAID x array. The operating system uses the spanned volume in the same way as a regular volume. Up to one drive in each sub-volume (RAID 1, 3 or 5) may fail without loss of data. Up to two drives in each sub-volume (RAID 6) may fail without loss of data.

The following illustration is an example of a RAID level-X0 logical drive.



RAID level-X0 allows more physical drives in an array. The benefits of doing so are larger volume sets, increased performance, and increased reliability.

NOTE

RAID level-30 50 and 60 can support up to eight sub-Volumes.

If the volume is RAID level-30, 50, or 60, you cannot change the volume to another RAID level. If the volume is RAID level-0, 1, 1E, 3, 5, or 6, you cannot change the volume to RAID level-30, 50, or 60.

1.2.9 Summary of RAID Levels

RAID subsystem supports RAID Levels 0, 1, 1E, 3, 5, 6, 30, 50 and 60. The following table provides a summary of RAID levels

RAID Level	Description	Disks requirement (Cost)	Data Reliability
0	Also known as stripping. Data distributed across multiple drives in the array. There is no data protection	N	* No data Protection.
1	Also known as mirroring. All data replicated on N Separated disks. N is almost always 2. This is a high availability Solution, but due to the 100% duplication, it is also a costly solution.	2	* Lower than RAID 6. * Higher than RAID 3, 5.
0+1	Also known Block-Interleaved Parity. Data and parity information is subdivided and distributed across all disk. Parity must be the equal to the smallest disk capacity in the array. Parity information normally stored on a dedicated parity disk.	N (N>2)	* Lower than RAID 6. * Higher than RAID 3, 5.
3	Also known Bit-Interleaved Parity. Data and parity information is subdivided and distributed across all disk. Parity must be the equal to the smallest disk capacity in the array. Parity information normally stored on a dedicated parity disk.	N+1	* Lower than RAID 1, 10, 6; * Higher than a single drive.
5	Also known Block-Interleaved Distributed Parity. Data and parity information is subdivided and distributed across all disk. Parity must be the equal to the smallest disk capacity in the array. Parity information normally stored on a dedicated parity disk.	N+1	* Lower than RAID 1, 10, and 6. * Higher than a single drive.
6	AS RAID level 5, but with additional independently computed redundant information	N+2	* Highest of all listed alternatives.
30	RAID 30 is a combination multiple RAID 3 volume sets with RAID 0 (striping)	(N+1) *2	Up to one disk failure in each sub-volume
50	RAID 50 is a combination multiple RAID 5 volume sets with RAID 0 (striping)	(N+1) *2	Up to one disk failure in each sub-volume
60	RAID 60 is a combination multiple RAID 6 volume sets with RAID 0 (striping)	(N+2) *2	Up to two disk failure in each sub-volume

1.2.10 Rebuild

If one physical disk of the RG which is set as protected RAID level (e.g.: RAID 3, RAID 5, or RAID 6) is FAILED or has been unplugged/removed, then the status of RG is changed to degraded mode, the system will search/detect spare disk to rebuild the degraded RG to a complete one. It will detect dedicated spare disk as rebuild disk first, then global spare disk.

Alnico iSCSI RAID support Auto-Rebuild. The following is the scenario:

Take RAID 6 for example:

When there is no global spare disk or dedicated spare disk in the system, controller will be in degraded mode and wait until (A) there is one disk assigned as spare disk, or (B) the failed disk is removed and replaced with new clean disk, then the Auto-Rebuild starts. The new disk will be a spare disk to the original RG automatically.

If the new added disk is not clean (with other RG information), it would be marked as RS (reserved) and the system will not start "auto-rebuild".

If this disk is not belonging to any existing RG, it would be FR (Free) disk and the system will start Auto-Rebuild.

If user only removes the failed disk and plugs the same failed disk in the same slot again, the auto-rebuild will start running. But rebuilding in the same failed disk may impact customer data if the status of disk is unstable. We suggests all customers not to rebuild in the failed disk for better data protection.

When there is enough global spare disk(s) or dedicated spare disk(s) for the degraded array, controller starts Auto-Rebuild immediately. And in RAID 6, if there is another disk failure occurs during rebuilding, controller will start the above Auto-Rebuild process as well. Auto-Rebuild feature only works at that the status of RG is **"Online"**. It will not work at **"Offline"**. Thus, it will not conflict with the **"Roaming"**.

In degraded mode, the status of RG is **"Degraded"**. When rebuilding, the status of RG/VD will be **"Rebuild"**, the column **"R%"** in VD will display the ratio in percentage. After complete rebuilding, the status will become "Online". RG will become completely one.

"Set dedicated spare" is not available if there is no RG or only RG of RAID 0, JBOD, because user can not set dedicated spare disk to RAID 0 & JBOD.

Sometimes, rebuild is called recover; they are the same meaning. The following

table is the relationship between RAID levels and rebuild.

RAID 0	Disk striping. No protection for data. RG fails if any hard drive fails or unplugs.
RAID 1	Disk mirroring over 2 disks. RAID 1 allows one hard drive fails or unplugging. Need one new hard drive to insert to the system and rebuild to be completed.
N-way mirror	Extension to RAID 1 level. It has N copies of the disk. N-way mirror allows N-1 hard drives failure or unplugging.
RAID 3	Striping with parity on the dedicated disk. RAID 3 allows one hard drive failure or unplugging.
RAID 5	Striping with interspersed parity over the member disks. RAID 5 allows one hard drive failure or unplugging.
RAID 6	2-dimensional parity protection over the member disks. RAID 6 allows two hard drives failure or unplugging. If it needs to rebuild two hard drives at the same time, it will rebuild the first one, then the other in sequence.
RAID 0+1	Mirroring of RAID 0 volumes. RAID 0+1 allows two hard drive failures or unplugging, but at the same array.
RAID 10	Striping over the member of RAID 1 volumes. RAID 10 allows two hard drive failure or unplugging, but in different arrays.
RAID 30	Striping over the member of RAID 3 volumes. RAID 30 allows two hard drive failure or unplugging, but in different arrays.
RAID 50	Striping over the member of RAID 5 volumes. RAID 50 allows two hard drive failures or unplugging, but in different arrays.
RAID 60	Striping over the member of RAID 6 volumes. RAID 40 allows four hard drive failures or unplugging, every two in different arrays.
JBOD	The abbreviation of “Just a Bunch Of Disks”. No data protection. RG fails if any hard drive failures or unplugs.

1.2.11 Disk roaming

RAID subsystem supports RAID Levels 0, 1, 1E, 3, 5, 6, 30, 50 and 60. The

following table provides a summary of RAID levels.

Physical disks can be re-sequenced in the same system or move all physical disks from system-1 to system-2. This is called disk roaming. System can execute disk roaming online. Please follow the procedures.

1. Select "/ Volume configuration / RAID group".
2. Mouse moves to the gray button next to the RG number; click "Deactivate".
3. Move all PDs related to the RG to another system.
4. Mouse moves to the gray button next to the RG number; click "Activate".
5. Done.

Disk roaming has some constraints as described in the followings:

Check the firmware of two systems first. It is better that both systems have the same firmware version or newer.

All physical disks of related RG should be moved from system-1 to system-2 together. The configuration of both RG and VD will be kept but LUN configuration will be cleared in order to avoid conflict with system.

The off-line RG from the AL-8161i and 8121i can't be moved to the AL-6080i and 6120i. Contrariwise.

Chapter 2. Configuration Methods

2.1 Overview

After the hardware installation, the SAS (or SATA) disk drives installed to the RAID must be configured and the volume set units initialized before they are ready to use. This can be accomplished by one of the following methods:

- **Front LCD control module**
- Remote utility connected through the **Console Serial Port** (VT-100 or Hyper terminal)
- Using **Remote Control-Secure Sell (SSH)** through the controller's 10/100 Ethernet LAN port .
- **Web GUI** RAID manager via the controller's 10/100 Ethernet LAN port.

Those user interfaces can access the built-in configuration and administration utility that resides in the controller's firmware. They provide complete control and management of the controller and disk arrays, eliminating the need for additional hardware or software.

There are two sets of login account supported by Alnico RAID iSCSI RAID:

Login name: **admin**

Default password: **0000**

Or login with read-only account which only allows reading the configuration and cannot change setting.

Login name: **user**

Default password: **1234**

The RAID subsystem allows only one method to access menus at a time.

2.2 Front LCD control module

The front panel keypad and liquid crystal display (LCD) is the primary user interface for the RAID subsystem. All configuration and management of the

RAID and its properly connected disk arrays can be performed from this interface.

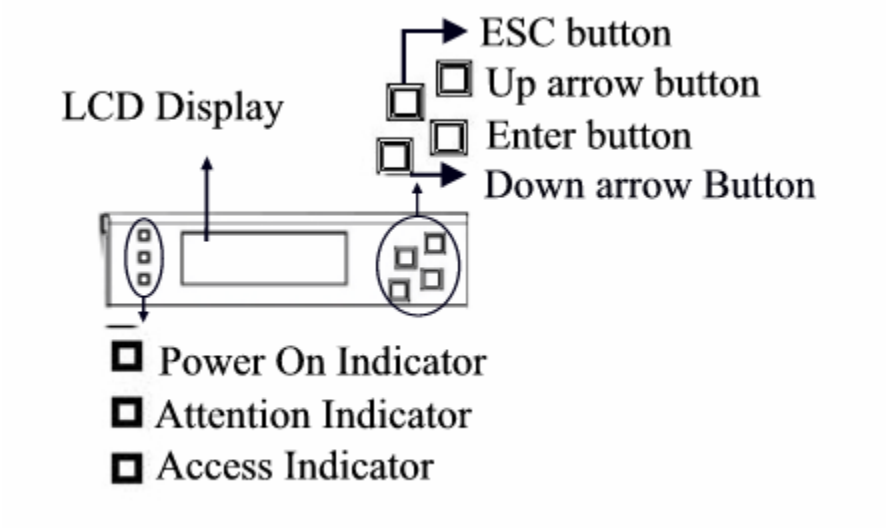
The front panel keypad and LCD are connected to the RAID subsystem to access the built-in configuration and administration utility that resides in the controller's firmware. Complete control and management of the array's physical drives and logical units can be performed from the front panel, requiring no additional hardware or software drivers for that purpose.

This Chapter provides, in quick reference form, procedures that use the built-in LCD panel to configure and operate the controller.

A touch-control keypad and a liquid crystal display (LCD) mounted on the front panel of the RAID subsystem is the primary operational interface and monitor display for the disk array controller. This user interface controls all configuration and management functions for the RAID subsystem controller and for all SAS (or SATA) disk array subsystems to which it is properly connected.

The LCD provides a system of screens with areas for information, status indication, or menus. The LCD screen displays up to two lines at a time of menu items or other information.

The Initial screen is as following:



The four function keys at the button of the front panel perform the following functions:

Key	Function
Up Arrow	Use to scroll the cursor Upward / Rightward
Down Arrow	Use to scroll the cursor Downward / Leftward
ENT Key	Submit Select ion Function (Confirm a selected item)
ESC Key	Return to Previous Screen (Exit a selection configuration)

There are three LED indicators on the front panel. Following table provides a summary of the meanings of these LED indicators:

LED Indicator	Normal Status	Problem Indication
Power On indicator	Bright Blue	This LED does not light up after power switched on
Fail Indicator	LED never lights up	LED lights up as Red.
Data Access Indicator	Blink blue during host computer accessing the RAID subsystem.	LED never flickers

For additional information on using the LCD panel and keypad to configure the RAID see ”LCD Control Module Configuration” on Chapter 3.

2.3 Console Serial Port

The serial port on the RAID subsystem’s back panel can be used in Remote manage mode. The provided interface cable converts the RS232 signal on the RAID subsystem into a RJ-11 male connector. The firmware-based terminal array management interface can access the array through this RS-232 port. You can attach a VT-100 compatible terminal or a PC running a “Hyper terminal” program to the serial port for accessing the text-based Setup Menu.

To ensure proper communications between the RAID subsystem and the VT-100 Terminal Emulation, Please configure the VT100 terminal emulation settings to the values shown below:

Terminal requirement	
Connection	Null-modem cable
Baud Rate	115,200
Data bits	8
Stop	1
Flow Control	None

The RAID Subsystem's 6-pin RJ-11 connector's pin assignments are defined as below :

Pin#	Signal	Pin#	Signal
1	NC	4	TX
2	GND	5	CTS
3	RX	6	NC

2.3.1 Keyboard Navigation

The following definition is the VT-100 RAID configuration utility keyboard navigation:

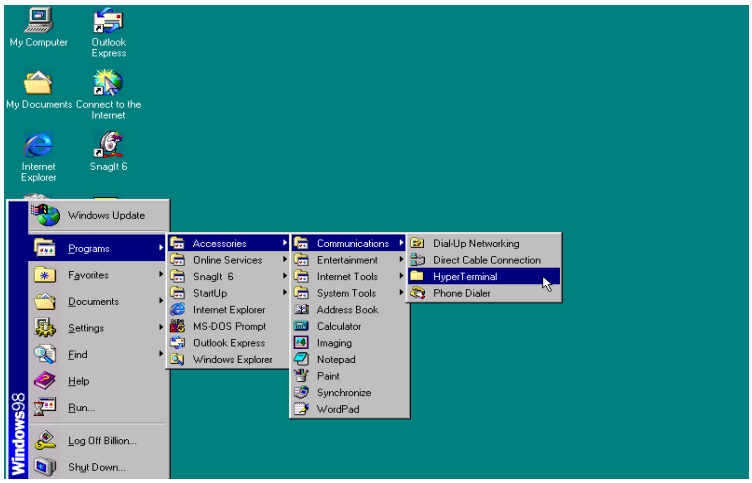
Key	Function
Arrow Key	Move cursor
Enter Key	Submit selection function
ESC Key	Return to previous screen

2.3.2 Start-up VT100 Screen

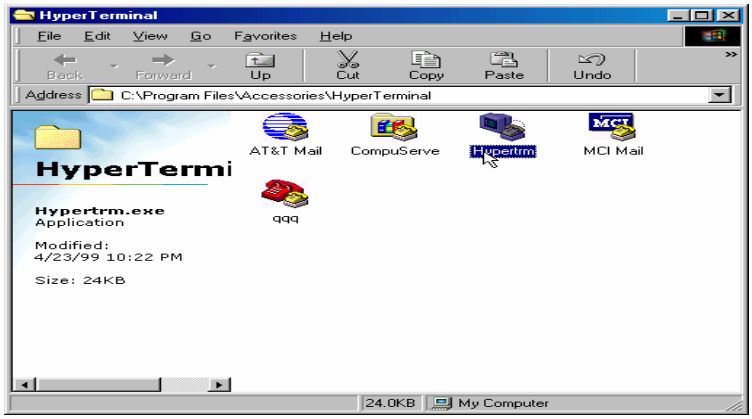
By connecting a VT100 compatible terminal, or a PC operating in an equivalent terminal emulation mode, all RAID subsystem monitoring, configuration and administration functions can be exercised from the VT100 terminal.

There are a wide variety of Terminal Emulation packages, but for the most part they should be very similar. The following setup procedure is an example Setup VT100 Terminal in Windows XP system using Hyper Terminal use Version 3.0 or higher.

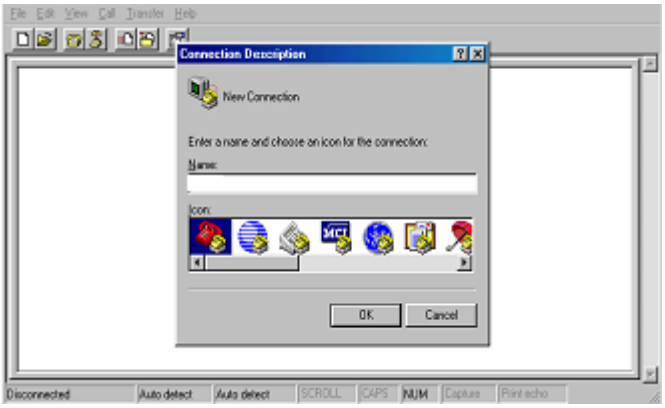
Step 1. From the Desktop open the Start menu. Pick Programs, Accessories, Communications and Hyper Terminal. Open Hyper Terminal (requires version 3.0 or higher)



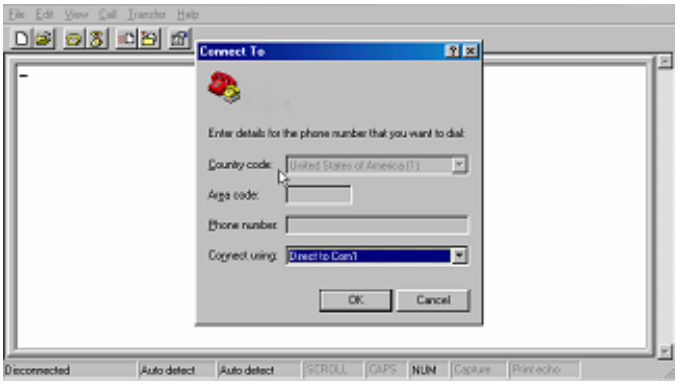
Step 2. Open HYPERTRM.EXE.



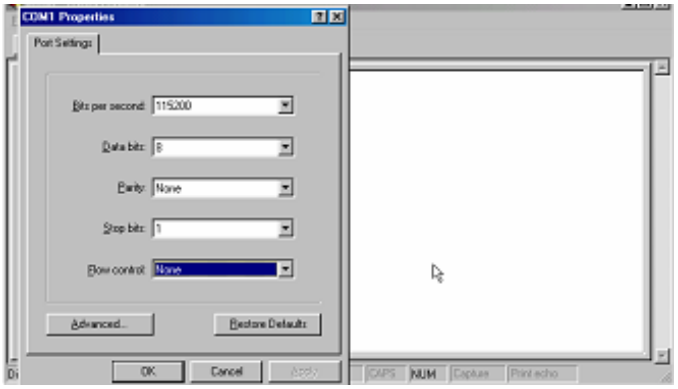
Step 3. Enter a name for your Terminal. Click OK.



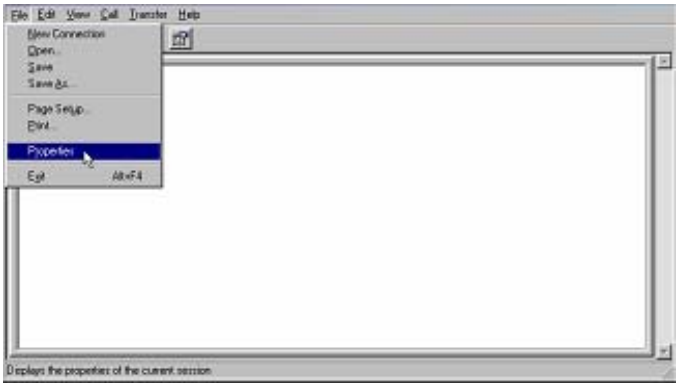
Step 4. Select an appropriate connecting port in your Terminal. Click OK



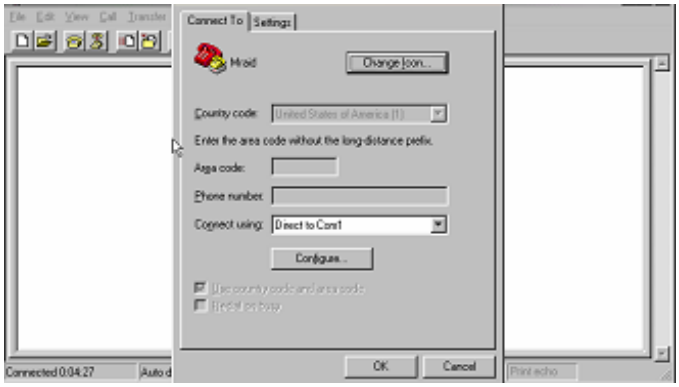
Step 5. Configure the port parameter settings. Bits per second: “115200”, Data bits: “8”, Parity: “None”, Stop bits: “1”, Flow control: “None”. Click OK



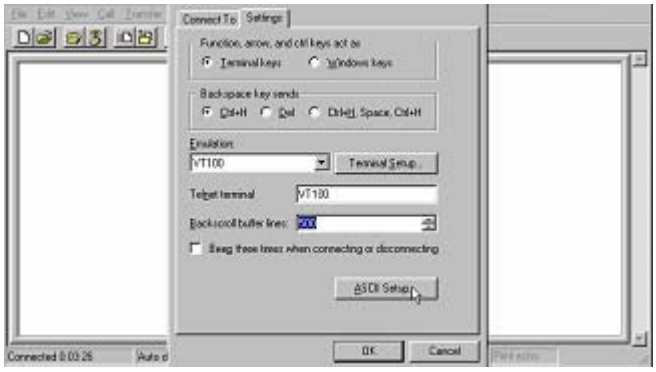
Step 6. Open the File menu, and then open Properties.



Step 7. Open the Settings Tab.



Step 8. Open the Settings Tab. Function, arrow and ctrl keys act as: Terminal Keys, Backspace key sends: Crtl+H, Emulation: VT100, Telnet terminal: VT100, Back scroll buffer lines: 500. Click OK.



Now, the VT100 is ready to use.

Press “Enter’ key to display the disk array Monitor Utility screen on your VT100 Terminal.

2.4 Remote Control-Secure Sell

Using the controller’s 10/100 Ethernet port and SSH client software to remote login to the RAID. Secure Shell is a program to log into another computer over a network, to execute commands in a remote machine, it provides strong authentication and secure communications over insecure channels. When using ssh's slogin (instead of rlogin) the entire login session, including transmission of **password,** is encrypted; therefore it is almost impossible for an outsider to collect passwords.

SSH client software is available at the following web site:

SSHWinClient WWW: **http://www.ssh.com/**

Putty WWW: **http://www.chiark.greenend.org.uk/**

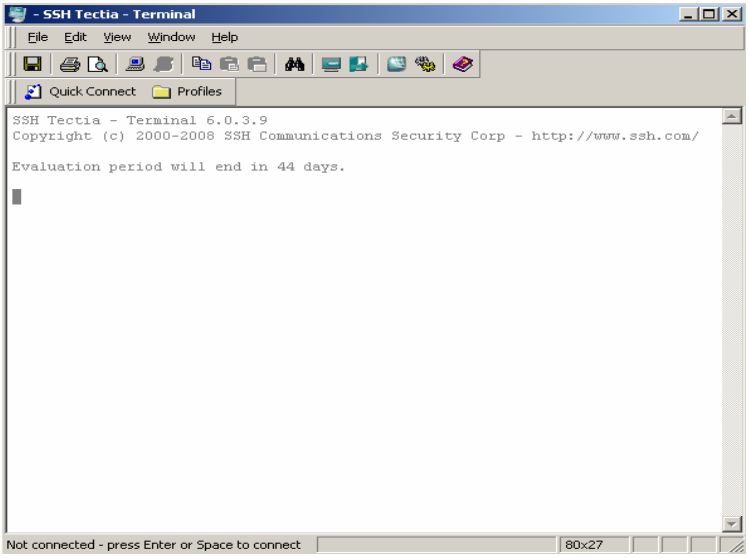
2.4.1 Keyboard Navigation

The following definition is the VT-100 RAID configuration utility keyboard navigation.

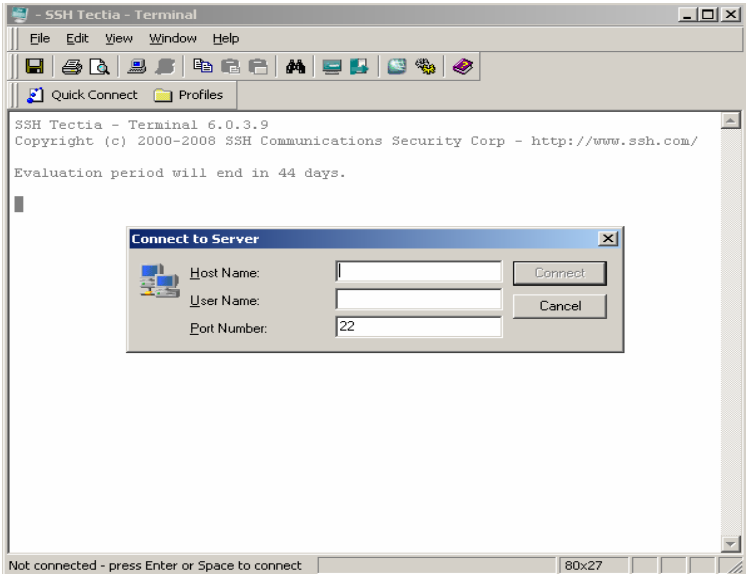
Key	**Function**
Arrow Key	Move cursor
Enter Key	Submit selection function
ESC Key	Return to previous screen

2.4.2 Start-up SSH client software

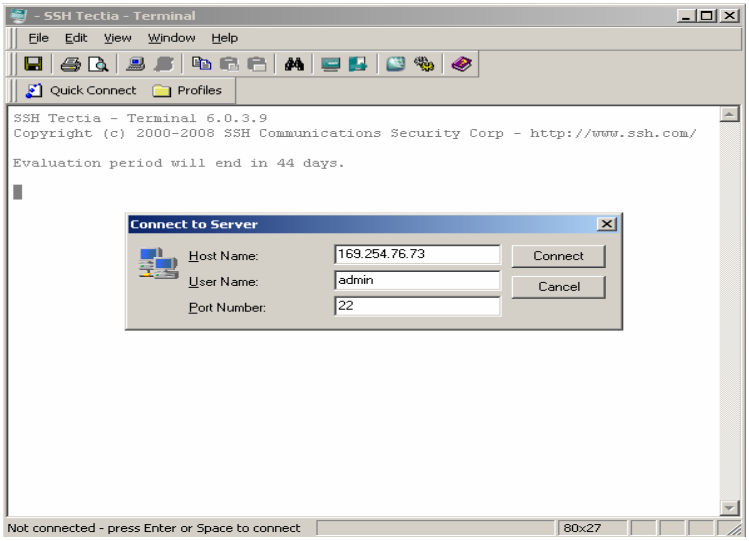
Step 1. Double clicks to execute SSH client software



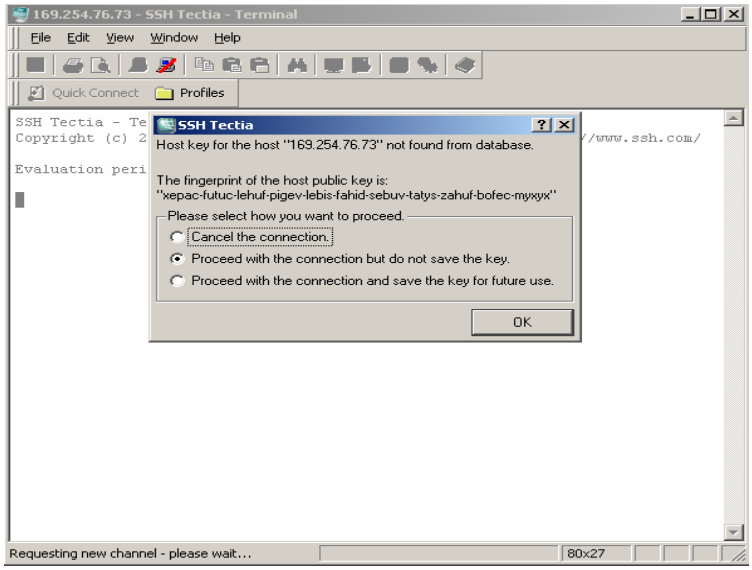
Step 2. Press a “Enter” to create a new connection.



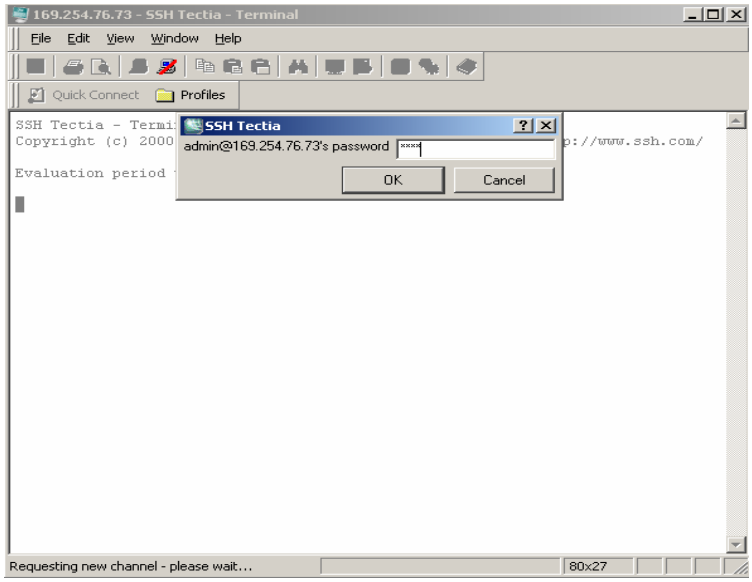
Step 3. Key in IP address into the field of Host name, it will be default shown on the LCD screen. Then login name in the field of User name. The defaults of Port Number is “22”.



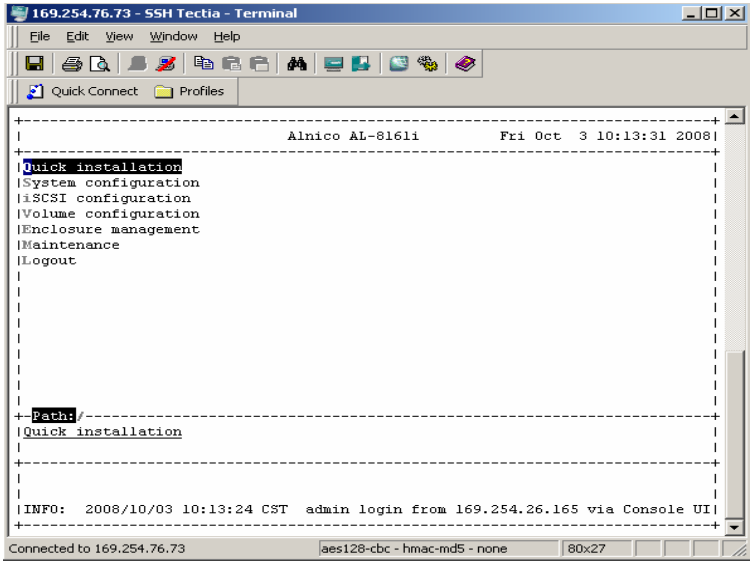
Step 4. Select “Proceed with the connection but do not save the key” to have higher security.



Step 5. Enter the password



Step 6. Then you will login into Alnico iSCSI RAID subsystems



Now, the SSH software is ready to use.

2.5 Web GUI RAID manager via the controller's 10/100 Ethernet LAN port.

The controller has embedded the TCP/IP & Web Browser-based RAID manager in the firmware. User can remotely manage the RAID system, without adding any specific software (platform independent), via standard web browsers directly connected to the 10/100 Ethernet RJ45 LAN port.

To configure RAID subsystem on a local or remote machine, you need to know its IP Address. The IP address will be default shown in the LCD screen. Launch your firmware-embedded TCP/IP & Web Browser-based RAID manager by entering http://[IP Address] in the web browser.

You must be logged in as administrator with local admin rights on the remote machine to remotely configure it. The RAID subsystem controller default username is ***"admin"*** *and the password is* ***"0000".***

Chapter 3.

Front LCD Control Module Configuration

The Alnico RAID's Front LCM is character-based which you can use after powering the unit. Use LCD Configuration panel to:

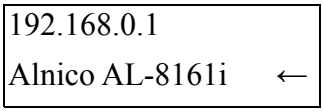
System Info.	Display system information.
Alarm Mute	Mute alarm when error occurs.
Reset/Shutdown	Reset or shutdown controller.
Quick Install	Quick steps to create a volume. Please refer to next chapter for operation in web UI for more convenience configuration.
Volume Wizard	Smart steps to create a volume. Please refer to next chapter for operation in web UI for more convenience configuration.
View IP Setting	Display current IP address, subnet mask, and gateway.
Change IP Config	Set IP address, subnet mask, and gateway. There are 2 options: DHCP (Get IP address from DHCP server) or static IP.
Reset to Default	Reset to default will set password to default: **0000**, and set IP address to default as static setting. Default IP address: **192.168.001.100** Default subnet mask: **255.255.255.0** Default gateway: **192.168.001.254**

LCM function keys are the basic user interface for the RAID subsystem, there are very limited features supported. If user would like to have more advanced configuration, please use Web GUI configuration, this is a primary user interface for the RAID subsystem.

3.1 Starting LCD Configuration Utility

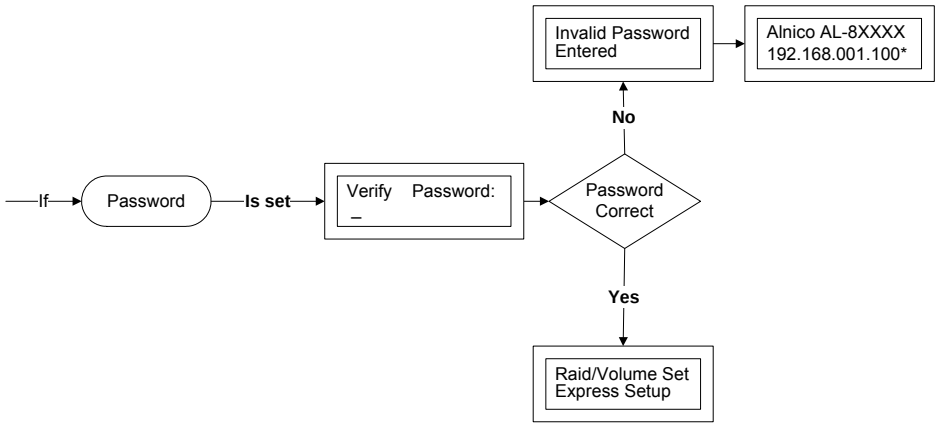
The main menu appears on the LCD screen, as shown below:

Use the up and down arrow buttons to move left and right to select a menu item. Press **ENT** to select the item. Press the **UP/DOWN** to browse the selection. Press **ESC** to return to the previous screen.



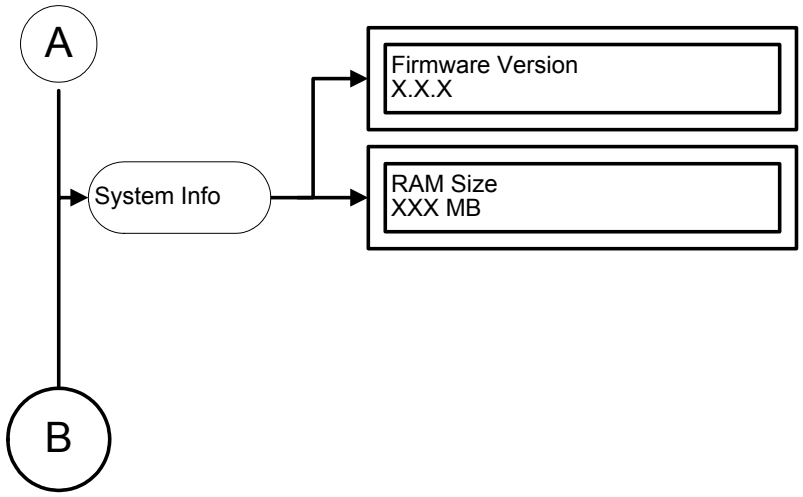
3.2 Navigation Map of the Configuration

The password option allows user to set or clear the raid subsystem's password protection feature. Once the password has been set, the user can only monitor and configure the raid subsystem by providing the correct password. The password is used to protect the internal RAID subsystem from unauthorized entry. The controller will check the password only when entering the Main menu from the initial screen. The RAID subsystem will automatically go back to the initial screen when it does not receive any command in twenty seconds. The RAID subsystem password's default setting is 0000 by the manufacturer.



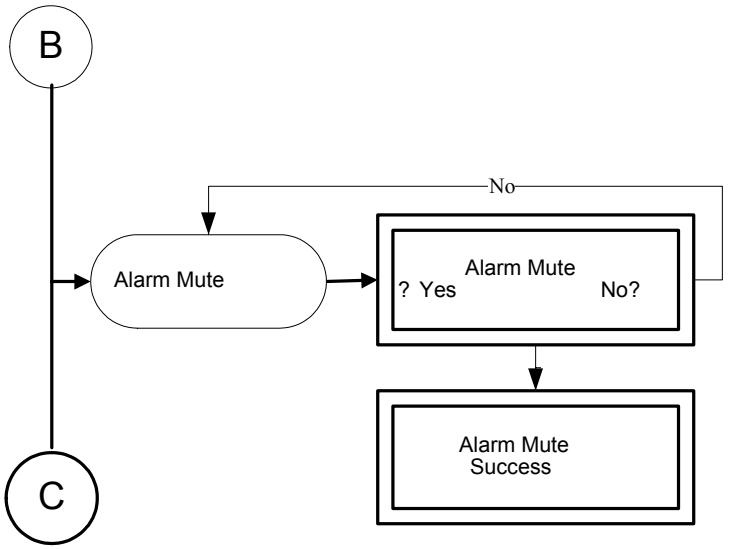
3.2.1 Show System Information

Choose this option to display firmware version and cache memory size. To check the system information, press **ENT** to enter the main menu. Press **UP/DOWN** to select the **Show System Information** option, and then press **ENT**. All major controller system information will be displayed. Press **UP/DOWN** to browse all the system information.



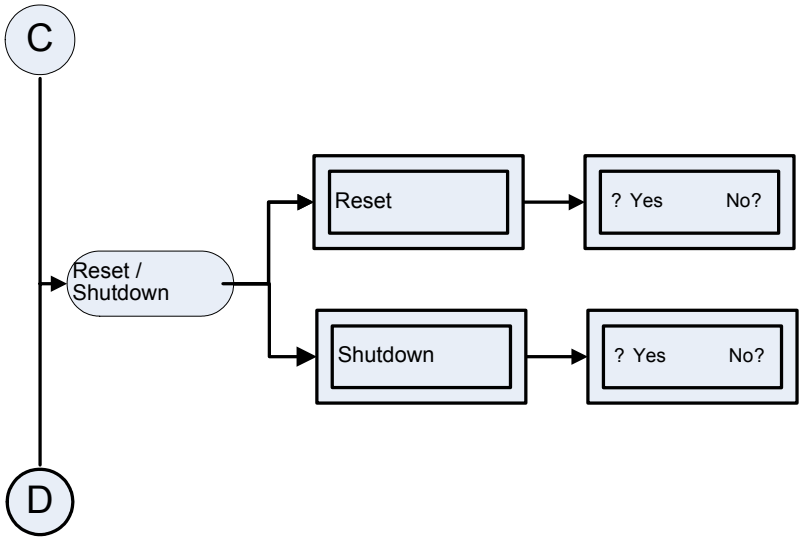
3.2.2 Alarm Mute

The Alarm Mute function item is used to control the RAID subsystem Beeper. Select the “No” and press **Enter** key in the dialog box to turn the beeper off temporarily. The beeper will still activate on the next event.



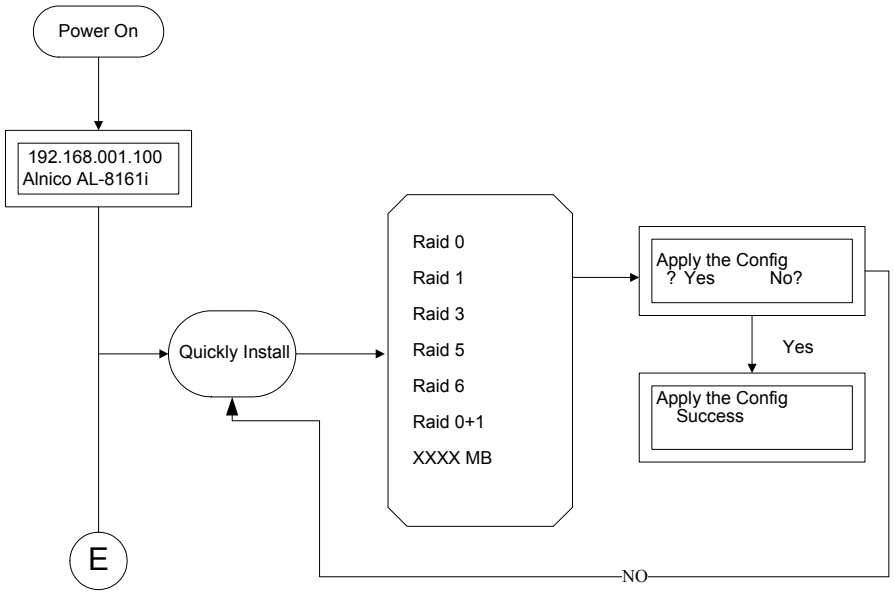
3.2.3 Reset / Shutdown

The Reset / Shutdown function item is used to control the RAID subsystem either to reset or shutdown the system. Select the “ Yes” or “No” and press **Enter** key to confirm the action.



3.2.4 Quickly Install

Quickly Install is the fastest way to prepare a RAID group and volume. It only needs a few keystrokes to complete it. Although disk drives of different capacity may be used in the RAID Group, it will use the smallest capacity of the disk drive as the capacity of all disk drives in the raid set. The Quick Volume and Raid Setup option creates a raid set with the following properties:



1. All of the physical disk drives are contained in a RAID group..

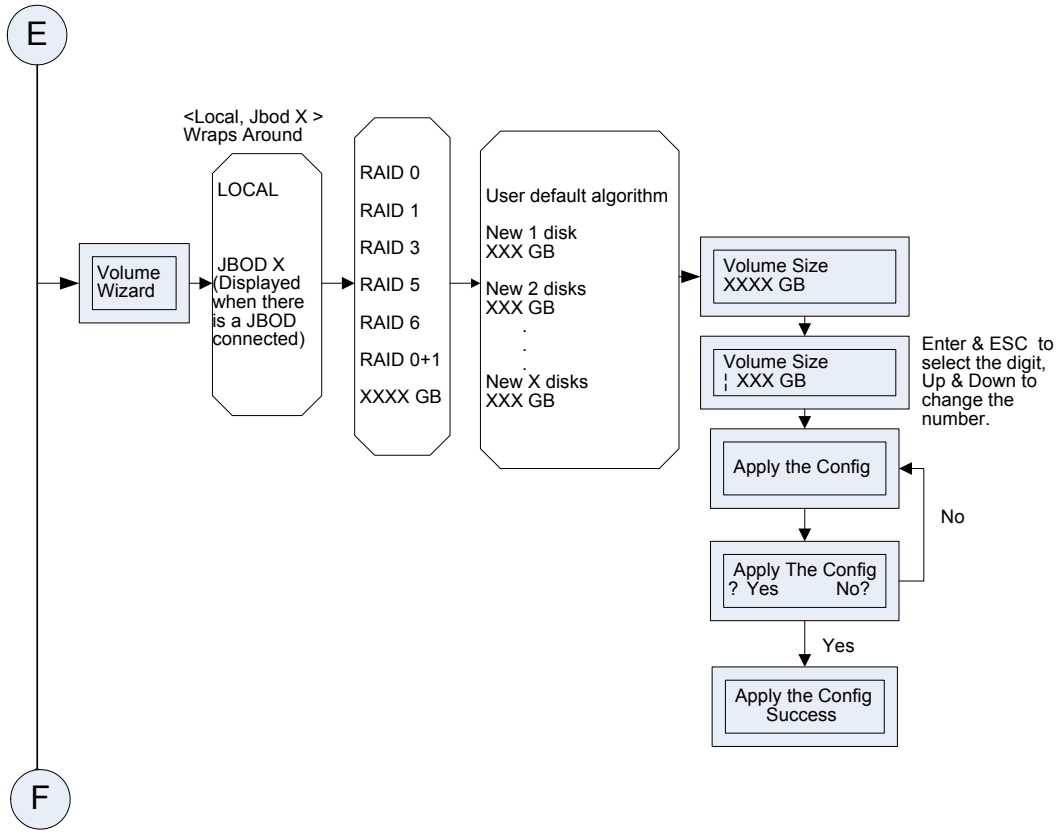
2. A single volume set is created and consumes all or a portion of the disk capacity available in this RAID group..

Detail procedure references to this chapter's section: **Volume Wizard.**

3.2.5 Volume Wizard

User manual configuration can completely control the raid set setting, but it will take longer time to complete than the Quickly install.. Select the Volume Wizard Function to manually configure the RAID group and Virtual Disk .

To enter a Volume Wizard Functions, press **ENT** to enter the Main menu. Press **UP/DOWN** to select the **Volume Wizard Functions** option and then press **ENT** to enter further submenus. All submenus will be displayed.

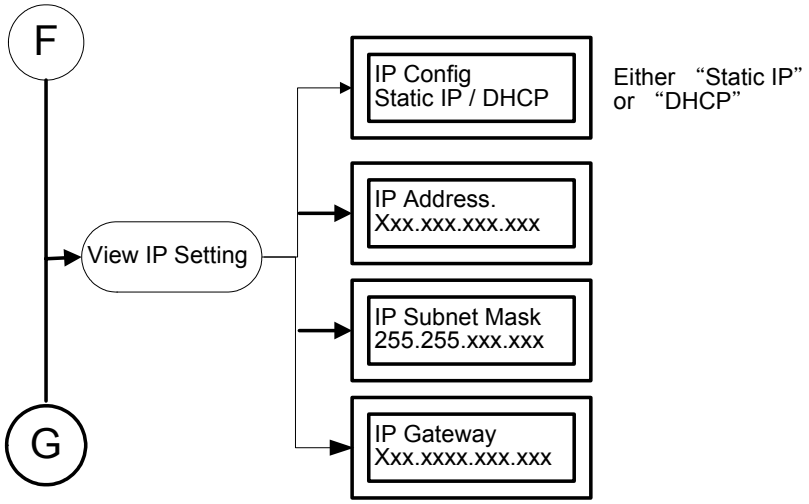


To Select "Use default algorithm", system will use all hard disks in RAID subsystem to create a RAID group and adjust the capacity to create a "Virtual Disk Volume". Or you

can manually to select “New X disks” to specify the numbers of disk for RAID group.

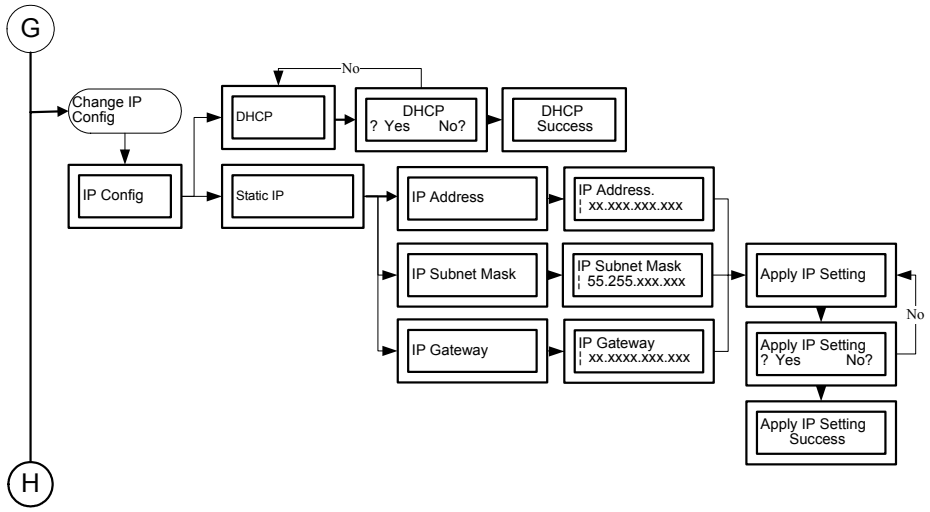
3.2.6 View IP setting

Use to check the setting of management Ethernet port of RAID subsystem.



3.2.7 Change IP Config

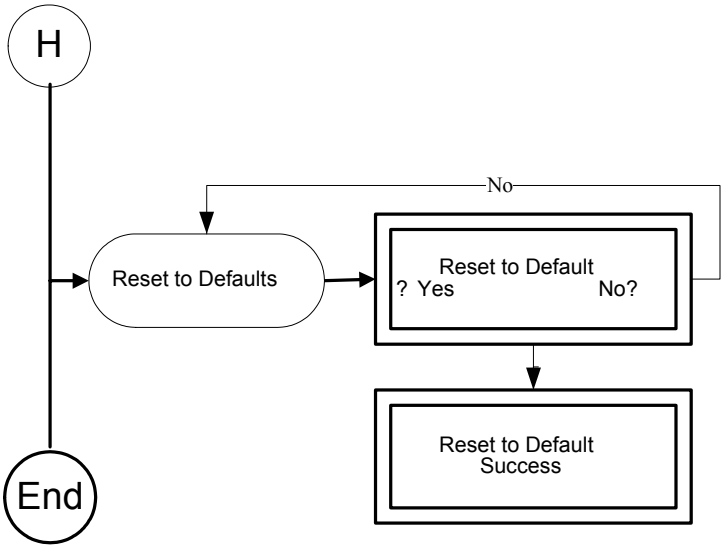
To change IP configuration, press **ENT** to enter the Main menu. Press **UP/DOWN** key to select the **Change IP Config** option, and then press **ENT.**



3.2.8 Reset to Default

Use this feature to Reset all parameters to Default volues.

Press **ENT** to enter the main menu. Press **UP/DOWN** to select the **Reset to Deafult**, and then press **ENT.**



Chapter 4. Web Browser- Based Configuration

This iSCSI RAID subsystem (TCP/IP protocol) web browser-based RAID manage interface is firmware-based and used to configure this iSCSI RAID subsystem. The table below unfolds the complete hierarchy of this interface:

Quick installation	→	Step 1 / Step 2 / Confirm
System configuration		
System setting	→	System name / Date and time
IP address	→	MAC address / Address / DNS / port
Login setting	→	Login configuration / Admin password / User password
Mail setting	→	Mail
Notification setting	→	SNMP / Messenger / System log server / Event log filter
iSCSI configuration		
Entity property	→	Entity name / iSNS IP
NIC	→	Aggregation / IP settings for iSCSI ports / Become default gateway / Enable jumbo frame
Node	→	Create / Authenticate / Rename / User / Delete
Session	→	Session information / Delete
CHAP account	→	Create / Modify user information / Delete
Volume configuration		
Volume create wizard		Step 1 / Step 2 / Step 3 / Step 4 / Confirm
Physical disk	→	Set Free disk / Set Global spare / Set Dedicated spare / Set property / More information

RAID group	→	Create / Migrate / Activate / Deactivate / Scrub / Delete / Set disk property / More information
Virtual disk	→	Create / Extend / Scrub / Delete / Set property / Attach LUN / Detach LUN / List LUN / Set snapshot space / Cleanup snapshot / Take snapshot / Auto snapshot / List snapshot / More information
Snapshot	→	Cleanup snapshot / Auto snapshot / Take snapshot / Export / Rollback / Delete
Logical unit	→	Attach / Detach
Enclosure management		
SES configuration	→	Enable / Disable
Hardware monitor	→	Auto shutdown
S.M.A.R.T.	→	S.M.A.R.T. information **(Only for SATA disks)**
UPS	→	UPS Type / Shutdown battery level / Shutdown delay / Shutdown UPS
Maintenance		
System information	→	System information
Upgrade	→	Browse the firmware to upgrade / Export configuration
Reset to default	→	Sure to reset to factory default?
Import and export	→	Import/Export / Import file
Event log	→	Download / Mute / Clear
Reboot and shutdown	→	Reboot / Shutdown
Logout		Sure to logout?

4.1 Firmware-embedded (TCP/IP protocol) web browser-based RAID manage interface (making use of the controller's 10/100 Ethernet LAN port)

To ensure proper communications between the RAID subsystem and the web browser-based RAID manage interface, please connect this iSCSI RAID subsystem Ethernet LAN port to any LAN switch port or NIC port.

This iSCSI RAID subsystem's firmware is embedded with a web browser-based RAID manage interface that follows TCP/IP protocol. The users are able to manage this RAID subsystem from the remote sides with standard web browsers like IE without the needs of installing any user-specific software (platform independent).

To configure this RAID subsystem from a local or remote server, you need to know this RAID subsystem's IP address. The default IP address is displayed on the LCD screen.

4.2 Login

Launch the firmware-embedded web browser-based RAID manage interface by entering http://[IP Address] in the web browser.

You must login as the administrator no matter from a local or remote server. The default User Name is **"admin"** and Password is **"0000".** Or login with read-only account whose default User Name is "**user"** and the Password is "**1234**". This special account allows the users to view the configuration only and cannot change the settings. Additionally, there are four languages available to be selected from the language menu: **English** \ **Simplified Chinese** \ **German** \ **French.**

After login, the main manage menu as below will be displayed on the left side of window to make configurations

There are six indicators at the top-right corner of the window:

RAID light: Green means RAID works well. Red represents RAID failure. When red appears, examine the event log (Maintenance → Event Log) to find out what error messages are issued; this is the first step to analyze RAID failure.

Temperature light: Green means normal temperature. Red represents abnormal temperature. When red appears, examine the event log (Maintenance → Event Log) to find out what error messages are issued; this is the first step to analyze over temperature.

Voltage light: Green means normal voltage. Red represents abnormal voltage. When red appears, examine the event log (Maintenance → Event Log) to find out what error messages are issued; this is the first step to analyze abnormal voltage.

UPS light: Green means UPS works well. Red represents UPS failure. When red appears, examine the event log (Maintenance → Event Log) to find out what error messages are issued; this is the first step to analyze UPS problem. What should be noted is this iSCSI RAID subsystem only supports APC UPS.

Fan light: Green means Fan works well. Red represents fan failure. When red appears, examine the event log (Maintenance → Event Log) to find out what error messages are issued; this is the first step to analyze FAN problem.

Power light: Green means Power works well. Red represents power failure. When red appears, examine the event log (Maintenance → Event Log) to find out what error messages are issued; this is the first step to analyze Power problem.

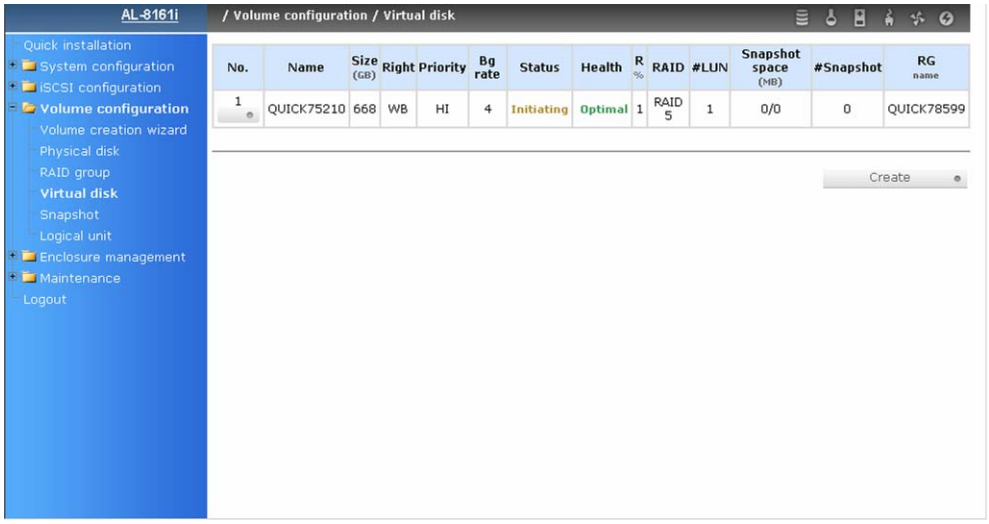
4.3 Quick Installation

It is easy to use **"Quick installation"** to create a volume. It uses whole physical disks to create a RG; the system will calculate maximum spaces on RAID levels 0/1/3/5/6/0+1. **"Quick installation"** will occupy all residual RG space for one VD, and it has no space for snapshot and spare. If snapshot is needed, please create volumes manually, and refer to snapshot configuration for more details. If some physical disks are used in other RG(s), **"Quick installation"** can not be run because "**Quick installation** "is valid only when all the physical disks in this iSCSI RAID subsystem are at free status. Below is one example of **Quick Installation**.

Step 1: Click **"Quick installation"**, then choose the RAID level. After choosing the RAID level, then click "Confirm".

Step 2: On Confirm page, if all settings are correct, click "Confirm"

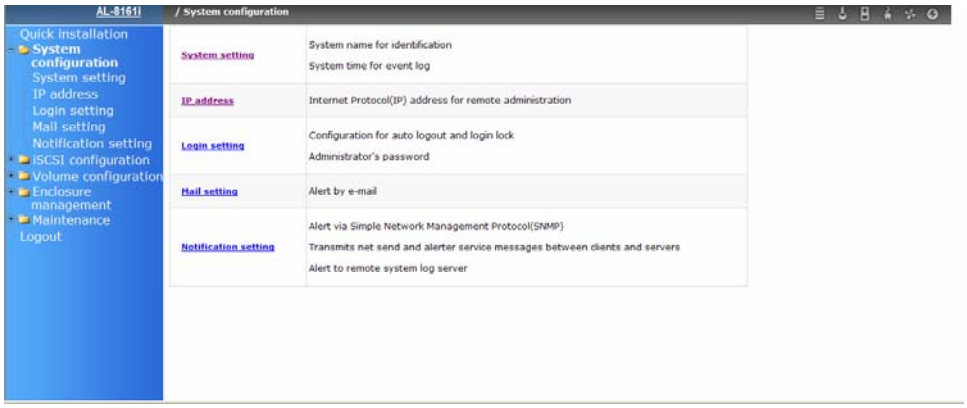
Then a VD will be created. Now you can start to use this RAID subsystem.



(A RAID 5 virtual disk, named “QUICK75120” with the total available volume size 668GB)

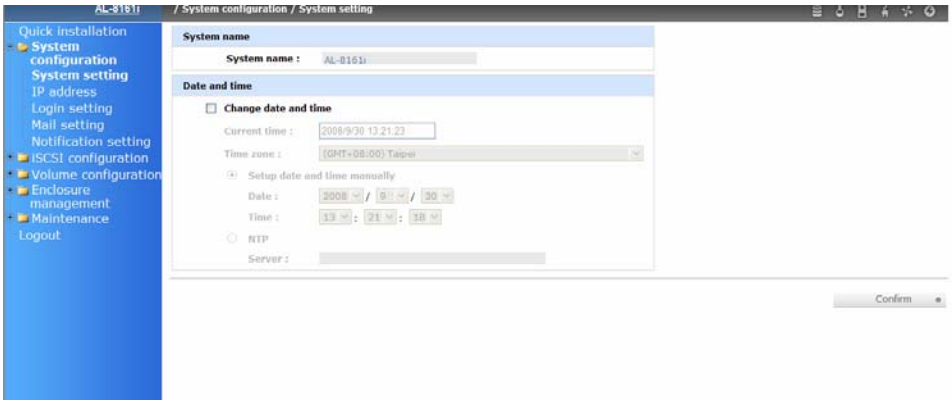
4.4 System configuration

“System configuration” is designed to setup the “System setting”, “IP address”, “Login setting”, “Mail setting”, and “Notification setting” for this iSCSI RAID subsystem.



4.4.1 System setting

"System setting" can set the system name and date.



Check **"Change date and time"** to setup the date, time, and time zone before using or synchronizing time with the NTP (Network Time Protocol) server.

The Network Time Protocol (NTP) is one way to ensure your clock stays accurate. Find out NTP server near you, and setup NTP server IP address. Finally click 

, the controller will connect to the NTP Time server and get time offered by the NTP server.

4.4.2 IP address

On this page, the users can change the iSCSI 's IP address、DNS address, even the HTTP、HTTPS, and SSH port number when the default port number is not allowed on the host/server. SSH (secure shell) is required when the users want to login this iSCSI RAID subsystem from a remote side. The SSH client software is available at the following web site:

SSHWinClient WWW: http://www.ssh.com/

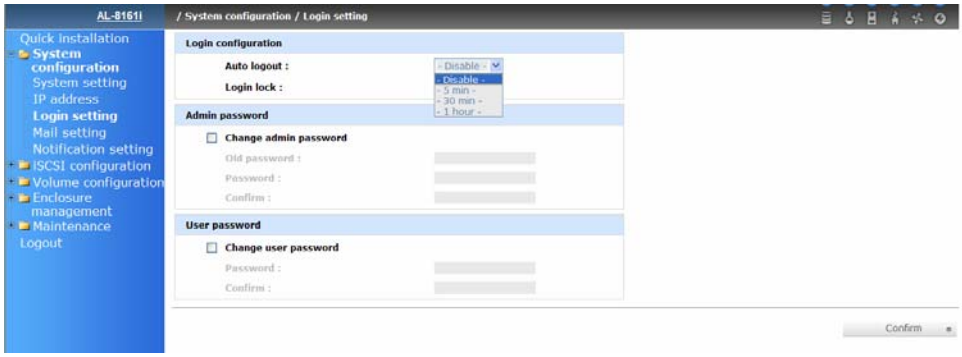
Putty WWW: http://www.chiark.greenend.org.uk/

Besides, there is no need to create a reserved space on the arrays prior to the running the Ethernet port and HTTP / HTTPS services. The firmware-embedded web browser-based RAID manage interface can be accessed with any standard internet browser that is installed on any host computer having TCP/IP protocol-based NICs inside. Thus, there is also no need to install any extra software or patches.

DHCP (Dynamic Host Configuration Protocol) is a protocol that lets network administrators manage centrally and automate the assignment of IP (Internet Protocol) configurations on a computer network. When using the Internet's set of protocols (TCP/IP), in order for a computer system to communicate to another computer system it needs a unique IP address. Without DHCP, the IP address must be entered manually at each computer system. DHCP lets a network administrator supervise and distribute IP addresses from a central point. The purpose of DHCP is to provide the automatic (dynamic) allocation of IP client configurations for a specific time period (called a lease period) and to eliminate the work necessary to administer a large IP network.

4.4.3 Login setting

“Login setting” can set single admin, auto logout time, and admin/user password. The single admin can prevent multiple users from accessing the same controller at the same time.



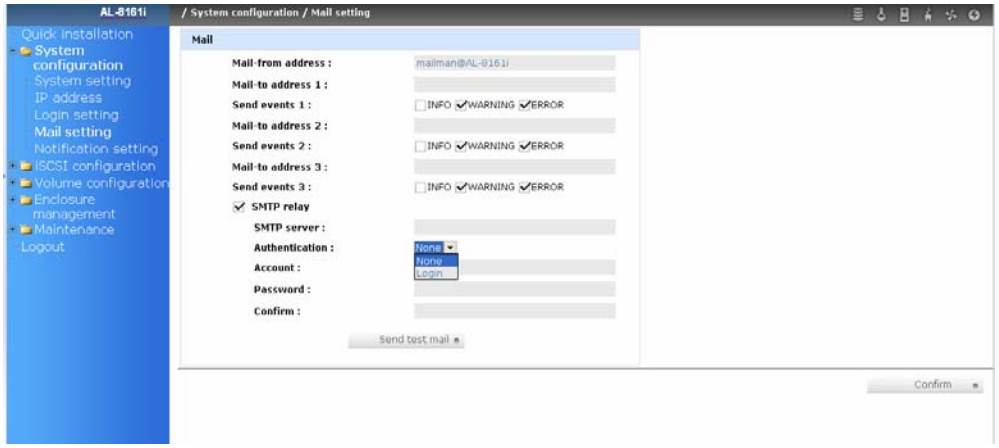
Auto logout: The options are (1) Disable; (2) 5 minutes; (3) 30 minutes; (4) 1 hour. The system will log out automatically when the web browser-based RAID manage interface has been inactive for 5 minutes \ 30 minutes \ I hour, depending on the Auto Logout setting.

Login lock: Disable/Enable. When the login lock is enabled, the web browser-based RAID manage interface allows only one user to login or modify system settings. Check “Change admin password” or “Change user password” to change admin or user password. The maximum length of password is 12 characters.

User password is used for the read-only account whose default User Name is “user” and the Password is “1234”. This special account allows the users to view the configuration only and cannot change the settings.

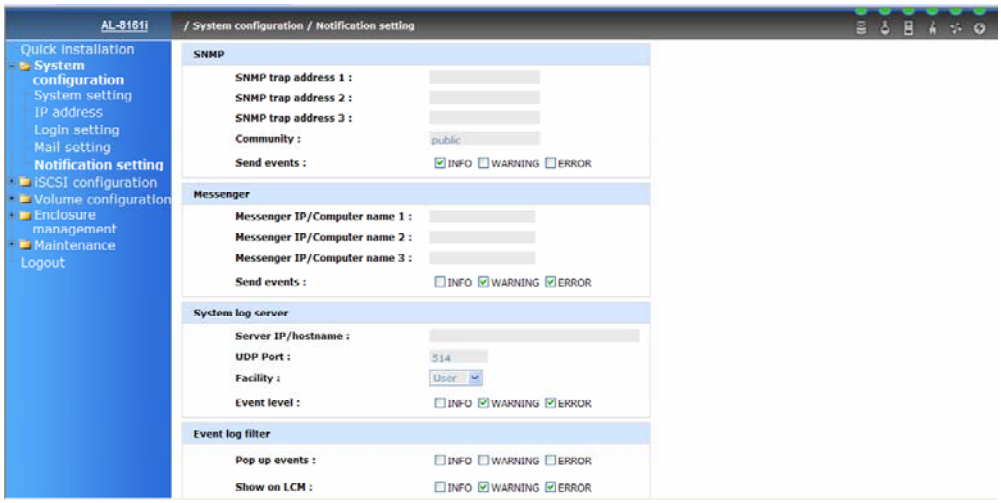
4.4.4 Mail setting

“Mail setting” can allow at most 3 mail addresses for receiving the event notification. The firmware contains SMTP manager, and it monitors all system events and the users can select either single or multiple user notifications to be sent via ‘Plain English’ e-mails without the need of installing any extra software or patches. Some mail servers would check **“Mail-from address”** and need authentication for anti-spam. Please fill the necessary fields and click **“Send test mail”** to test whether email functions are available. In addition to that, the users can also select which levels of event logs are needed to be sent via Mail. Default setting only enables ERROR and WARNING event logs.



4.4.5 Notification setting

“Notification setting” allows the users to setup event log levels, SNMP trap, Windows messenger (not MSN), or alert event logs via syslog protocol.



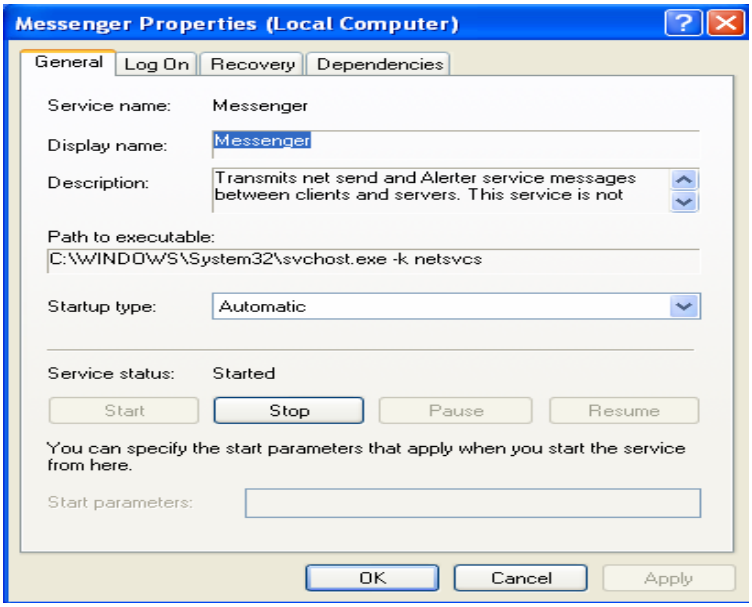
1.“SNMP” allows up to 3 SNMP trap addresses. Default community setting is “public”. User can choose the event log levels, and default setting only enables INFO event log in SNMP. There are many SNMP tools. The following web sites are for your reference:

SNMPc: http://www.snmpc.com/

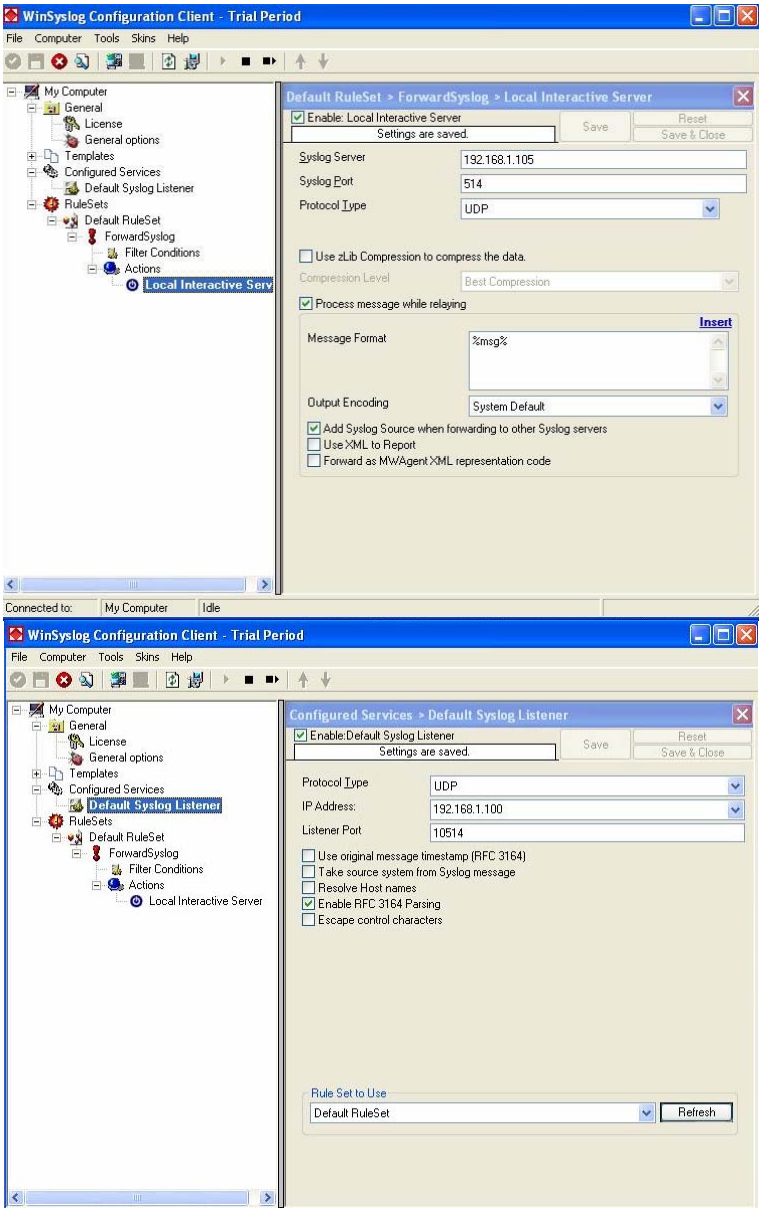
Net-SNMP: http://net-snmp.sourceforge.net/

2.Using **"Messenger"**, the users must enable the service "Messenger" in Windows

(Start → Control Panel → Administrative Tools → Services → Messenger), and then event logs can be received. It allows up to 3 messenger addresses. The users can choose the event log levels. The default setting enables the WARNING and ERROR event logs.



3.Using **"System log server"**, the users can choose the facility and the event log level. The default port of syslog is 514. The default setting enables event level: INFO, WARNING and ERROR event logs.



There are some syslog server tools. The following web sites are for your reference:

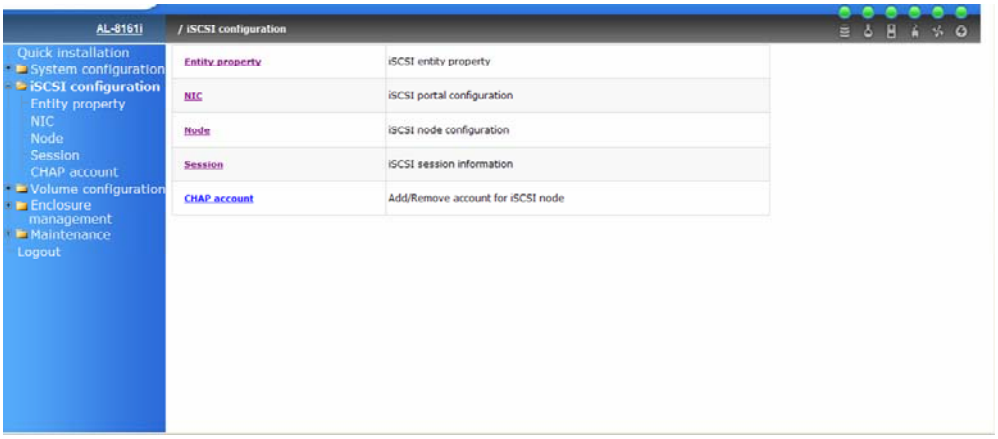
WinSyslog: http://www.winsyslog.com/

Kiwi Syslog Daemon: http://www.kiwisyslog.com/

4."Event log filter" allows the users to setup event log levels for "Pop up events" and "LCM". The levels are: INFO, WARNING and ERROR

4.5 iSCSI Configuration

"iSCSI configuration" is designed to setup the "Entity Property", "NIC", "Node", "Session", and "CHAP account".



4.5.1 Entity property

"Entity property" can view the entity name of this iSCSI RAID subsystem, and setup the **"iSNS IP"** for iSNS (Internet Storage Name Service). The iSNS protocol is designed to facilitate the automated discovery, management, and configuration of iSCSI devices on a TCP/IP network environment. iSNS provides intelligent storage discovery and management services comparable to those found in Fibre Channel networks, allowing a commodity IP network to function in a similar capacity as a storage area network. To use iSNS, it needs to install a iSNS server. Add an iSNS server IP address into the iSNS server lists so that a iSCSI initiator service can send queries.

NOTE

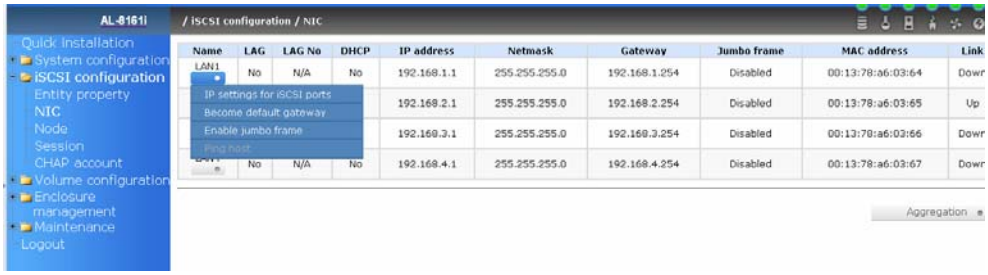
1: *the server that functions as ISNS server must not be installed with Microsoft iSCSI initiator.*

2: *the entity name of the iSCSI RAID subsystem quad-port models can be changed but dual-port model doesn't support entity name changing.*

4.5.2 NIC

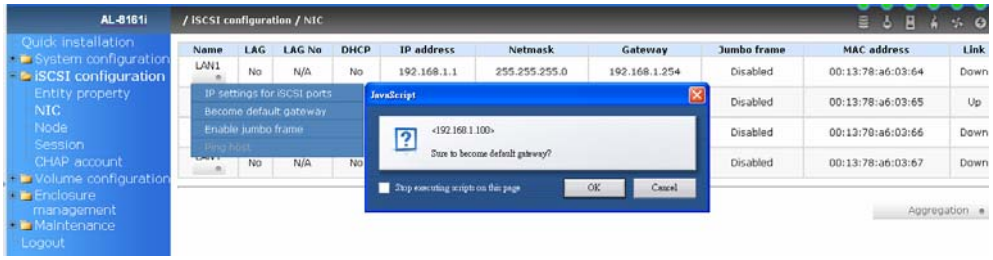
"NIC" can change the IP addresses of iSCSI host ports. This iSCSI RAID subsystem has four Gb/s LAN ports working as the host port to transmit data. Each of them must be assigned with a unique IP address unless the link aggregation or Trunking mode has been selected. If any two or more ports are set in link aggregation or Trunking mode, they will display same IP.

The iSCSI RAID subsystem AL-8121i and AL-8161i have four gigabit LAN ports to transmit data, but AL-6080i and AL-6120i has two ports only.

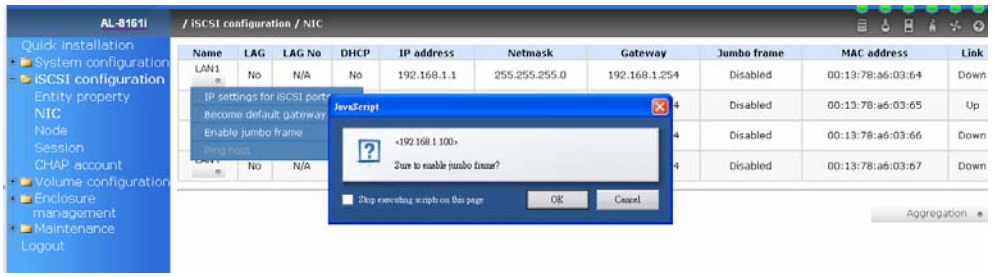


1.Click **"IP settings for iSCSI ports"**; the users now can change the IP address by moving mouse to the gray button of LAN port. There are 2 selections, DHCP (Get IP address from DHCP server) and Static IP.

2.Click **"Become default gateway"**; then the default gateway now can be changed by moving mouse to the gray button of LAN port, and enter in the right gateway IP address.



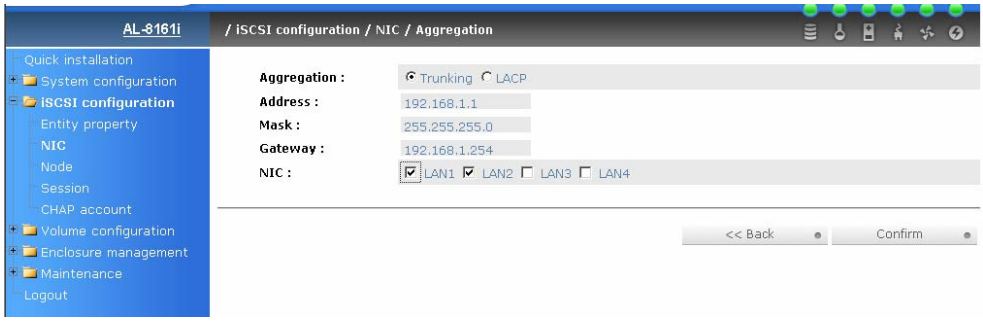
3. Click **"Enable jumbo frame"**; then the users can enable or disable jumbo frame by moving mouse to the gray button of LAN port, and clicking **"Enable jumbo frame"**.

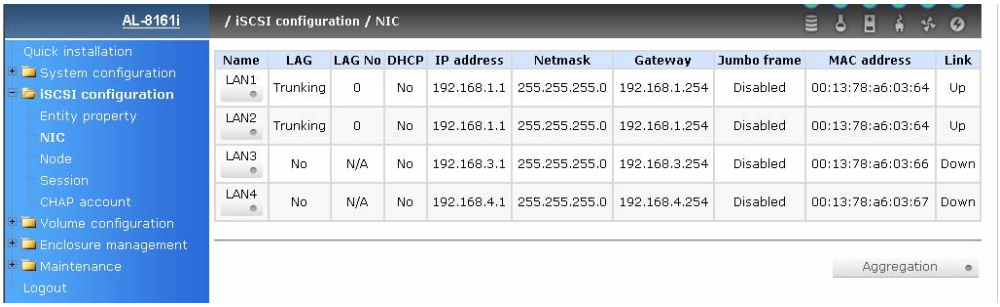


Jumbo Frame is designed to enhance Ethernet networking throughput and largely lower the CPU consumption of large file transfers by enabling more efficient larger payloads per packet. Conventionally, jumbo frames can carry up to 9,000 bytes of payload. Basically, a data transfer path from the iSCSI to the server includes at least a NIC and iSCSI itself. To prove jumbo frame really works on this path, the jumbo frame function of both the iSCSI and the NIC must be enabled. If an Ethernet switch is involved in this path, please enable the jumble frame function of this switch, too, and ensure MTU (maximum transmission unit) are all identical. "**Wireshark** "can be used to obtain the current MTU of any devices supporting jumbo frame.

4.Click "Aggregation **"**; then the users can select "**Trunking**" or "**LCAP**" to increase the data transfer speed beyond the limits of any one single

cable/port, or increase the redundancy for higher availability by paralleling multiple Ethernet network cables/ports.





The following is the description of Trunking /LACP:

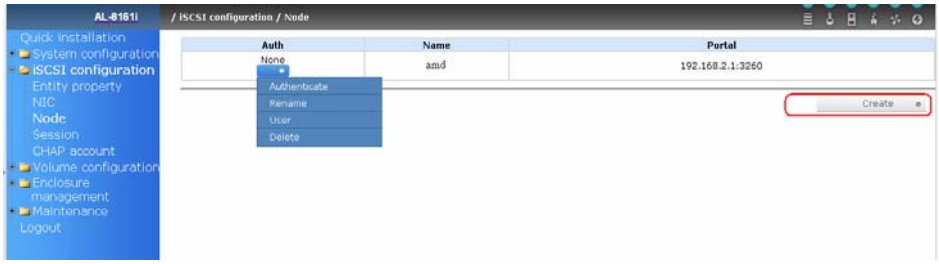
Trunking: It is defined as combining multiple ports in order to form faster logical communication links between devices. For example, connect all four data ports to the Gb/s Ethernet switch to form a single logical 4 Gb/s path.

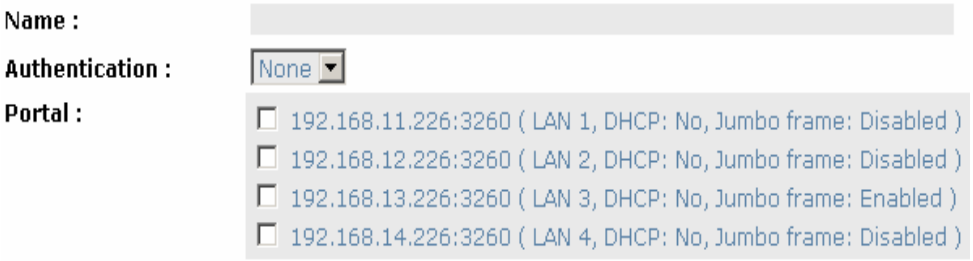
LACP: The Link Aggregation Control Protocol (LACP) is part of IEEE specification 802.3ad that allows bundling several physical ports together to form a single logical channel. LACP allows a network switch to negotiate an automatic bundle by sending LACP packets to the peer. The advantages of LACP are (1) increases the bandwidth. (2) failover when link status fails on a port.

To remove Trunking/LACP setting, mouse move to the gray button of LAN port, click “Delete link aggregation”. Then a confirmation message will pop up.

4.5.3 Node

"Node" allows the users to setup the target name and enable CHAP for the iSCSI initiator. This iSCSI RAID subsystem supports multiple nodes, and there is no default node; it is empty, and must be created first.





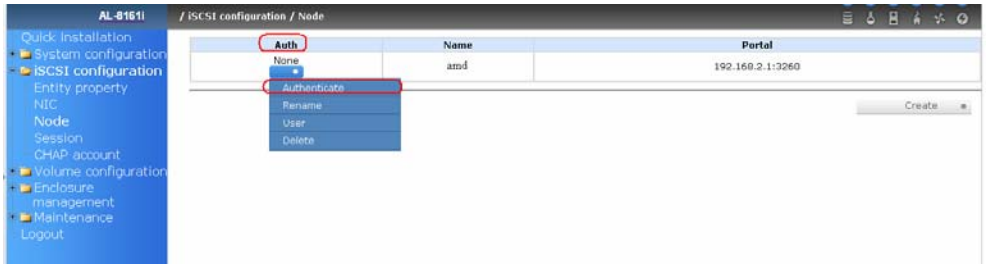
NOTE

*1. After the executing **"Quick installation"**, a node will be auto-created.*

*2. The **iSCSI** RAID subsystem quad-port models support multi-node and renaming node's name. Unlike the quad-port models, the dual-port model only supports single-node, and the node name exists by default and can not be changed.*

To use CHAP authentication, please follow the steps below:

Step 1: Mouse moves to the gray button of "Auth" column, click "Authenticate".

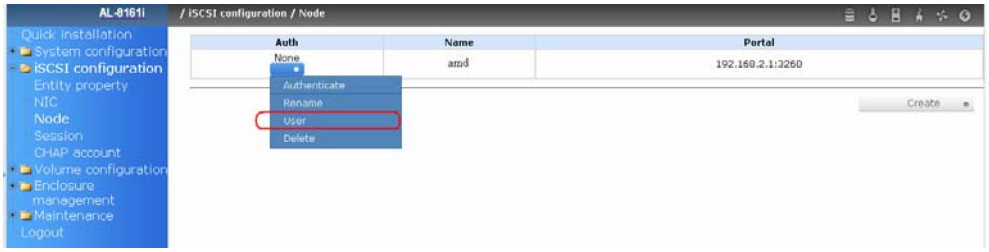


Step 2: Select **"CHAP"**.

Step 3: Click " 

".

Step 4: Mouse moves to the gray button of **"Auth"** column, click **"User"**.



Step 5: Select CHAP user(s) that will be used. It's a multi option; it can be one or more. If choosing none, CHAP can not work.

Node : all

	User
☑	chap1
☑	chap2

Step 6: Click “ Confirm ”.

Step 7: Mouse moves to the gray button of “Auth” column, click “Authenticate”, select “None” when you want to disable CHAP for the existing node.

4.5.4 Session

“Session” can display iSCSI session and connection information, including the following items:

1. Host (Initiator Name)
2. Error Recovery Level
3. Error Recovery Count
4. Detail of Authentication status and Source IP: port number

Mouse moves to the gray button of session number, click **“List connection”**. It will list all connection(s) of the session.

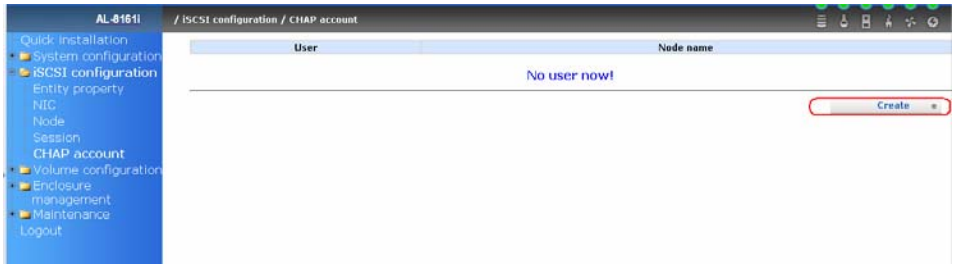
Error Recovery Level: To provide a technique whereby a value of an error recovery level determined in negotiation processing between an initiator and a target can be set to a suitable value that is intended by a manager. A storage system comprises a storage section containing a target module that is connected to an initiator device; and a management section that manages the storage section. The target module carries out negotiation processing with the initiator device so as to determine a value of a first error recovery level. The first error recovery level is determined as the smaller of a value of a second error recovery level of the initiator device and a value of a third error recovery level of the target module. The management section carries out setting processing for allocating the initiator device that is to be connected to the target module to the target module, according to an instruction from a manager. In the setting processing, the value of third error recovery level is notified to the manager.

4.5.5 CHAP Account

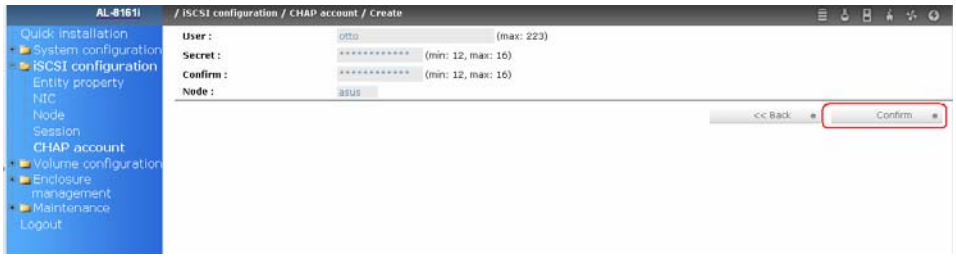
"CHAP account" can allow the users to create multiple CHAP accounts for node authentication.

To create CHAP account, please follow the steps below:

Step 1: Click " Create ".

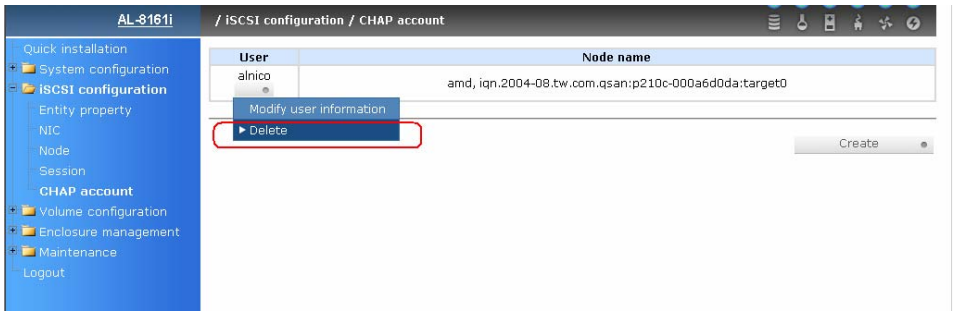


Step 2: Enter **"User"**, **"Secret"**, and **"Confirm"** secret (re-enter the secret password). **"Node"** can be selected here. If **none** is selected here, it still can be enabled in **"/ iSCSI configuration / Node / User"**.



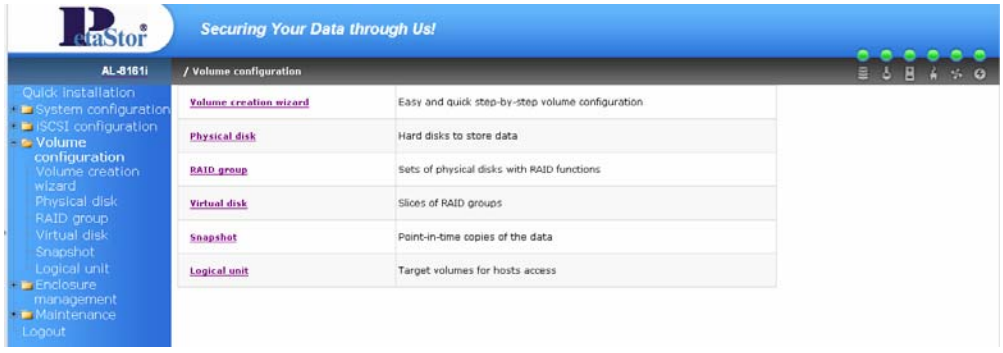
Step 3: Click "Confirm".

Step 4: If wanting to delete existing CHAP accounts, click **"Delete"** to delete existing CHAP accounts.



4.6 Volume configuration

"Volume configuration" is mainly designed to setup the volume configuration which includes "Volume create wizard", "Physical disk", "RAID group", "Virtual disk", "Snapshot", and "Logical unit".



4.6.1 Volume create wizard

“Volume create wizard” has a smarter policy. When this iSCSI RAID subsystem is inserted with some hard drives, “Volume create wizard” will list all the possible RAID level and capacities that the users can choose. For example, the users choose RAID 5 and the array has 12*200G + 4*80G hard drives inserted. If the users want to make use of all the 16 hard drives for a RAID 5, the maximum capacity of the volume is 1200G (80G*15). Taking advantage of “Volume create wizard, this iSCSI RAID subsystem will take a smarter check and find out the most efficient way of using all the available hard drives; thus, in this case, the wizard will only uses the 200G hard drives, making a RAID 5 volume consisted of 200G*11=2200G.. The volume capacity, by doing so, becomes bigger, and the maximum hard drive capacity is fully used, too.

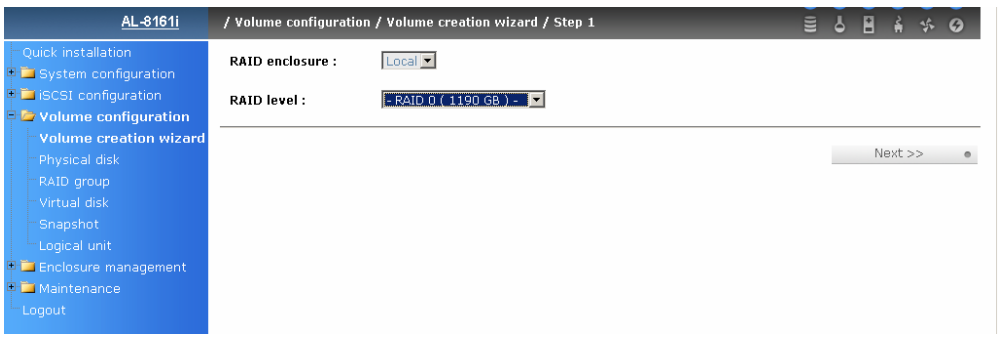
The smarter policy gives the users:

1. Biggest capacity of RAID level for the users to choose

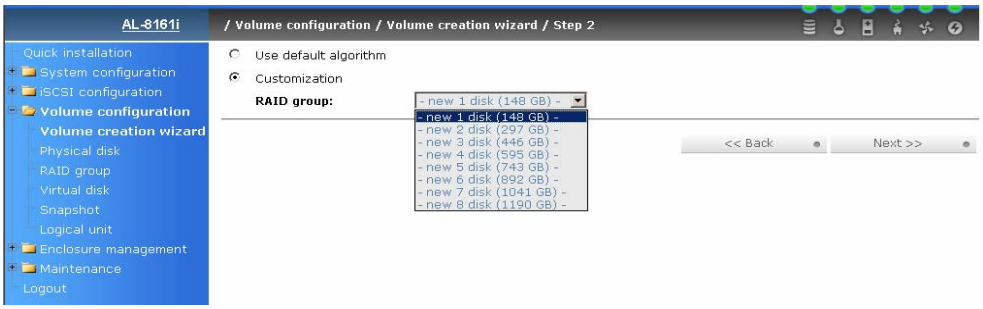
2. The fewest disk number for RAID level / volume size

To use Volume create wizard, please follow the steps below:

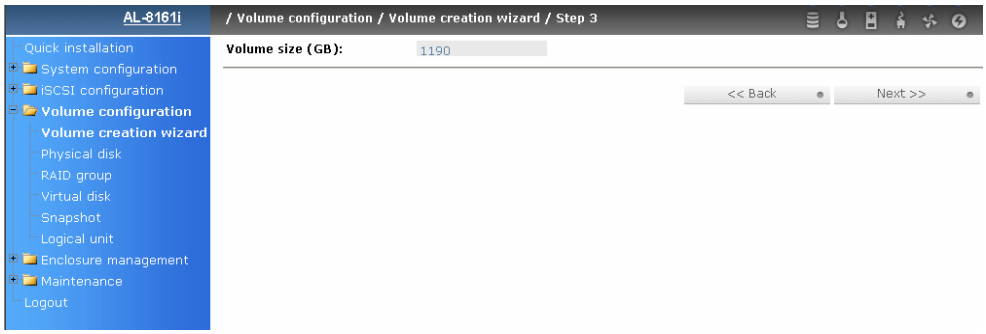
Step 1: Select **“Volume create wizard”** and then choose the RAID level. After the RAID level is chosen, click “ Next >> ”. Then it will link to next page.



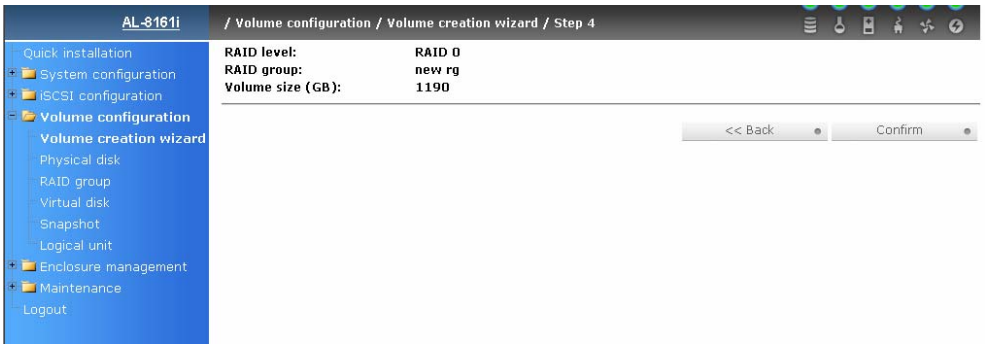
Step 2: Please select the combination of the RG (RAID Group) capacity, or **“Use default algorithm”** for maximum RG capacity. After RG capacity is chosen, click “ Next >> ”.



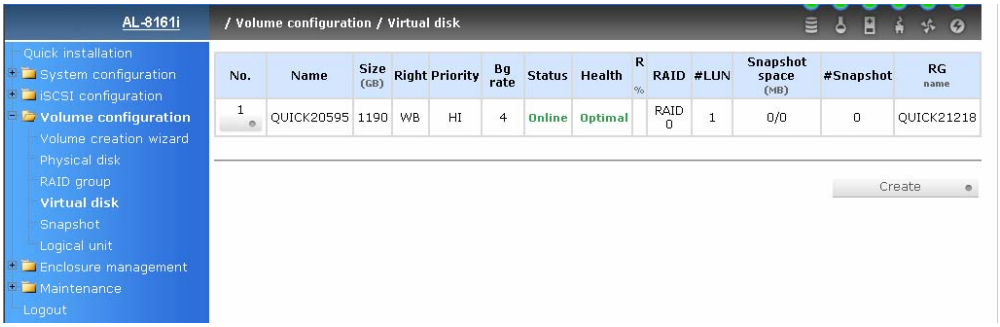
Step 3: Decide VD (Virtual Disk) capacity. The users can enter a number less or equal to the default capacity. Then click "Next >>".



Step 4: Confirm page. Click "Confirm" if all settings are correct. Then a VD will be created.



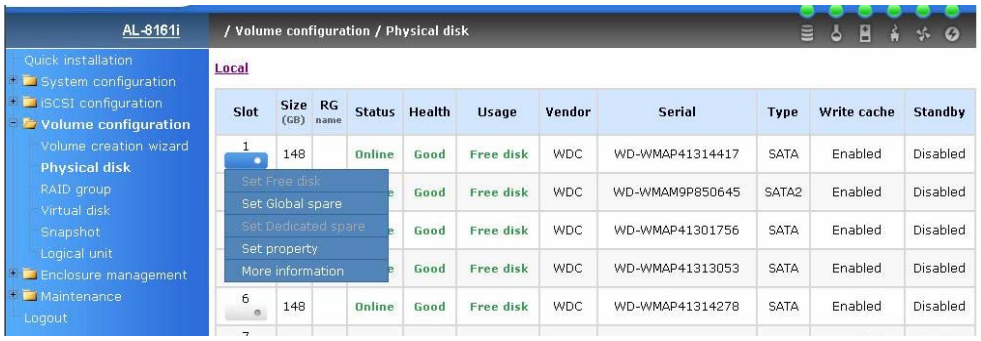
Done. You can start to use the system now.



(A RAID 0 virtual disk, named “QUICK20595” with the total available volume capacity 1190GB)

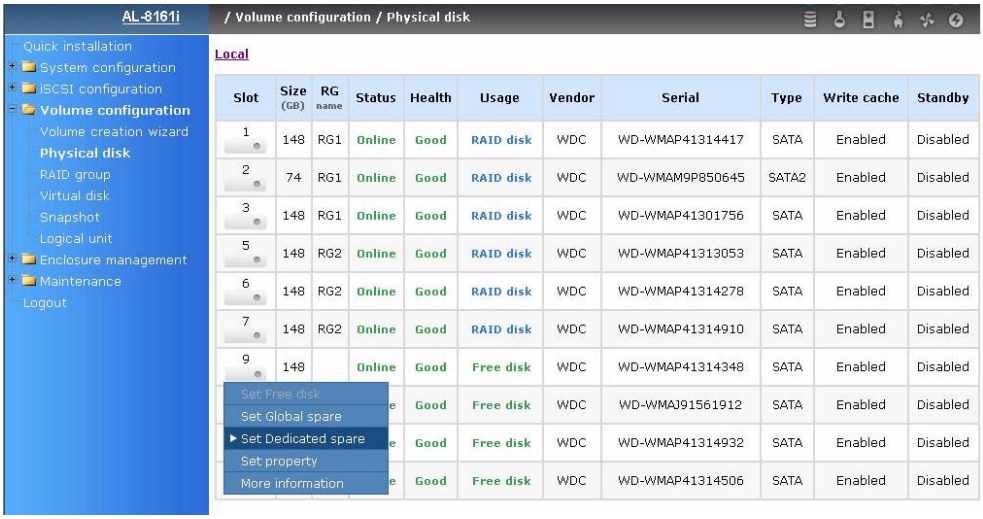
4.6.2 Physical disk

“Physical disk” allows the users to view the status of inserted hard drives in the iSCSI RAID subsystem. Besides, when moving mouse to the gray button next to the number of slot, the users will find that an submenu will be automatically pulled down, on which, functions that can be executed will not shown in gray color.

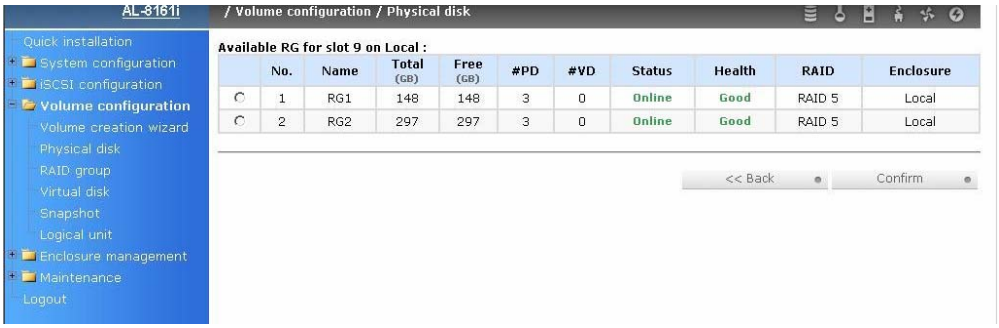


1. Set PD slot number 9 to Ddicated spare disk.

Step 1: Mouse moves to the gray button of PD 9, select **“Set Dedicated spare”**.



Step 2: Maybe there are some existing RG(s); select one existing RG that will use your created Dedicated spare, then click "Confirm".



2. Set PD slot number 1 to Global spare disk.

Step 1: Mouse moves to the gray button of PD 1, select **"Set Global"**.

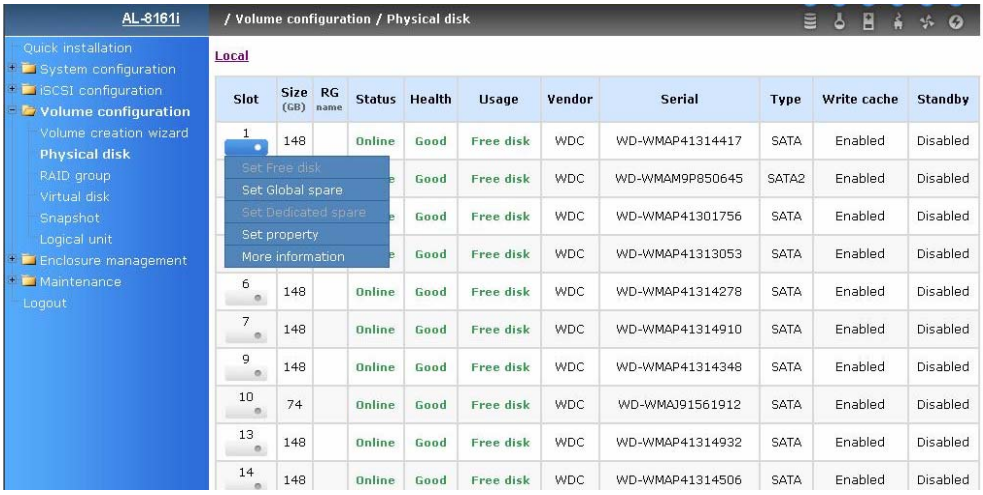
Slot	Size (GB)	RG name	Status	Health	Usage	Vendor	Serial	Type	Write cache	Standby
1	148		Online	Good	Free disk	WDC	WD-WMAP41314417	SATA	Enabled	Disabled
				Good	Free disk	WDC	WD-WMAM9P850645	SATA2	Enabled	Disabled
				Good	Free disk	WDC	WD-WMAP41301756	SATA	Enabled	Disabled
				Good	Free disk	WDC	WD-WMAP41313053	SATA	Enabled	Disabled
6	148		Online	Good	Free disk	WDC	WD-WMAP41314278	SATA	Enabled	Disabled
7	148		Online	Good	Free disk	WDC	WD-WMAP41314910	SATA	Enabled	Disabled
9	148		Online	Good	Free disk	WDC	WD-WMAP41314348	SATA	Enabled	Disabled
10	74		Online	Good	Free disk	WDC	WD-WMAJ91561912	SATA	Enabled	Disabled
13	148		Online	Good	Free disk	WDC	WD-WMAP41314932	SATA	Enabled	Disabled
14	148		Online	Good	Free disk	WDC	WD-WMAP41314506	SATA	Enabled	Disabled

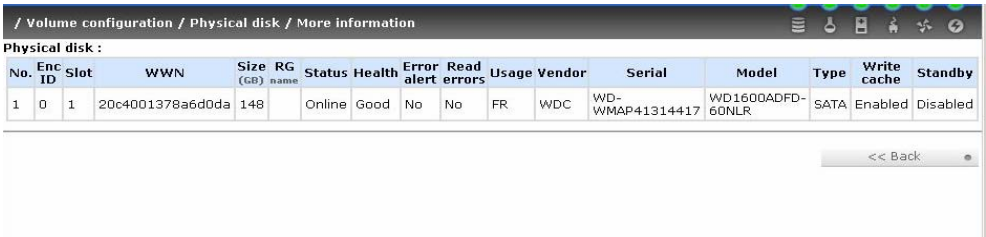
Step 2: Confirm or not

Slot	Size (GB)	RG name	Status	Health	Usage	Vendor	Serial	Type	Write cache	Standby
1	148		Online	Good	Free disk	WDC	WD-WMAP41314417	SATA	Enabled	Disabled
							WD-WMAM9P850645	SATA2	Enabled	Disabled
							WD-WMAP41301756	SATA	Enabled	Disabled
							WD-WMAP41313053	SATA	Enabled	Disabled
6	148		Online	Good	Free disk	WDC	WD-WMAP41314278	SATA	Enabled	Disabled
7	148		Online	Good	Free disk	WDC	WD-WMAP41314910	SATA	Enabled	Disabled
9	148		Online	Good	Free disk	WDC	WD-WMAP41314348	SATA	Enabled	Disabled
10	74		Online	Good	Free disk	WDC	WD-WMAJ91561912	SATA	Enabled	Disabled
13	148		Online	Good	Free disk	WDC	WD-WMAP41314932	SATA	Enabled	Disabled
14	148		Online	Good	Free disk	WDC	WD-WMAP41314506	SATA	Enabled	Disabled

3. Show the information of hard drive 1 in detail.

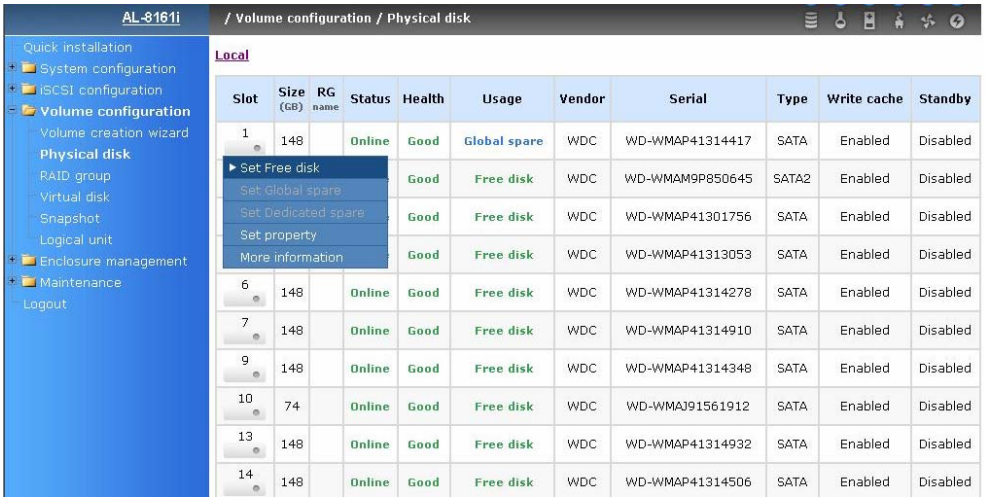
Step 1: Move mouse to the gray button next to the number of slot 1, and select **“More information”**.





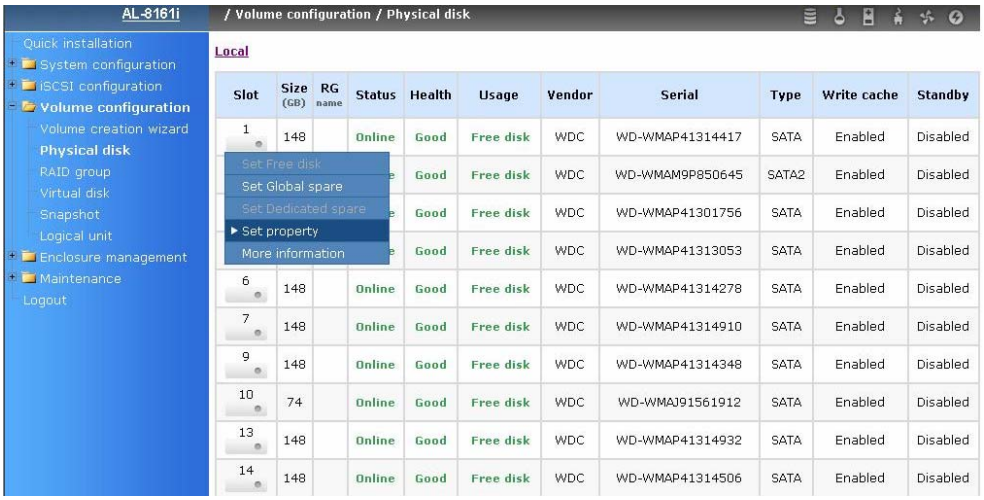
4. Set hard drive 1 as free disk.

Step 1: Move mouse to the gray button next to the number of slot 1, and select **"Set free disk"**.



5. Set hard drive 1 property.

Step 1: Move mouse to the gray button next to the number of slot 1, and select **"Set property"**.



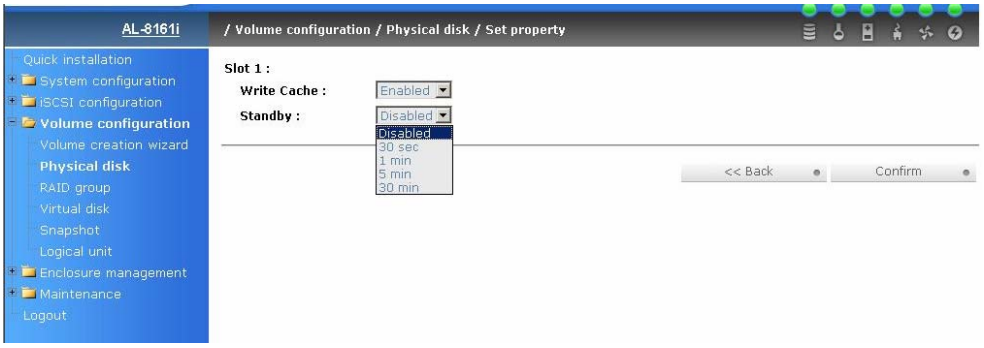
Slot	Size (GB)	RG name	Status	Health	Usage	Vendor	Serial	Type	Write cache	Standby
1	148		Online	Good	Free disk	WDC	WD-WMAP41314417	SATA	Enabled	Disabled
				Good	Free disk	WDC	WD-WMAM9P850645	SATA2	Enabled	Disabled
				Good	Free disk	WDC	WD-WMAP41301756	SATA	Enabled	Disabled
				Good	Free disk	WDC	WD-WMAP41313053	SATA	Enabled	Disabled
6	148		Online	Good	Free disk	WDC	WD-WMAP41314278	SATA	Enabled	Disabled
7	148		Online	Good	Free disk	WDC	WD-WMAP41314910	SATA	Enabled	Disabled
9	148		Online	Good	Free disk	WDC	WD-WMAP41314348	SATA	Enabled	Disabled
10	74		Online	Good	Free disk	WDC	WD-WMAJ91561912	SATA	Enabled	Disabled
13	148		Online	Good	Free disk	WDC	WD-WMAP41314932	SATA	Enabled	Disabled
14	148		Online	Good	Free disk	WDC	WD-WMAP41314506	SATA	Enabled	Disabled

Write cache options:

1. Enabled → Enable disk write cache.
2. Disabled → Disable disk write cache.

Standby options:

1. Disabled → Disable spin down.
2. 30 sec / 1 min / 5 min / 30 min → Enable hard drive auto spin down to save power in the period of time.



PD column description :

Slot	The position of hard drives. The button next to the number of slot shows the functions which can be executed.
Size (GB)	Capacity of hard drive.
RG Name	Shows the RAID group of the hard drives
Status	The status of hard drive. “Online” → the hard drive is online. “Rebuilding” → the hard drive is being rebuilt. “Transition” → the hard drive is being migrated or is replaced by another disk when rebuilding occurs. “Missing” → the hard drive has already joined a RG but not plugged into the disk tray of current system.
Health	The health of hard drive. “Good” → the hard drive is good. “Failed” → the hard drive is failed. “Error Alert” → S.M.A.R.T. error alert. “Read Errors” → the hard drive has unrecoverable read errors.
Usage	“RD” → RAID Disk. This hard drive has been set to RAID. “FR” → FRee disk. This hard drive is free for use. “DS” → Dedicated Spare. This hard drive has been set to the dedicated spare of the RG. “GS” → Global Spare. This hard drive has been set to a global spare of all RGs. “RS” → ReServe. The hard drive contains the RG information but cannot be used. It may be caused by an uncompleted RG set, or hot-plug of this disk in the running time. In order to protect the data in the disk, the status changes to reserve. It can be reused after setting it to “FR” manually.
Vendor	Hard drive vendor.
Serial	Hard drive serial number.
Type	Hard drive type. “SATA” → SATA disk.

	“SATA2” → SATA II disk. “SAS” → SAS disk.
Write cache	Hard drive write cache is enabled or disabled.
Standby	HDD auto spin down to save power. The default value is disabled.

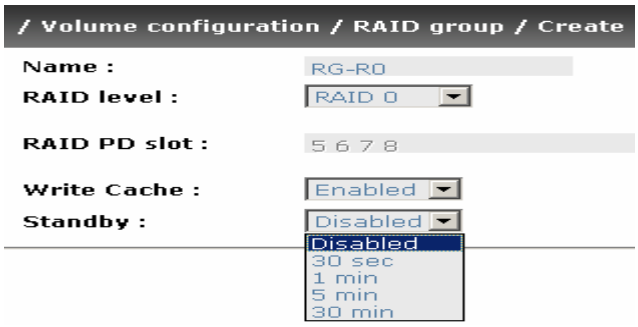
PD operations description :

Set Free disk	Make the selected hard drive to be free for use.
Set Global spare	Set the selected hard drive to global spare of all RGs.
Set Dedicated spares	Set hard drive to dedicated spare of selected RGs.
Set property	Change the status of write cache and standby. Write cache options: “Enabled” → Enable disk write cache. “Disabled” → Disable disk write cache. Standby options: “Disabled” → Disable spin down. “30 sec / 1 min / 5 min / 30 min” → Enable hard drive auto spin down to save power in the period of time.
More information	Show hard drive detail information.

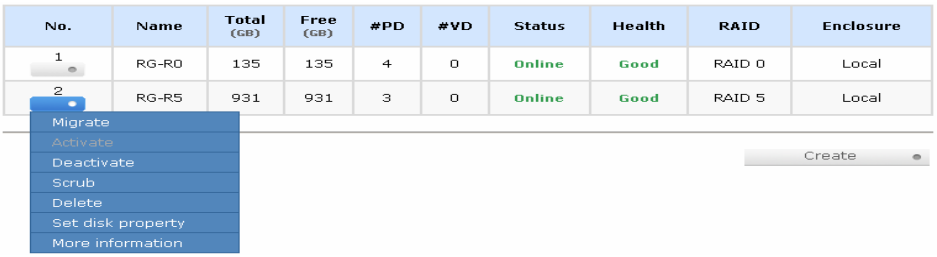
4.6.3 RAID group

“RAID group” can allow the users to create RG and view the status of each RAID group. The following is an example to create a RG.

Step 1: Click “ Create ”, enter **“Name”**, choose **“RAID level”**, click “ Select PD ” to select PD. Then click “ Next >> ”.

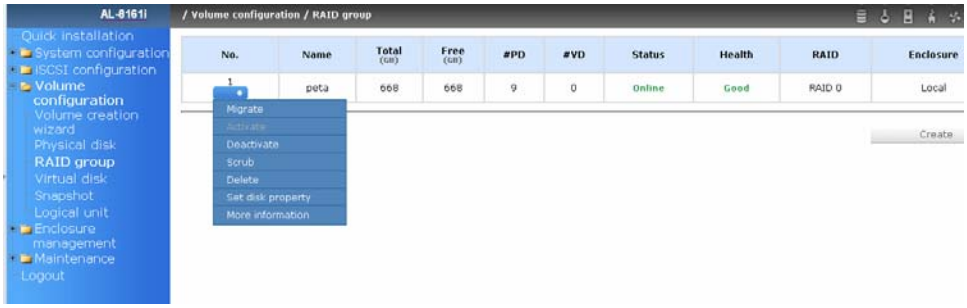


Step 2: Confirm page. Click "Confirm" if all settings are correct.



(There is a RAID 0 with 4 physical disks, named "RG-R0", total capacity is 135GB. Another is a RAID 5 with 3 physical disks, named "RG-R5")

RAID group submenu:

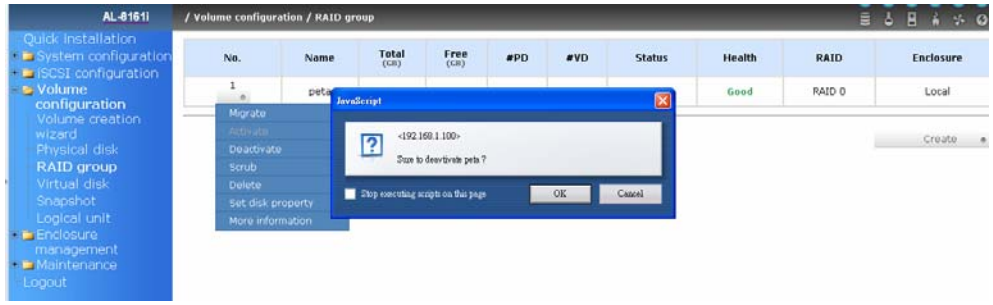


1. Deactivate

Deactivating a RAID group allows the users to array roam the whole RAID group to another iSCSI RAID subsystem without powering off this iSCSI RAID subsystem.

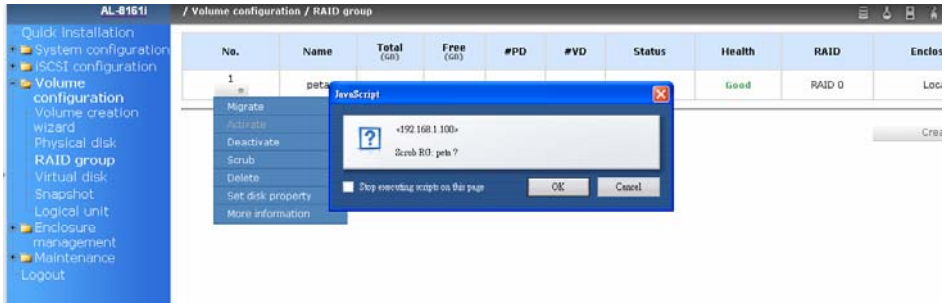
2. Activate

Activating a RAID group allows the users to restore the off-line status RAID group. After a RAID group is array roamed to another iSCSI RAID subsystem, the users have to execute this function to activate the moved RAID group.

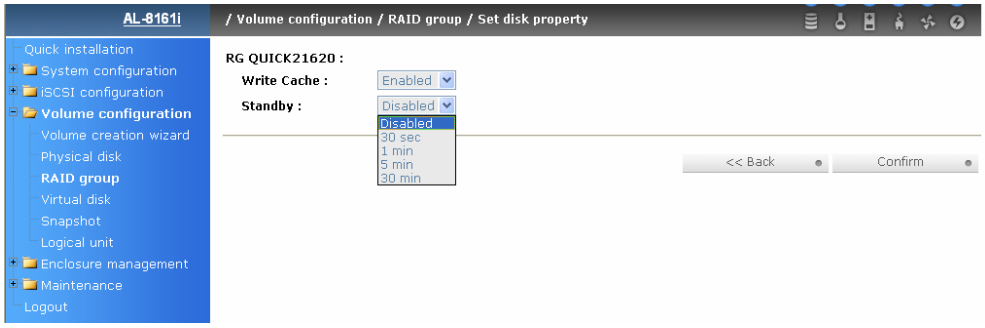


3. Scrub.

Scrubbing a RAID group in order to remap bad blocks; this function is to make parity regeneration, supporting RAID 3 / 5 / 6 / 30 / 50 / 60 only.



4. Set disk property



Write cache options:

1. Enabled → Enable disk write cache.

2. Disabled → Disable disk write cache.

Standby options:

1. Disabled → Disable spin down.
2. 30 sec / 1 min / 5 min / 30 min → Enable hard drive auto spin down to save power in the period of time.

5. Delete

Delete existing RAID groups.

If the RAID group contains VD (Virtual Disk), the VD has to be deleted prior to the deletion of RAID group.

6. More information

Display the RAID group information in detail

7. Migrate

To migrate the RAID level, please follow the steps below:

1. Select **"/ Volume configuration / RAID group"**.
2. Mouse moves to the gray button next to the RG number; click **"Migrate"**.
3. Change the RAID level by clicking the down arrow to **"RAID 5"**. There will be a pup-up which indicates that HDD is not enough to support the new setting of RAID level, click " Select PD " to increase hard drives, then click " Confirm " to go back to setup page. When doing

migration to lower RAID level, for example the original RAID level is RAID 6 and the user wants to migrate to RAID 0, the RAID subsystem will evaluate whether this operation is safe or not, and appear a message of **"Sure to migrate to a lower protection array?"** to give user warning.

4. Double check the setting of RAID level and RAID PD slot. If there is no problem, click "Next >> ".

5. Finally a confirmation page shows the detail of RAID information. If there is no problem, click " Confirm " to start migration. System also pops up a message of **"Warning: power lost during migration may cause damage of data!"** to give user warning. When the power is abnormally off during the migration, the data is in high risk.

6. Migration starts and it can be seen from the **"status"** of a RG with **"Migrating"**. In **"/ Volume configuration / Virtual disk"**, it displays a **"Migrating"** in **"Status"** and complete percentage of migration in **"R%"**.

No.	Name	Total (GB)	Free (GB)	#PD	#VD	Status	Health	RAID	Enclosure
1	RG-R0->R5	1396	1386	4	1	Migrating	Good	RAID 5	Local

(A RAID 0 with 4 physical disks migrates to RAID 5 with 5 physical disks)

No.	Name	Size (GB)	Right	Priority	Bg rate	Status	Health	R %	RAID	#LUN	Snapshot (MB)	#Snapshot	RG name
1	VD-R0->R5	10	WB	HI	4	Migrating	Optimal	6	RAID 5	0	0/0	0	RG-R0->R5

(A RAID 0 migrates to RAID 5, the complete percentage is 14%)

To do migration, the total size of RG must be larger or equal to the original RG. It does not allow expanding the same RAID level with the same hard disks of original RG.

When RG is being migrated, the iSCSI RAID subsystem would reject following operations:

1. Add dedicated spare.
2. Remove a dedicated spare.
3. Create a new VD.
4. Delete a VD.
5. Extend a VD.
6. Scrub a VD.
7. Perform yet another migration operation.
8. Scrub entire RG.
9. Take a new snapshot.
10. Delete an existing snapshot.
11. Export a snapshot.
12. Rollback to a snapshot.

RG Migration cannot be executed during rebuild or VD extension.

RG column description :

No.	Number of RAID group. The button next to the No. shows the functions which can be executed.
Name	RAID group name.
Total(GB)	Total capacity of this RAID group.
Free(GB)	Free capacity of this RAID group.
#PD	The number of physical disks in RAID group.
#VD	The number of virtual disks in RAID group.
Status	The status of RAID group. "Online" → the RAID group is online. "Offline" → the RAID group is offline. "Rebuild" → the RAID group is being rebuilt. "Migrate" → the RAID group is being migrated. "Scrub" → the RAID group is being scrubbed.
Health	The health of RAID group. "Good" → the RAID group is good. "Failed" → the hard drive is failed. "Degraded" → the RAID group is not completed. The reason could be lack of one disk or disk failure.
RAID	The RAID level of the RAID group.
Enclosure	RG locates on local or JBOD enclosure.

RG operations description :

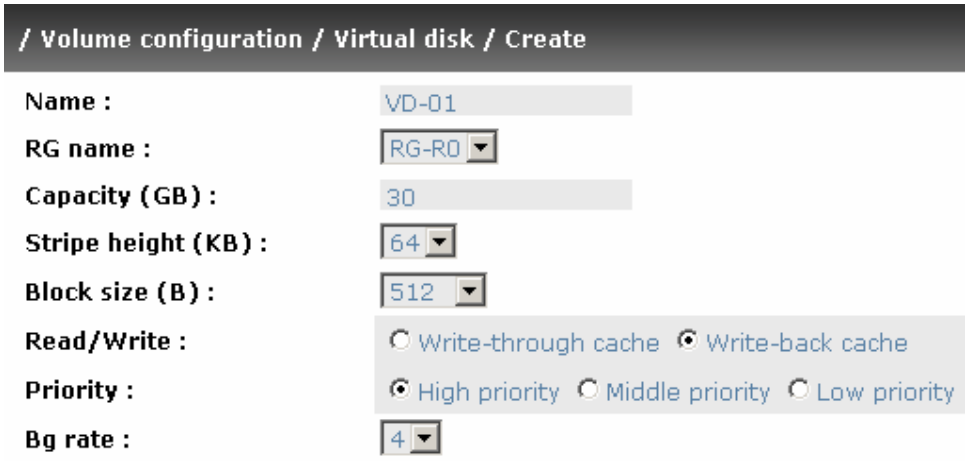
Create	Create a RAID group.
Migrate	Migrate a RAID group to different RAID level
Activate	Activate a RAID group; it can be executed when RG status is offline. This is for online roaming purpose.
Deactivate	Deactivate a RAID group; it can be executed when RG status is online. This is for online roaming purpose.
Scrub	Scrub a RAID group. It's a parity regeneration. It supports RAID 3 / 5 / 6 / 30 / 50 / 60 only.

Delete	Delete a RAID group.
Set disk property	Change the disk status of write cache and standby. Write cache options: "Enabled" → Enable disk write cache. "Disabled" → Disable disk write cache. Standby options: "Disabled" → Disable spin down. "30 sec / 1 min / 5 min / 30 min" → Enable hard drive auto spin down to save power in the period of time.
More information	Show RAID group detail information.

4.6.4 Virtual disk

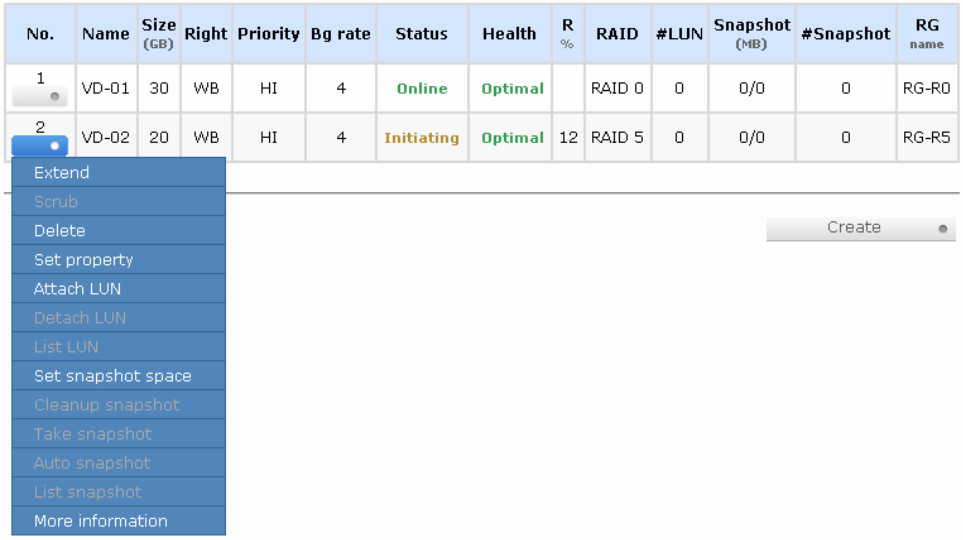
"Virtual disk" (VD) can allow the users to create VD, snapshot, and view the status of each existing VD. The following is an example to create a VD.

Step 1: Click "Create", enter **"Name"**, choose **"RG name"**, **"Stripe height (KB)"**, **"Block size (B)"**, **"Read/Write"** mode, **"Priority"**, **"Bg rate"** (Background task priority), change **"Capacity (GB)"** if necessary. Then click "Confirm".



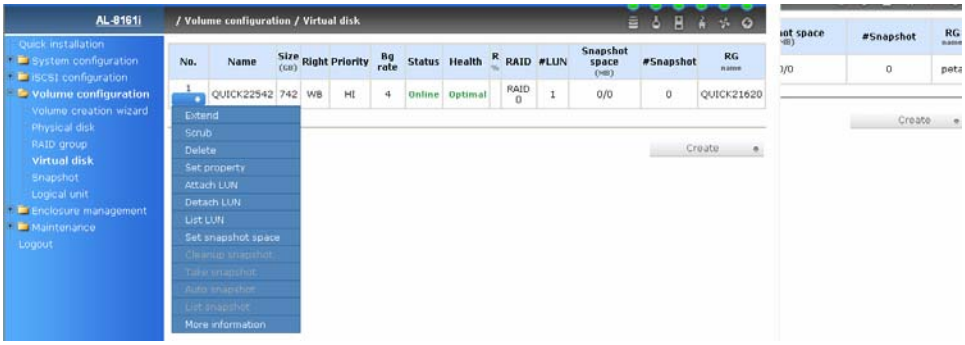
Step 2: Confirm page. Click "Confirm" if all setups are

correct.



(Create a VD named “VD-01”, related to “RG-R0”, size is 30GB. The other VD is named “VD-02”, initializing to 12%)

Virtual disk express menu:



1. Extend

To extend VD (Virtual Disk) capacity, please follow the steps below:

1. Select “/ Volume configuration / Virtual disk”.

2. Mouse moves to the gray button next to the VD number; click “Extend”.

3. Change the size. The size must be larger than the original, and then click “ Confirm “ to start extension.

Step 4: Extension starts. If VD needs initialization, it will display an “Initiating” in “Status” and complete percentage of initialization in “R%”.

No.	Name	Size (GB)	Right	Priority	Bg rate	Status	Health	R %	RAID	#LUN	Snapshot (MB)	#Snapshot	RG name
1	VD-R0->R5	20	WB	HI	4	Initiating	Optimal	69	RAID 5	0	0/0	0	RG-R0->R5

(Extend VD-R5 from 20GB to 40GB)

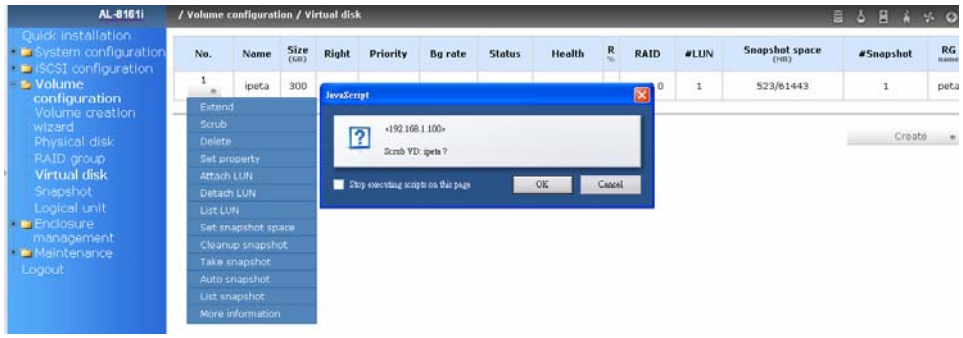
NOTE

1.*The capacity of VD extension must be larger than original one.*

2.*VD Extension cannot be executed during rebuild or migration.*

2. Scrub

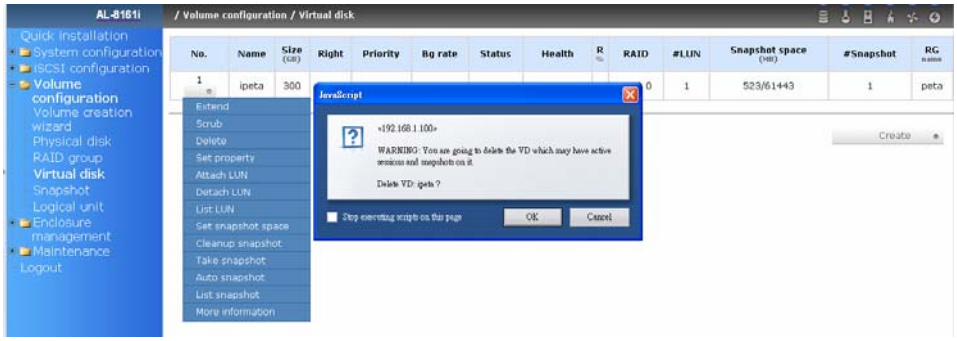
Scrubbing a VD in order to remap bad blocks; this function is to make parity regeneration, supporting RAID 3 / 5 / 6 / 30 / 50 / 60 only.



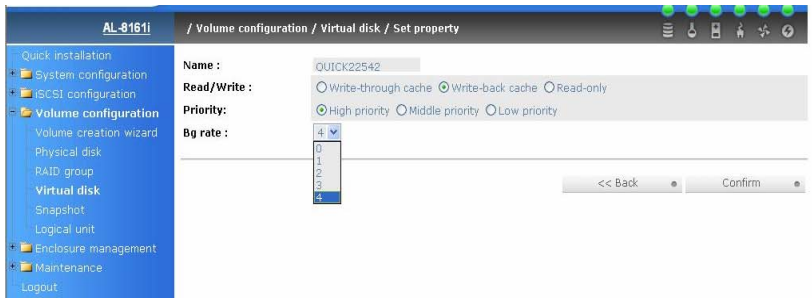
3. Delete

Delete existing VD; when deleting VD, the attached LUN(s) related to this VD

will be detached automatically.



4. Set property



Change the VD name, right, priority and bg rate. Right options:

"WT" → Write Through.

"WB" → Write Back.

"RO" → Read Only.

Write-Back Cache: When the system writes to a memory location that is currently held in cache, it only writes the new information to the appropriate cache line. When the cache line is eventually needed for some other memory address, the changed data is "written back" to system memory. This type of cache provides better performance than a write-through cache, because it saves on (time-consuming) write cycles to memory.

Write-Through Cache: When the system writes to a memory location that is currently held in cache, it writes the new information both to the appropriate cache line and the memory location itself at the same time. This type of caching provides worse performance than write-back, but is simpler to implement and has the advantage of internal consistency, because the cache is never out of sync with the memory the way it is with a write-back cache.

Priority options:

"HI" → HIgh priority.

"MD" → MiD priority.

"LO" → LOw priority.

***T**his function is used to set the priorities of RAID level initialization and I/O accessing for the case of multiple VDs.*

Bg rate options:

"4 / 3 / 2 / 1 / 0" → Default value is 4. The higher number the background priority of a VD has, the more background I/O will be scheduled to execute.

5. Detach LUN

To detach LUN from a VD, please follow the steps below:

1. Mouse moves to the gray button next to the Host; click **"Detach"**. There will be a confirmation page coming out.
2. Choose "OK".

3. Done.

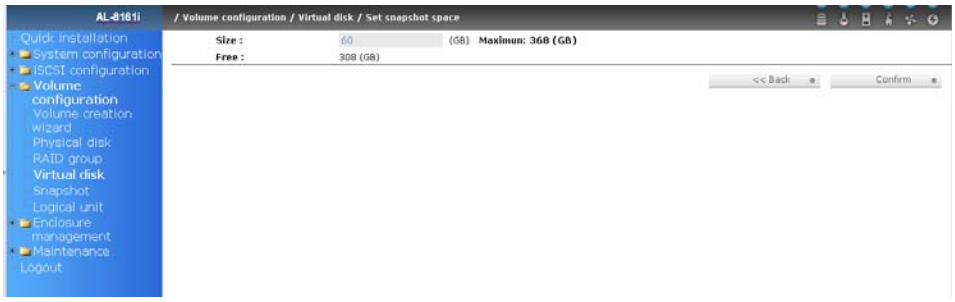
6. Attach LUN

To attach LUN to a VD, please follow the steps below:

1. Select a VD.
2. Input **"Host"** name, or fill-in wildcard **"*",** which means every host can access to this volume.
3. Choose LUN and permission for the VD to be read only or be able to be read and written.
4. Finally, then click "Confirm".

7. Set snapshot space

Set up the size for snapshot. The minimum size is suggested to be **20%** of VD size, then click "Confirm". For more details, please refer to 4.6.5



8. More information

Show the properties of VD, Logical LUN, and Snapshot

10. List LUN

Display the attached LUNs.

VD column description:

No.	Number of this Virtual disk. The button next to the VD No. shows the functions which can be executed.
Name	Virtual disk name.
Size(GB)	Total capacity of the Virtual disk.
Right	“WT” → Write Through. “WB” → Write Back. “RO” → Read Only.
Priority	“HI” → HIgh priority. “MD” → MiD priority. “LO” → LOw priority.
Bg rate	Background task priority. “4 / 3 / 2 / 1 / 0” → Default value is 4. The higher number the background priority of a VD has, the more background I/O will be scheduled to execute.
Status	The status of Virtual disk.

	“Online” → the Virtual disk is online. “Offline” → the Virtual disk is offline. “Initiating” → the Virtual disk is being initialized. “Rebuild” → the Virtual disk is being rebuilt. “Migrate” → the Virtual disk is being migrated. “Rollback” → the Virtual disk is being rolled back. “Scrub” → the Virtual disk is being scrubbed.
Health	The health of Virtual disk. “Optimal” → the Virtual disk is operating and has experienced no failures of the disks that comprise the RG. “Degraded” → At least one disk which comprises space of the Virtual disk has been marked as failed or has been plugged. “Missing” → the Virtual disk has been marked as missing by the system. “Failed” → the Virtual disk has experienced enough failures of the disks that comprise the VD for unrecoverable data loss to occur. “Part optimal” → the Virtual disk has experienced disk failures.
R %	Ratio of initializing or rebuilding.
RAID	The levels of RAID that Virtual disk is using.
#LUN	Number of LUN(s) that Virtual disk is attaching.
Snapshot (MB)	The Virtual disk size that used for snapshot. The number means “Used snapshot space” / “Total snapshot space”. The unit is in megabytes (MB).
#Snapshot	Number of snapshot(s) that Virtual disk is taken.
RG name	The Virtual disk is related to the RG name

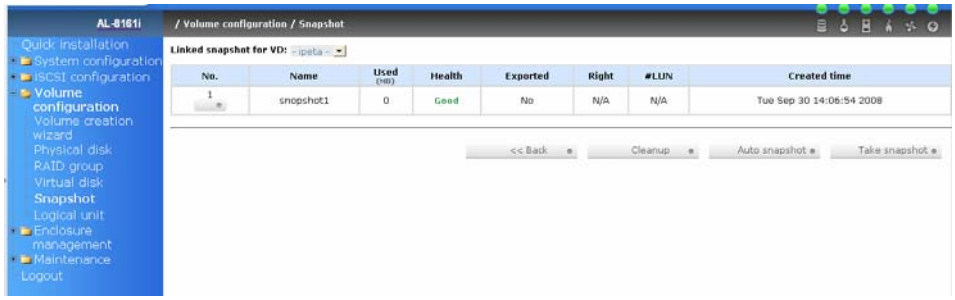
VD operations description:

Extend	Extend a Virtual disk capacity.
Scrub	Scrub a Virtual disk. It’s a parity regeneration. It supports RAID 3 / 5 / 6 / 30 / 50 / 60 only.

Delete	Delete a Virtual disk.
Set property	Change the VD name, right, priority and bg rate. Right options: “WT” → Write Through. “WB” → Write Back. “RO” → Read Only. Priority options: “HI” → HIgh priority. “MD” → MiD priority. “LO” → LOw priority. Bg rate options: “4 / 3 / 2 / 1 / 0” → Default value is 4. The higher number the background priority of a VD has, the more background I/O will be scheduled to execute.
Attach LUN	Attach to a LUN.
Detach LUN	Detach to a LUN.
List LUN	List attached LUN(s).
Set snapshot space	Set snapshot space for executing snapshot. Please refer to 4.6.5 for more detail.
Cleanup snapshot	Clean all snapshot VD related to the Virtual disk and release snapshot space.
Take snapshot	Take a snapshot on the Virtual disk.
Auto snapshot	Set auto snapshot on the Virtual disk.
List snapshot	List all snapshot VD related to the Virtual disk.
More information	Show Virtual disk detail information.

4.6.5 Snapshot

Snapshot-on-the-box captures the instant state of data stored in the target volume in a logical sense. The underlying logic is Copy-on-Write -- moving out the data which would be written to certain location where a write action occurs since the time of data capture. The certain location, named as “Snap VD”, is essentially a new VD.which can be attached to a LUN provisioned for a host as a disk like other ordinary VDs in the system. Rollback restores the data back to the state of any time which was previously captured in case for any unfortunate reason it might be (e.g. virus attack, data corruption, human errors and so on). Snap VD is allocated within the same RG in which the snapshot is taken, we suggest to reserve 20% of RG size or more for snapshot space. Snapshot / rollback features need **512MB** RAM at least.



Create snapshot volume

To take a snapshot of the data, please follow steps below:

1. Select **“/ Volume configuration / Virtual disk”**.

2. Mouse moves to the gray button next to the VD number; click **“Set snapshot space”**.

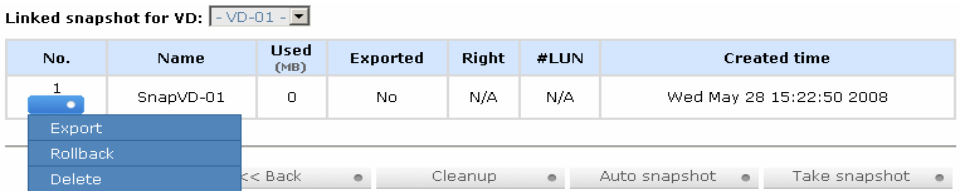
3. Set up the size for snapshot. The minimum size is suggested to be **20%** of VD size, then click “ Confirm ”. It will go back to the VD page and the size will show in snapshot column. It may not be the same as the number entered because some size is reserved for snapshot internal usage. There will be 2 numbers in

“Snapshot (MB)” column. These numbers mean **“Used snapshot space”** and **“Total snapshot space”**.

4. There are two methods to take snapshot. In **“/ Volume configuration / Virtual disk”**, mouse moves to the gray button next to the VD number; click **“Take snapshot”**. Or in **“/ Volume configuration / Snapshot”**, click “Take snapshot”.

5. Enter a snapshot name, then click “Confirm”. A snapshot VD is created.

6. Select **“/ Volume configuration / Snapshot”** to display all snapshot VDs related to the VD.



(This is Snap VD, but it is not exported)

7. Mouse moves to the gray button next to the Snapshot VD number; click **“Export”**. Enter a capacity for snapshot VD. If the size is zero, the exported snapshot VD will be **read only**. Otherwise, the exported snapshot VD can be **read/written**, and the size will be the maximum capacity to read/write.

8. Attach a LUN for snapshot VD. Please refer to 4.6.6 for attaching a LUN.

9. Done. It can be used as a disk.

(This is the list of "VD-01". There are two snapshots in "VD-01". Snapshot VD "SnapVD-01" is exported to read only, "SnapVD-02" is exported to read/write)

10. There are two methods to clean all snapshots. In **"/ Volume configuration / Virtual disk"**, mouse moves to the gray button next to the VD number; click **"Cleanup snapshot"**. Or in **"/ Volume configuration / Snapshot"**, click "Cleanup".

11. Cleanup will delete all snapshots related to the VD and release snapshot space.

Snapshot has some constraints as follows:

1. Minimum RAM size of enabling snapshot is **512MB**.

2. For performance and future rollback, the RAID subsystem saves snapshot with names in sequences. For example, three snapshots has been taken and named "SnapVD-01"(first), "SnapVD-02" and "SnapVD-03"(last). When deleting "SnapVD-02", both of "SnapVD-02" and "SnapVD-03" will be deleted because "SnapVD-03" is related to "SnapVD-02".

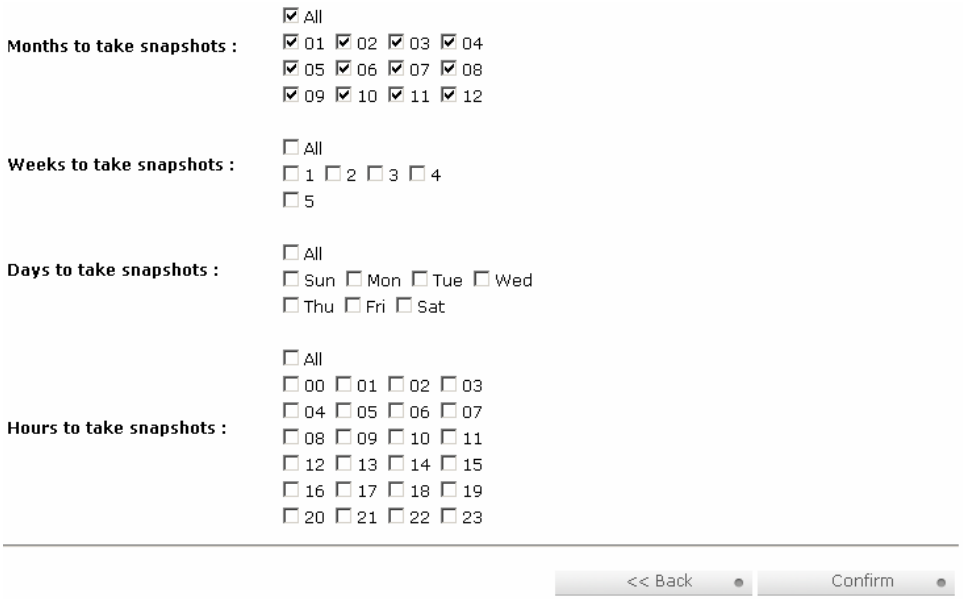
3. For resource management, maximum number of snapshots in the RAID subsystem is **32**.

4. If the snapshot space is full, system will send a warning message of space full and the new taken snapshot will replace the oldest snapshot in rotational sequence by executing auto snapshot, but new snapshot can not be taken by manual because system does not know which snapshot VDs can be deleted.

Auto snapshot

The snapshot copies can be taken manually or by schedule such as hourly or daily. Please follow the steps:

1. There are two methods to set auto snapshot. In **"/ Volume configuration / Virtual disk"**, mouse moves to the gray button next to the VD number; click **"Auto snapshot"**. Or in **"/ Volume configuration / Snapshot"**, click "Auto snapshot".
2. The auto snapshot can be set monthly, weekly, daily, or hourly.
3. Done. It will take snapshots automatically.



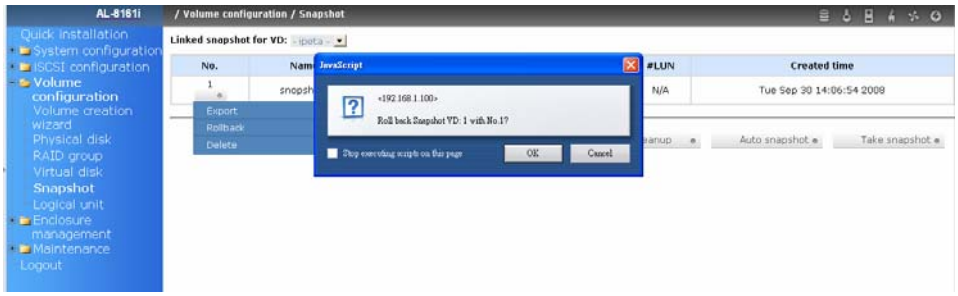
(It will take snapshots every month, and keep the last 32 snapshot copies)

Daily snapshot will be taken at every 00:00. Weekly snapshot will be taken every Sunday 00:00. Monthly snapshot will be taken every first day of month 00:00.

Rollback

The data in snapshot VD can rollback to the original VD. Please follow the steps below:

1. Select **"/ Volume configuration / Snapshot"**.
2. Mouse moves to the gray button next to the Snap VD number which user wants to rollback the data; click **"Rollback"**.



3. Done, the data in snapshot VD will rollback to the original VD.

Rollback has some constraints as described in the followings:

1. Minimum RAM size of enabling rollback is **512MB**.
2. When making rollback, the original VD cannot be accessed for a while. At the same time, the system connects to original VD and snaps VD, and then starts rollback.
3. During rollback, data from snap VD to the original VD, the original VD can be accessed and the data in VD just like it has finished rollback. At the same time, the other related snap VD(s) can not be accessed.
4. After rollback, the other snapshot VD(s) after the VD which is doing rollback will be deleted.

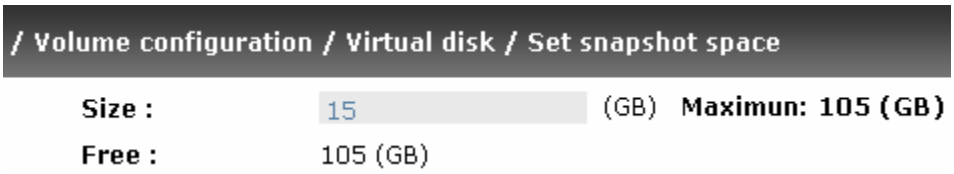
Caution

Before executing rollback, it is better to dismount file system for flushing data from cache to disks in OS first. System sends pop-up message when user executes rollback function.

The following is an example to take a snapshot:

Step 1: Create snapshot space. In **"/ Volume configuration / Virtual disk"**, Mouse moves to the gray button next to the VD number; click **"Set snapshot space"**.

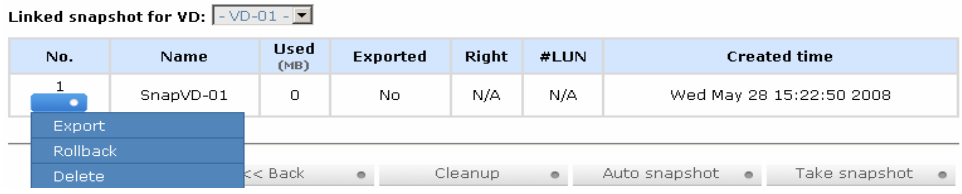
Step 2: Set snapshot space. Then click " Confirm ". The snapshot space is created.



No.	Name	Size (GB)	Right	Priority	Bg rate	Status	Health	R %	RAID	#LUN	Snapshot (MB)	#Snapshot	RG name
1	VD-01	30	WB	HI	4	Online	Optimal		RAID 0	0	263/15360	0	RG-R0
2	VD-02	20	WB	HI	4	Online	Optimal		RAID 5	0	0/0	0	RG-R5

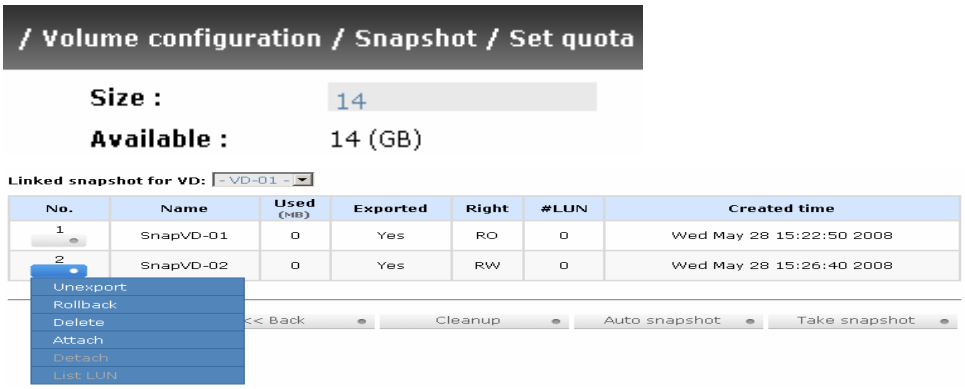
("VD-01" snapshot space has been created, snapshot space is 15360MB, and used 263MB for saving snapshot index)

Step 3: Take a snapshot. In **"/ Volume configuration / Snapshot"**, click " Take snapshot ". It will link to next page. Enter a snapshot name.



Step 4: Export the snapshot VD. Mouse moves to the gray button next to the

Snapshot VD number; click **"Export"**. Enter a capacity for snapshot VD. If the size is zero, the exported snapshot VD will be read only. Otherwise, the exported snapshot VD can be read/written, and the size will be the maximum capacity to read/write.



(This is the list of "VD-01". There are two snapshots in "VD-01". Snapshot VD "SnapVD-01" is exported to read only, "SnapVD-02" is exported to read/write)

Step 5: Attach a LUN to snapshot VD. Please refer to 4.6.5.4 for attaching a LUN.

Done: Snapshot VD can be used.

Snapshot column description:

No.	Number of this snapshot VD. The button next to the snapshot VD No. shows the functions which can be executed.
Name	Snapshot VD name.
Used (MB)	The amount of snapshot space that has been used.
Exported	Snapshot VD is exported or not.
Right	**"RW"** → **R**ead **/ W**rite. The snapshot VD can be read / write.

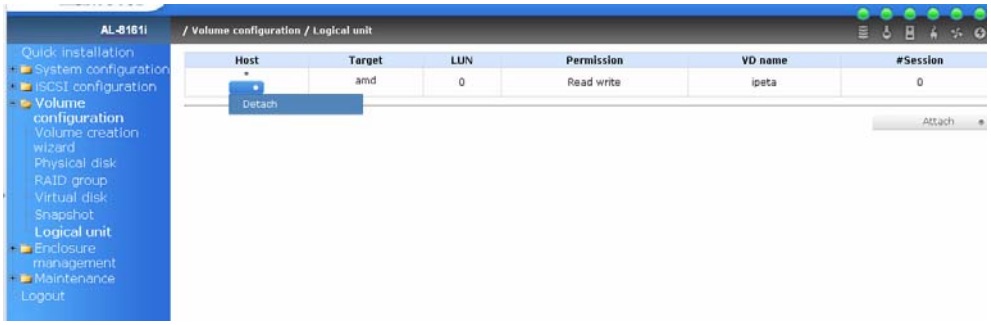
	"RO" → **R**ead **O**nly. The snapshot VD can be read only.
#LUN	Number of LUN(s) that snapshot VD is attaching.
Created time	Snapshot VD created time.

Snapshot operations description:

Export / Unexport	Export / unexport the snapshot VD.
Rollback	Rollback the snapshot VD to the original.
Delete	Delete the snapshot VD.
Attach	Attach to a LUN.
Detach	Detach to a LUN.
List LUN	List attached LUN(s).

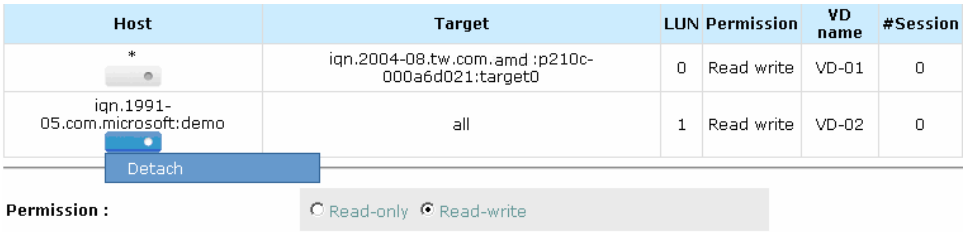
Logical unit

"Logical unit" can view the status of attached logical unit number of each VD.



The users can attach LUN to a VD or snapshot VD by clicking the

“ Attach ”. **“Host”** must enter an iSCSI node name for access control, or fill-in wildcard **“*”,** which means every host can access the volume. Choose LUN number and permission, then click “ Confirm ”.



(VD-01 is attached to LUN 0 and every host can access. VD-02 is attached to LUN 1)

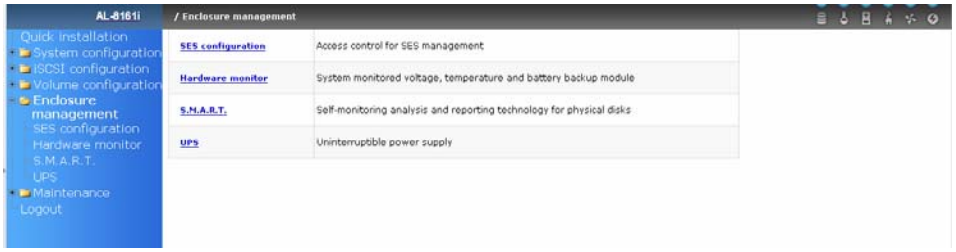
LUN operations description:

Attach	Attach a logical unit number to a Virtual disk.
Detach	Detach a logical unit number from a Virtual disk.

The matching rules of access control are inspected from top to bottom in sequence. For example: there are 2 rules for the same VD, one is “*”, LUN 0; and the other is “iqn.host1”, LUN 1. The other host “iqn.host2” can login successfully because it matches the rule 1. The access will be denied when there is no matching rule.

4.7 Enclosure management

“Enclosure management” allows the users to manage and observe the enclosure information that include **“SES configuration”**, **“Hardware monitor”**, **“S.M.A.R.T.”** and **“UPS”**.



To have the enclosure management work correctly, there are many sensors deployed inside of this iSCSI RAID subsystem for different purposes, such as temperature sensors, voltage sensors, hard disks, fan sensors, power sensors, and LED status. Depending on different hardware characteristics, the sensors have different polling intervals.

Below are the details of polling time intervals:

1. Temperature sensors: 1 minute.
2. Voltage sensors: 1 minute.
3. Hard disk sensors: 10 minutes.
4. Fan sensors: 10 seconds . When there are 3 errors consecutively, controller sends ERROR event log.
5. Power sensors: 10 seconds, when there are 3 errors consecutively, controller sends ERROR event log.
6. LED status: 10 seconds.

4.7.1 SES configuration

Most recent SCSI enclosure products support a protocol called **SCSI Enclosure Services** (SES). The initiator communicates with the enclosure using a specialized set of SCSI commands to access power, cooling, and other non-data characteristics. To enable or disable the SES support, give **"SES Configuration"** a click.

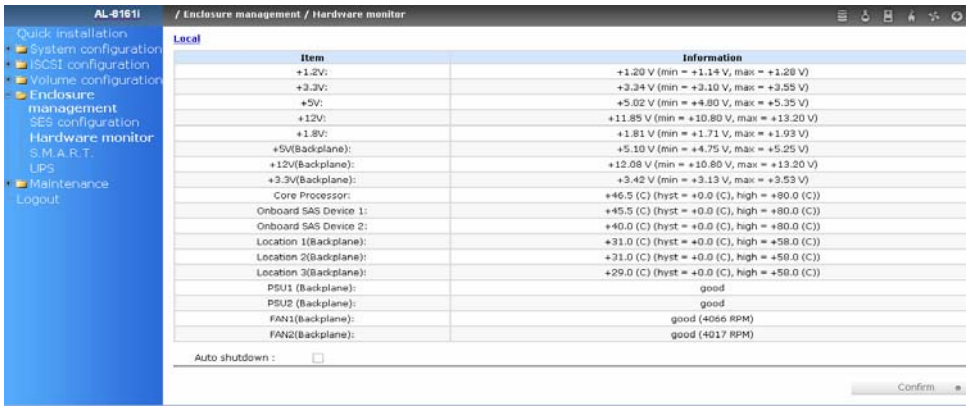
(Enable SES in LUN 0)

The SES client software is also available at the following web site:

SANtools: http://www.santools.com/

4.7.2 SES Hardware monitor

"Hardware monitor" allows the users to view all the information about the current status of voltages and temperatures read from the monitored components.



NOTE

If "Auto shutdown" has been checked, this RAID subsystem will shutdown automatically when monitored voltage or temperature is out of the normal range. For securer system and data protection, please check "Auto Shutdown". To avoid the possibility of system auto shutdown that is triggered by any single short period of high temperature or abnormal voltage, this iSCSI RAID subsystem uses multiple condition judgments for auto shutdown.

Below are the details about the conditions under which the auto shutdown will be triggered automatically:

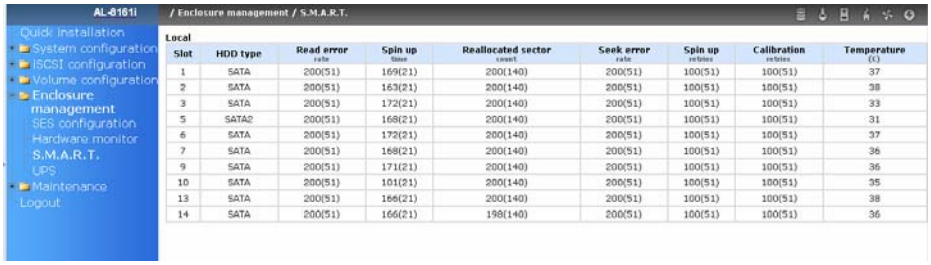
1. There are 3 sensors deployed on the RAID controllers for monitoring temperature; one is on the core processor, another is on the PCI-X bridge, and the final one is on the daughter board. The RAID controller will check each sensor every 30 seconds. When one of these sensor is over high temperature for 3 minutes continuously, auto shutdown will be triggered immediately.

2. The core processor temperature limit is 85℃. The PCI-X bridge temperature limit is 80℃. The daughter board temperature limit is 80℃.

3. If the high temperature situation doesn't last for 3 minutes continuously, the RAID controller will not launch auto shutdown.

4.7.3 S.M.A.R.T.

S.M.A.R.T. (**S**elf-**M**onitoring **A**nalysis and **R**eporting **T**echnology) is a diagnostic tool for hard drives to deliver warning of drive failures prior to the occurrence of serious hard drive failure. Thus S.M.A.R.T. provides the users with the chances to take data saving actions before possible drive failure.



Slot	HDD type	Read error rate	Spin up time	Reallocated sector count	Seek error rate	Spin up retries	Calibration retries	Temperature (C)
1	SATA	200(51)	169(21)	200(140)	200(51)	100(51)	100(51)	37
2	SATA	200(51)	163(21)	200(140)	200(51)	100(51)	100(51)	38
3	SATA	200(51)	172(21)	200(140)	200(51)	100(51)	100(51)	33
5	SATA2	200(51)	168(21)	200(140)	200(51)	100(51)	100(51)	31
6	SATA	200(51)	172(21)	200(140)	200(51)	100(51)	100(51)	37
7	SATA	200(51)	168(21)	200(140)	200(51)	100(51)	100(51)	36
9	SATA	200(51)	171(21)	200(140)	200(51)	100(51)	100(51)	36
10	SATA	200(51)	101(21)	200(140)	200(51)	100(51)	100(51)	35
13	SATA	200(51)	166(21)	200(140)	200(51)	100(51)	100(51)	38
14	SATA	200(51)	166(21)	198(140)	200(51)	100(51)	100(51)	36

How S.M.A.R.T. works is to measure many attributes coming from the hard drive and inspects the properties of hard drives all the time. The advanced notice of possible hard drive failure can allow the users to back up the hard drive data or replace the hard drive prior to the occurrence of serious hard drive failure.

Clicking "**S.M.A.R.T."** to view the current S.M.A.R.T. information of each hard drives. The number out of the parenthesis is the current value; the number inside of the parenthesis is the threshold value. Depending on the hard drive vendors, the threshold values will be some different; please refer to hard drive vendors' specification for details.

S.M.A.R.T. only supports SATA drive. SAS drive does not have this function, and will be displayed as "N/A.

Local

Slot	HDD type	Read error rate	Spin up time	Reallocated sector count	Seek error rate	Spin up retries	Calibration retries	Temperature (C)
1	SATA	59(6)	98(0)	100(36)	87(30)	100(97)	N/A	32
2	SATA	N/A	220(63)	180(63)	253(0)	253(157)	253(223)	37
3	SATA	N/A	227(63)	253(63)	253(0)	253(157)	253(223)	32
4	SATA	100(51)	100(25)	98(11)	100(51)	100(51)	100(0)	29
5	SATA	100(60)	147(24)	100(5)	100(67)	100(60)	N/A	33
6	SATA	100(60)	149(24)	100(5)	100(67)	100(60)	N/A	31
7	SATA	N/A	220(63)	253(63)	253(0)	253(157)	253(223)	36
8	SATA	100(51)	100(25)	100(11)	100(51)	100(51)	100(0)	23
9	SATA	100(60)	140(24)	100(5)	100(67)	100(60)	N/A	33
10	SATA	100(51)	100(25)	100(11)	100(51)	100(51)	84(0)	30
11	SATA	100(51)	100(25)	100(11)	100(51)	100(51)	100(0)	30
12	SATA	57(6)	98(0)	100(36)	80(30)	100(97)	N/A	34
13	SATA	100(51)	100(25)	100(11)	100(51)	100(51)	100(0)	29
14	SATA	61(6)	98(0)	100(36)	82(30)	100(97)	N/A	33
15	SATA	69(6)	98(0)	100(36)	81(30)	100(97)	N/A	34
16	SATA	65(6)	98(0)	100(36)	81(30)	100(97)	N/A	30

4.7.4 UPS

The item **"UPS"** allows the users to setup UPS (**U**ninterruptible **P**ower **S**upply) support for specific UPS models.

Presently, this iSCSI RAID subsystem merely supports and communicates with the smart-UPS of APC (American Power Conversion Corp.). Please check out the details from the website: http://www.apc.com/. Below are the procedures about how to quickly setup the APC UPS:

Step1: First, connect the system and APC UPS via RS-232 for communication.

Step2: Setup the shutdown values when power is failed.

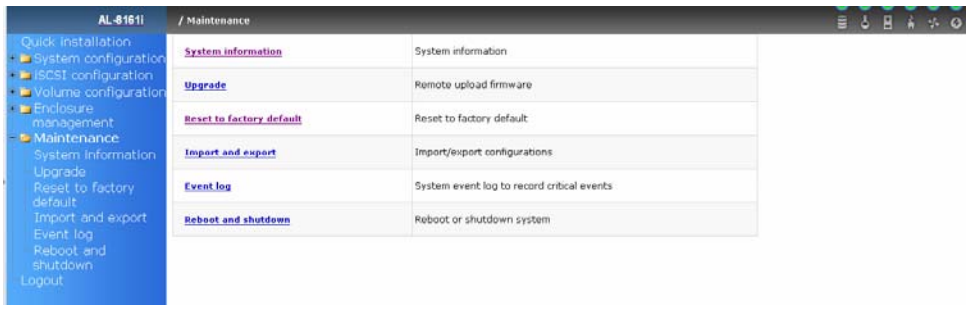
UPS column descriptions:

UPS Type	Select UPS Type. Choose Smart-UPS for APC, None for other vendors or no UPS.
Shutdown	When below the setting level, the system will shutdown.

Battery Level (%)	Setting level to “0” will disable UPS.
Shutdown Delay (s)	If power failure occurred, and system can not return to value setting status, the system will shutdown. Setting delay to “0” will disable the function.
Shutdown UPS	Select ON, when power is gone, UPS will shutdown by itself after the system shutdown successfully. After power comes back, UPS will start working and notify system to boot up. OFF will not.
Status	The status of UPS. “Detecting…” “Running” “Unable to detect UPS” “Communication lost” “UPS reboot in progress” “UPS shutdown in progress” “Batteries failed. Please change them NOW!”
Battery Level (%)	Current percentage of battery level.

4.8 System maintenance

“Maintenance” allows the users to take the following operations that include “System information” to view this iSCSI RAID subsystem main information, “Upgrade” to upgrade the ISCSI firmware version, “Reset to factory default” to reset all the RAID controller configurations to the factory configurations, “Import and export” to import and export this iSCSI RAID subsystem configurations, “Event log” to view system event logs, and “Reboot and shutdown” to either reboot or shutdown this iSCSI RAID subsystem.

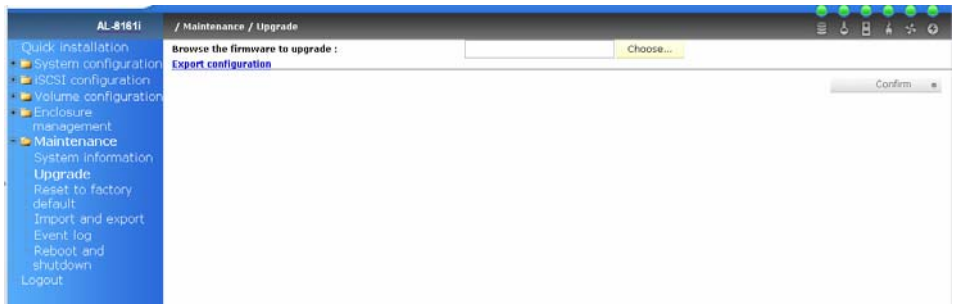


4.8.1 System information

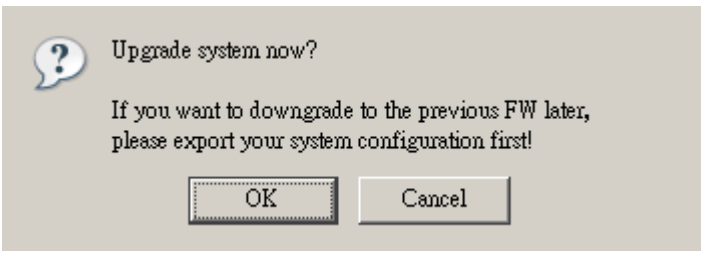
"System information" can display this iSCSI RAID subsystem system information that include firmware version, CPU type, system memory size, and controller serial number.

4.8.2 Upgrade

"Upgrade" allows the users to upgrade the firmware version. Please prepare new firmware file named **"xxxx.bin"** in local hard drive, then click "Browse..." to select the firmware file. Once the firmware files is selected, click "Confirm".



Then there will be a pop-up message as follows:



Click **"Cancel"** to export this iSCSI RAID subsystem configurations in advance, or click **"OK"** to start to upgrade firmware. When upgrading firmware starts, there will be a progress bar showing the upgrading process. When the firmware upgrading is completed, this iSCSI RAID subsystem must be rebooted manually in order to make the new firmware upgrading effective.

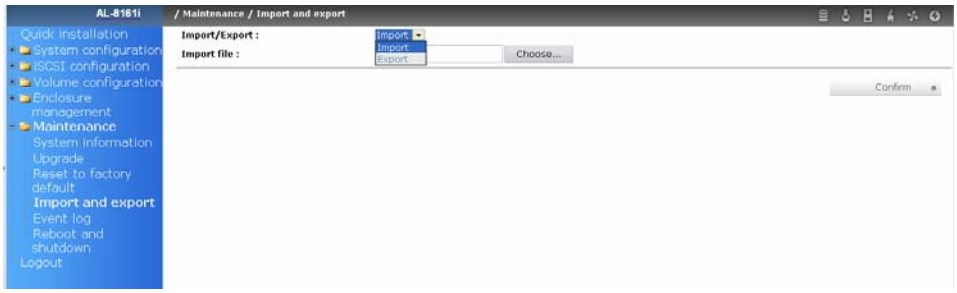
4.8.3 Reset to factory default

"Reset to factory default" allows the users to reset this iSCSI RAID subsystem configurations to the factory default configurations.

4.8.4 Import and export

"Import and export" allows the users to backup this iSCSI RAID subsystem configurations into a file.

1. **Export:** Export this iSCSI RAID subsystem configurations into a file.
2. **Import:** Import this iSCSI RAID subsystem configurations excluding volume configuration.

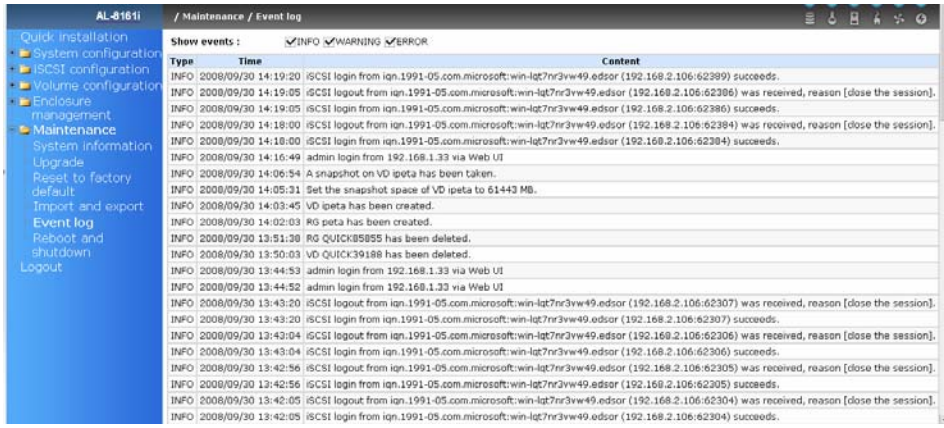


For the volume configuration setting, the values are available in Export and not available in Import to avoid confliction/date-deleting between two RAID controllers. That is, if a RAID controller already keeps valuable data in the disks and the users may forget to overwrite it, using Import could get all the original configurations back. But if the volume setting is also imported, the user's current data will be overwritten.

4.8.5 Event log

"Event log" can view the event messages. Check the checkbox of INFO, WARNING, and ERROR to choose the event log level of display event log.

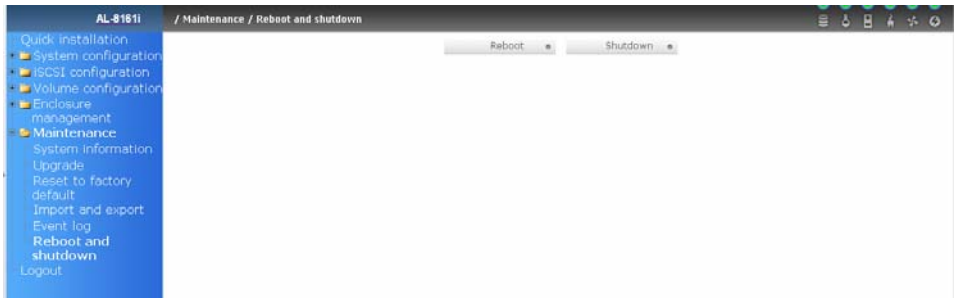
1. Click "Download" button to save the whole event log as a text file.
2. Click "Clear" button to clear event log.
3. Click "Mute" button to stop alarm if this iSCSI RAID subsystem alerts.



The event log is displayed in reverse order which means the latest event log is always listed on top of the first page. The event logs are actually saved in the first four hard drives; each hard drive has one copy of the complete event logs. For one controller, there are four copies of event logs to ensure the users can check event log any time even though there is one or two hard drives fail simultaneously.

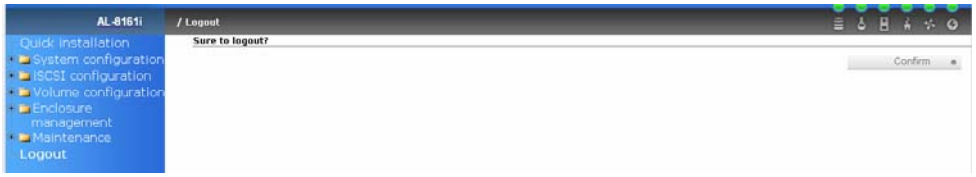
4.8.6 Reboot and shutdown

“Reboot and shutdown” allows the users to safely reboot or shutdown this iSCSI RAID subsystem. Making use of **“Shutdown”** to power off this iSCSI RAID subsystem is a good way to prevent any data loss, because **Shutdown** execution gets this iSCSI RAID subsystem to flush the data from the cache memory to the physical disks first, a necessity for data protection.



4.9 Logout

For security reason, **“Logout”** allows users to logout when no user is operating this iSCSI RAID subsystem. To re-login, please enter username and password again



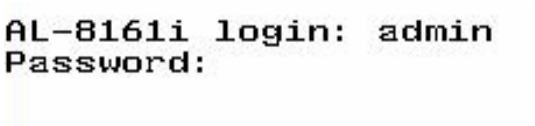
Chapter 5.

Console Port-base RAID Management

This iSCSI RAID subsystem console port-based configuration menu is mainly designed to be used as a RAID manage interface for the users who have no web browsers and want to quickly configure the RG (RAID group), VD (Virtual Disk), iSCSI settings, and so on.

5.1 Login

The users must login as administrator. The default User Name is **"admin"** and the Password is **"0000"**.



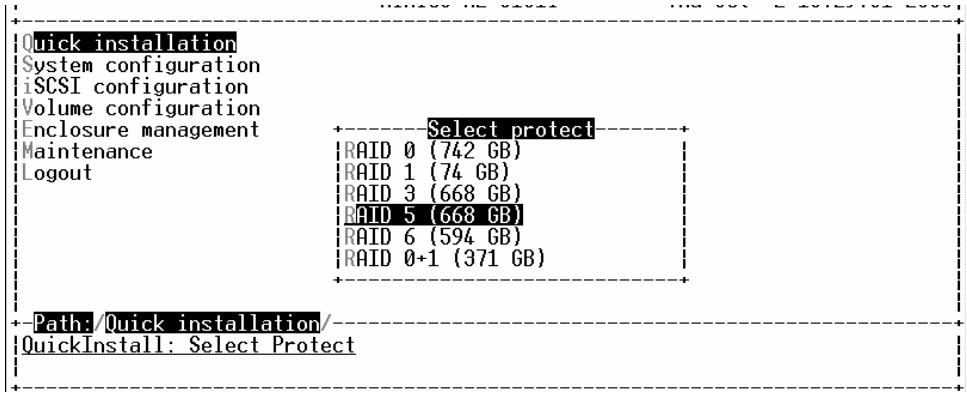
After the login, the main configuration menu as below will pop up automatically.

5.2 Quick Installation

It is easy to use "**Quick installation"** to create RG (RAID group) and VD (Virtual disk). Quick installation takes the whole physical disks to create a RG and VD; Quick installation itself will calculate the maximum space of RAID levels 0/1/3/5/6/0+1 respectively, depending on the number of physical disk. Quick installation will occupy all residual RG space for one VD, and it has no space for

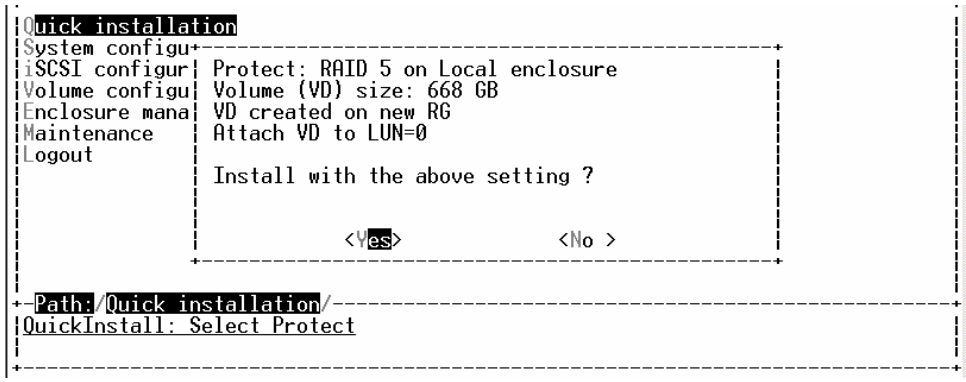
snapshot and spare. If snapshot is needed, please create RG and VD by manual, and refer to snapshot configuration for more details. If some physical disks are already being used by other RGs, “Quick installation” can not be executed because Quick installation is valid only when all physical disks in RAID subsystem are free. Below is one example of Quick Installation.

Step 1: Click **“Quick installation”**, then choose the RAID level. After RAID level choosing, press the enter key.



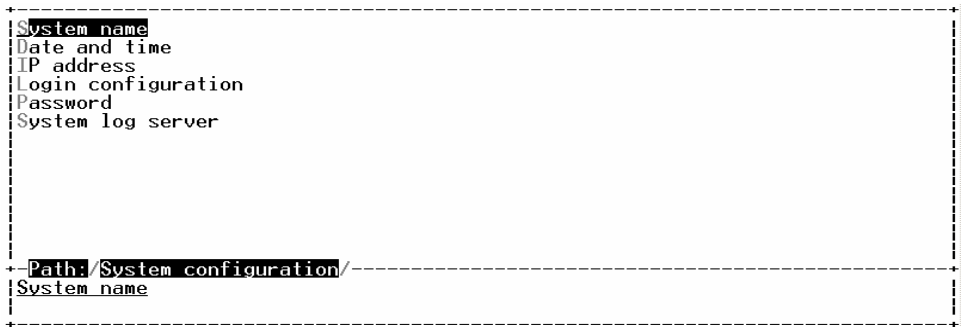
Step 2: On Confirm page, if all setups are correct, select Yes.

Then a RG and VD will be created. Now you can start to use the RAID subsystem.



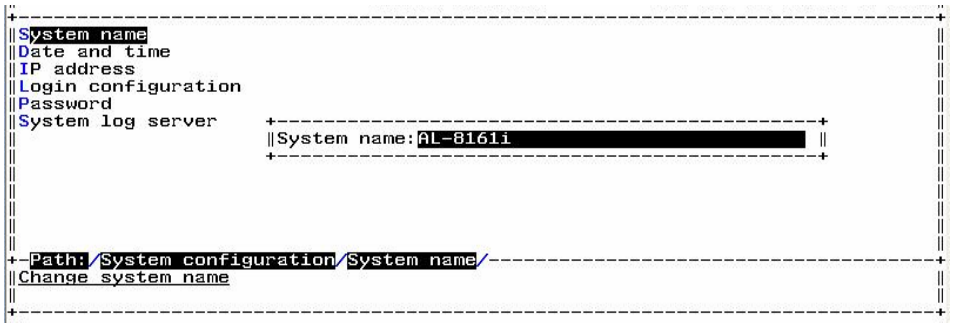
5.3 System configuration

“System configuration” is designed to setup the “System Name”, “Data and Time”, “IP address”, “Login configuration”, “Password”, and “System log server”.



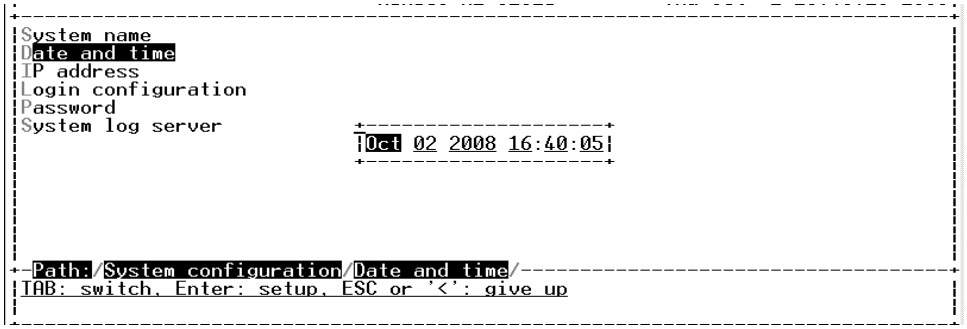
5.3.1 System name

“System name” allows the users to name the RAID subsystem. Default system name composes of model name of this RAID subsystem.



5.3.2 Data and time

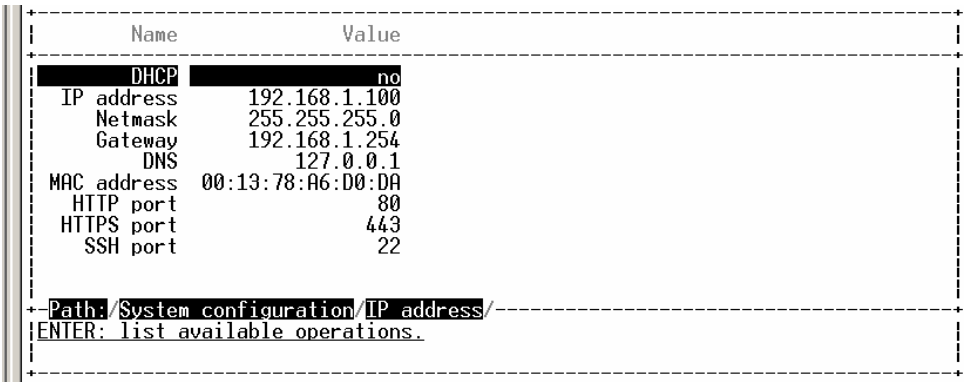
Check **“Change date and time”** to setup the system date and time.



5.3.3 IP address

On this setting page, the users can change this iSCSI RAID subsystem IP

address、DNS address, even the HTTP、 HTTPS, and SSH port number when the default port numbers are not allowed on the host or server.



SSH (secure shell) is required when the users want to login this iSCSI RAID subsystem from the remote side. The SSH client software is available at the following web site:

SSHWinClient WWW: http://www.ssh.com/

Putty WWW: http://www.chiark.greenend.org.uk/

5.3.4 Login configuration

"Login configuration" allows the users to enable or disable **"Auto Logout** and **Login lock**".

Auto logout: The options are (1) Disable; (2) 5 minutes; (3) 30 minutes; (4) 1 hour. The system will log out automatically when this iSCSI RAID subsystem console port-based configuration menu is inactive over 5 minutes \ 30 minutes \ I hour, depending on the Auto Logout setting.

Login lock: Disable/Enable. When the login lock is enabled, this iSCSI RAID subsystem console port-based configuration menu allows merely only one user to login or modify the RAID subsystem settings.

5.3.5 Password

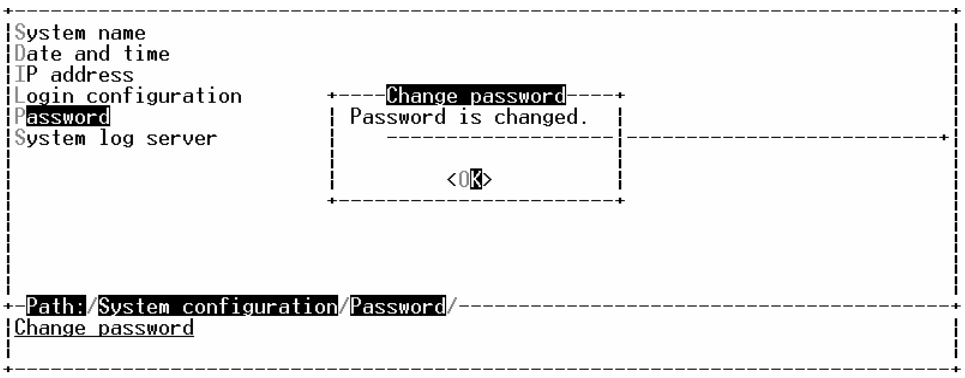
The users can change the password. Below are the steps:

Step 1: Type the old password

Step 2: Type the new password

Step 3: Re-type the new password

Step 4: Done



5.3.6 System log server

Using **"System log server"**, the users can choose the facility and the event log level. The default port of syslog is 514. The default setting enables event log level: WARNING and ERROR.

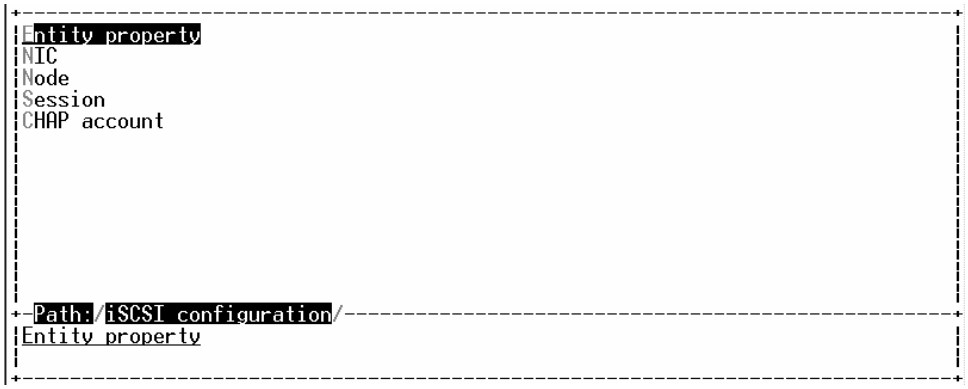
There are some syslog server tools. The following web sites are for your reference:

WinSyslog: http://www.winsyslog.com/

Kiwi Syslog Daemon: http://www.kiwisyslog.com/

5.4 iSCSI Configuration

"iSCSI configuration" is designed to setup the "Entity Property", "NIC", "Node", "Session", and "CHAP account".



5.4.1 Entity property

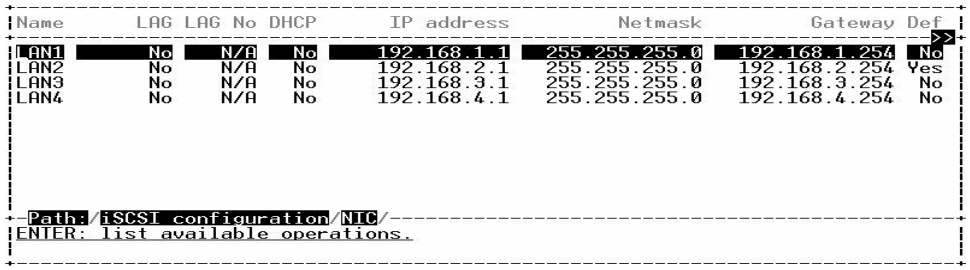
"Entity property" can view the entity name of this iSCSI RAID subsystem, and setup the **"iSNS IP"** for iSNS (Internet Storage Name Service). The iSNS protocol is designed to facilitate the automated discovery, management, and configuration of iSCSI devices on a TCP/IP network environment. iSNS provides intelligent storage discovery and management services comparable to those found in Fibre Channel networks, allowing a commodity IP network to function in a similar capacity as a storage area network. To use iSNS, it needs to install a iSNS server. Add an iSNS server IP address into the iSNS server lists so that a iSCSI initiator service can send queries.

The server that functions as ISNS server must not be installed with iSCSI initiator.

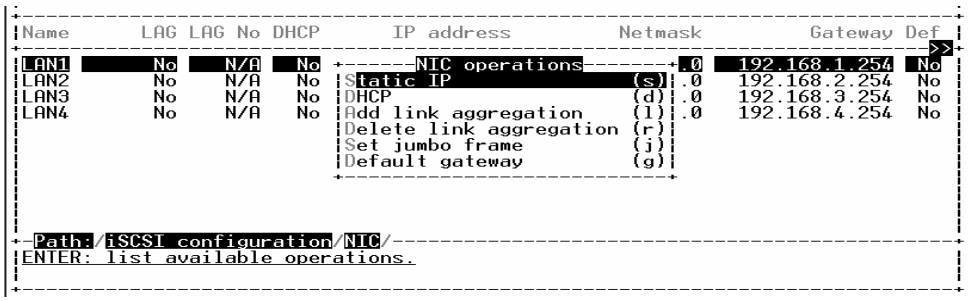
5.4.2 NIC

"NIC" can change the IP addresses of iSCSI host ports. This iSCSI RAID subsystem has four Gb/s LAN ports working as the host ports to transmit data. Each port must be assigned with a unique IP address unless the link aggregation or Trunking mode has been selected. If any two or more ports are set in link aggregation or Trunking mode, they will display the same IP.

Select a LAN port, and press the enter key.

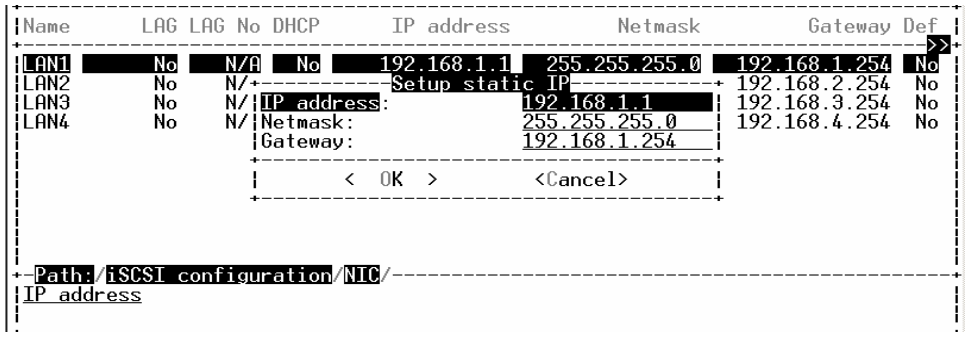


Then a submenu will pop up.

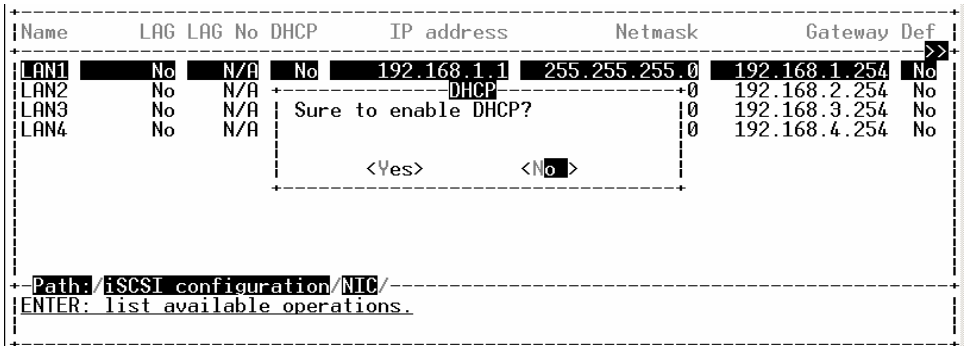


Below are the descriptions about this submenu:

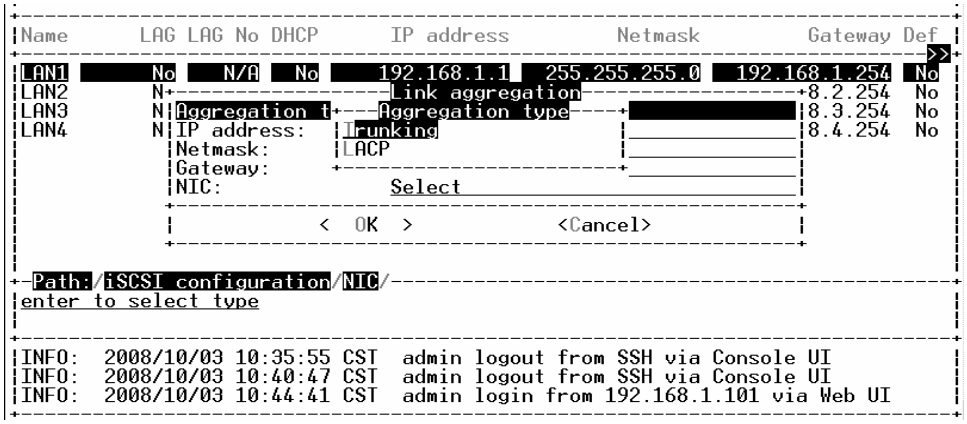
1. Select **"Static IP"**; then the users now can change the static IP address of the selected host port.



2. Select **"DHCP"**; then the users now can decide to use DHCP or not for the selected host port.



3. Select **"Add link aggregation"**; then the users can select "Trunking" or "LCAP" to increase the data transfer speed beyond the limits of any one single cable/port, or increase the redundancy for higher availability by paralleling multiple Ethernet network cables/ports.

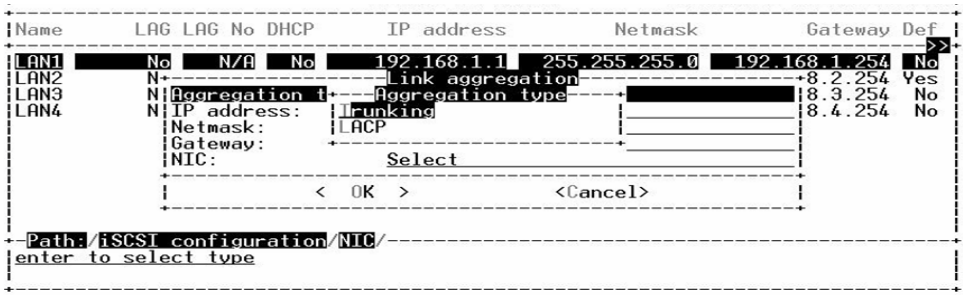


Descriptions of Trunking /LACP:

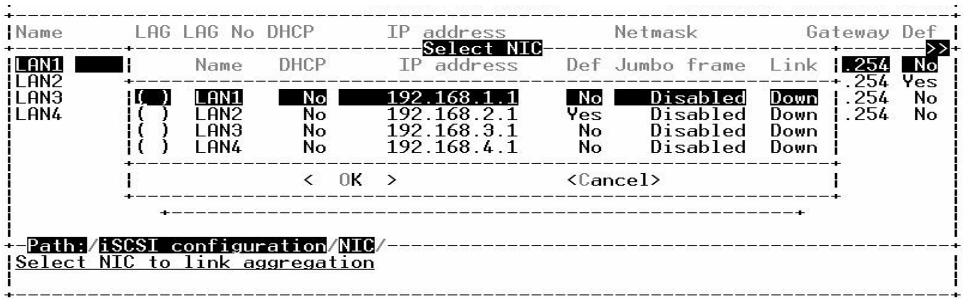
Trunking: It is defined as combining multiple ports in order to form faster logical communication links between devices. For example, connect all four data ports to the Gb/s Ethernet switch to form a single logical 4 Gb/s path.

LACP: The Link Aggregation Control Protocol (LACP) is part of IEEE specification 802.3ad that allows bundling several physical ports together to form a single logical channel. LACP allows a network switch to negotiate an automatic bundle by sending LACP packets to the peer. The advantages of LACP are (1) increases the bandwidth. (2) failover when link status fails on a port.

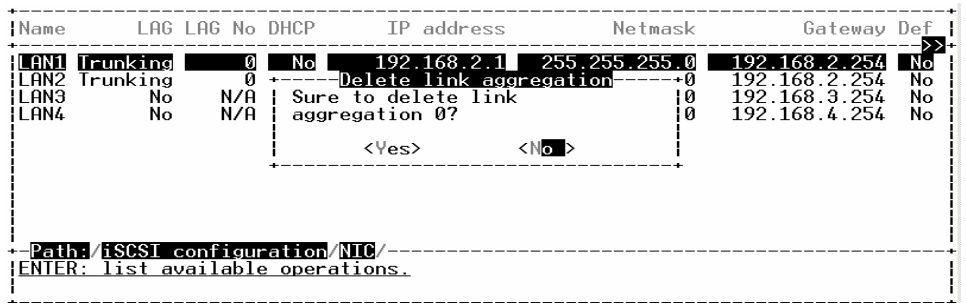
Select **"Aggregation type"**. Then press the enter key to select Trunking or LCAP.



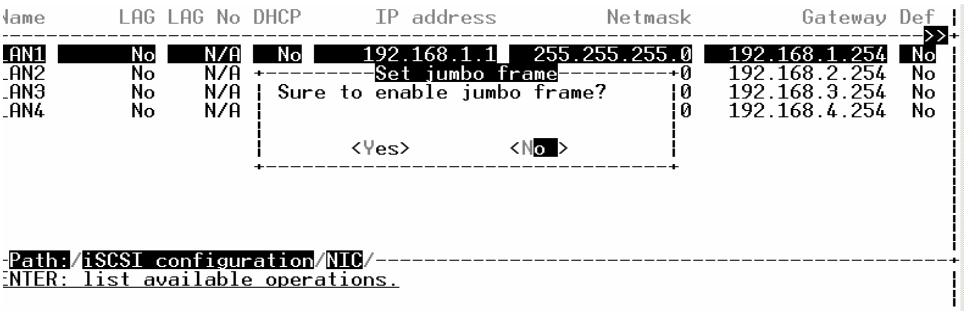
Select **"NIC"**. Then press the enter key to select the host ports for Trunking or LCAP.



4. Select **"Delete link aggregation"** to get the host ports that are assigned as Trunking or LACP back to the without-aggregation status.



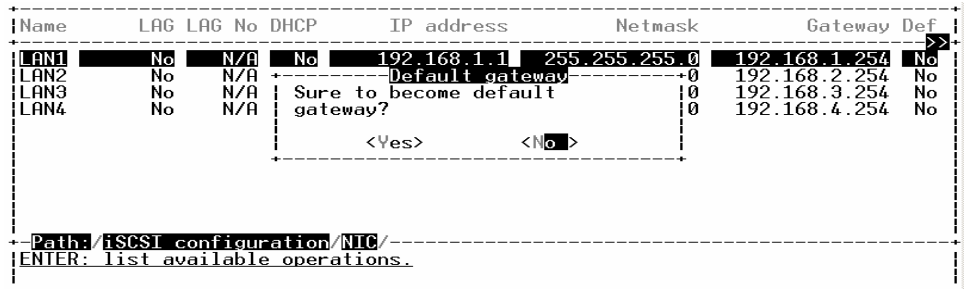
5. Select **"Set jumbo frame"**; then the users now can enable or disable jumbo frame.



Jumbo Frame is designed to enhance Ethernet networking throughput and

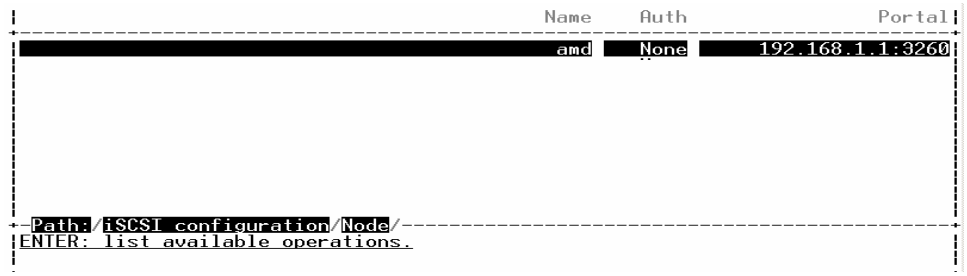
largely lower the CPU consumption of large file transfers by enabling more efficient larger payloads per packet. Conventionally, jumbo frames can carry up to 9,000 bytes of payload. Basically, a data transfer path from this iSCSI RAID subsystem to the server includes at least a NIC and this iSCSI RAID subsystem itself. To prove jumbo frame really work on this path, the jumbo frame function of both this iSCSI RAID subsystem and the NIC must be enabled. If a Ethernet switch is involved in this path, please enable the jumble frame function of this switch, too, and ensure MTU (maximum transmission unit) are all identical. "**Wireshark** "can be used to obtain the current MTU of any devices supporting jumbo frame.

6. Select **"Default gateway"**; then this iSCSI RAID subsystem's gateway address will be reset to the factory default IP address.

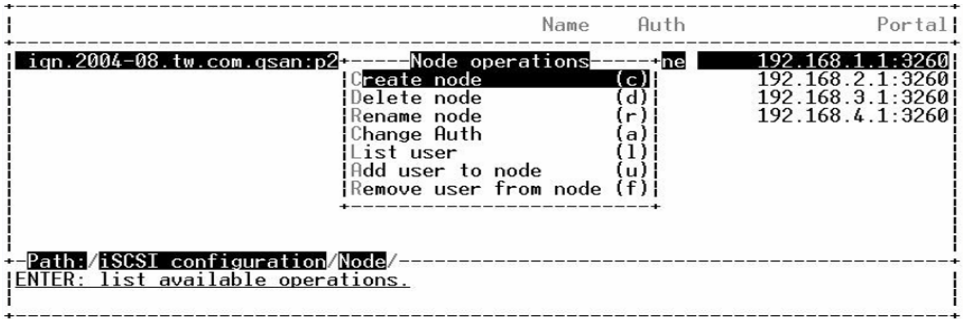


5.4.3 Node

"Node" allows the users to setup the target name and CHAP for the iSCSI initiator. This iSCSI RAID subsystem supports multiple nodes, and there is no default node name on This iSCSI RAID subsystem; it is empty, and must be created first.

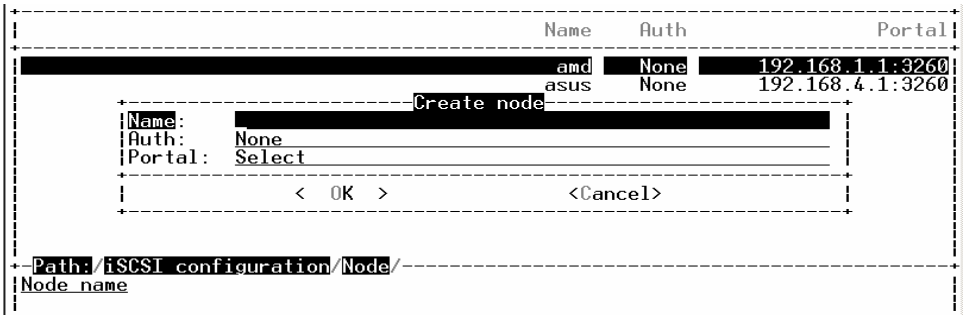


Select any created node, and press the enter key. Then a submenu will pop up as below.



Below are the descriptions about this submenu:

1. Select **"Create node"**; then the users now can create new node.

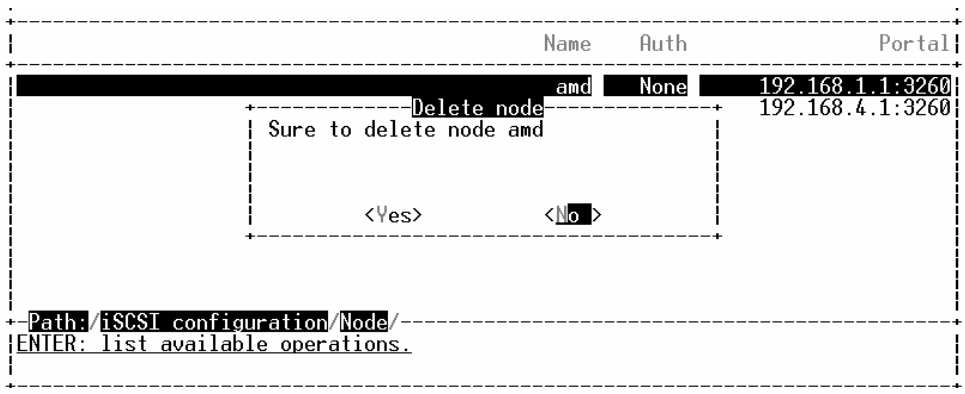


Step 1: Type a new node name.

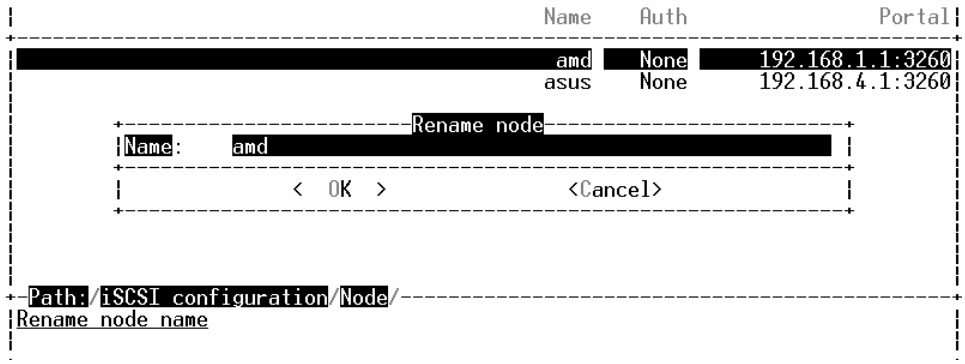
Step 2: Choose to apply "Auth" (CHAP) or not (None).

Step 3: Choose host ports, from which the created new node can be detected.

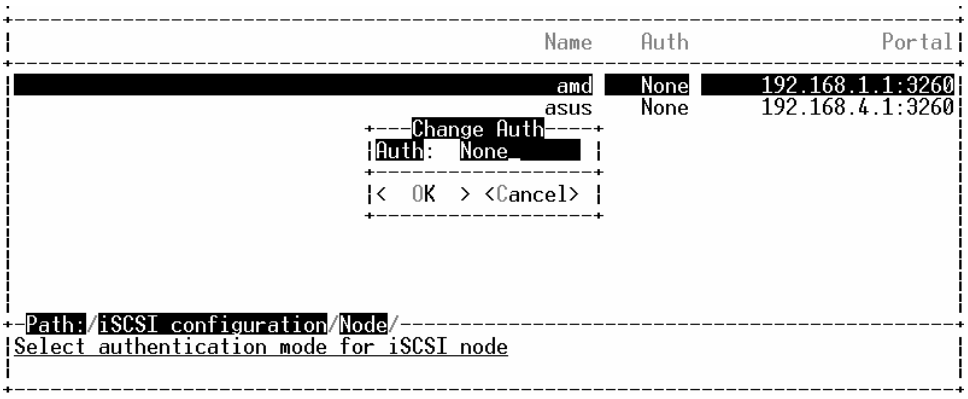
2. Select **"Delete node"** to delete the existing nodes.



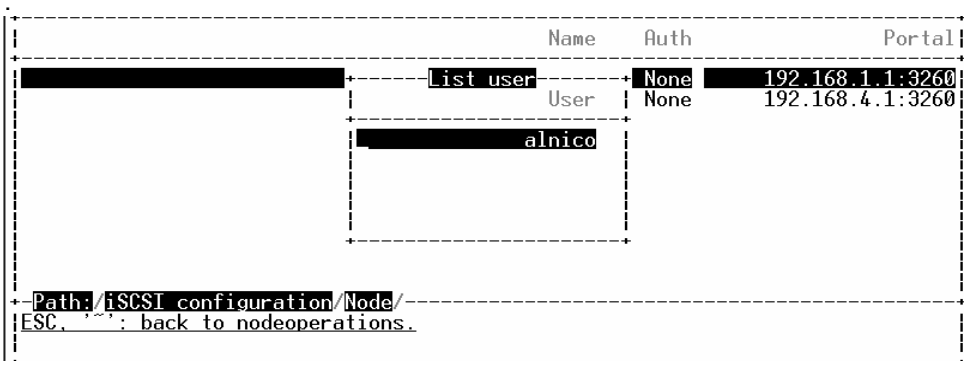
3. Select **"Rename node** to rename the existing node names.



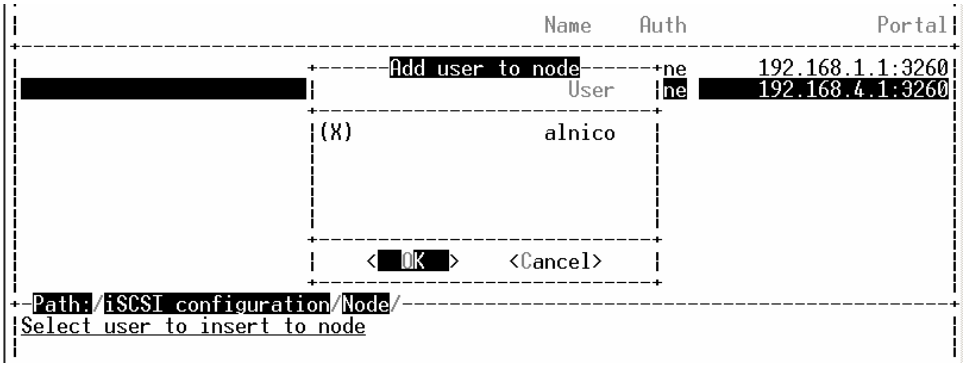
4. Select **"Change Auth"** to re-decide whether to use CHAP or not.



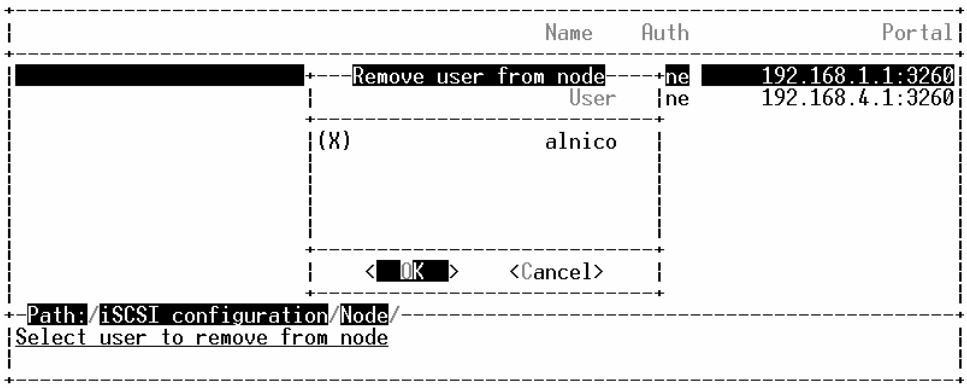
5. Select **" List user"** to display the user name (CHAP accounts).



6. Select **" Add user to node"** to add new user to node

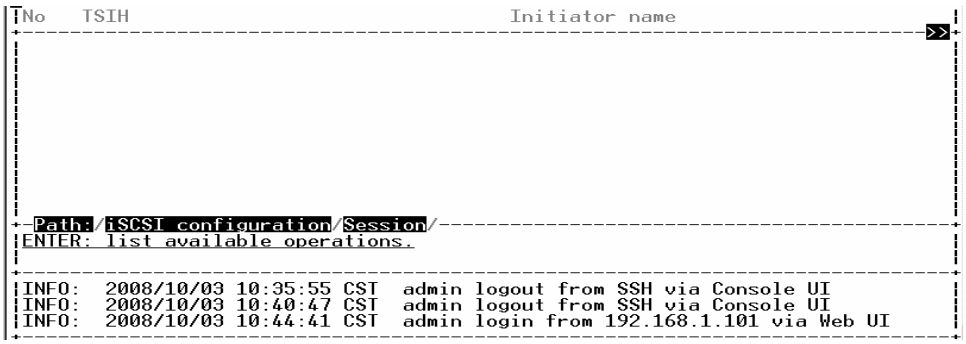


7. Select **"Remove user from node"** to remove the existing users from node



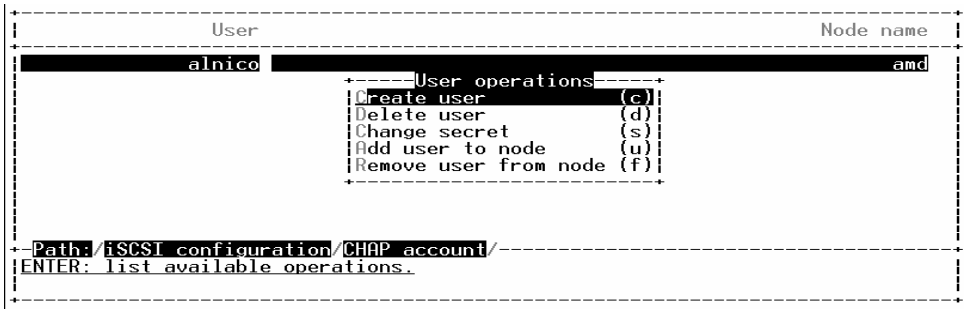
5.4.4 Session

"Session" can display iSCSI session and connection information



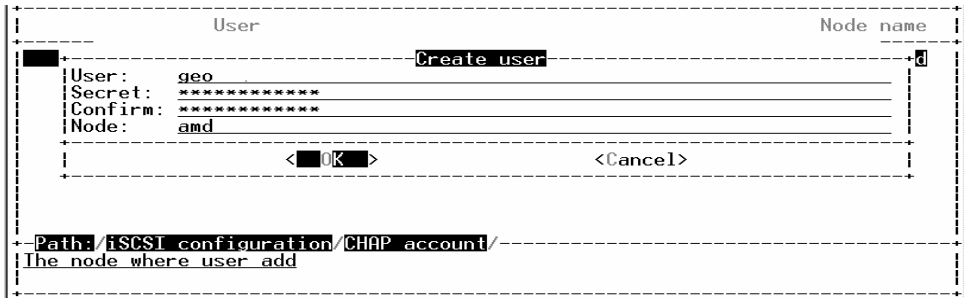
5.4.5 CHAP account

"CHAP account" can allow the users to create multiple CHAP accounts for node authentication.



Below are the descriptions about this submenu:

1. Select **"Create user"**; then the users now can create new CHAP accounts.



Step 1: Type a user name for a new CHAP account.

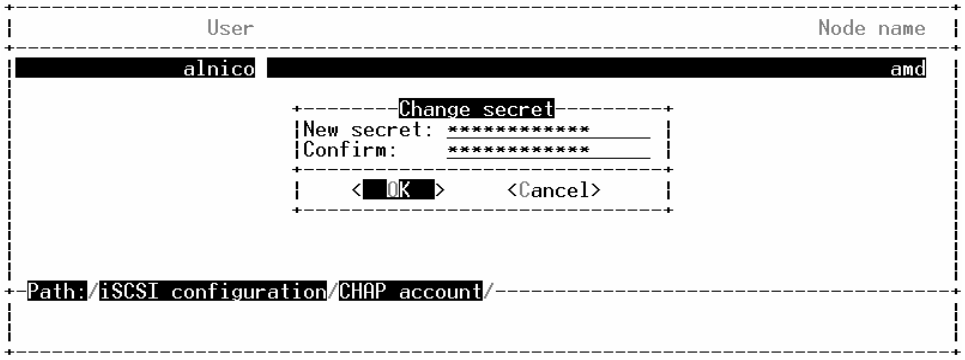
Step 2: Type Secret (password); the min is 12; the max is 16.

Step 3: Re-type the Secret.

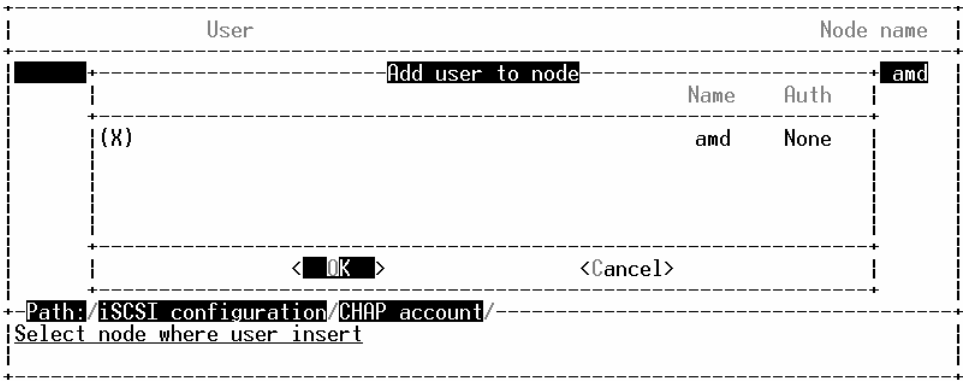
Step 4: Select a node for the newly created CHAP account.

2. Select **"Delete user"**; then the users now can delete existing CHAP accounts.

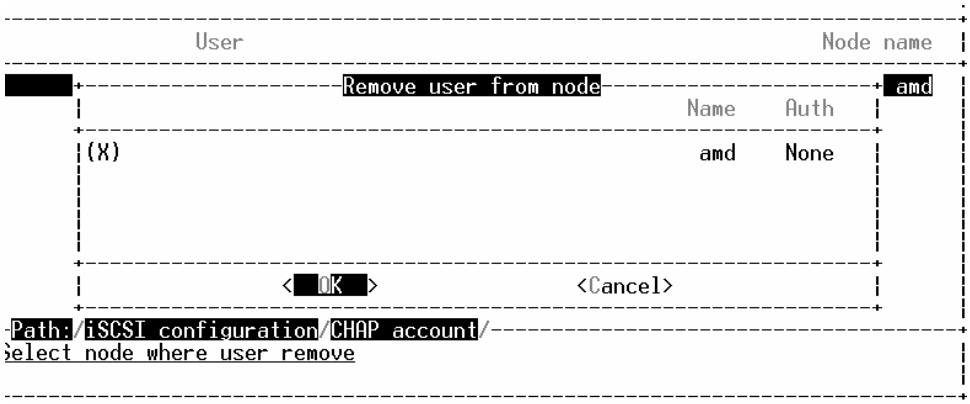
3. Select **"Change secret"** to change secret.



4. Select **"Add user to node"** to add existing CHAP accounts to nodes.

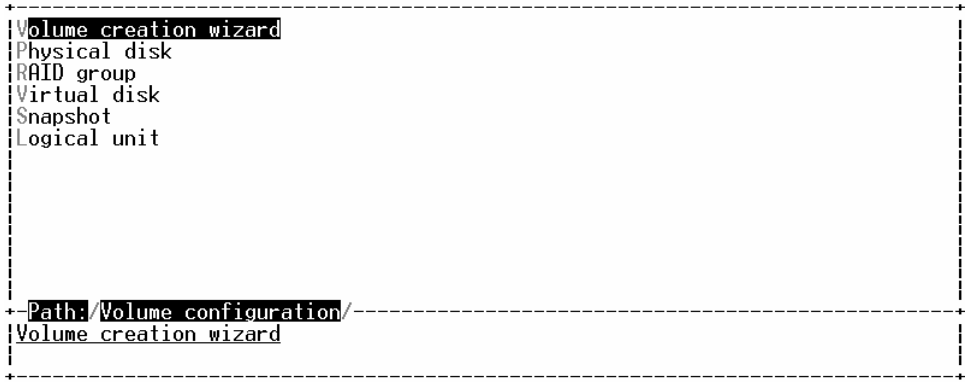


5. Select **"Remove user from node"** to do anti-add-users-to-node.



5.5 Volume configurations

"Volume configuration" is designed to setup the volume configuration which includes "Volume create wizard", "Physical disk", "RAID group", "Virtual disk", "Snapshot", and "Logical unit".



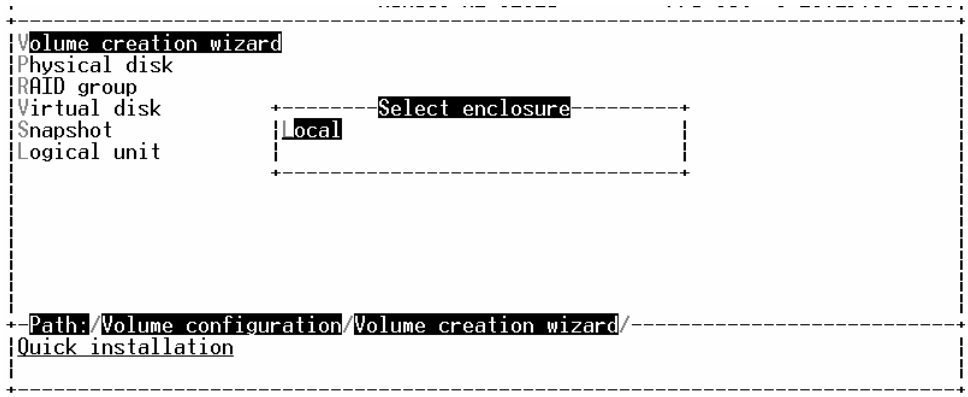
5.5.1 Volume creation wizard

"Volume create wizard" has a smarter policy. When this iSCSI RAID subsystem is inserted with some hard disks, "Volume create wizard" will list all the possible RAID level and capacities that the users can choose. For example, the users choose RAID 5 and the controller has 12*200G + 4*80G hard disks inserted. If the users want to make use of all the 16 hard disks for a RAID 5, the maximum capacity of the volume is 1200G (80G*15). Taking advantage of "Volume create wizard, this iSCSI RAID subsystem will take a smarter check and find out the most efficient way of using all the available hard disks; thus, in this case, the wizard will only uses the 200G hard disks, making a RAID 5 volume consisted of 200G*11=2200G.. The volume capacity, by doing so, becomes bigger, and the maximum hard disk capacity is fully used, too. The smarter policy gives the users:

1. Biggest capacity of RAID level for user to choose.

2. The fewest disk number for RAID level / volume size.

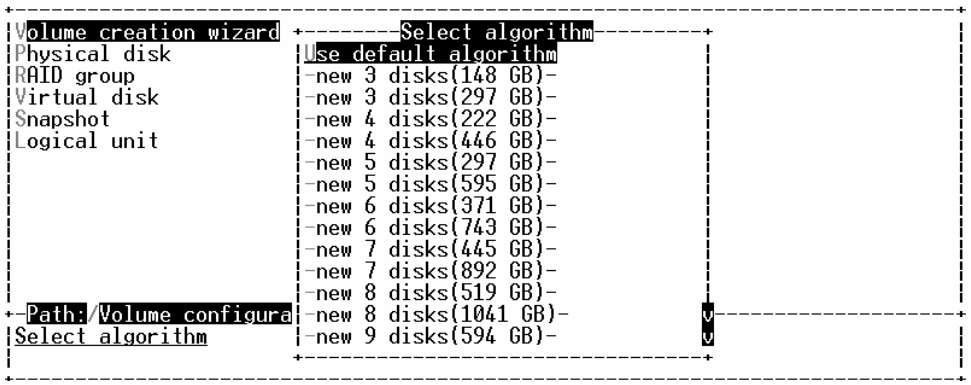
Step 1: Select **"Volume creation wizard"** and then select an enclosure.



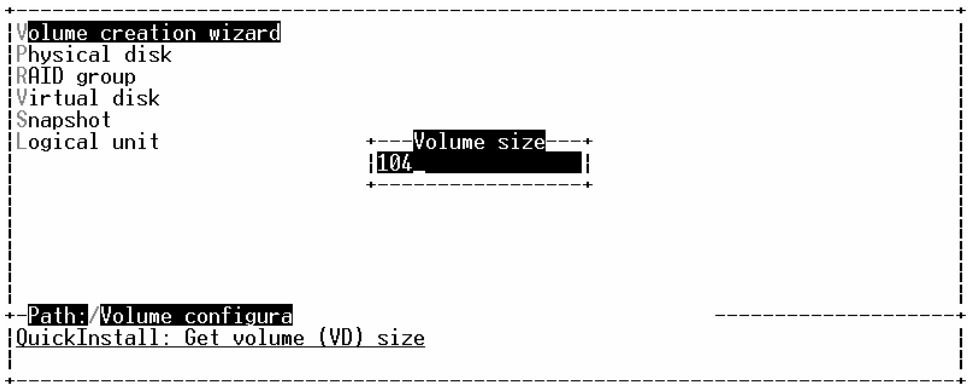
Step 2: Select RAID level.

Step 3: Select the combination of the RG (RAID Group) capacity, or “Use default algorithm”

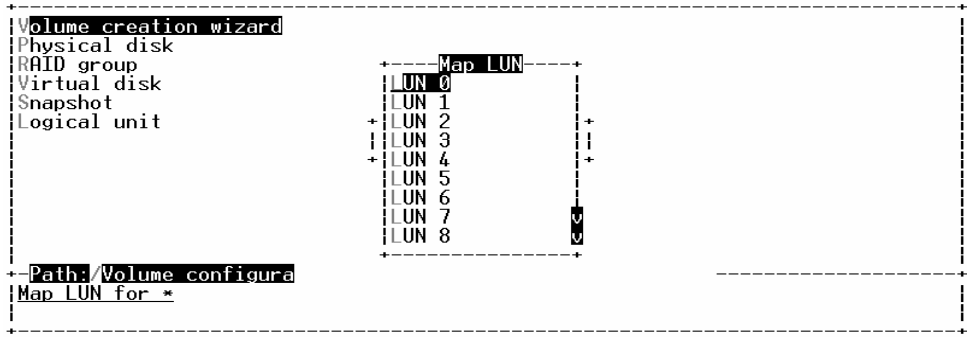
for maximum RG capacity.



Step 4: Decide VD (Virtual Disk) capacity. User can enter a number less or equal to the default capacity.



Step 5: Assign the volume with a LUN.



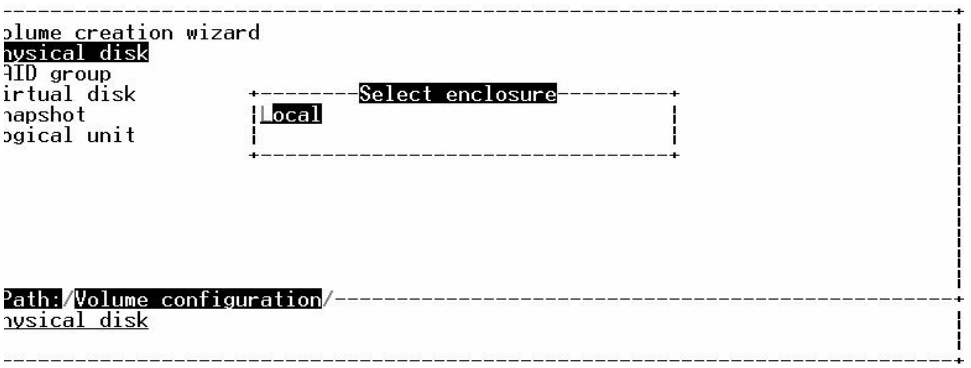
Step 6: Final confirm.

5.5.2 Physical disk

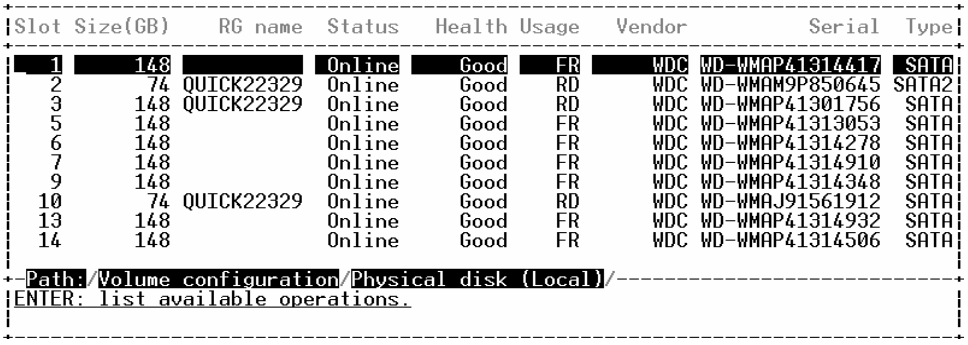
"Physical disk" can view the status of hard disks in the RAID subsystem, set spare disks, and standby mode.

1. View hard disk status and call up a submenu to setup hard spare and standby mode.

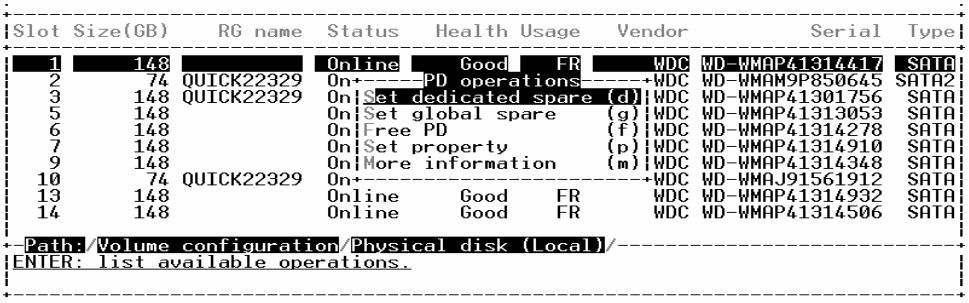
Step 1: Select enclosure.



Step 2: Select any hard disk **"slot"**.



Step 3: Press the enter key.

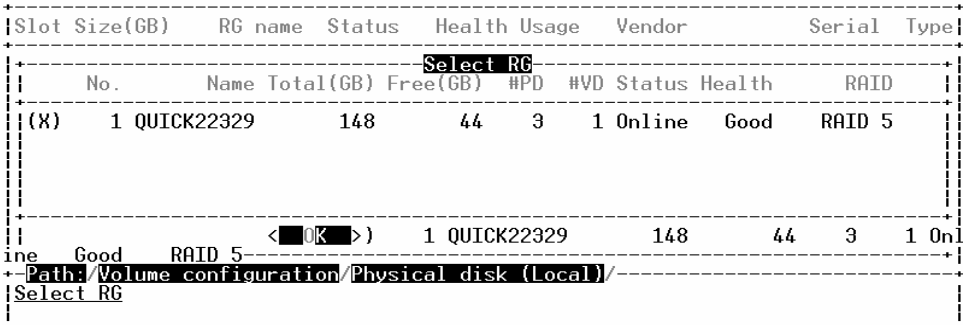


Below are the descriptions about this submenu:

1. Select **"Set dedicated spare"** to create a dedicated spare.

Dedicated spare can be created only when there are multiple RGs (RAID group) created before.

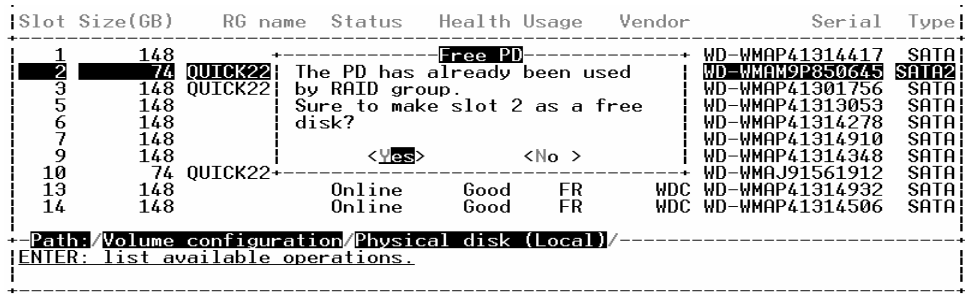
Select one RG that you wan to have the created dedicated spare used for. By doing so, the dedicated spare will only work for the selected RG.



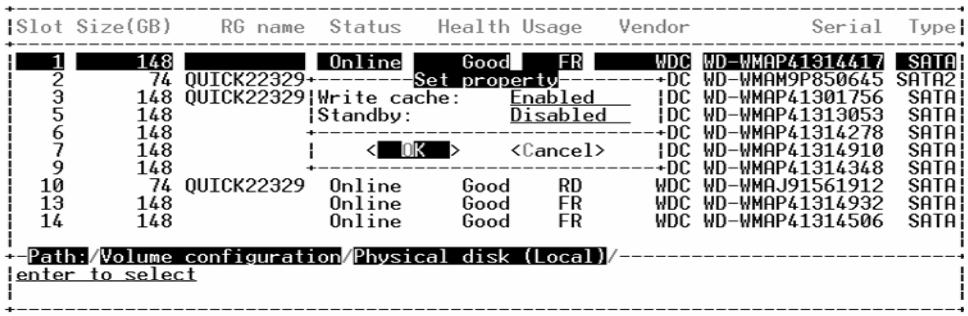
2. Select **"Set global spare"** to create a global spare.

Unlike dedicated spare, global spare can be used for any created RG. Thereby, there is no need to create RGs before creating global spare.

3. Select **"Free PD"** to set the selected hard disk as a free disk.



4. Select **"Set property"** to setup standby mode or enable\ disable write cache.



Write cache options:

1. Enabled → Enable disk write cache.

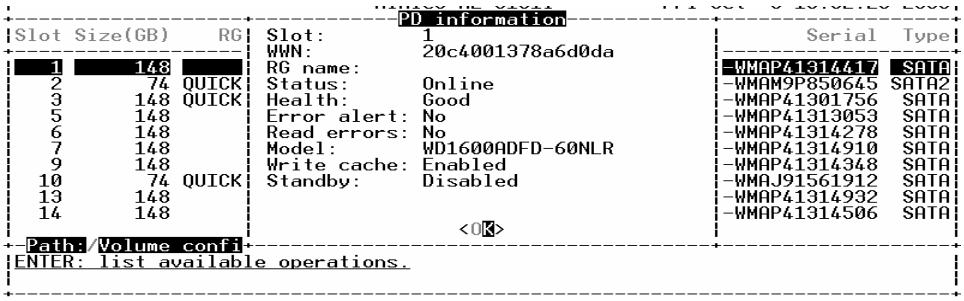
2. Disabled → Disable disk write cache.

Standby options:

1. Disabled → Disable spin down.

2. 30 sec / 1 min / 5 min / 30 min → Enable hard disk auto spin down to save power in the period of time.

3. Select **"PD information"** to view detailed hard disk information.



5.5.3 RAID group

"RAID group" can allow the users to create RG, view the status of each RAID group, migrate RAID group, and so on.

1. To create a RG (RAID group), please take the steps as below:

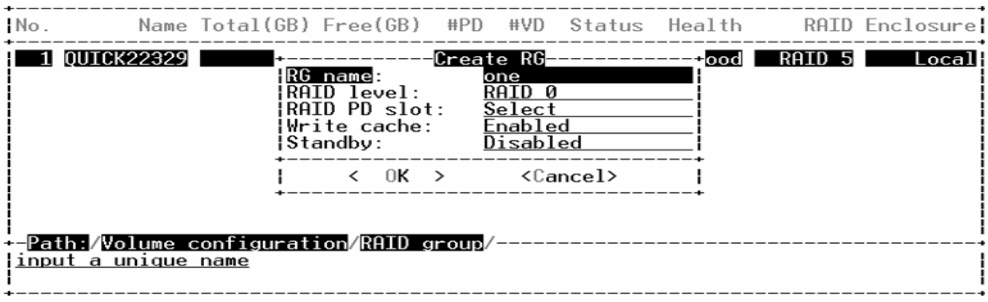
Step 1: Give the new RG a name.

Step 2: Select a RAID Level.

Step 3: Select hard disks to be used for RG.

Step 4: Setup write cache and standby mode policy.

Finally select **OK**.



Write cache options:

1. Enabled → Enable disk write cache.

2. Disabled → Disable disk write cache.

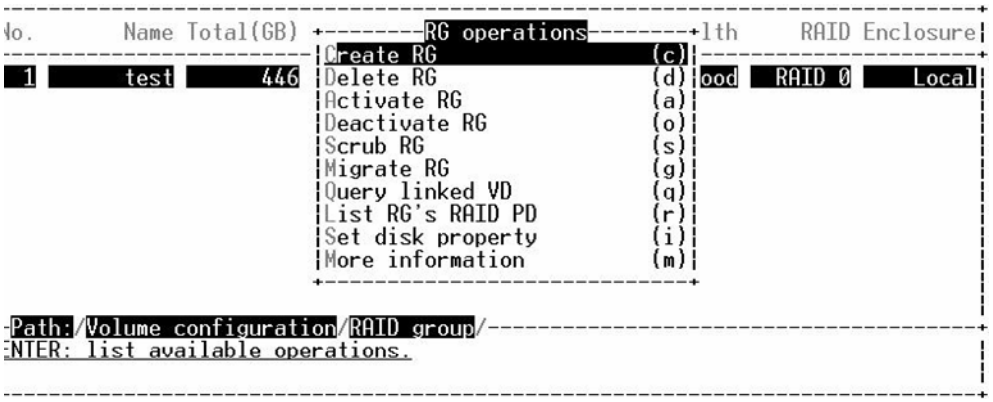
Standby options:

1. Disabled → Disable spin down.

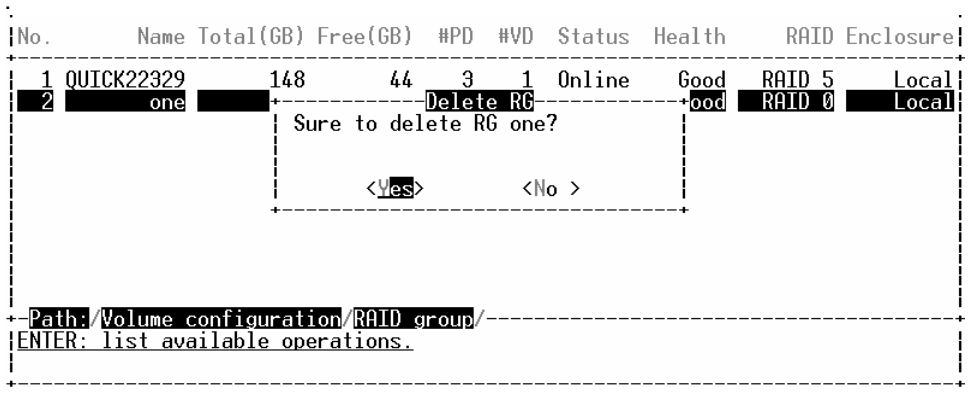
2. 30 sec / 1 min / 5 min / 30 min → Enable hard disk auto spin down to save power in the period of time.

RG can be created only when there are free hard disks available.

Below are the descriptions about this submenu of RG:



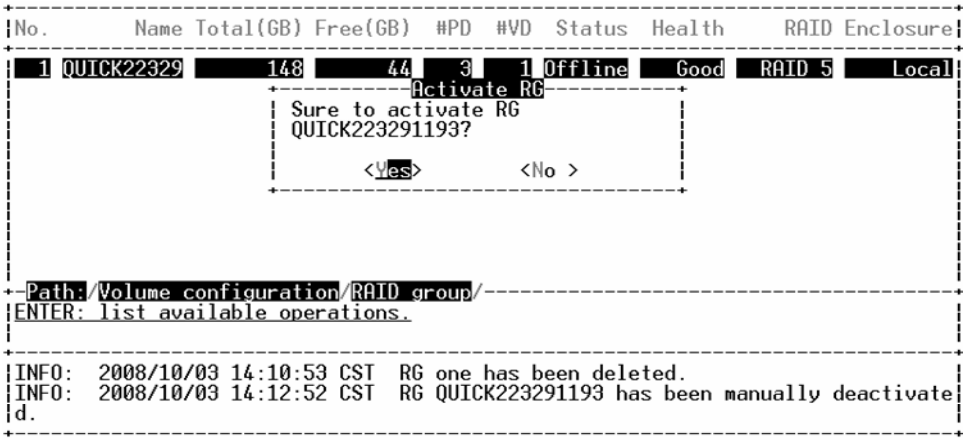
1. Select **"Delete RG"** to delete created RG.



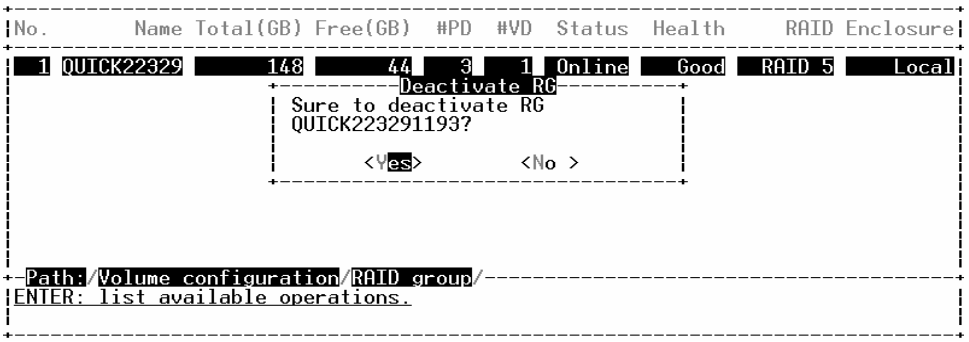
NOTE

RG can be deleted only when there is no created VD (Virtual disk) inside of the going-to-be-deleted RG.

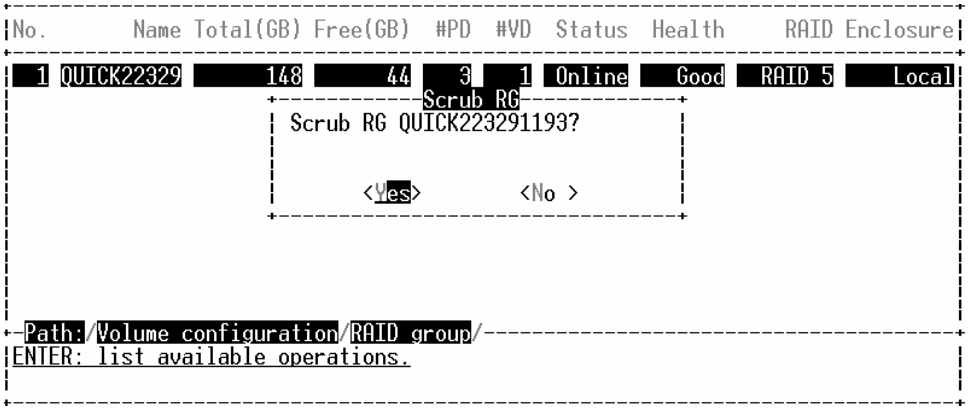
2. Select **"Activate RG"** to re-activate the deactivated RG. Activating a RAID group allows the users to restore the off-line status RAID group. After a RAID group is array roamed to another iSCSI RAID subsystem, the users have to execute this function to activate the moved RAID group.



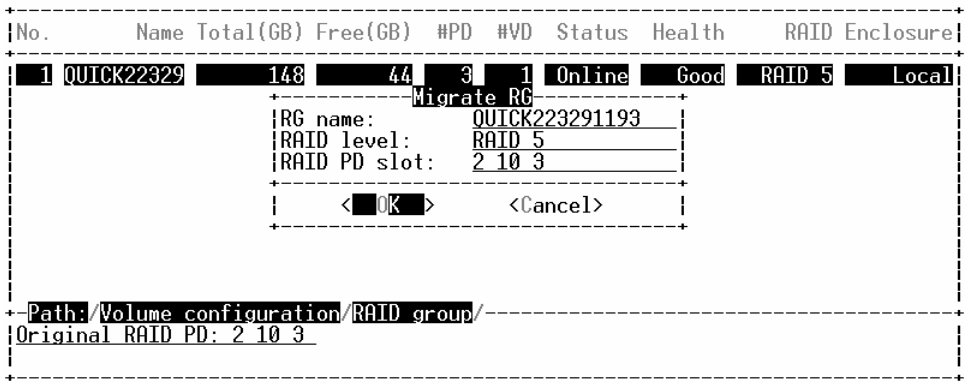
3. Select **"Deactivate RG"** to deactivate the active RGs. Deactivating a RAID group allows the users to array roam the whole RAID group to another iSCSI RAID subsystem without powering off the system.



4. Select **"Scrub RG"** to scrub a RAID group in order to remap bad blocks; this function is to make parity regeneration, supporting RAID 3 / 5 / 6 / 30 / 50 / 60 only.



5. Select **"Migrate RG"** to migrate the RAID level.



To do migration, the total size of RG must be larger or equal to the original RG. It does not allow expanding the same RAID level with the same hard disks of original RG.

The operation is not allowed when RG is being migrated. System would reject following operations:

1.Add dedicated spare.

2.Remove a dedicated spare.

3.Create a new VD.

4.Delete a VD.

5.Extend a VD.

6.Scrub a VD.

7.Perform yet another migration operation.

8.Scrub entire RG.

9.Take a new snapshot.

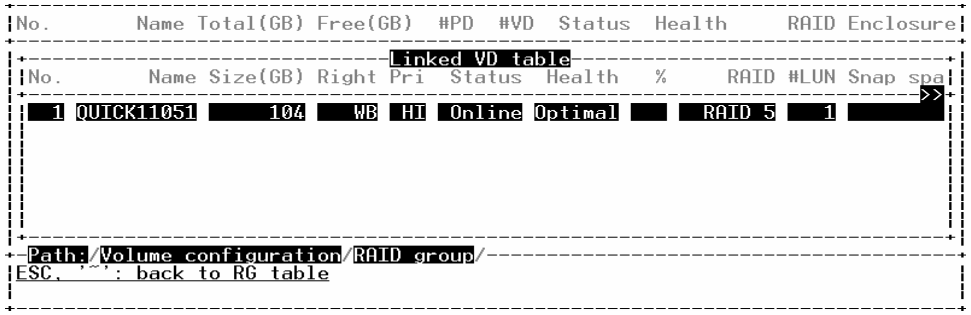
10.Delete an existing snapshot.

11.Export a snapshot.

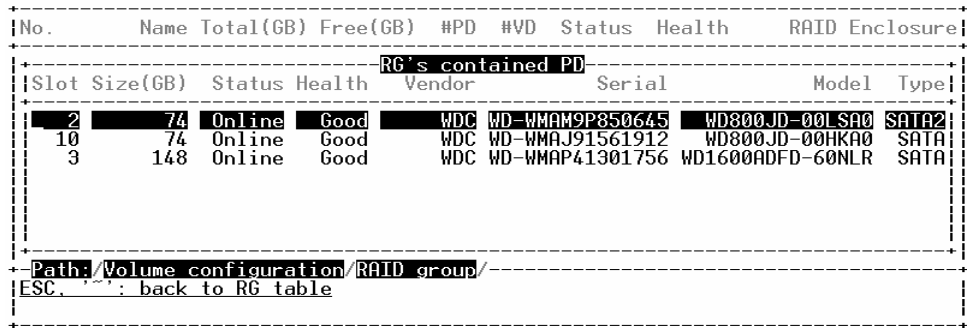
12.Rollback to a snapshot.

RG Migration cannot be executed during rebuild or VD extension.

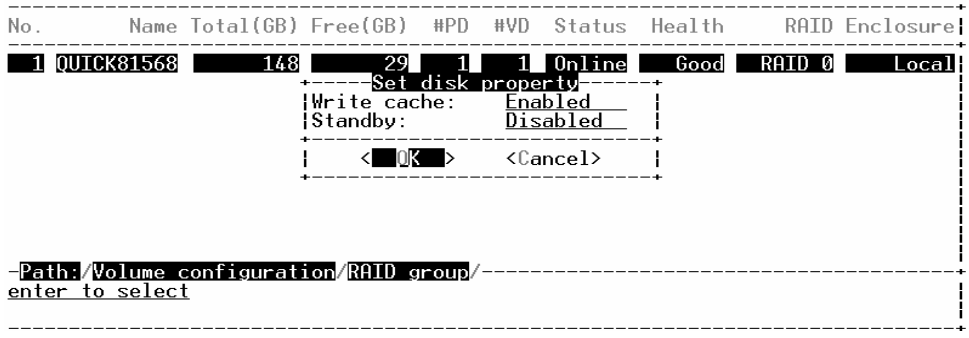
6. Select **"Query linked VD"** to display the created VD (Virtual disk) that is inside of the selected RG.



7. Select **"List RG's RAID PD"** to view which hard disks are used by the selected RG.



8. Select **"Set disk property"** to setup standby mode or enable\ disable write cache.



Write cache options:

1. Enabled → Enable disk write cache.

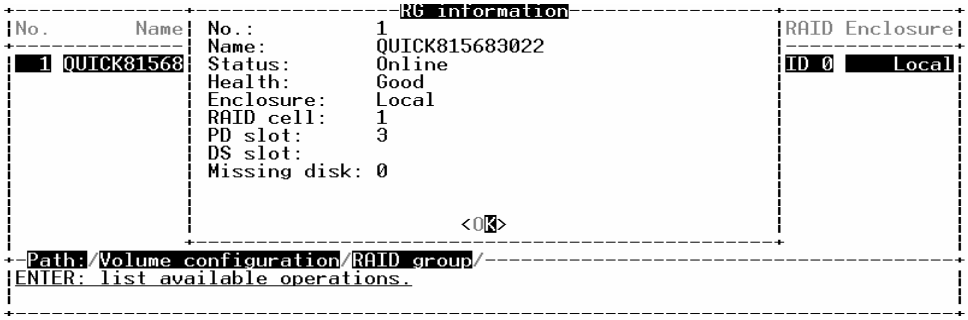
2. Disabled → Disable disk write cache.

Standby options:

1. Disabled → Disable spin down.

2. 30 sec / 1 min / 5 min / 30 min → Enable hard disk auto spin down to save power in the period of time.

9. Select “More information” to view detailed RG information.



5.5.4 Virtual disk

“Virtual disk” can allow the users to create VD, view the status of each VD, and so on.

To create a VD (Virtual disk), please take the steps as below:

Step 1: Give the new VD a name.

Step 2: Select an existing RG.

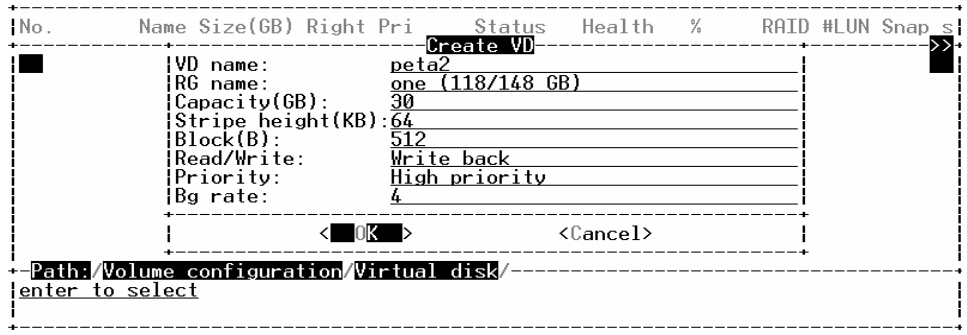
Step 3: Select VD capacity

Step 4: Select stripe size, and block size.

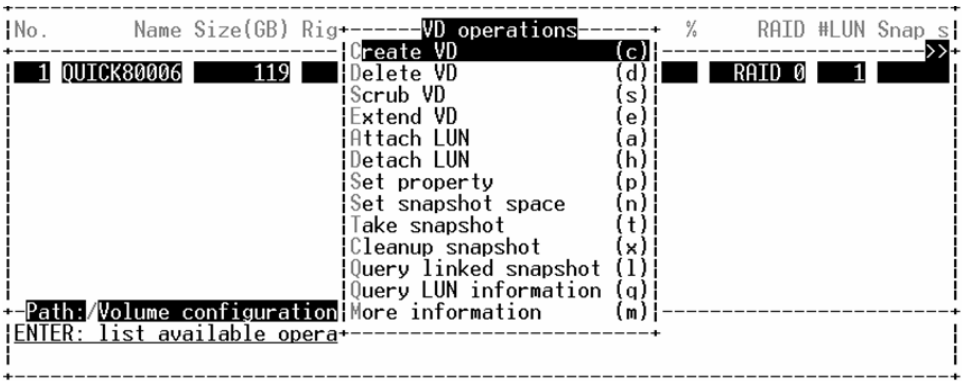
Step 5: Select write back or write through

Step 6: Select priority, and Bg rate.

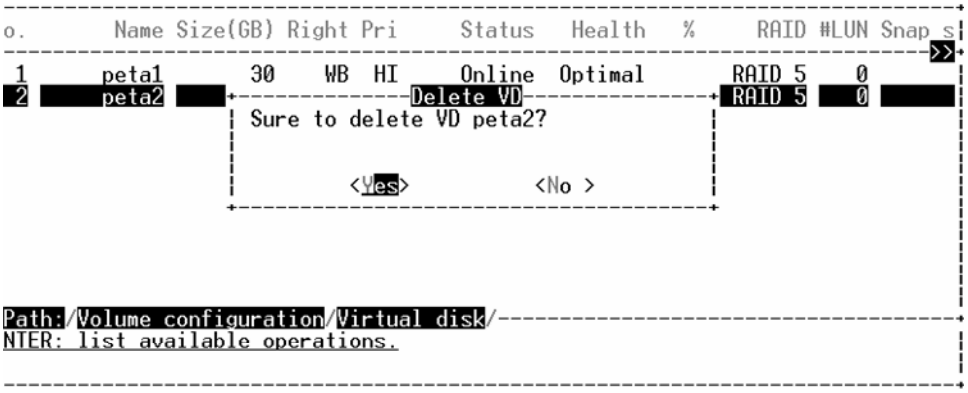
Finally select **OK**.



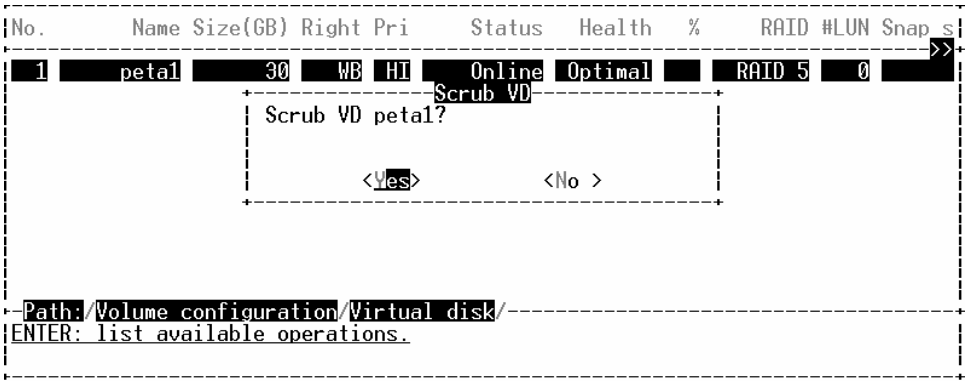
Below are the descriptions about this submenu of RG:



1. Select **“Delete VD”** to delete existing VDs.



2. Select **“Scrub VD”** to scrub a VD in order to remap bad blocks; this function is to make parity regeneration, supporting RAID 3 / 5 / 6 / 30 / 50 / 60 only.



3. Select **"Extend VD"** to extend the existing VD capacity.

1.*The capacity of VD extension must be larger than original.*

2.*VD Extension cannot be executed during rebuild or migration.*

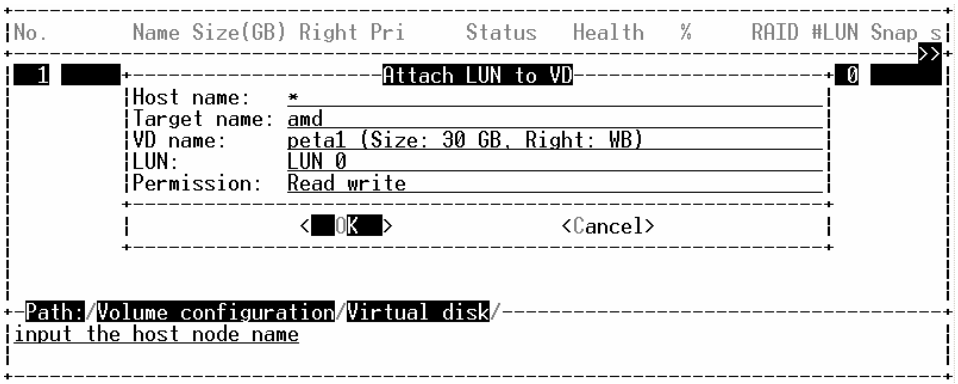
4. Select **"Attach LUN"** to attach LUN to a VD. Please follow the steps as below:

Step 1: Input "Host" name, or fill-in wildcard **"*",** which means every host can access to this volume.

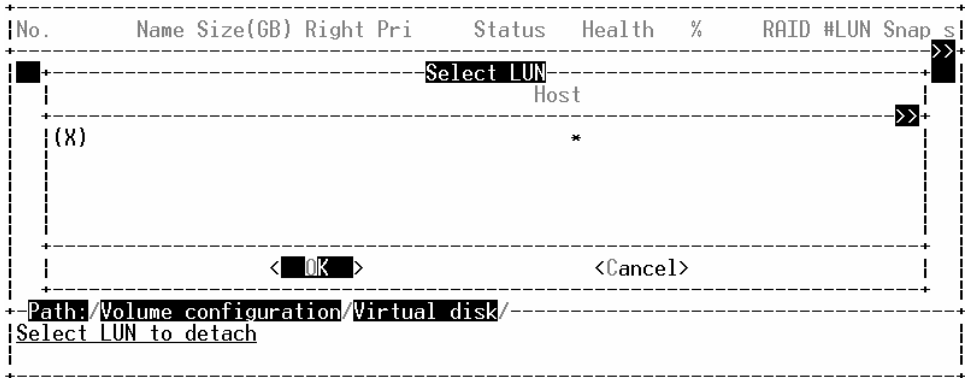
Step 2: Select target name and existing VD.

Step 3: Choose LUN

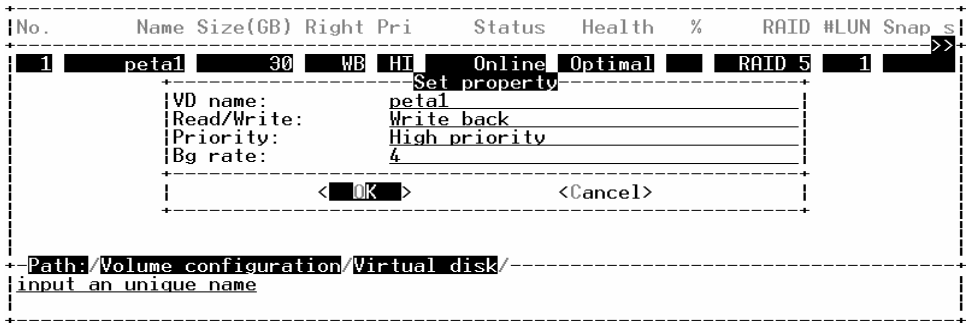
Step 4: Select permission to make the VD read-only or read /written.



5. Select **"Detach LUN"** to detach LUN from a VD.



6. Select **"Set property"** to change read/write policy, and priority/ Bg rate configurations.



A. Read / Write

Write-Back Cache: When the system writes to a memory location that is currently held in cache, it only writes the new information to the appropriate cache line. When the cache line is eventually needed for some other memory address, the changed data is "written back" to system memory. This type of cache provides better performance than a write-through cache, because it saves on (time-consuming) write cycles to memory.

Write-Through Cache: When the system writes to a memory location that is currently held in cache, it writes the new information both to the appropriate cache line and the memory location itself at the same time. This type of caching provides worse performance than write-back, but is simpler to implement and has the advantage of internal consistency, because the cache is never out of sync with the memory the way it is with a write-back cache.

Read Only: VD can is set to "read only".

B. Priority

a. High priority

b. Mid priority

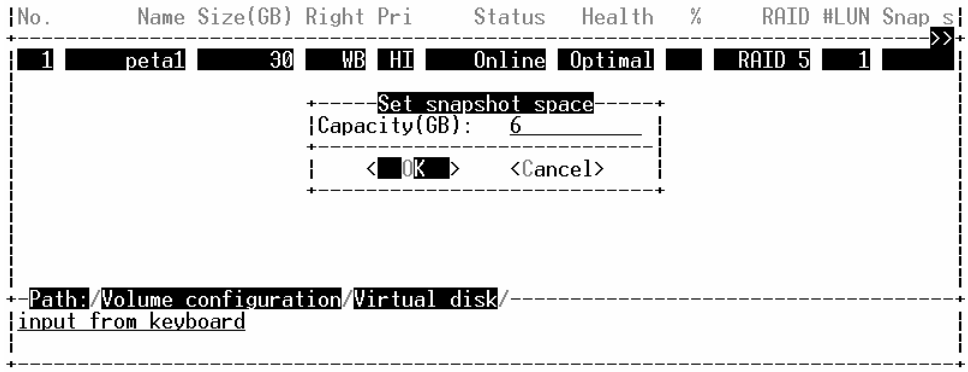
c. Low priority

This function is used to set the priorities of RAID level initialization and I/O accessing for the case of multiple VDs.

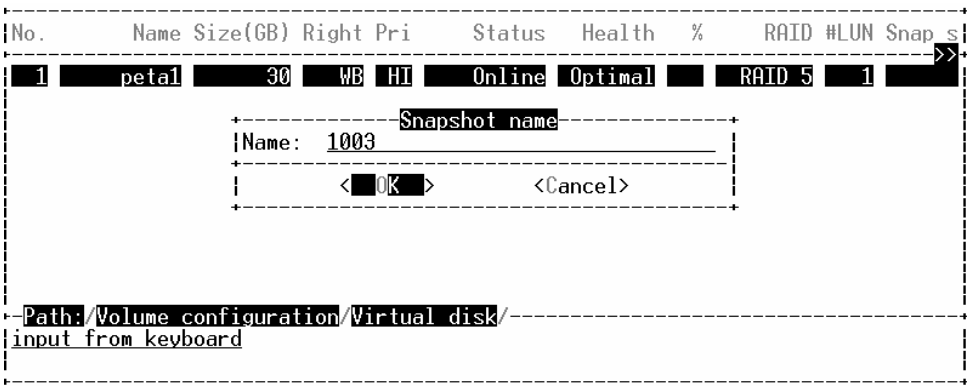
C. Bg Rate

"4 / 3 / 2 / 1 / 0" → Default value is 4. The higher number the background priority of a VD has, the more background I/O will be scheduled to execute.

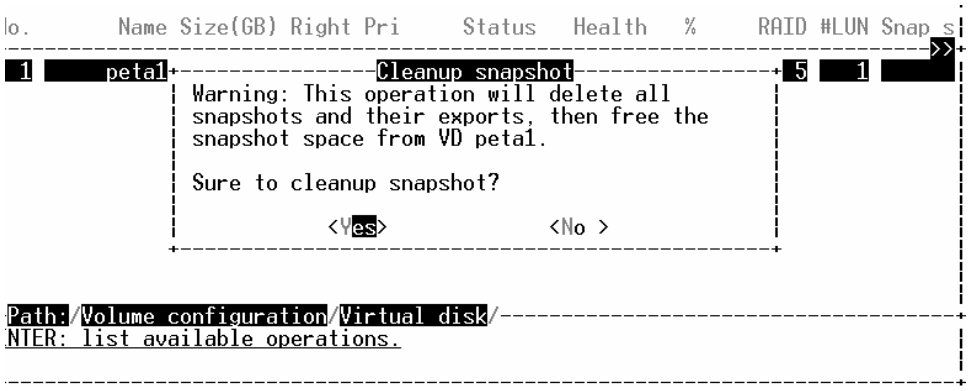
7. Select **"Set snapshot space"** to setup the size for snapshot to use. The minimum size is suggested to be **20%** of VD size.



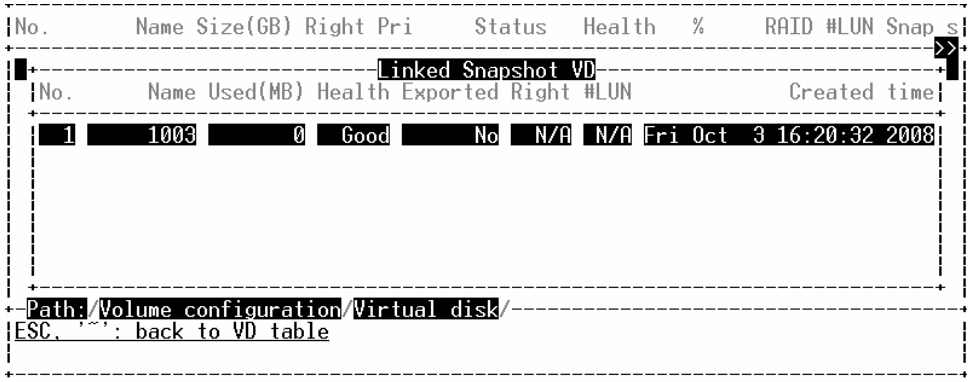
8. Select **"Take snapshot"** to take a snapshot.



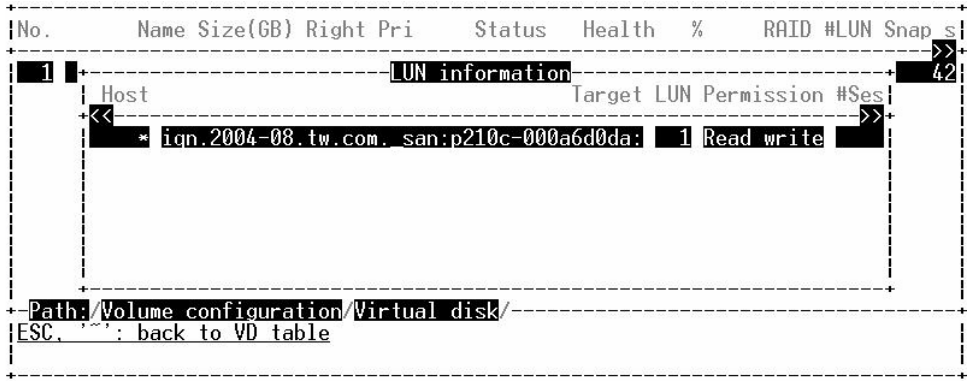
9. Select **"Cleanup snapshot"** to clean up the existing snapshots.



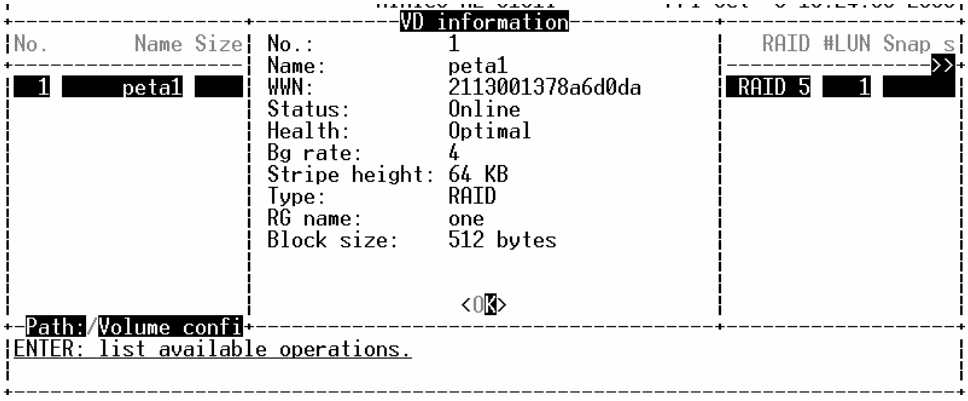
10. Select **"Query linked snapshot"** to view the taken snapshots.



11. Select **"Query LUN information"** to view the LUNs presently used.



12. Select **"More information"** to view detailed VD information.

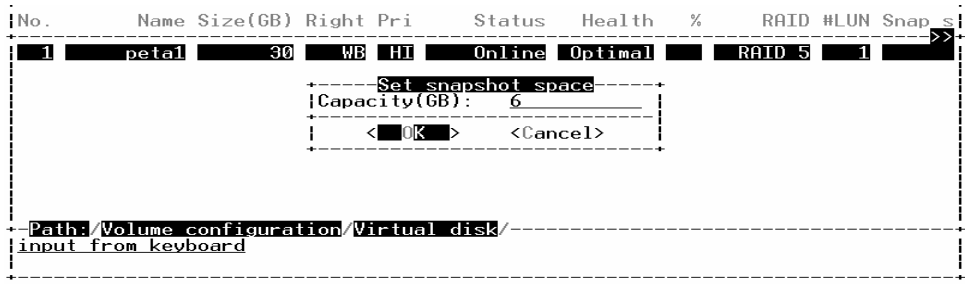


5.5.5 Snapshot

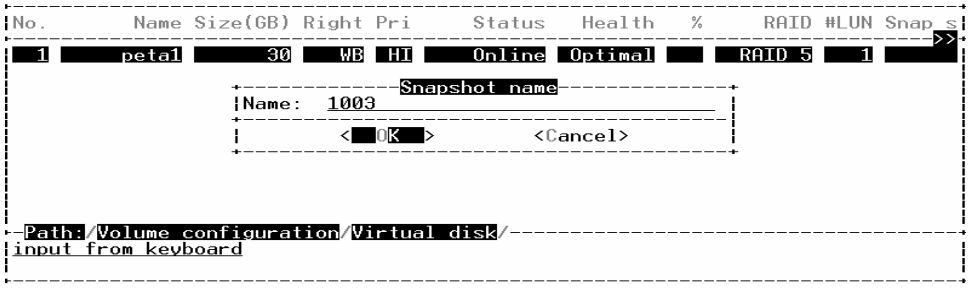
Snapshot-on-the-box captures the instant state of data stored in the target volume in a logical sense. The underlying logic is Copy-on-Write -- moving out the data which would be written to certain location where a write action occurs since the time of data capture. The certain location, named as “Snap VD”, is essentially a new VD.which can be attached to a LUN provisioned for a host as a disk like other ordinary VDs in the system. Rollback restores the data back to the state of any time which was previously captured in case for any unfortunate reason it might be (e.g. virus attack, data corruption, human errors and so on). Snap VD is allocated within the same RG in which the snapshot is taken, we suggest to reserve 20% of RG size or more for snapshot space. Snapshot / rollback features need **512MB** RAM at least.

Below are the steps to create a snapshot:

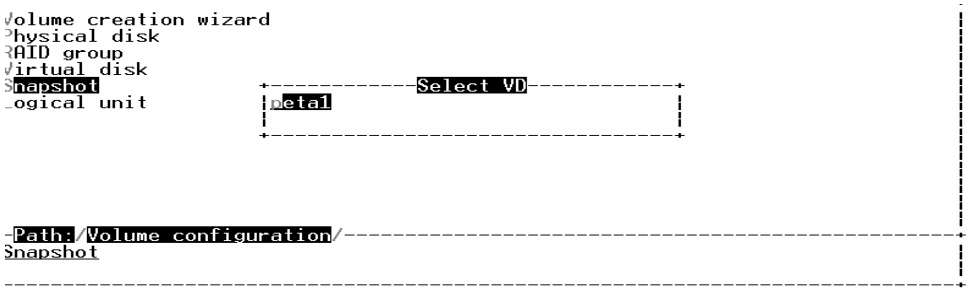
Step 1: Select **“Set snapshot space”** from **“Volume configuration/Virtual disk/”**.



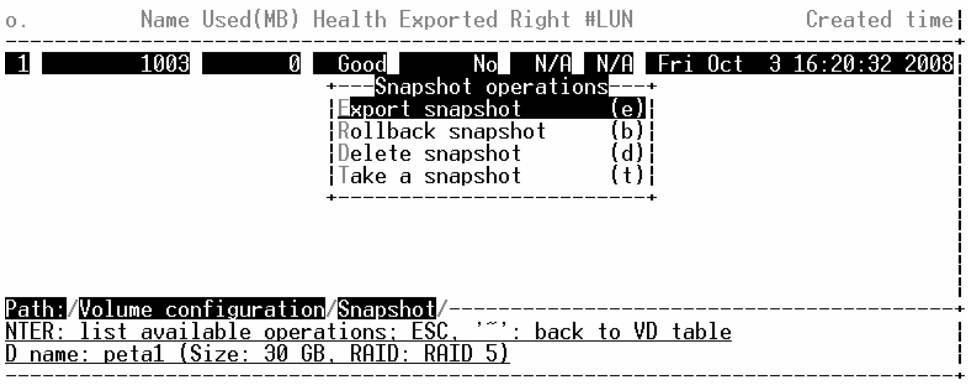
Step 2: Select **“Take a snapshot”** from **“Volume configuration/Virtual disk/”**.



Step 3 Select a VD that has snapshots taken.



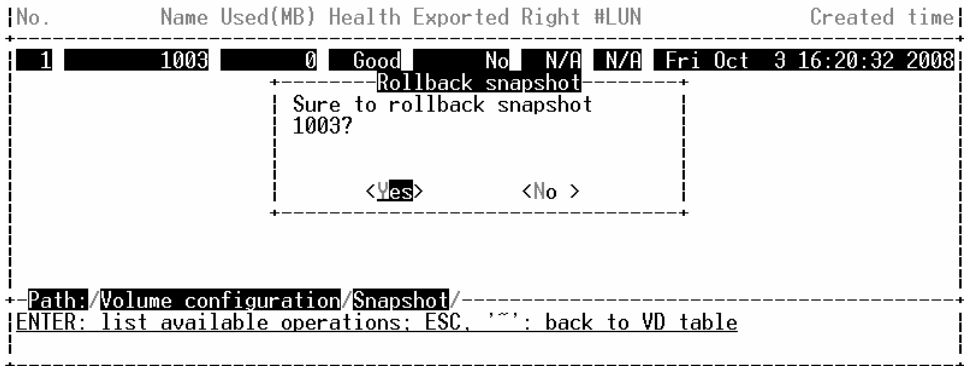
Below are the descriptions about this submenu of Snapshot:



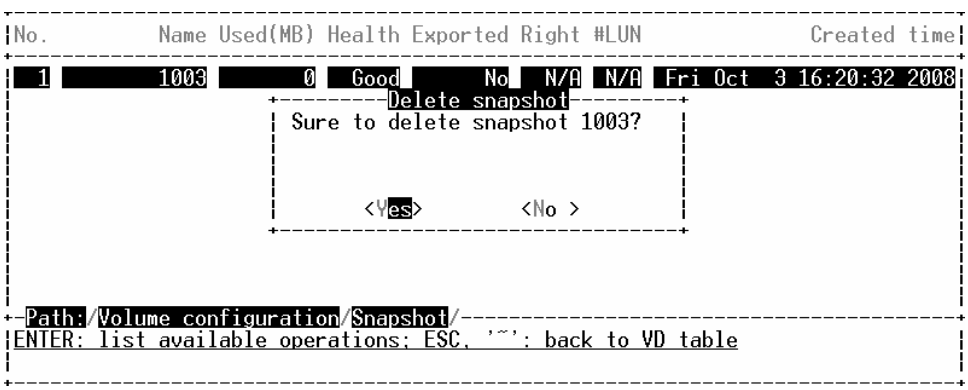
1. Select **"Export snapshot"** to export snapshot VD.

Enter a capacity for the about-to-be exported snapshot VD. If no capacity is entered, the exported snapshot VD will be read only. Otherwise, the exported snapshot VD can be read/written, and the entered capacity will be the maximum capacity to read/write.

2. Select **"Rollback snapshot"** to get the data in snapshot VD rollbacked to original VD.



3. Select **"Delete snapshot"** to delete existing snapshot VD



4. Select **"Take a snapshot"** to take a snapshot from the original VD.

.

Snapshot has some constraints as follows:

1.Minimum RAM size of enabling snapshot is 512MB.

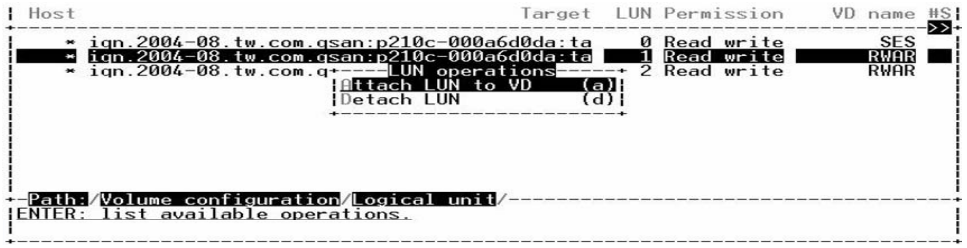
2.For performance and future rollback, system saves snapshot with names in sequences. For example, three snapshots has been taken and named “SnapVD-01”(first), “SnapVD-02” and “SnapVD-03”(last). When deleting “SnapVD-02”, both of “SnapVD-02” and “SnapVD-03” will be deleted because “SnapVD-03” is related to “SnapVD-02”.

3.For resource management, maximum number of snapshots in system is 32.

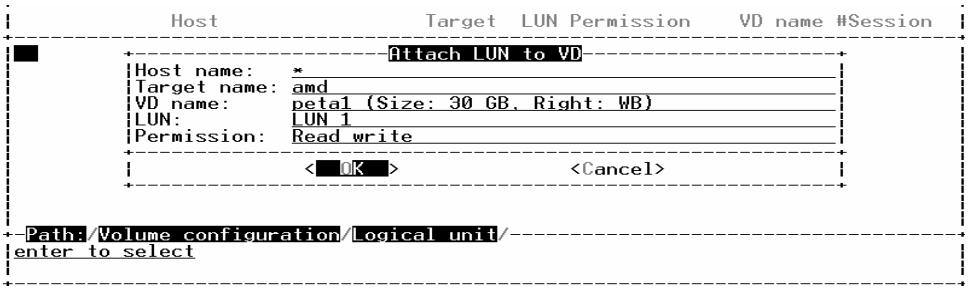
4.If the snapshot space is full, system will send a warning message of space full and the new taken snapshot will replace the oldest snapshot in rotational sequence by executing auto snapshot, but new snapshot can not be taken by manual because system does not know which snapshot VDs can be deleted.

5.5.6 Logical unit

“Logical unit” can view the status of attached logical unit number of each VD. The users can also attach LUN to or detach LUN from the existing VDs or snapshot VDs.



1. Select **“Attach LUN to VD”** to attach a logical unit number to a VD.



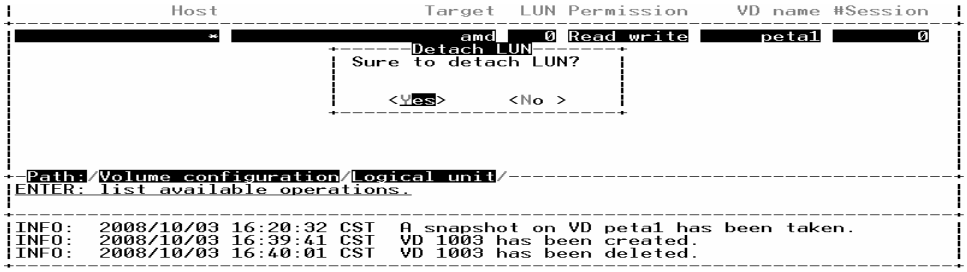
Below are the steps:

Step 1: Input “Host” name, or fill-in wildcard **“*”,** which means every host can access to this volume.

Step 2: Select target name and existing VD.

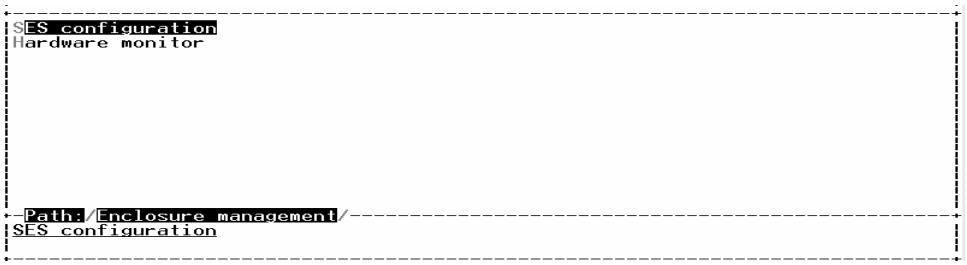
Step 3: Choose LUN and permission for the VD to be read only or be able to be read and written.

2. Select **"Detach VD"** to detach LUN from VD.



5.6 Enclosure management

"Enclosure management" allows the users to enable SES support, and view the current status of kinds of voltages and temperatures read from the monitored components.



To have the enclosure management work correctly, there are many sensors deployed inside of this iSCSI RAID subsystem for different purposes, such as temperature sensors, voltage sensors, hard disks, fan sensors, power sensors, and LED status. Depending on different hardware characteristics, the sensors have different polling intervals.

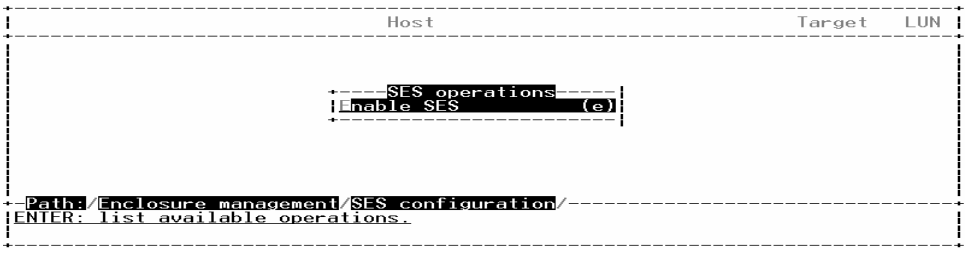
Below are the details of polling time intervals:

1. Temperature sensors: 1 minute.
2. Voltage sensors: 1 minute.
3. Hard disk sensors: 10 minutes.
4. Fan sensors: 10 seconds . When there are 3 errors consecutively, controller sends ERROR event log.
5. Power sensors: 10 seconds, when there are 3 errors consecutively, controller sends ERROR event log.
6. LED status: 10 seconds.

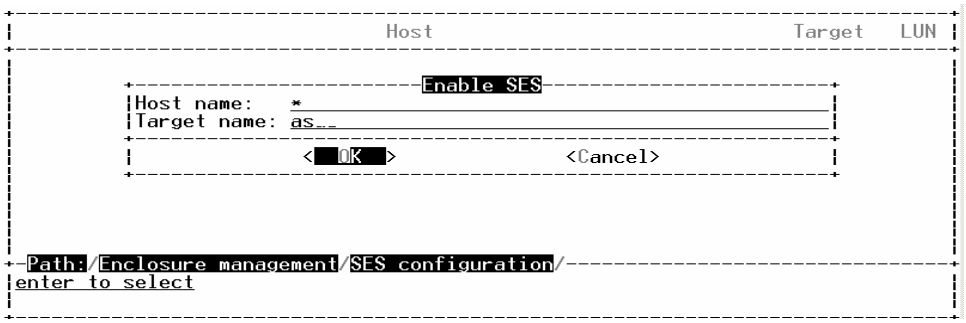
5.6.1 SES configuration

Most recent SCSI enclosure products support a protocol called **SCSI Enclosure Services** (SES). The initiator communicates with the enclosure using a specialized set of SCSI commands to access power, cooling, and other non-data characteristics.

To enable or disable the SES support, please select **"SES Configuration"**, then press the enter key.



Then, select Host name, and Target name.



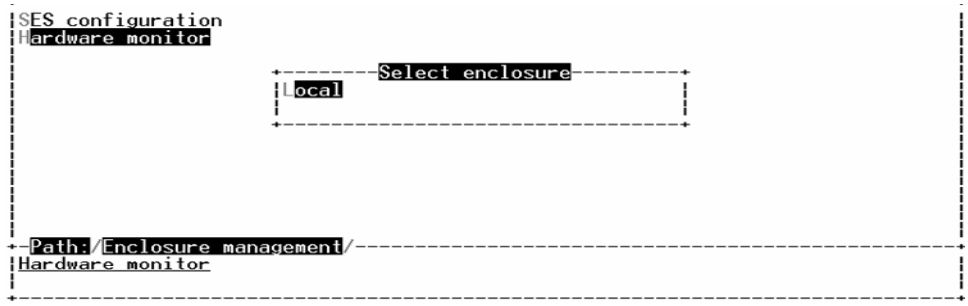
The SES client software is also available at the following web site:

SANtools: http://www.santools.com/

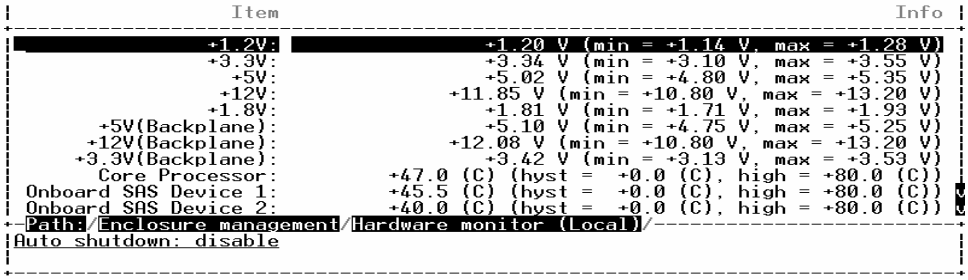
5.6.2 Hardware monitor

"Hardware monitor" allows the users to view all the information about the current status of kinds of voltages and temperatures read from the monitored components.

Step 1: Select enclosure



Step 2: Press the enter key to view the hardware monitor.



If "Auto shutdown" has been checked, this iSCSI RAID subsystem will shutdown automatically when monitored voltage or temperature is out of the normal range. For securer system and data protection, please check "Auto Shutdown". To avoid the possibility of system auto shutdown that is triggered by any single short period of high temperature or abnormal voltage, this iSCSI RAID subsystem uses multiple condition judgments for auto shutdown; below are the details about the conditions under which the auto shutdown will be triggered automatically:

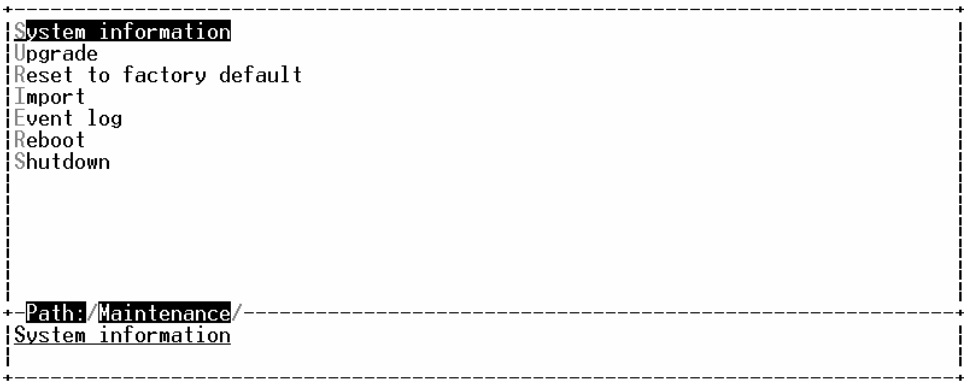
1. There are 3 sensors deploayed on the RAID controllers for monitoring temperature; one is on the core processor, another is on the PCI-X bridge, and the final one is on the daughter board. The RAID controller will check each sensor every 30 seconds. When one of these sensor is over high temperature for 3 minutes continuously, auto shutdown will be triggered immediately.

2. The core processor temperature limit is 85℃. The PCI-X bridge temperature limit is 80 ℃. The daughter board temperature limit is 80℃.

3. If the high temperature situation doesn't last for 3 minutes continuously, the RAID controller will not launch auto shutdown.

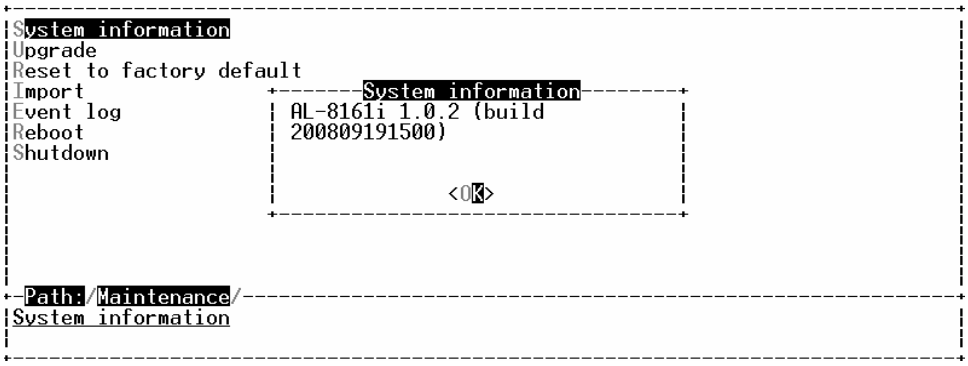
5.7 Maintenance

"Maintenance" allows the users to take the following operations that include "System information" to view this iSCSI RAID subsystem main information, "Upgrade" to upgrade this iSCSI RAID subsystem firmware version, "Reset to factory default" to reset all the RAID controller configurations to the factory configurations, "Import and export" to import and export all the RAID controller configurations , "Event log" to view this iSCSI RAID subsystem event logs, and "Reboot and shutdown" to either reboot or shutdown this iSCSI RAID subsystem.



5.7.1 System information

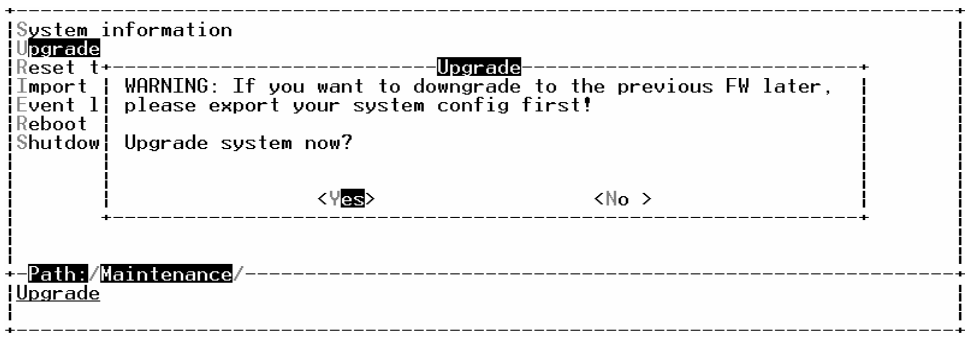
“System information” can display this iSCSI RAID subsystem used firmware version information.



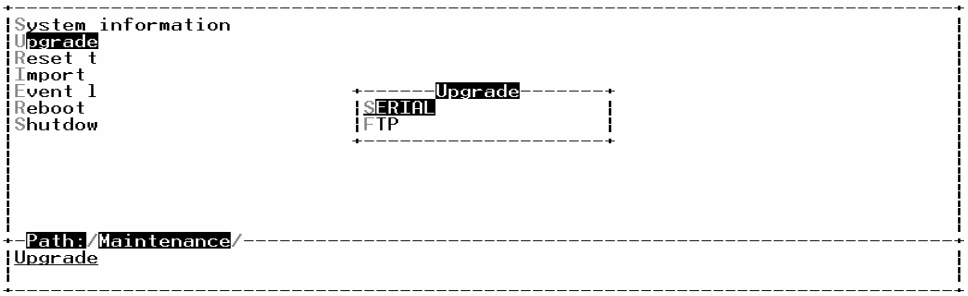
5.7.2 Upgrade

“Upgrade” allows the users to upgrade the firmware version.

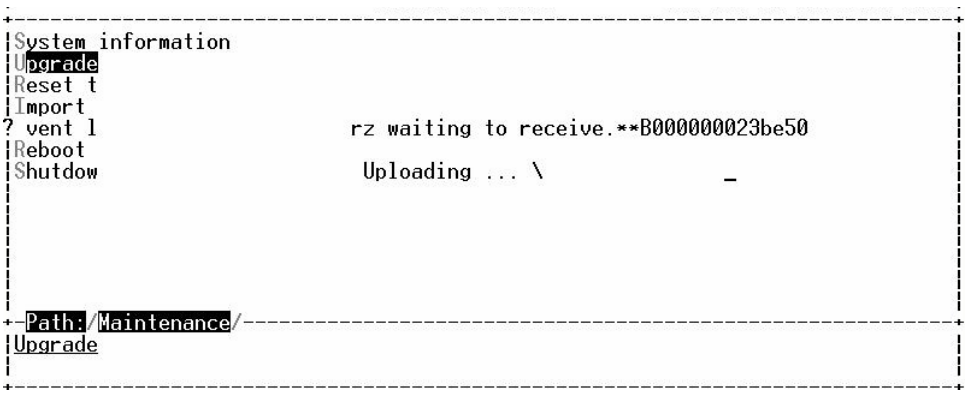
Step 1: Warn the user to export current system configurations before firmware upgrading processes.



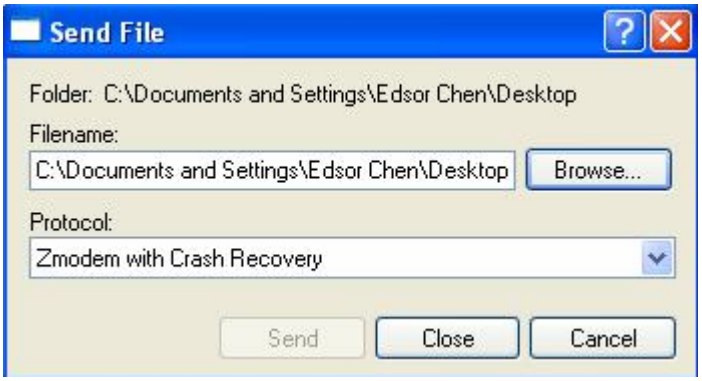
Step 2: Upgrading firmware via Serial Port or FTP.



Step 3: Wait the user to load in the firmware file that will be used to upgrade the old firmware version.

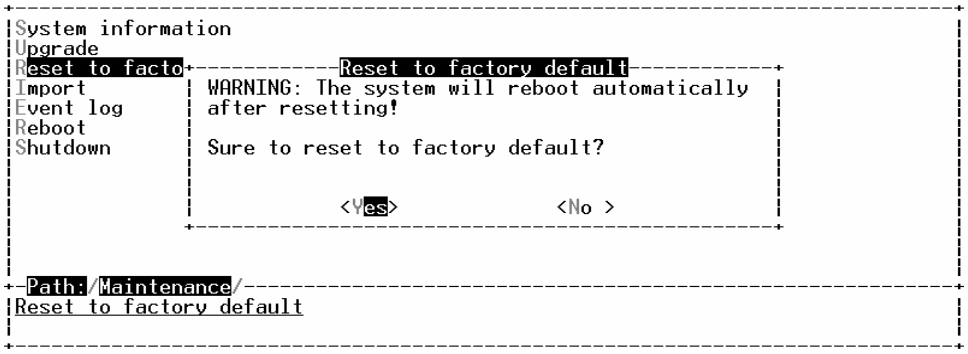


Step 4: Run “Send File” of HyperTerminal. Then load in the right firmware file. The protocol must be **“Zmodem”** or **“Zmodem with Crash Recovery**”.



5.7.3 Reset to factory default

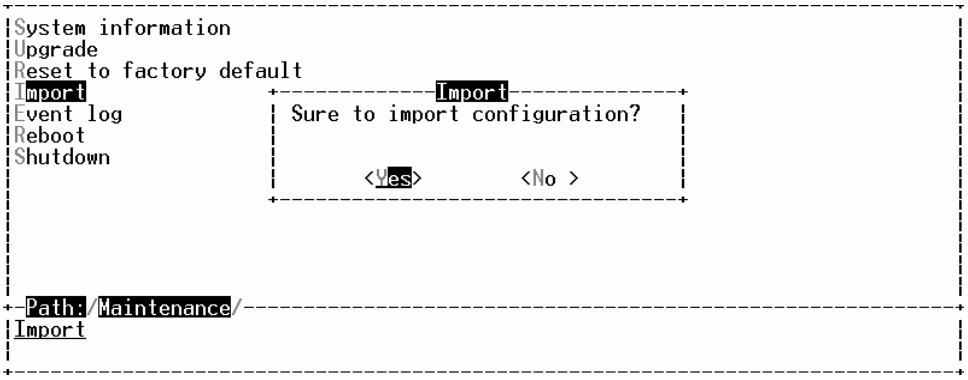
“Reset to factory default” allows the users to reset the RAID controller configurations to the factory default configurations.



Resetting to factory default will also get the password and user name back to the factory default ones. The factory default user name is **"admin"**, the password is **"0000"**.

5.7.4 Import and export

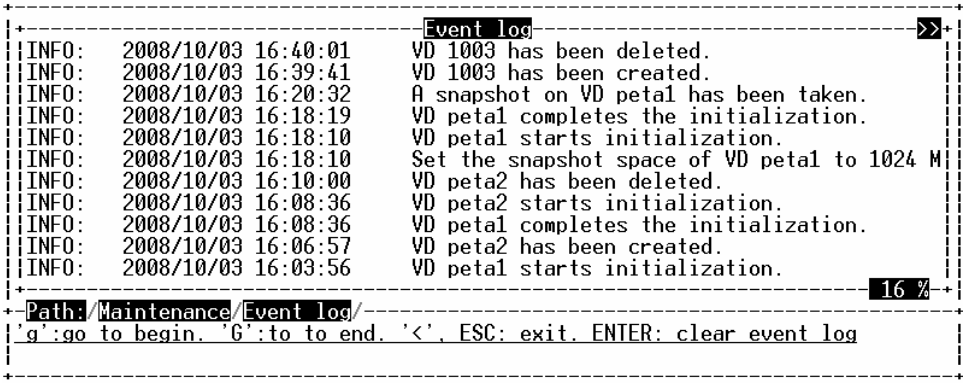
"Import": Import all the RAID controller configurations excluding volume configuration back into this iSCSI RAID subsystem.



For the volume configuration setting, the values are not available in Import to avoid confliction/date-deleting between two RAID controllers. That is, if a RAID controller keeps valuable data in the disks and the user may forget to overwrite it, using import could get all the original configuration back. But if the volume setting is also imported, the user's current data will be overwritten.

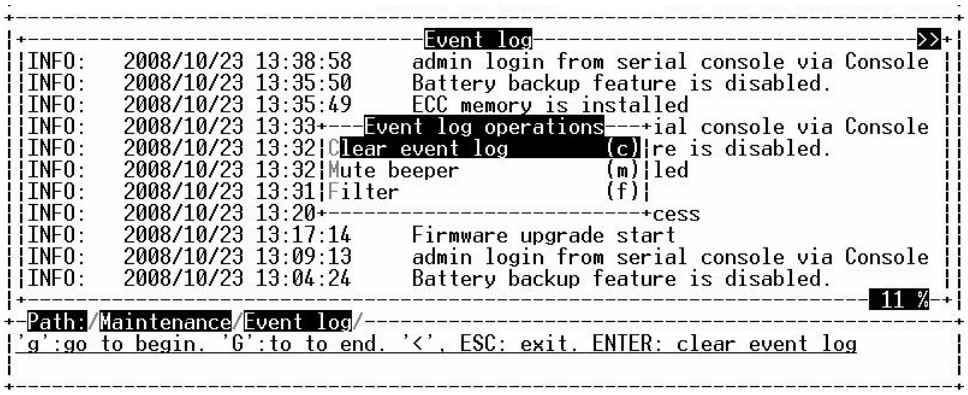
5.7.5 Event log

"Event log" can view the event messages.



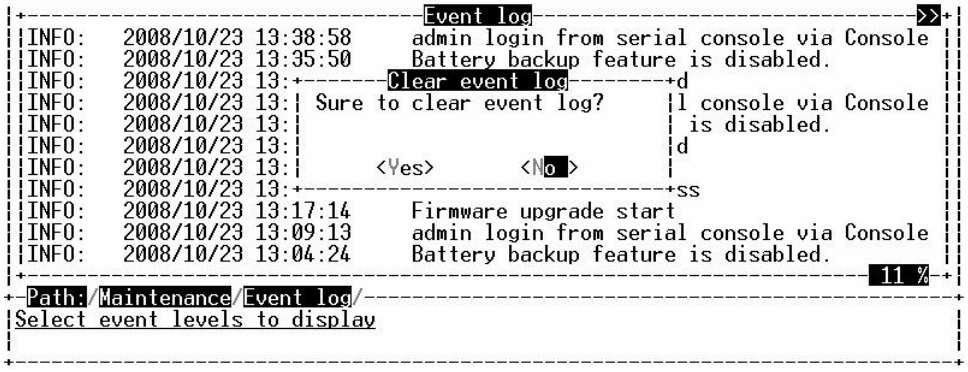
The event log is displayed in reverse order which means the latest event log is always listed on the first page. The event logs are actually saved in the first four hard disks; each hard disk has one copy of the complete event logs. For one controller, there are four copies of event logs to ensure the users can check event log any time even though there is one or two hard disks fail simultaneously.

Press the enter key to call up a submenu

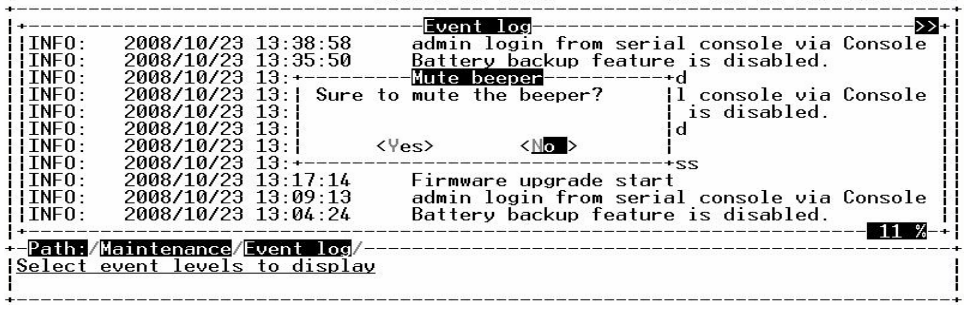


Below are the function descriptions of the event log submenu:

1. Select **"Clear event log"** to clear event log.



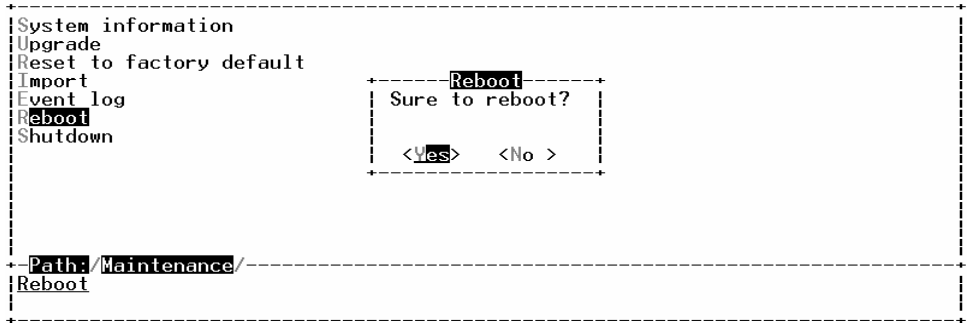
2. Select **"Mute beeper"** to stop system alarm.



3. Select **"Filter"** to decide the level of display event log. There are three levels: INFO, WARNING, and ERROR.

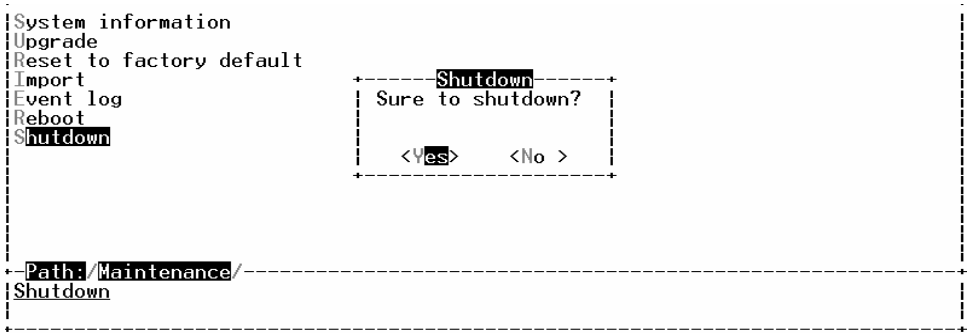
5.7.6 Reboot

"Reboot" allows the users to safely reboot this iSCSI RAID subsystem.



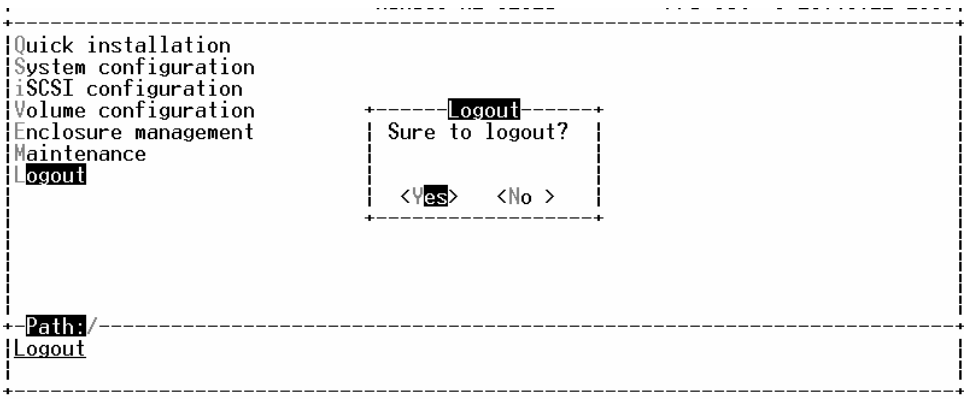
5.7.7 Shutdown

"Shutdown" allows the users to power off this iSCSI RAID subsystem with a safe way to prevent any data loss, because **Shutdown** execution gets this iSCSI RAID subsystem to flush the data from cache to physical disks first, a necessity for data protection.



5.8 Logout

For security reason, **"Logout"** allows the users to logout when there is no user is operating this iSCSI RAID subsystem. To re-login this iSCSI RAID subsystem, please enter the user name and password again.

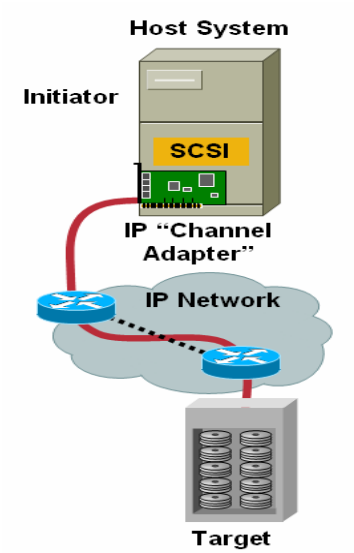

Quick installation
System configuration
iSCSI configuration
Volume configuration
Enclosure management
Maintenance
Logout
Logout
Sure to logout?
<Yes>
<No >
Path:/
Logout

Appendix A.

iSCSI & iSCSI Initiator

iSCSI Overview

iSCSI or Internet SCSI is a TCP/IP-based protocol that is mainly designed to be used for linking data storage devices over a network and enabling the transfer of data. Thereby, iSCSI offers a mechanism for capturing SCSI commands on an IP network, and carries SCSI commands over IP networks. Since iSCSI fully takes advantage of the ubiquitous TCP/IP-based Ethernet environments, it offers enormous potential for low-cost centralization of storage. Accordingly, if the customers want to make use of existing IT network infrastructure expertise to get into storage networking, iSCSI is an easy approach as well.



The main advantages of iSCSI include consolidated data storage systems, remote backup of data with easiness, more flexible and cost-effective server clustering deployments, and replication and recovery. Furthermore, since Microsoft released the first version of the iSCSI Software Initiator in June of 2003, storage over IP has accelerated storage area network adoption strikingly. That's because iSCSI offers the benefits of storage area networks (SANs).

IP SANs allow servers to attach to a number of storage volumes by using iSCSI over TCP/IP networks. IP SANs can scale the storage capacity coming from any type and brand of storage system. In addition, using any type of network (Ethernet, Fast Ethernet, Gigabit Ethernet) and combining operating systems within the SAN network. IP-SANs also include mechanisms for security, data replication, multi-path and high availability.

Finally, storage protocol plays a very important role behind iSCSI. Storage protocol in iSCSI, has “two ends” in the connection. The two ends are the initiator and the target. In iSCSI we call them iSCSI initiator and iSCSI target. The iSCSI initiator requests or initiates any iSCSI communication. It requests all SCSI operations like read or write. An initiator is usually located on the host/server side. The iSCSI target is the storage device itself or an appliance which controls and serves volumes or virtual volumes. The target is the device which performs SCSI commands or bridges it to an attached storage device. iSCSI targets can be disks, tapes, RAID arrays, tape libraries, and etc.

iSCSI Initiator Overview

An **initiator** functions as an iSCSI client. An initiator typically serves the same purpose to a computer as a SCSI bus adapter would, except that instead of physically cabling SCSI devices (like hard drives and tape changers), an iSCSI initiator sends SCSI commands over an IP network. An initiator falls into two broad types:

Software initiator

A software initiator uses code to implement iSCSI. Typically, this happens in a kernel-resident device driver that uses the existing NIC and network stack to emulate SCSI devices for a computer by speaking the iSCSI protocol. Software initiators are available for most mainstream operating systems, and this type is the most common mode of deploying iSCSI on computers.

Hardware initiator

A hardware initiator uses dedicated hardware, typically in combination with software (firmware) running on that hardware, to implement iSCSI. A hardware initiator mitigates the overhead of iSCSI and TCP processing and Ethernet interrupts, and therefore may improve the performance of servers that use iSCSI.

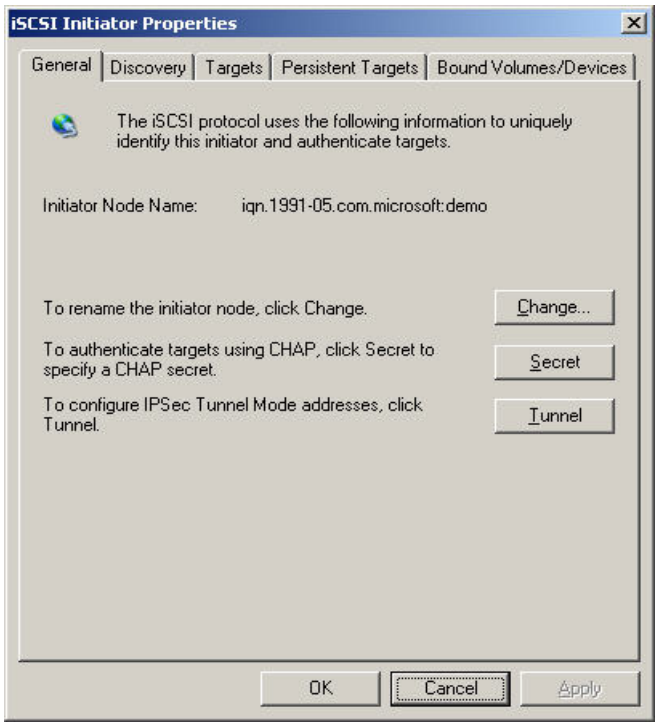
Below is an example about how to setup Microsoft iSCSI:

Below are the steps about how to setup Microsoft iSCSI Initiator. Please visit Microsoft website for latest iSCSI initiator. Microsoft iSCSI Initiator Download Linkage:

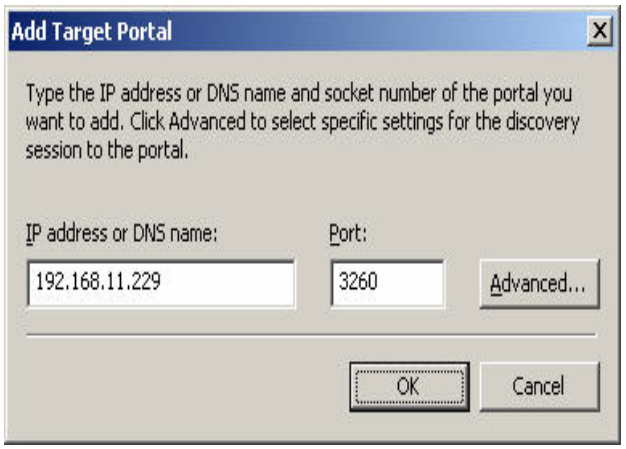
http://www.microsoft.com/downloads/details.aspx?familyid=12cb3c1a-15d6-45

85-b385-befd1319f825&displaylang=en

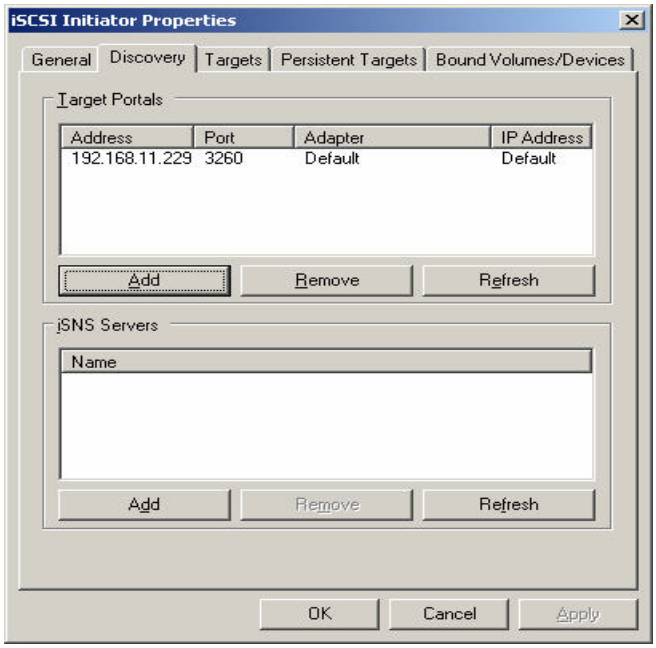
1. Run Microsoft iSCSI Initiator version 2.07.
2. Click **"Discovery".**



3. Click **"Add"**. Input IP address or DNS name of iSCSI storage device.

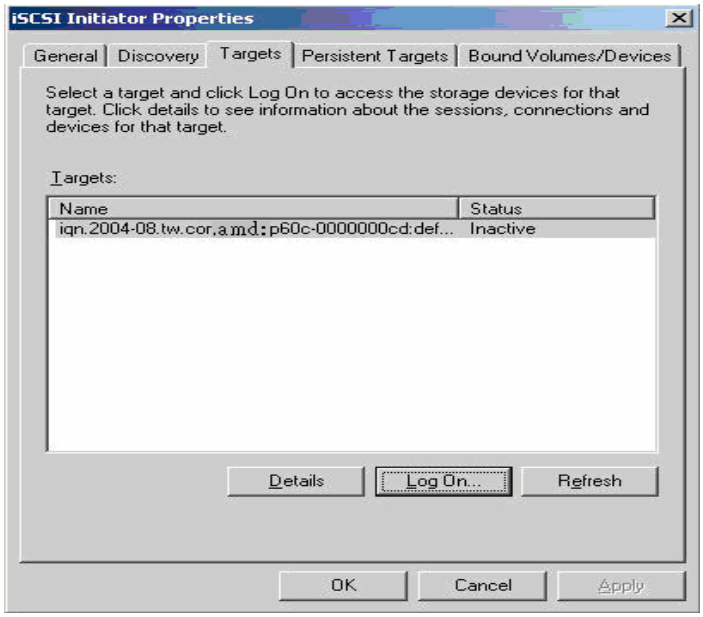


4. Click **"OK"**.

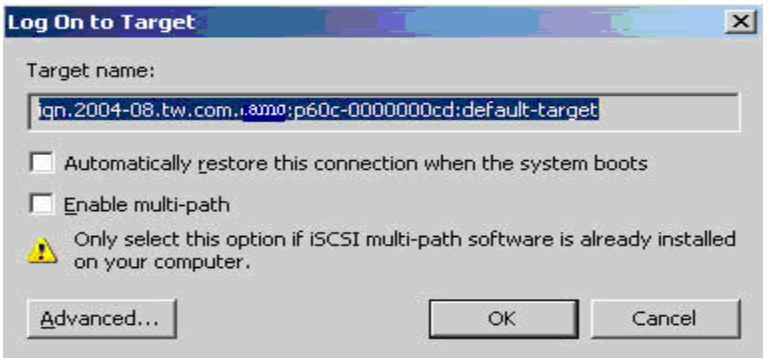


5. Click **"Targets"**. .

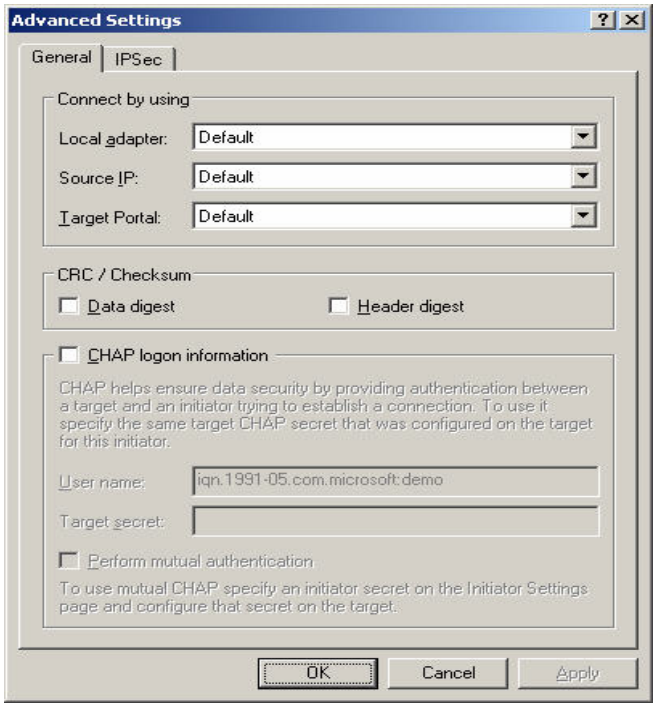
6. Click **"Log On"**. Check **"Enable multi-path"** if running MPIO.



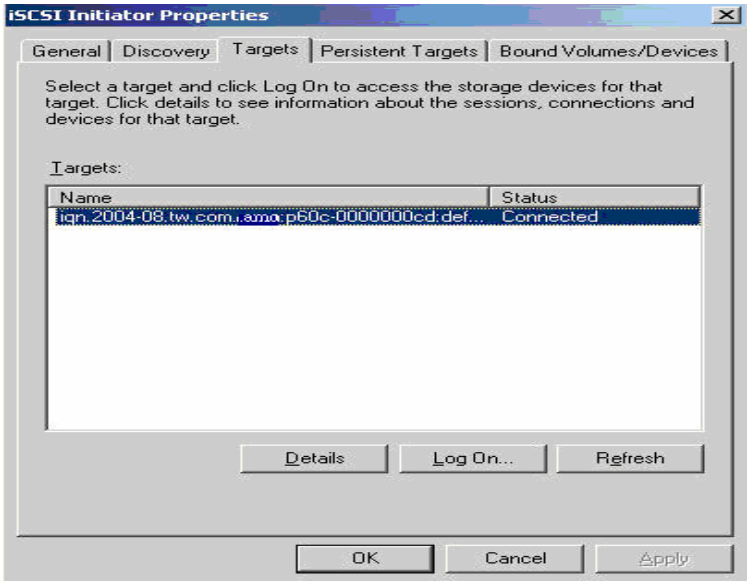
7. Click **"Advance…"** if CHAP information is needed.



8. Click **"OK"**. The status would be "Connected".

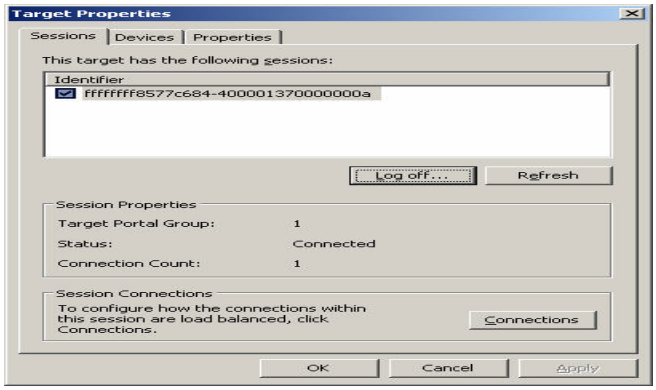


9. Done, it can connect to an iSCSI disk.



The steps below are to log off iSCSI device:

1. Click “Details”.



2. Check the Identifier, which will be deleted.
3. Click “Log off”.
4. Done, the iSCSI device log off successfully.

Appendix B.

iSCSI Advanced Applications and Configurations

MPIO and MC/S Overview

Storage area networks unlock storage from the server—storage resources are centralized onto a network, and provisioning and management are simplified. But to thoroughly safeguard your stored resources, each path between server and storage must be protected—a single link between the two is also a single point of failure, and if the link goes down, that server's access to storage is lost. With the appropriate software support, however, the administrator can implement a high availability solution through deployment of multiple paths between servers and storage. Multipathing provides an automatic means of persisting I/O without error, failing over the workload to a redundant path should one path fail.

The Microsoft iSCSI Software Initiator provides sophisticated high availability solutions through:

1. Multiple Connections per Session (MC/S)

MC/S allows multiple TCP/IP connections between the initiator (server) and target (storage array) during the same iSCSI session, either on the same or a different physical link. This allows load balancing and failover over among multiple network interface cards (NICs).

2. Microsoft MPIO support

Microsoft MPIO support allows the initiator to log in multiple sessions to

the same target, enabling load balancing and failover among multiple NICs and iSCSI Host Bus Adapters (HBAs).

Both methods support failover only (no load balancing, all other paths on standby), as well as a failover plus I/O load balancing. Load balancing policies include:

A. Round robin (all paths active, I/O sent in round robin fashion).

B. Round robin with a subset of active paths.

C. Weighted path, in which I/O is distributed to the path with the lowest assigned weight.

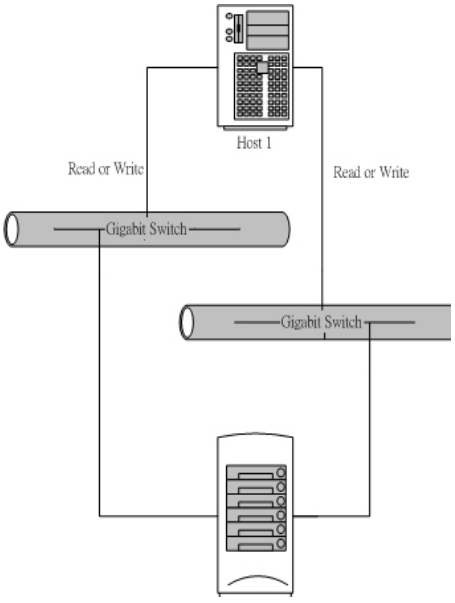
D. Least Queue Depth, in which I/O is sent on the path with the shortest I/O queue. This is only available for MC/S.

MPIO and MC/S setup instructions

Below are steps to setup MPIO. There are 2 kinds of scenarios for MPIO and MC/S. We suggest use scenario 2 for better performance.

Scenario 1

Scenario 2



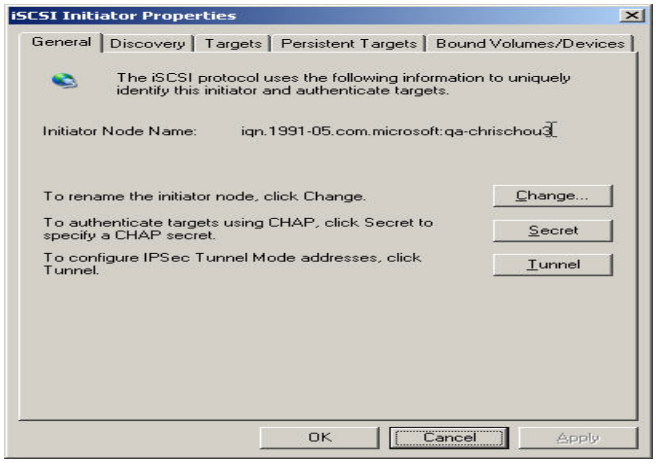
1. Create a RG (RAID group) with RAID 5, using 3 HDDs.

No.	Name	Total (GB)	Free (GB)	#PD	#VD	Status	Health	RAID
1	test	1862	1862	3	0	Online	Good	RAID 5

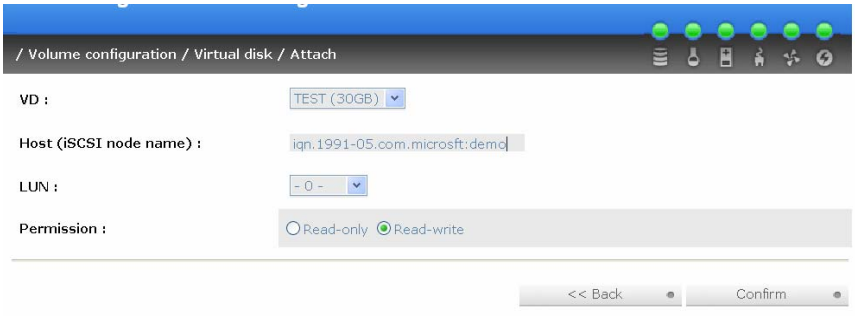
2. Create a VD (virtual disk) by using RAID 5 RG (RAID group).

No.	Name	Size (GB)	Right	Priority	Bg rate	Status	Health	R %	RAID	#LUN	Snapshot space (GB)	#Snapshot	RG name
1	TEST	30	WB	HI	4	Initiating	Optimal	58	RAID 5	0	0/0	0	test

3. Run Microsoft iSCSI initiator and check the Initiator Node Name.



4. Attaching LUN to R5 VD (virtual disk). Input the Initiator Node Name in host field.

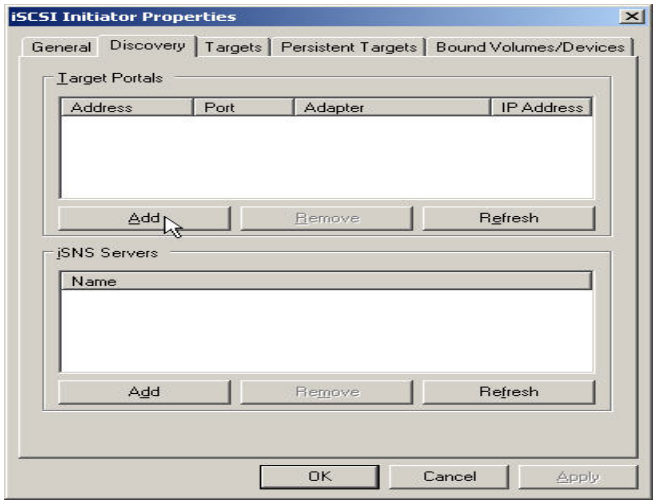


5. The volume config setting is done.

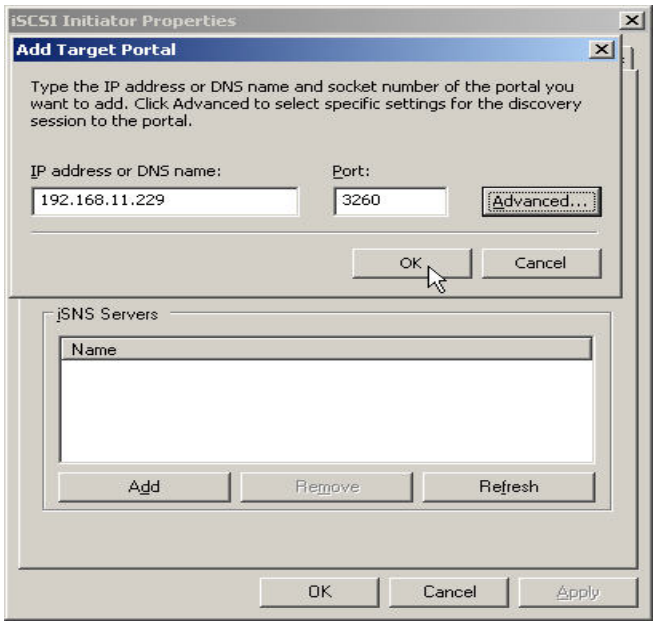
6. Check iSCSI settings. The IP address of iSCSI data port 1 is 192.168.11.229, port 2 is 192.168.12.229 for example.

Name	LAG	LAG No	DHCP	IP address	Netmask	Gateway	Jumbo frame	MAC address	Link
LAN1	No	N/A	No	192.168.11.229	255.255.255.0	192.168.11.254	Disabled	00:13:78:a8:07:58	Down
LAN2	No	N/A	No	192.168.12.229	255.255.255.0	192.168.12.254	Disabled	00:13:78:a8:07:59	Down

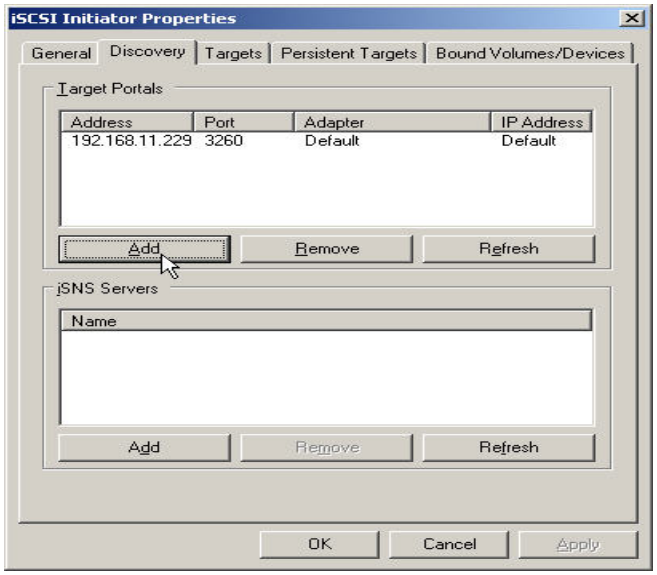
7. Add Target Portals on Microsoft iSCSI initiator 2.07.



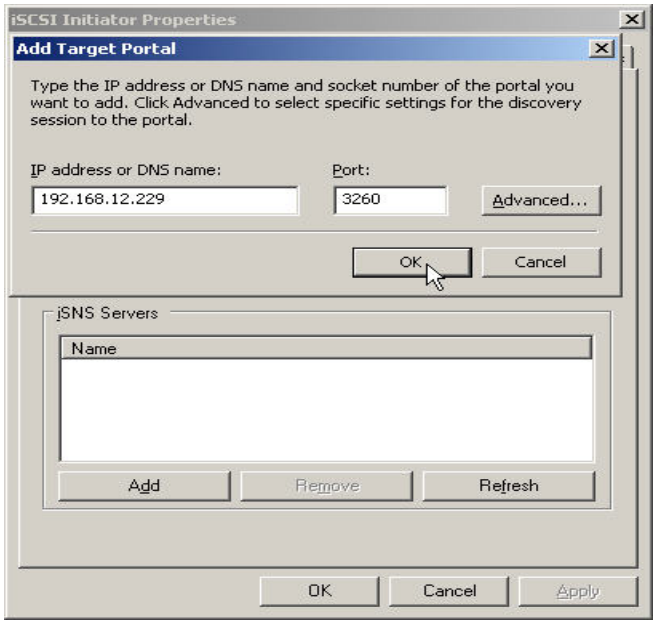
8. Input the IP address of iSCSI data port 1 (192.168.11.229 as mentioned in previous page).



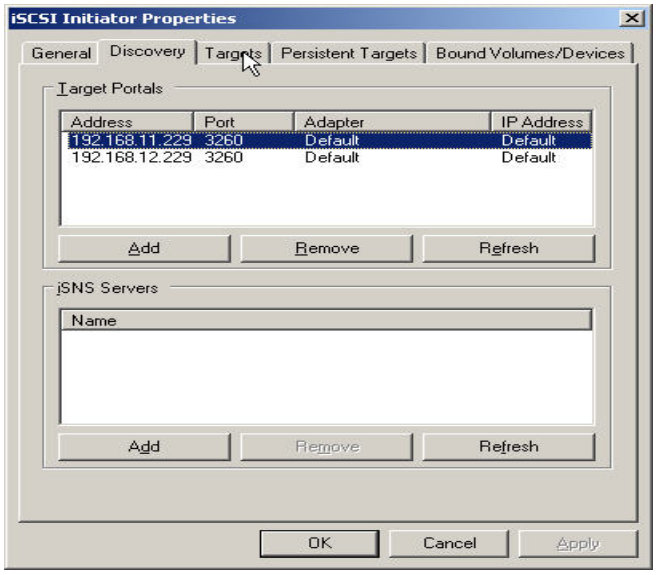
9. Add second Target Portals on Microsoft iSCSI initiator 2.07.



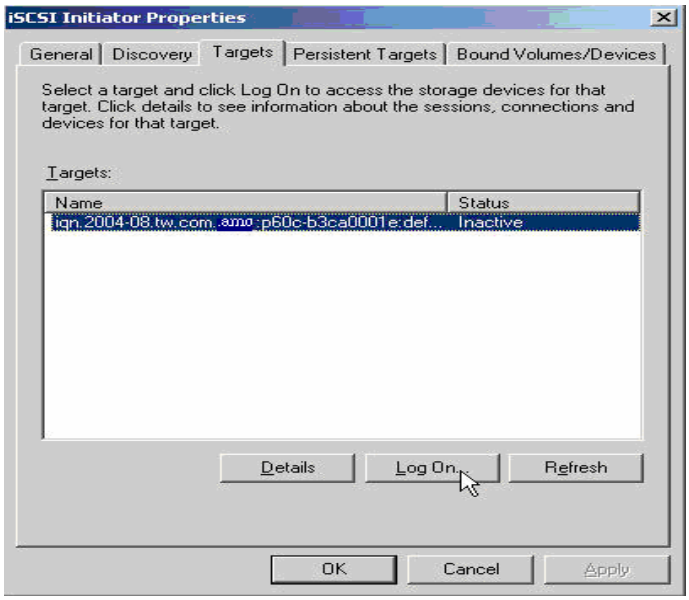
10. Input the IP address of iSCSI data port 2 (192.168.12.229 as mentioned in previous page).



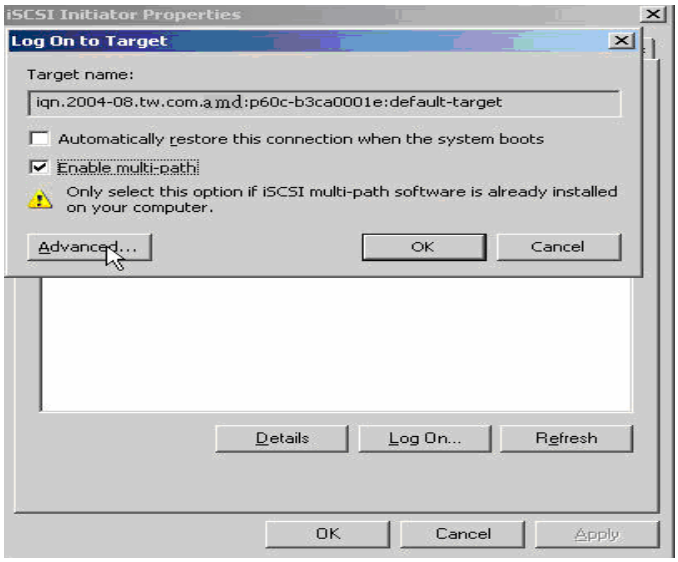
11. The initiator setting is done.



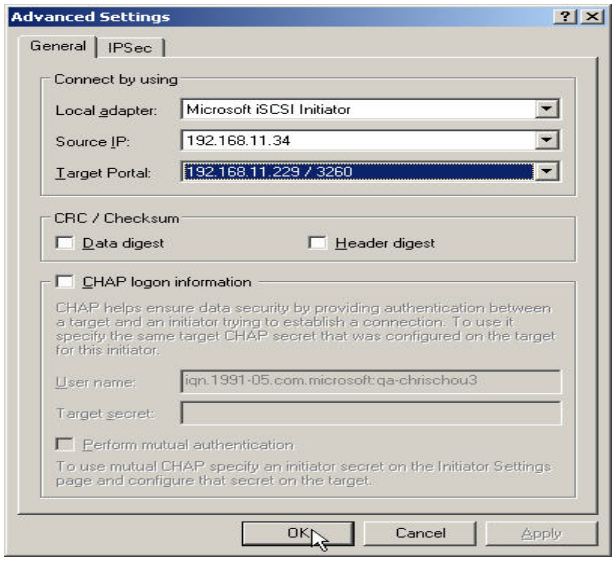
12. Log on.



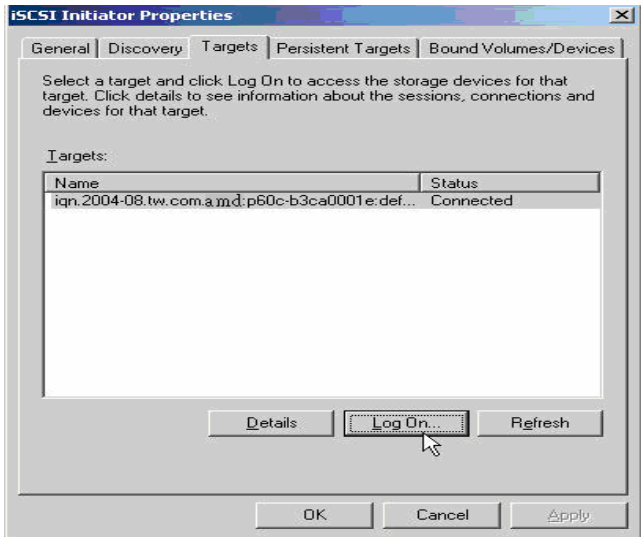
13. Enable **"Enable multi-path"** checkbox. Then click **"Advanced"**.



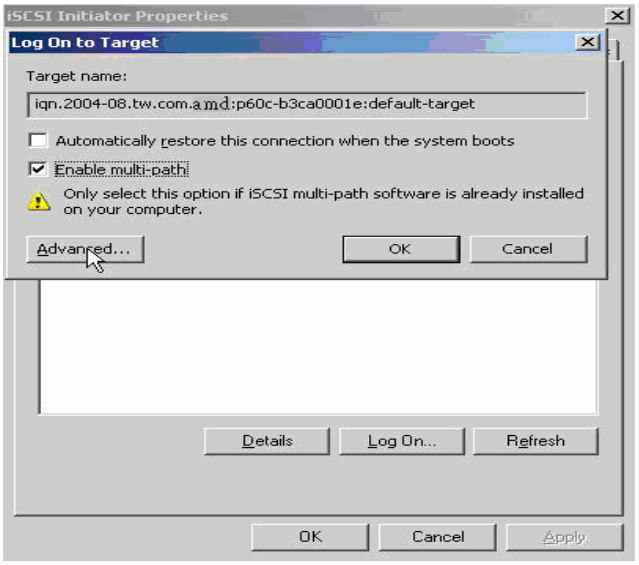
14. Select Target Portal to iSCSI data port 1 (192.168.11.229). Then click **"OK"**



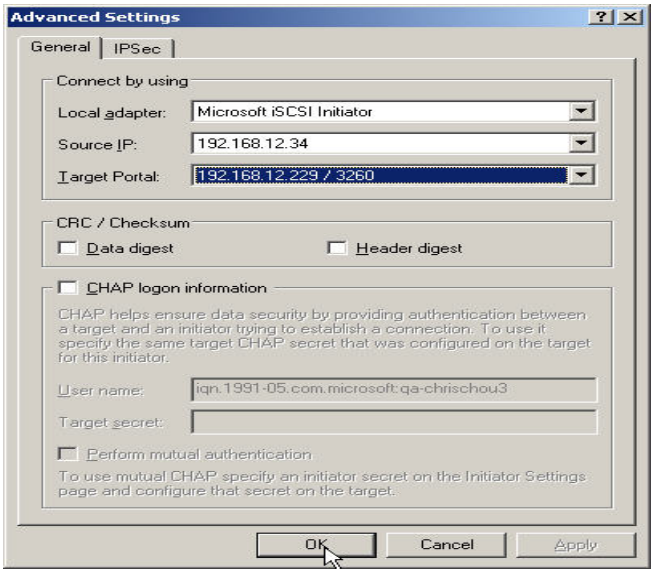
15. Log on **"Enable multi-path"** again.



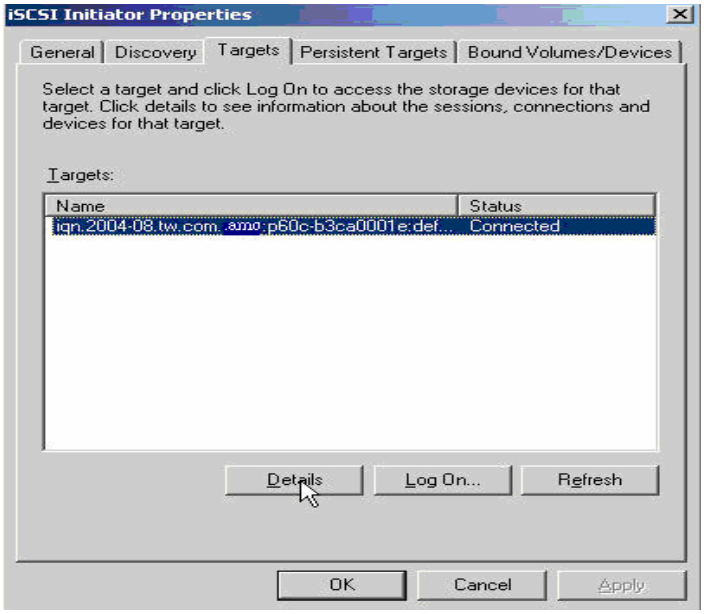
16. Enable **"Enable multi-path"** checkbox. Then click **"Advanced…"**.



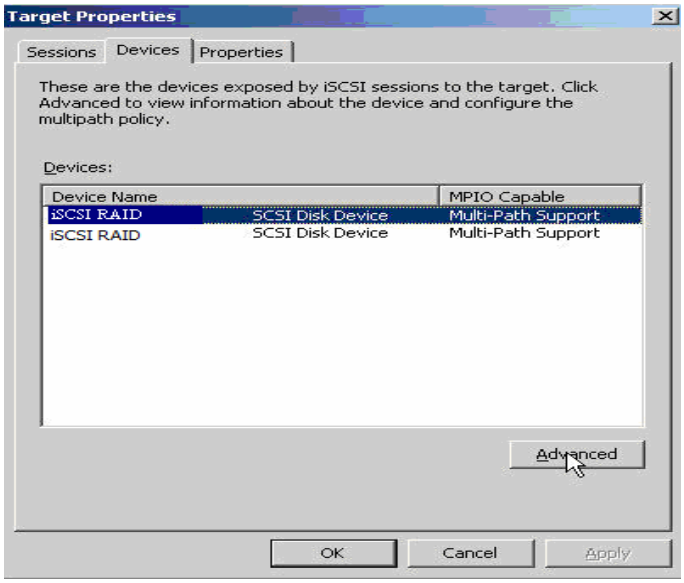
17. Select Target Portal to iSCSI data port 2 (192.168.12.229). Then select **"OK"**



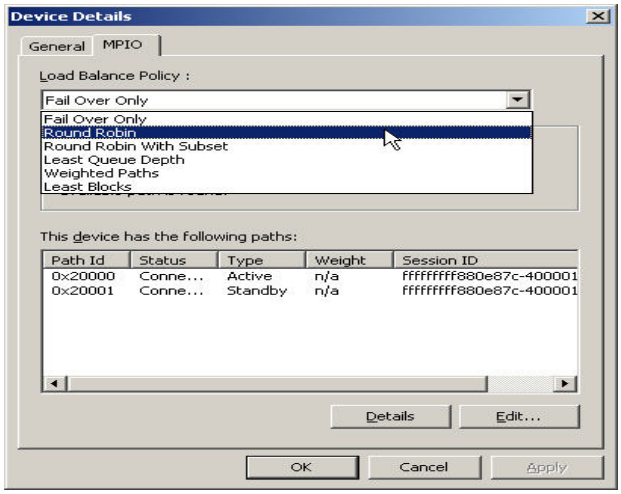
18. iSCSI device is connected. Click **"Details"**.



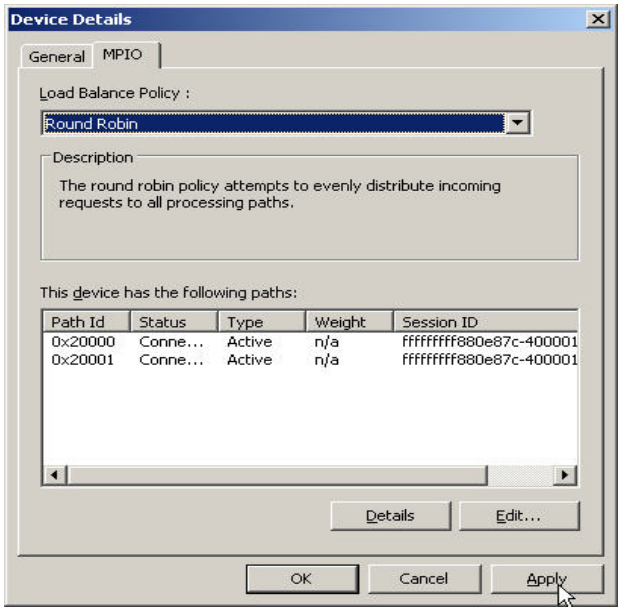
19. Click **"Device"** tab, then click **"Advanced"**.



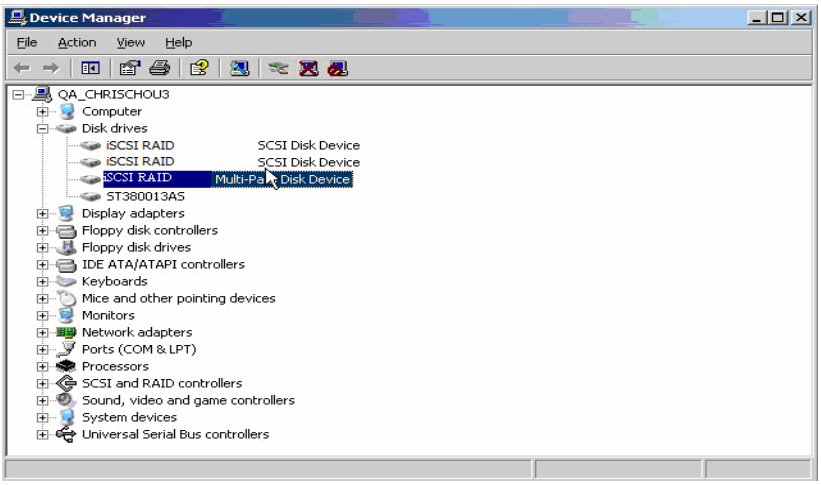
20. Click **"MPIO"** tab, select **"Load Balance Policy"** to **"Round Robin"**.



21. Click **"Apply"**.

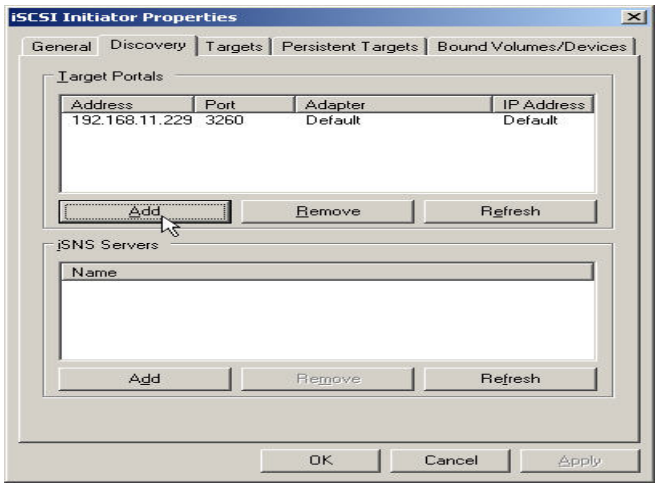


22. Run **"Device Manage"** in Windows. Make sure MPIO device is available. Then the disk can be tested about performance by IOMETER.

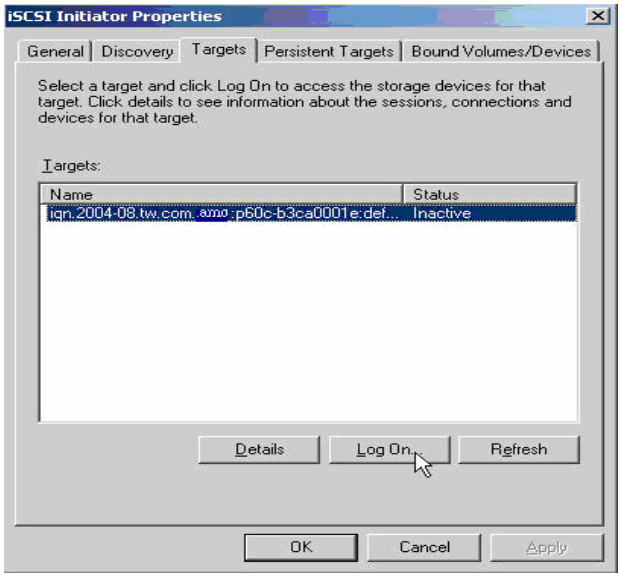


The **MC/S** setup instructions are very similar to MPIO, detail steps are in the following figures. For the target side setting, the steps are exactly the same as MPIO. Please refer to **Figure F.1 to Figure F.9**.

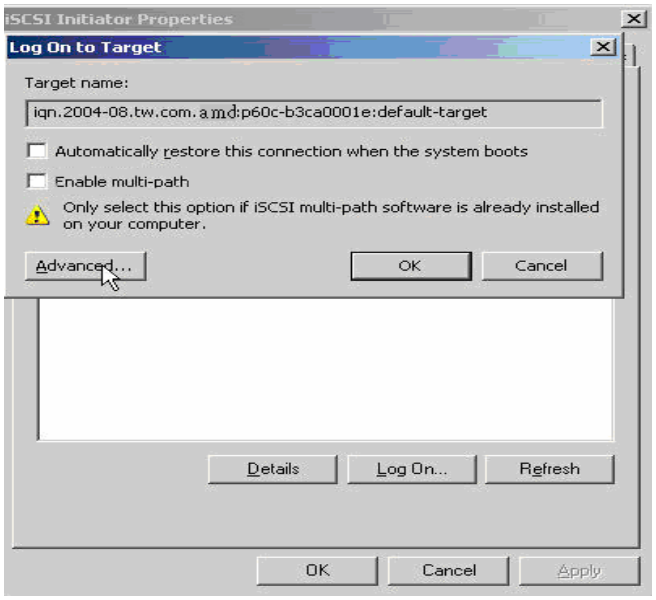
1. Create a RG (RAID group) with RAID 5, using 3 HDDs.
2. Create a VD (virtual disk) by using RAID 5 RG (RAID group).
3. Run Microsoft iSCSI initiator 2.07 and check the Initiator Node Name.
4. Attaching LUN to R5 VD (virtual disk). Input the Initiator Node Name in Host field.
5. The volume config setting is done.
6. Check iSCSI settings. The IP address of iSCSI data port 1 is 192.168.11.229, port 2 is 192.168.12.229 for example.
7. Add Target Portals on Microsoft iSCSI initiator 2.07.
8. Input the IP address of iSCSI data port 1 (192.168.11.229 as mentioned in previous pages). For MC/S, there is only ONE **"Target Portals"** in the **"Discovery"** tab.



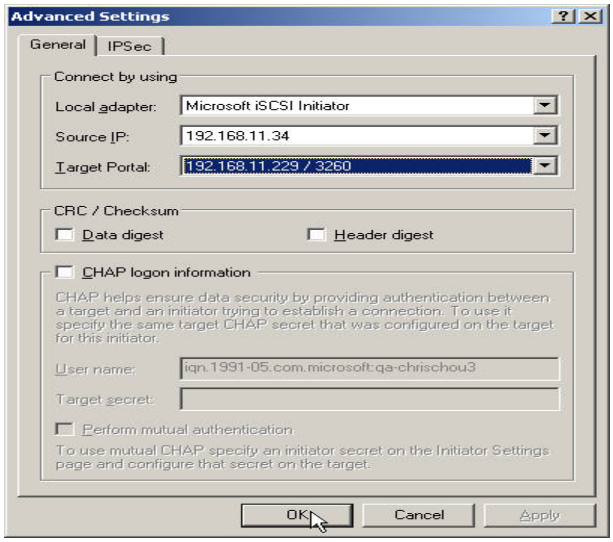
9. Log on.



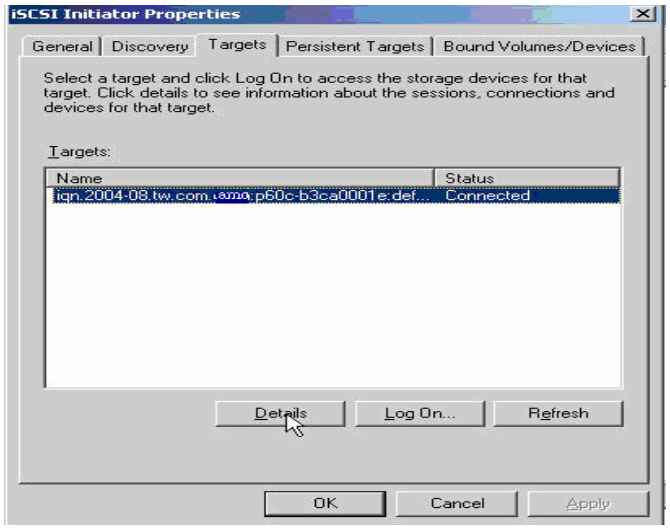
10. Then click **"Advanced…"**.


iSCSI Initiator Properties
Log On to Target
Target name:
iqn.2004-08.tw.com.amd:p60c-b3ca0001e:default-target
Automatically restore this connection when the system boots
Enable multi-path
Only select this option if iSCSI multi-path software is already installed on your computer.
Advanced...
OK
Cancel
Details
Log On...
Refresh
OK
Cancel
Apply

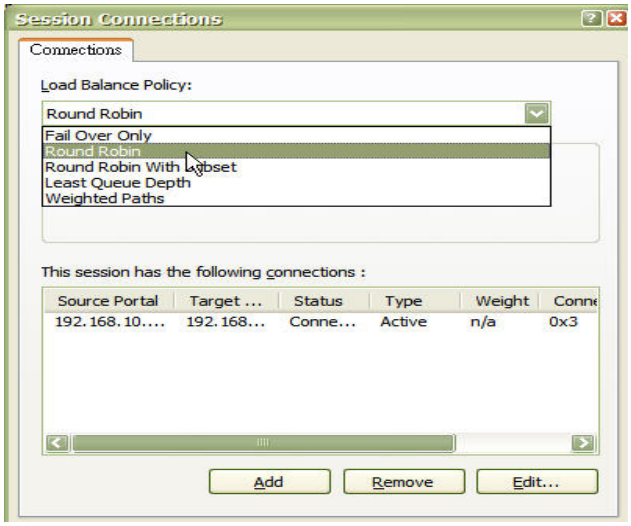
11. Select set Local Adapter, Source IP, and Target Portal to iSCSI data port 1 (192.168.11.229). Then click “OK”.



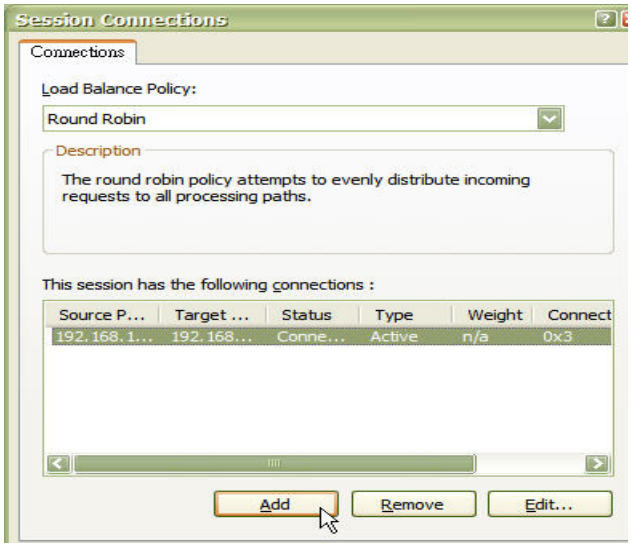
12. After connected, click “Details”, then in the “Session” tab, click “Connections”.

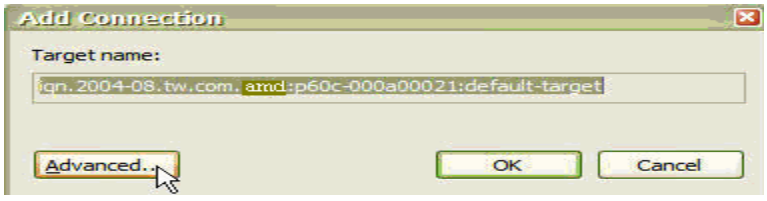


13. Choose **“Round Robin”** for Load Balance Policy

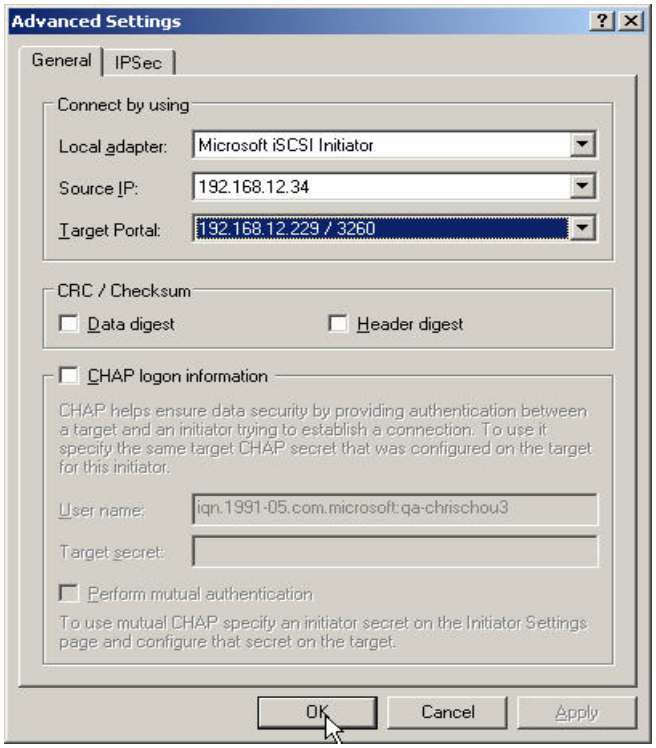


14. **"Add"** Source Portal for the iSCSI data port 2(192.168.12.229)





15. Select Local adapter, Source IP, and Target Portal to iSCSI data port 2 (192.168.12.229). Then select **"OK"**.



16. The MC/S setting is done.

Trunking / LCAP Overview

LACP: Link Aggregation Control Protocol

IEEE specification (802.3ad)

Bundle several physical ports together to form a single logical channel

Allows a switch to negotiate

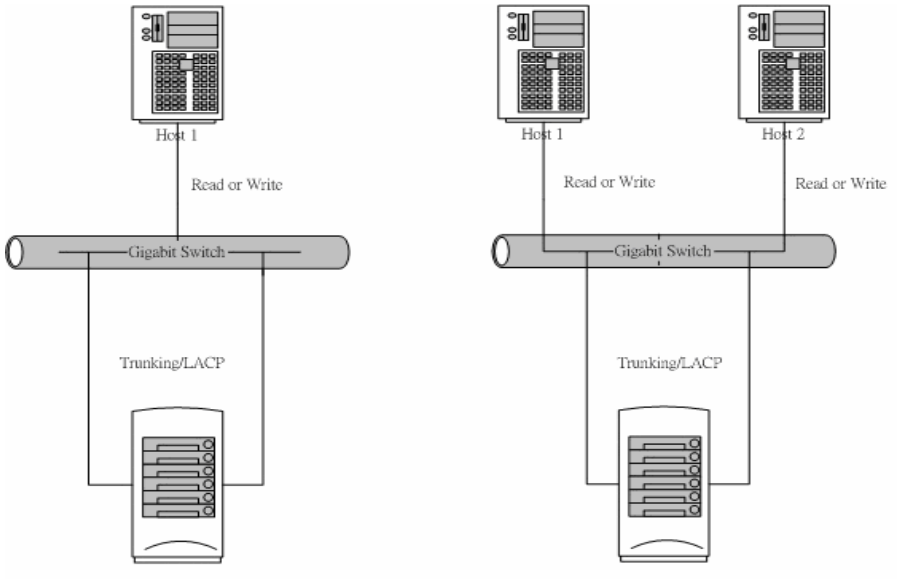
Trunking:

Similar to 802.3ad

Protocol-independent

Trunking / LCAP Setup Instructions

Below are the steps to setup Trunking and LACP. There are 2 kinds of scenarios for Trunking/LACP.



Network diagram of Trunking/LACP.

1. Create a RG (RAID group) with RAID 5, using 3 HDDs.

/ Volume configuration / RAID group

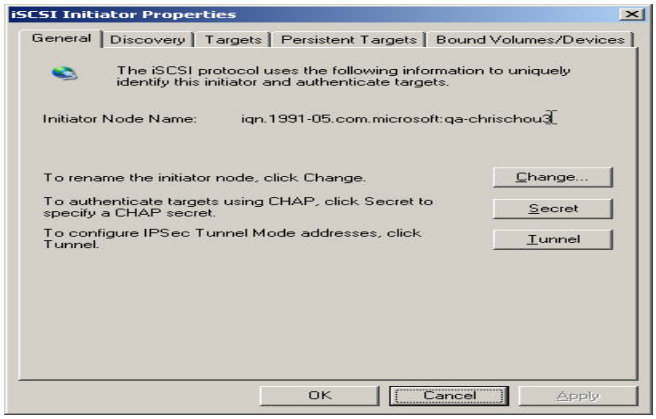
No.	Name	Total (GB)	Free (GB)	#PD	#VD	Status	Health	RAID
1	test	1862	1862	3	0	Online	Good	RAID 5

2. Create a VD (virtual disk) by using the RAID 5 RG (RAID group).

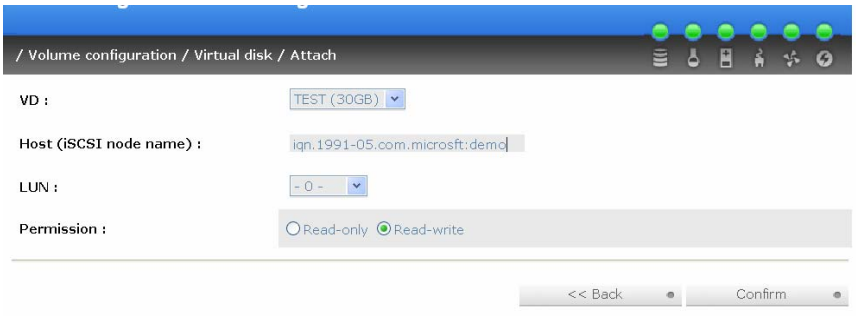
/ Volume configuration / Virtual disk

No.	Name	Size (GB)	Right	Priority	Bg rate	Status	Health	R %	RAID	#LUN	Snapshot space (GB)	#Snapshot	RG name
1	TEST	30	WB	HI	4	Initiating	Optimal	58	RAID 5	0	0/0	0	test

3. Run Microsoft iSCSI initiator 2.07 and check the Initiator Node Name.



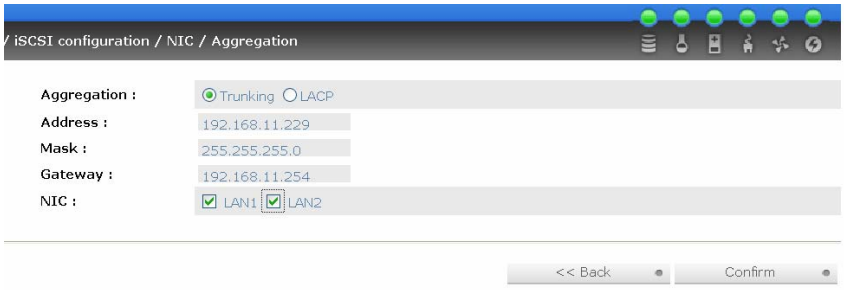
4. Attaching LUN to R5 VD (virtual disk). Input the Initiator Node Name in the Host field.



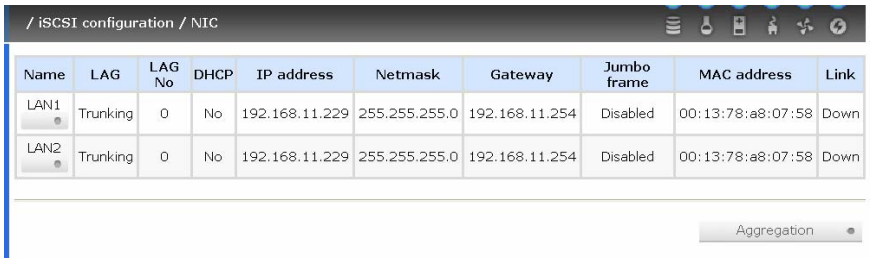
5. Done, please check the settings.

6. Check iSCSI settings. The IP address of iSCSI data port 1 is 192.168.11.229. Using port 1 as Trunking or LACP. Click the blue square in “Aggregation” field to set Trunking or LACP.

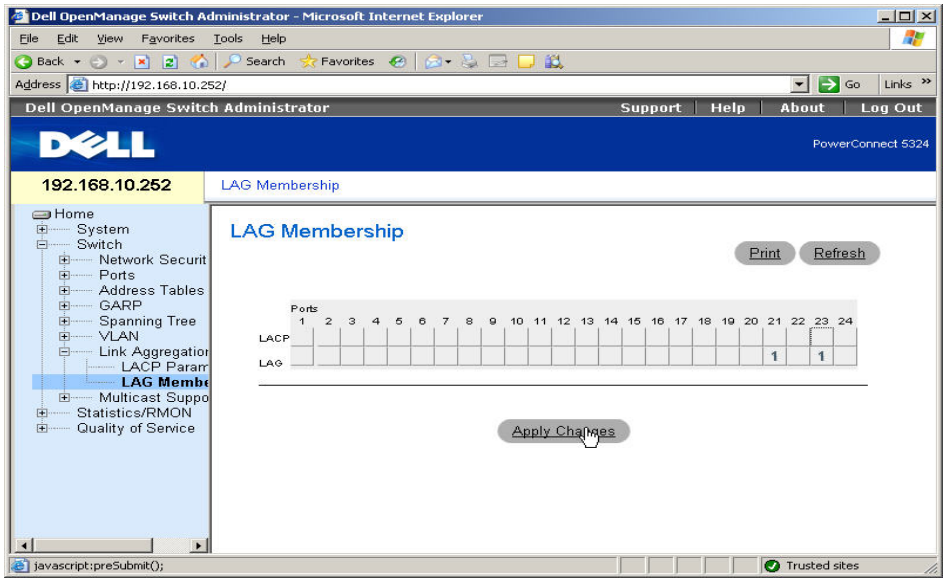
7. Select “Trunking”. If LACP is needed..



8. Now, the setting is in Trunking mode.

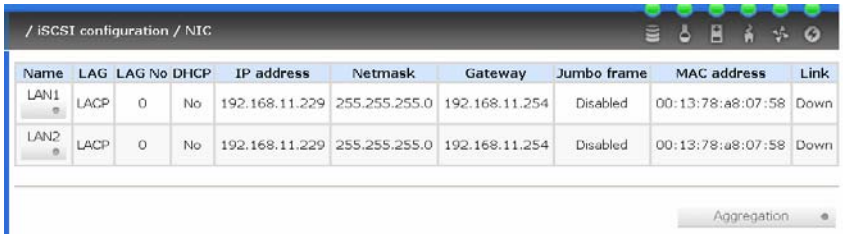


9. Enable switch Trunking function of port 21 and 23. Below is an example of Dell PowerConnect 5324.

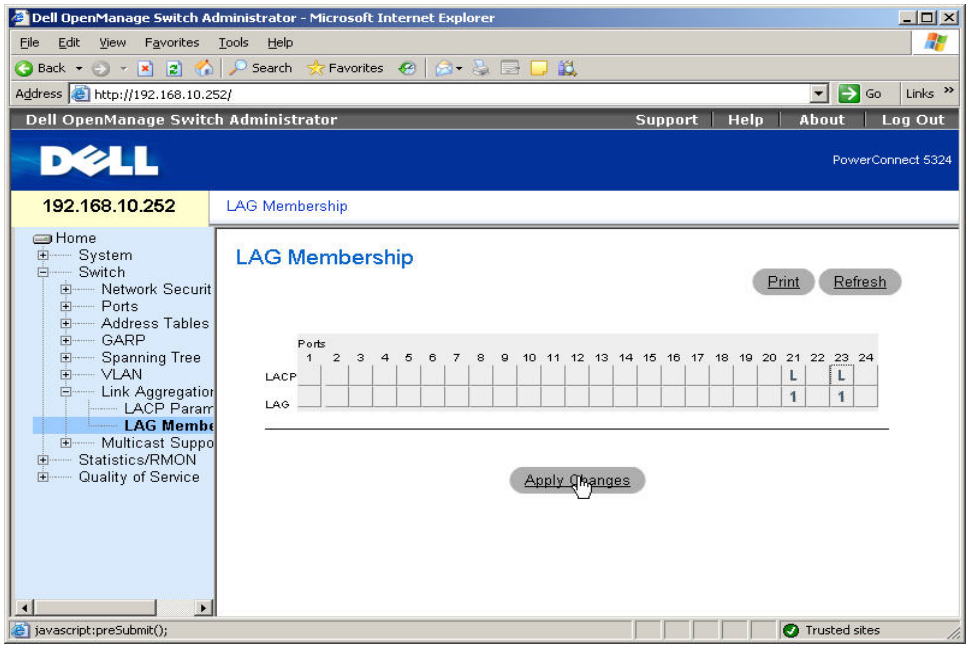


10. Select “LACP”. If LACP is needed,

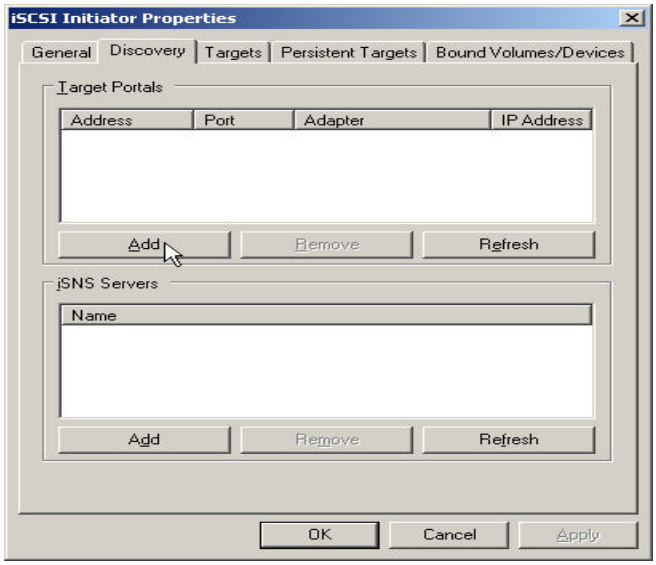
11. Now, the setting is LACP mode.



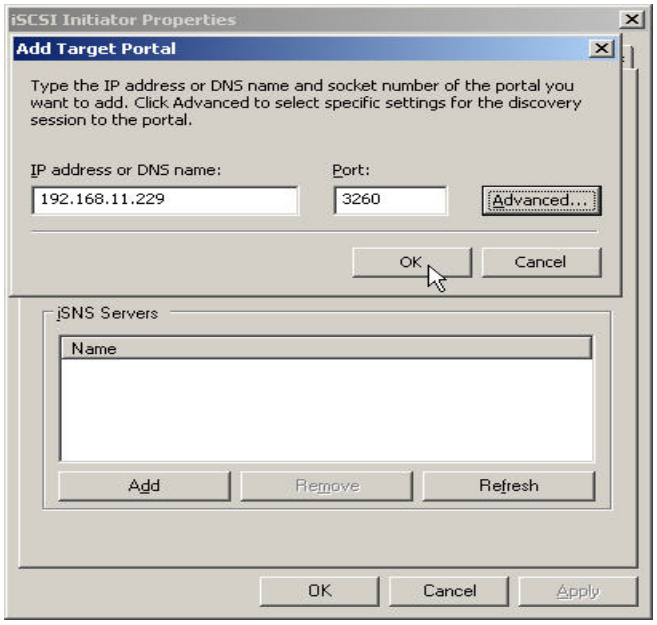
12. Enable switch LACP function of port 21 and 23. Below is an example of Dell PowerConnect 5324.



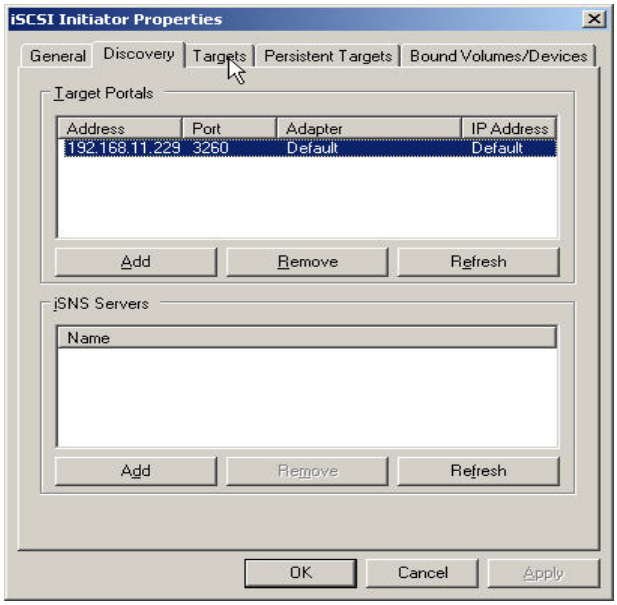
13. Add Target Portals in Microsoft iSCSI initiator 2.07.



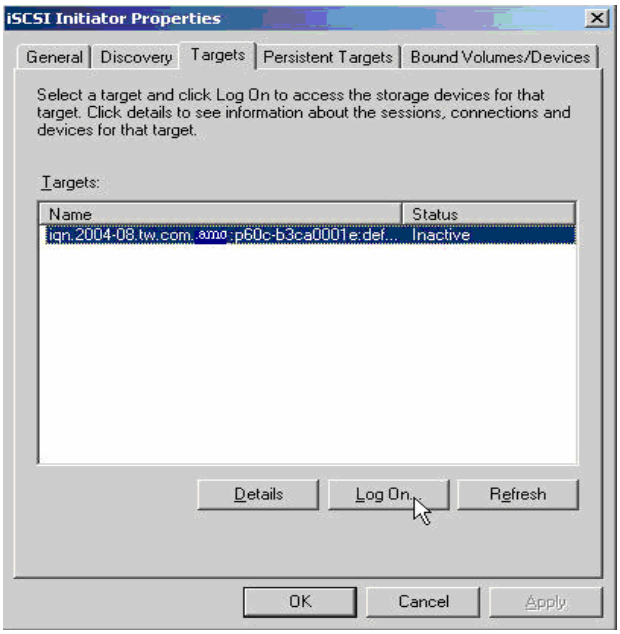
14. Input the IP address of iSCSI data port 1 (192.168.11.229 as mentioned in previous page).



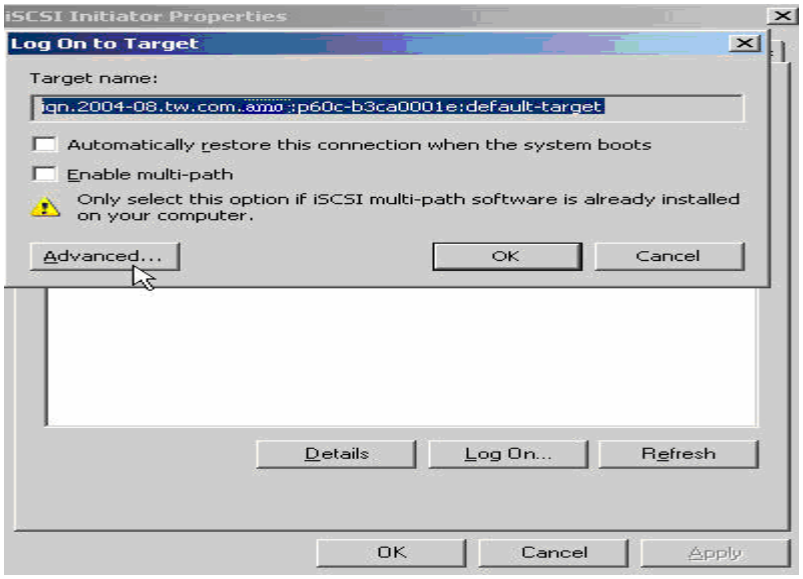
15. Click “Targets” to log on.



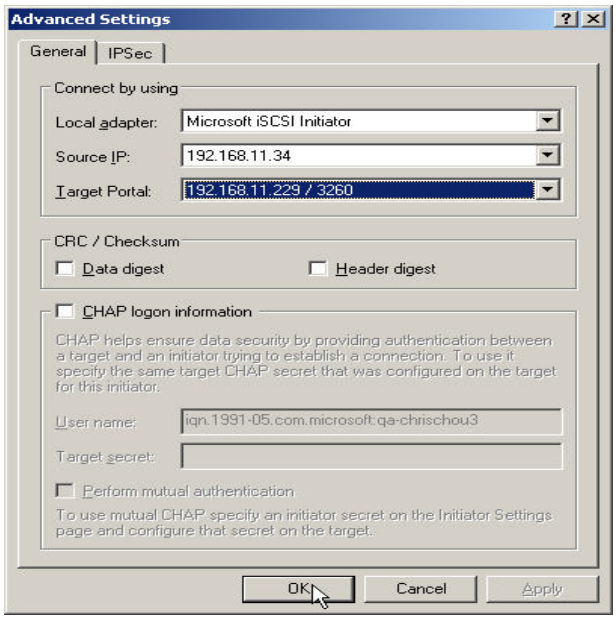
16. Log on.



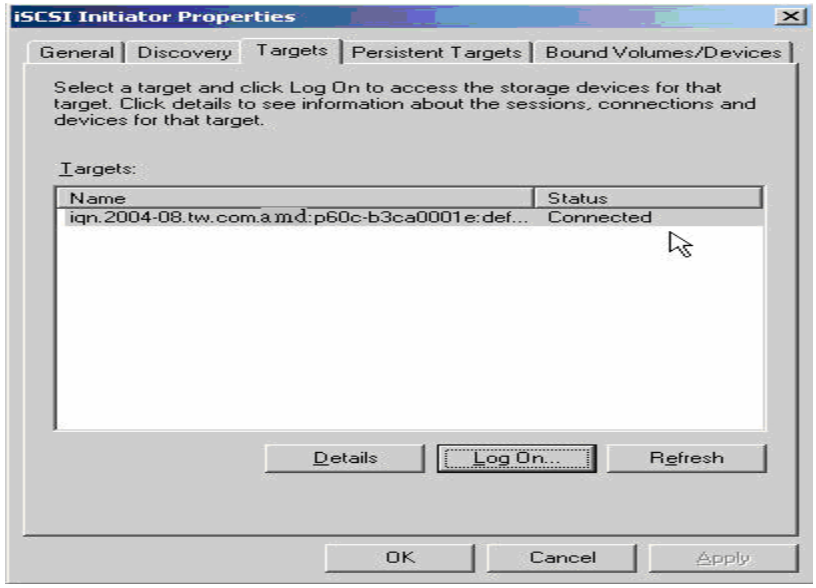
17. Click “Advanced”.



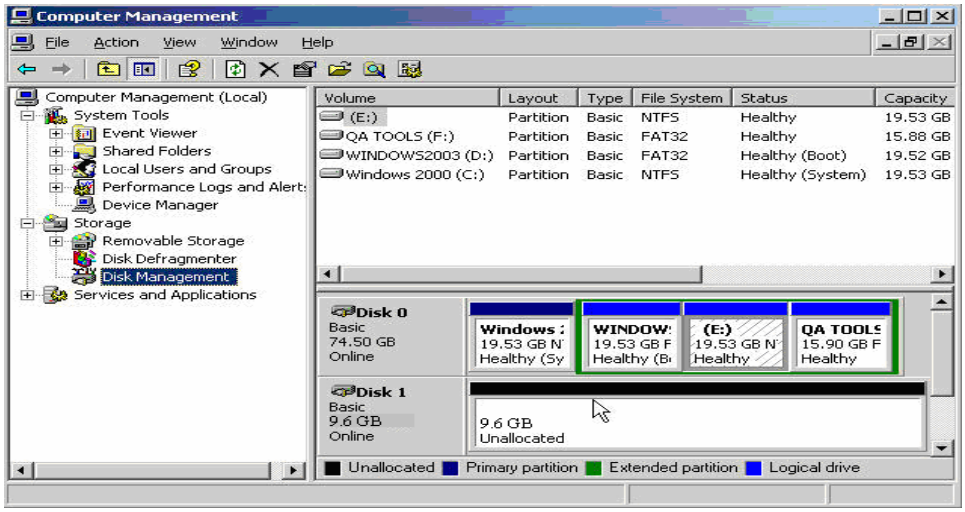
18. Select Target Portal to iSCSI data port 1 (192.168.11.229). Then click “OK”.



19. The setting is completed.



20. Run “Computer Management” in Windows. Make sure the disks are available. Then the disks can be tested for performance by IOMETER.


Computer Management
File Action View Window Help
Computer Management (Local)
System Tools
Event Viewer
Shared Folders
Local Users and Groups
Performance Logs and Alert
Device Manager
Storage
Removable Storage
Disk Defragmenter
Disk Management
Services and Applications
Volume Layout Type File System Status Capacity
(E:) Partition Basic NTFS Healthy 19.53 GB
QA TOOLS (F:) Partition Basic FAT32 Healthy 15.88 GB
WINDOWS2003 (D:) Partition Basic FAT32 Healthy (Boot) 19.52 GB
Windows 2000 (C:) Partition Basic NTFS Healthy (System) 19.53 GB
Disk 0
Basic
74.50 GB
Online
Windows :
19.53 GB N
Healthy (Sy
WINDOW
19.53 GB F
Healthy (B
(E:)
19.53 GB N
Healthy
QA TOOLS
15.90 GB F
Healthy
Disk 1
Basic
9.6 GB
Online
9.6 GB
Unallocated
Unallocated Primary partition Extended partition Logical drive

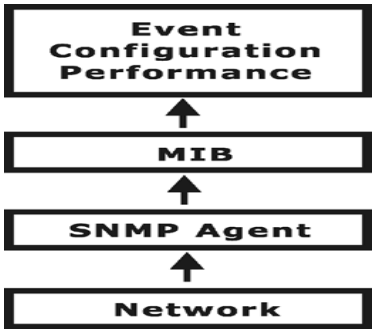
Appendix C

Firmware Upgrading & SNMP

SNMP Overview

(Simple Network Management Protocol) A widely used network monitoring and control protocol. Data are passed from SNMP agents, which are hardware and/or software processes reporting activity in each network device (hub, router, bridge, etc.) to the workstation console used to oversee the network. The agents return information contained in a MIB (Management Information Base), which is a data structure that defines what is obtainable from the device and what can be controlled (turned off, on, etc.). Originating in the Unix community, SNMP has become widely used on all major platforms.

The Definition SNMP



SNMP Installation

Step 1: Installing the SNMP Manager software on the client server.

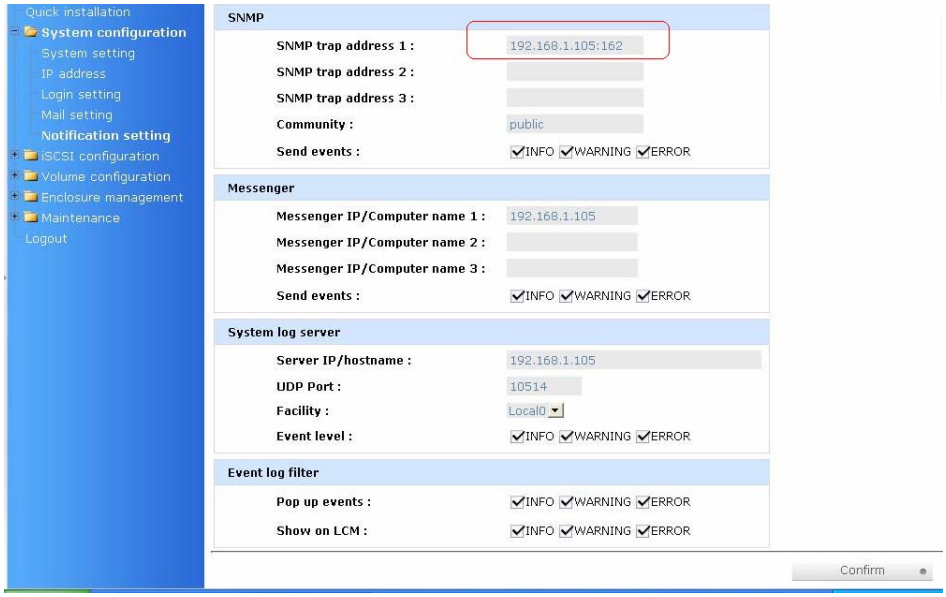
Step 2: Placing a copy of the management information base (MIB) in a directory which is accessible to the SNMP management application

Step 3: Compiling the MIB description file with the SNMP management

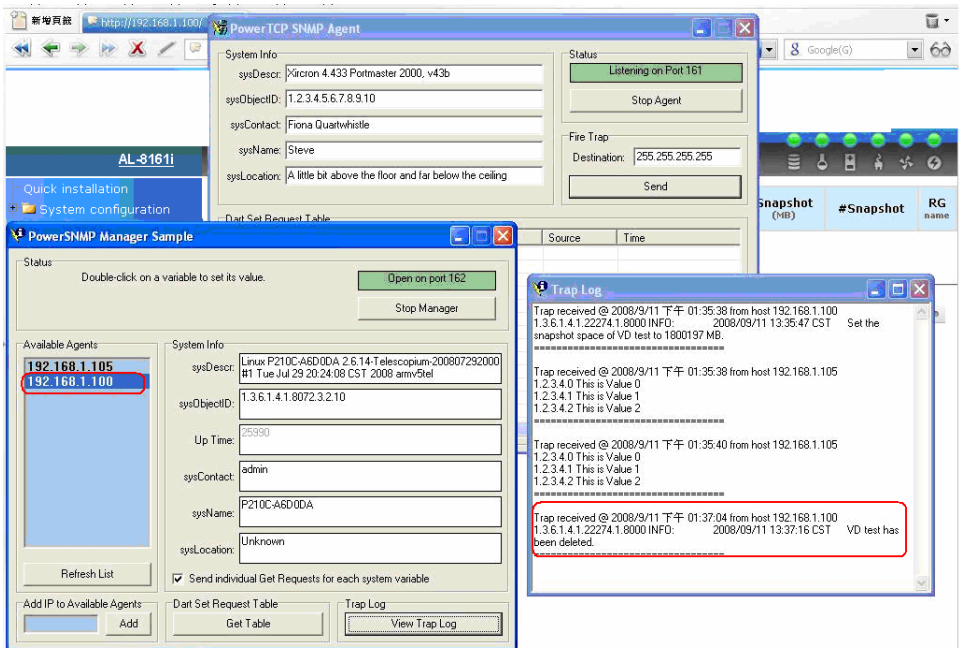
application

Below is one example of PowerSNMP working with this iSCSI RAID subsystem ‘s SNMP configurations:

1. Set SNMP Trap address for the AL-8161i



2. PowerSNMP detects a VD (Virtual Disk) has been deleted



MIB Compilation and Definition File creation

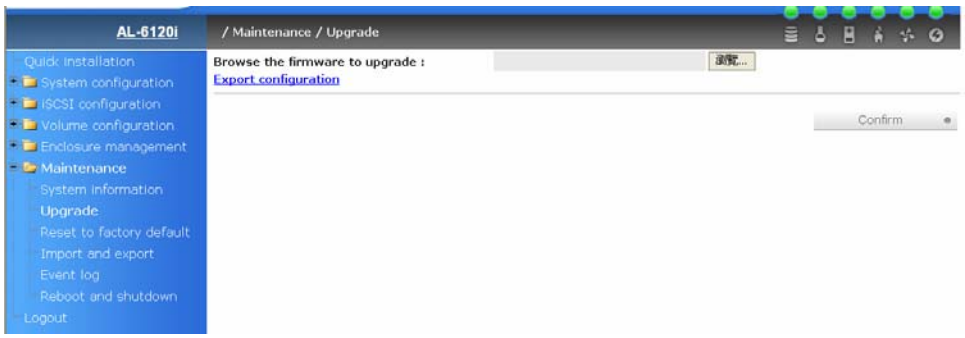
Before the SNMP manager application accesses the RAID controller, user needs to integrate the MIB into the SNMP management application's database of events and status indicator codes. This process is known as compiling the MIB into the SNMP application. This process is highly vendor-specific and should be well-covered in the User's Guide of your SNMP application.

Upgrading Firmware

Since the RAID controller features flash firmware, it is not necessary to change the hardware flash chip in order to upgrade the RAID firmware. The user can simply re-program the firmware through the RS-232 port or 10/100 Ethernet port.

Upgrading Firmware Through Web Browser Management

1. To upgrade the RAID subsystem firmware, move the mouse cursor to **"Maintenance"**, then click **"Upgrade"**

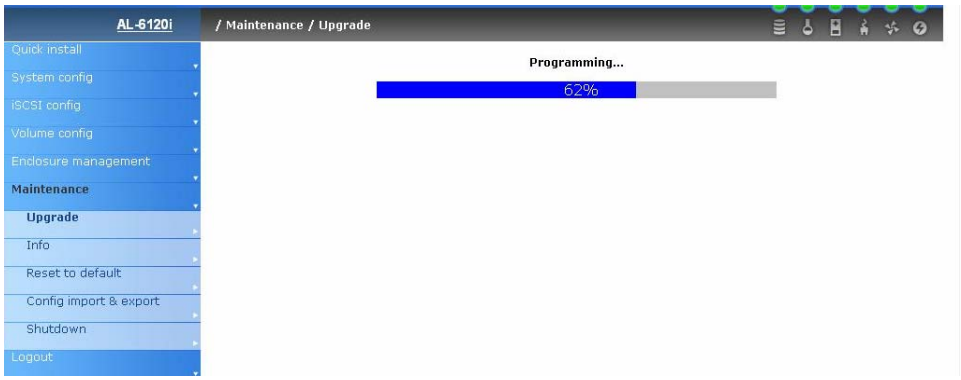


2. Click Browse. Look in the location where the new firmware is located. Select the file "Firmware" Then click **"open"**.

3. Click the **"Confirm."** Then a warning dialogue box as below will pop up. Click **"OK"** to continue the firmware upgrading process.

4. The new firmware file is being uploaded to the RAID subsystem.

5. The firmware version is being upgraded.



6. When the upgrading is completed, there will be a dialogue box as below.

Appendix D

Installation Steps for Greater Than 2TB Volume

Overview:

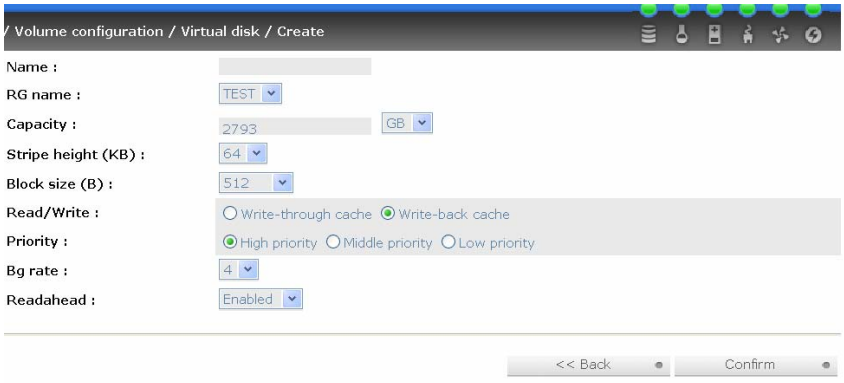
This iSCSI RAID subsystem is capable of supporting greater than 2TB volumes. When connecting the RAID controller to 64bit OS installed host/server, the host/server is inherently capable for greater than 2TB volumes from the 64bit address. On the other side, if the host/server is installed with 32bit OS, the user has to change the block size to 1KB, 2KB or 4KB to support volumes up to 4TB, 8TB or 16TB, for the 32bit host/server doesn't support LBA (Logical Block Addressing) 64bit. But if the 32bi OS supports LBA 64bit, for example, Windows Serve 2003 with SP1, Linux kernel 2.6.x, or FreeBSD 5.2.1, there is no need to make use of changing the block size mentioned above to support greater than 2TB volumes. For detail installation steps, please refer to following steps below:

Step A: configure your target

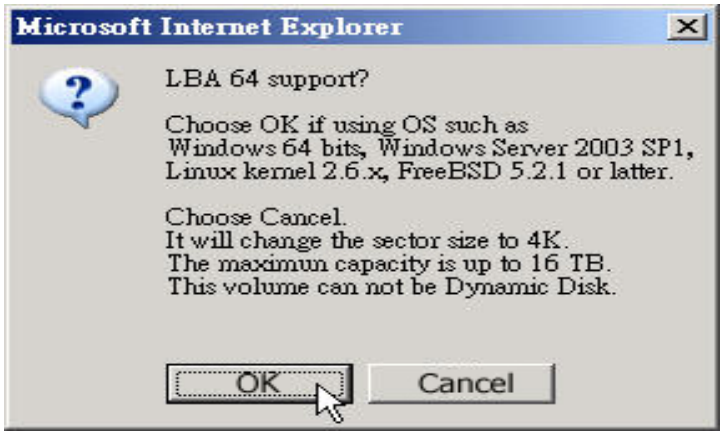
1. Create a RG (RAID group) which is large than 2TB .

2. Create a VD (virtual disk).

3. Setup capacity, stripe height, and block size for VD (virtual disk).



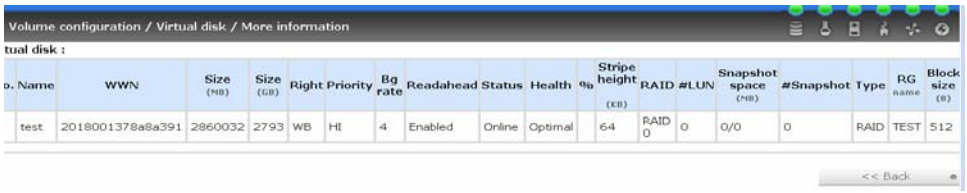
4. When the capacity (GB) is greater than 2TB, there will be a dialogue box as below pops up capacity.



A 2793G VD (virtual disk) is created.

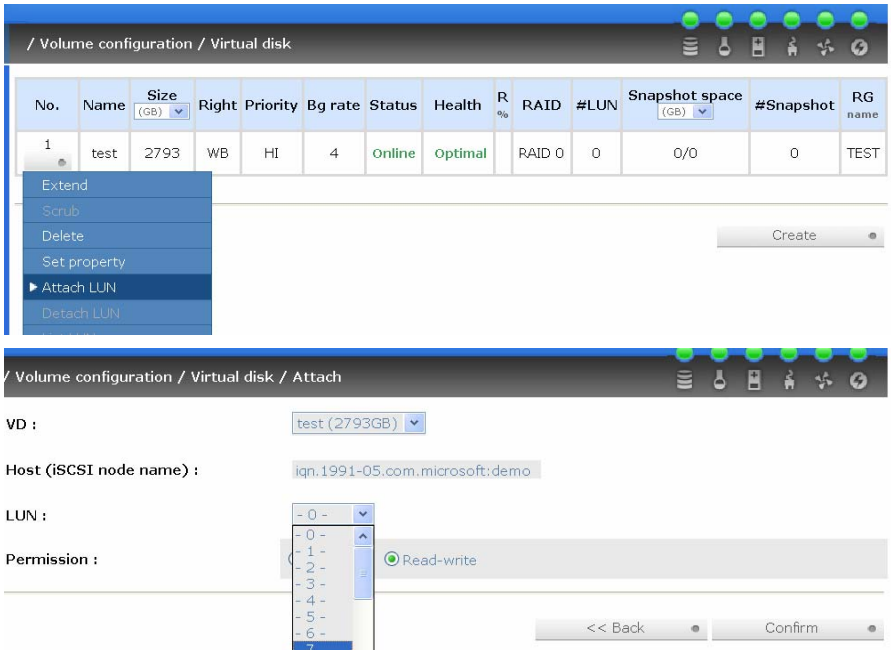
5. Check the detail information.

With LBA 64 supporting, block size = 512B.



Without LBA 64 supporting, block size = 4K.

6. Attach LUN.

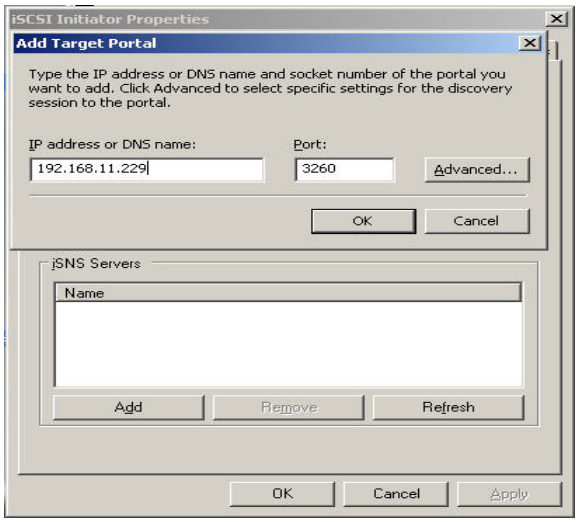


Step B: configure your host/server

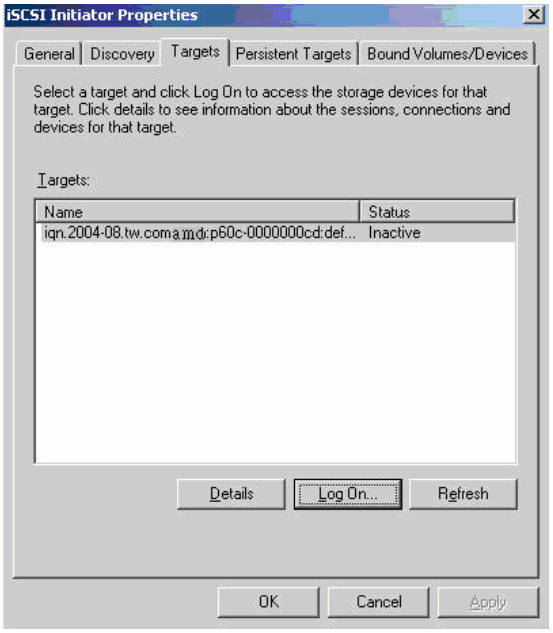
Below is the configuration for Windows Server 2003 with Microsoft iSCSI initiator. Please install the latest Microsoft iSCSI initiator from following link :

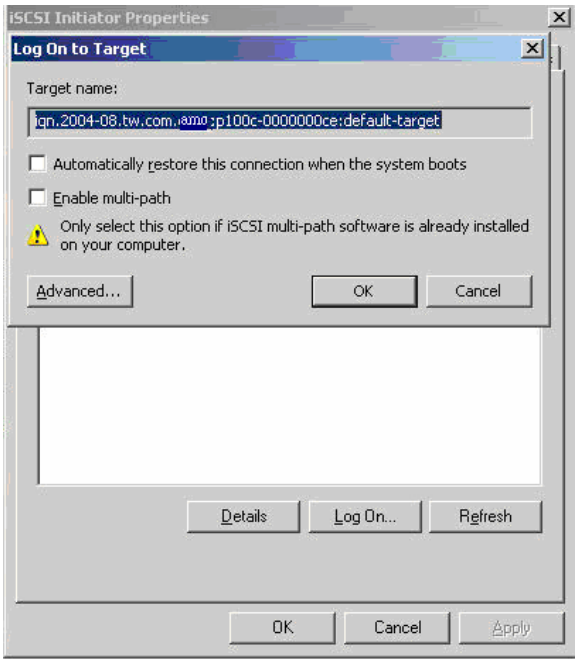
http://www.microsoft.com/downloads/details.aspx?familyid=12cb3c1a-15d6-4585-b385-befd1319f825&displaylang=en

1. Run MS iSCSI initiator, go to “Discovery” tab, add target portal (iSCSI data).

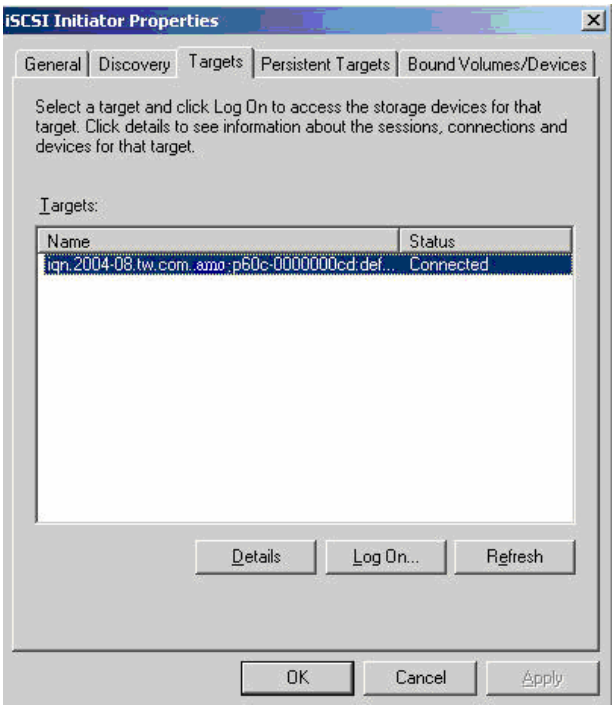


2. Go to “Targets” tab, click “Refresh”, and then “Log On…” the target



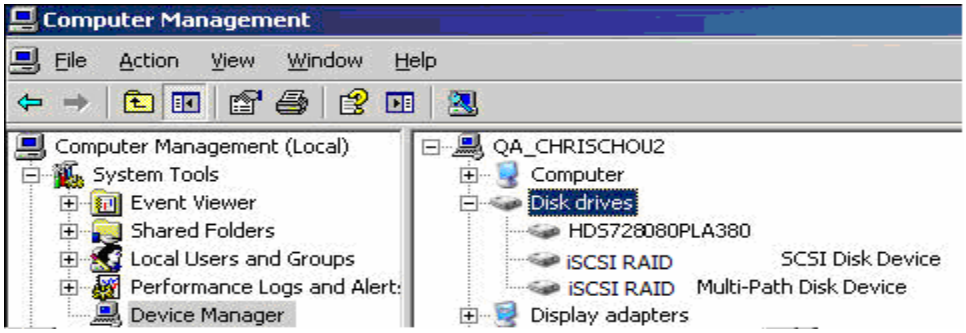


3. Status is “Connected”, the initiator setting is done



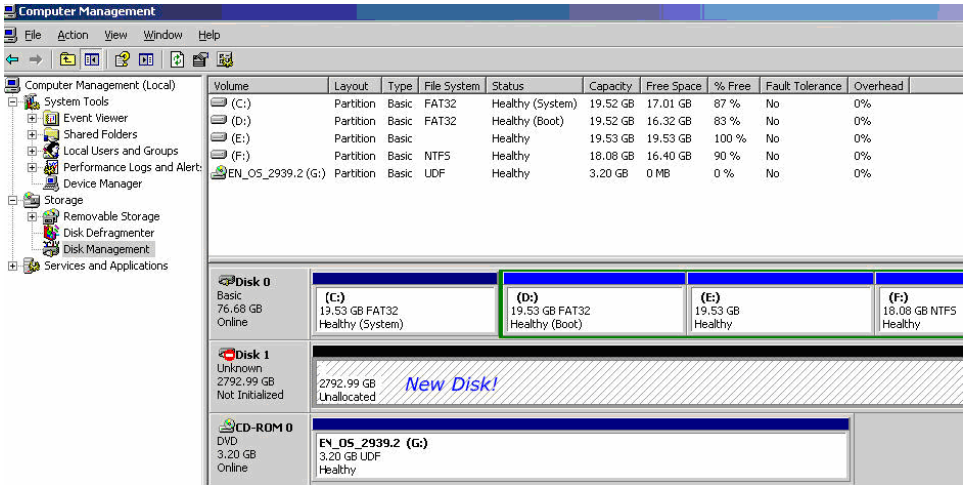
Step C: Initialize/Format/Mount the disk

1. Go to Start → Control Panel → Computer Management → Device Manger → Disk drives

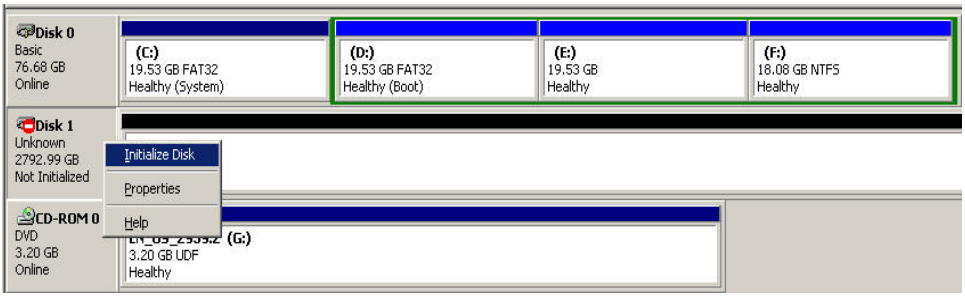


Disk drive status of the iSCSI RAID controller

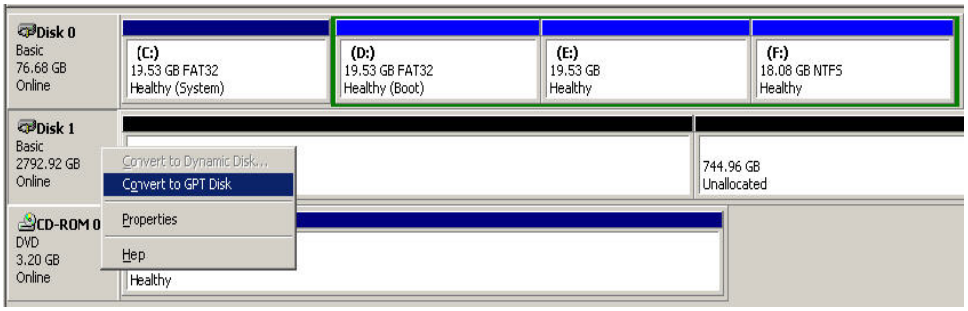
2. Go to Start → Control Panel → Computer Management → Disk Management, it displays a new disk.



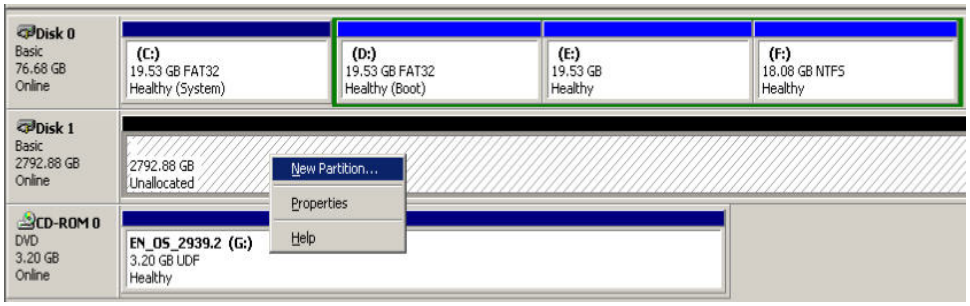
3. Initialize disk.



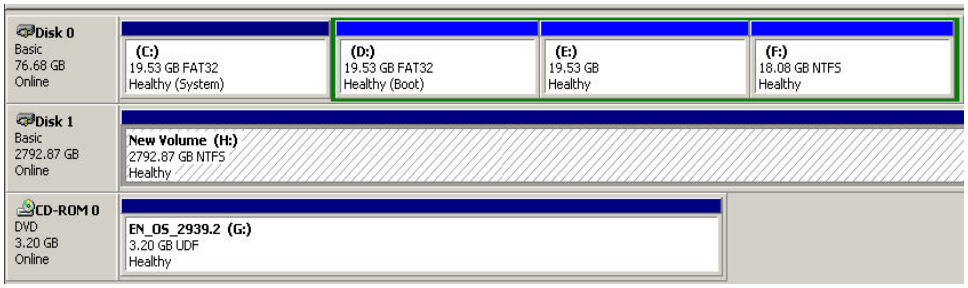
4. Convert to GPT disk for over 2TB capacity. For more detail information about GPT, please visit **http://www.microsoft.com/whdc/device/storage/GPT_FAQ.mspx**



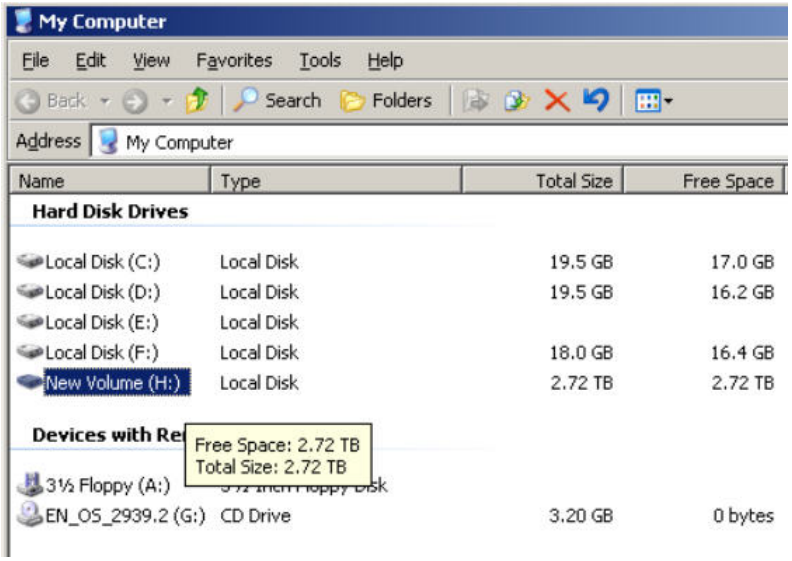
5. Format disk.



6. Format disk is done.



7. The new disk is ready to go, available size = 2.72TB.



Appendix E.

Event Notifications (Logs)

PD events

Level	Type	Description
INFO	Disk inserted	Disk <slot> is inserted into system.
WARNING	Disk removed	Disk <slot> is removed from system.
ERROR	HDD failure	Disk <slot> is disabled.

HW events

Level	Type	Description
WARNING	ECC error	Single-bit ECC error is detected.
ERROR	ECC error	Multi-bit ECC error is detected.
INFO	ECC info	ECC memory is installed.
INFO	ECC info	Non-ECC memory is installed.
INFO	SCSI info	Received SCSI Bus Reset event at the SCSI Bus <number>.

EMS events

Level	Type	Description
INFO	Power installed	Power <number> is installed.
ERROR	Power absent	Power <number> is absent.
INFO	Power work	Power <number> is restored to work.
ERROR	Power warning	Power <number> is out of work.
WARNING	Power detect	PSU signal detection <number>.
INFO	Fan work	Fan <number> is restored to work.

ERROR	Fan warning	Fan <number> is out of work.
INFO	Fan installed	Fan <number> is installed.
ERROR	Fan not present	Fan <number> is not present.
WARNING	Thermal warning	System temperature <location> is a little bit higher.
ERROR	Thermal critical	System Overheated <location>!!!
ERROR	Thermal critical shutdown	System Overheated <location>!!! The system will do the auto shutdown immediately.
WARNING	Thermal ignore value	Unable to update thermal value on <location>.
WARNING	Voltage warning	System voltage <location> is a little bit higher/lower.
ERROR	Voltage critical	System voltages <location> failed!!!
ERROR	Voltage critical shutdown	System voltages <location> failed!!! The system will do the auto shutdown immediately.
INFO	UPS info	UPS detection succeeded.
WARNING	UPS error	UPS detection failed.
ERROR	UPS error	AC loss for the system is detected.
ERROR	UPS error	UPS Power Low!!! The system will do the auto shutdown immediately.
WARNING	SMART T.E.C.	Disk <slot> S.M.A.R.T. Threshold Exceed Condition occurred for attribute <item>.
WARNING	SMART failure	Disk <slot>: Failure to get S.M.A.R.T information.

RMS events

Level	**Type**	**Description**
INFO	Console Login	<username> login from <IP or serial console> via Console UI.
INFO	Console Logout	<username> logout from <IP or serial console> via Console UI.
INFO	Web Login	<username> login from <IP> via Web UI.
INFO	Web Logout	<username> logout from <IP> via Web UI.

LVM3 events

Level	Type	Description
INFO	RG created	RG <name> has been created.
INFO	RG creation failed	Failed to create RG <name>.
INFO	RG deleted	RG <name> has been deleted.
INFO	VD created	VD <name> has been created.
INFO	VD creation failed	Failed to create VD <name>.
INFO	VD deleted	VD <name> has been deleted.
INFO	VD renamed	Name of VD <name> has been renamed to <name>.
INFO	Read-only caching enabled	Cache policy of VD <name> has been set as read only.
INFO	Writeback caching enabled	Cache policy of VD <name> has been set as write-back.
INFO	Write-through caching enabled	Cache policy of VD <name> has been set as write-through.
INFO	VD extended	Size of VD <name> extends.
INFO	VD initialization started	VD <name> starts initialization.
INFO	VD initialization finished	VD <name> completes the initialization.
WARNING	VD initialization failed	Failed to complete initialization of VD <name>.
INFO	VD rebuild started	VD <name> starts rebuilding.
INFO	VD rebuild finished	VD <name> completes rebuilding.
WARNING	VD rebuild failed	Failed to complete rebuild of VD <name>.
INFO	VD migration	VD <name> starts migration.

	started	
INFO	VD migration finished	VD <name> completes migration.
ERROR	VD migration failed	Failed to complete migration of VD <name>.
INFO	VD scrubbing started	VD <name> starts scrubbing.
INFO	VD scrubbing finished	VD <name> completes scrubbing.
INFO	RG migration started	RG <name> starts migration.
INFO	RG migration finished	RG <name> completes migration.
INFO	RG activated	RG <name> has been manually activated.
INFO	RG deactivated	RG <name> has been manually deactivated.
INFO	VD rewrite started	Rewrite at LBA <address> of VD %s starts.
INFO	VD rewrite finished	Rewrite at LBA <address> of VD %s completes.
WARNING	VD rewrite failed	Rewrite at LBA <address> of VD %s failed.
WARNING	RG degraded	RG <name> is under degraded mode.
WARNING	VD degraded	VD <name> is under degraded mode.
ERROR	RG failed	RG <name> is failed.
ERROR	VD failed	VD <name> is failed.
WARNING	Recoverable read error occurred	Recoverable read error occurred at LBA <address>-<address> of VD <name>.
WARNING	Recoverable write error occurred	Recoverable write error occurred at LBA <address>-<address> of VD <name>.
ERROR	Unrecoverable read error occurred	Unrecoverable read error occurred at LBA <address>-<address> of VD <name>.
ERROR	Unrecoverable write error	Unrecoverable write error occurred at LBA <address>-<address> of VD <name>.

	occurred	
INFO	Dedicated spare configured	PD <slot> has been configured to RG <name> as a dedicated spare disk.
INFO	Global spare configured	PD <slot> has been configured as a global spare disk.
WARNING	PD read error occurred	Read error occurred at LBA <address>-<address> of PD <slot>.
WARNING	PD write error occurred	Write error occurred at LBA <address>-<address> of PD <slot>.
WARNING	Parity wrong when scrubbing	The parity data is wrong at LBA <address>-<address> when scrubbing VD <name>.
WARNING	Data recovered when scrubbing	Data at LBA <address>-<address> has been recovered when scrubbing VD <name>.
INFO	PD freed	PD <slot> has been removed from RG <name>.
INFO	RG imported	Configuration of RG<name> has been imported.
INFO	RG restored	Configuration of RG <name> has been restored.
INFO	VD restored	Configuration of VD <name> has been restored.

- **Snapshot events**

Level	Type	Description
INFO	Snapshot deleted	The snapshot VD <name> has been deleted.
INFO	Snapshot auto deleted	The oldest snapshot VD <name> has been deleted to obtain extra snapshot space.
INFO	Snapshot taken	A snapshot on VD <name> has been taken.
INFO	Snapshot space	Set the snapshot space of VD <name> to

	configured	<number> MB.
INFO	Snapshot rollback started	Snapshot rollback of VD <name> has been started.
INFO	Snapshot rollback finished	Snapshot rollback of VD <name> has been finished.
WARNING	Snapshot quota reached	The quota assigned to snapshot <name> is reached.

iSCSI events

Level	Type	Description
INFO	iSCSI login succeeds	iSCSI login from <IP> succeeds.
INFO	iSCSI login rejected	iSCSI login from <IP> was rejected, reason [<string>]
INFO	iSCSI logout	iSCSI logout from <IP> was received, reason [<string>].

Battery backup events

Level	Type	Description
INFO	BBM sync data	Abnormal shutdown detected, start flushing battery-backuped data (<number> KB).
INFO	BBM sync data	Abnormal shutdown detected, flushing battery-backuped data finishes.
INFO	BBM detected	Battery backup module is detected.
INFO	BBM is good	Battery backup module is good.
INFO	BBM is charging	Battery backup module is charging.
WARNING	BBM is failed	Battery backup module is failed.
INFO	BBM	Battery backup feature is <item>.

JBOD events

Level	Type	Description
INFO	Disk inserted	JBOD <number> disk <slot> is inserted into system.
Warning	Disk removed	JBOD <number> disk <slot> is removed from system.
ERROR	HDD failure	JBOD <number> disk <slot> is disabled.
INFO	JBOD inserted	JBOD <number> is inserted into system
WARNING	JBOD removed	JBOD <number> is removed from system
WARNING	SMART T.E.C	JBOD <number> disk <slot>: S.M.A.R.T. Threshold Exceed Condition occurred for attribute %s
WARNING	SMART Failure	JBOD <number> disk <slot>: Failure to get S.M.A.R.T information
INFO	Dedicated spare configured	JBOD <number> PD <slot> has been configured to RG <name> as a dedicated spare disk.
INFO	Global spare configured	JBOD <number> PD <slot>d has been configured as a global spare disk.
WARNING	PD read error occurred	Read error occurred at LBA <address>-<address> of JBOD <number> PD <slot>.
WARNING	PD write error occurred	Write error occurred at LBA <address>-<address> of JBOD <number> PD <slot>.
INFO	PD freed	JBOD <number> PD <slot> has been removed from RG <name>.

System maintenance events

Level	Type	Description
INFO	System shutdown	System shutdown.
INFO	System reboot	System reboot.
INFO	FW upgrade start	Firmware upgrade start.
INFO	FW upgrade success	Firmware upgrade success.
WARNING	FW upgrade failure	Firmware upgrade failure.