JetStor SAS 712iS

User Manual

Revision 1.0

Table of Contents

2882888888888888888282828888

Before You Begin

Before going through with this manual, you should read and focus to the following safety guidelines. Notes about the subsystem's controller configuration and the product packaging and delivery are also included.

Safety Guidelines

To provide reasonable protection against any harm on the part of the user and to obtain maximum performance, user is advised to be aware of the following safety guidelines particularly in handling hardware components:

Upon receiving of the product:

❖ Place the product in its proper location.
❖ To avoid unnecessary dropping out, make sure that somebody is around for immediate assistance.
❖ It should be handled with care to avoid dropping that may cause damage to the product. Always use the correct lifting procedures.

Upon installing of the product:

❖ Ambient temperature is very important for the installation site. It must not exceed 30℃. Due to seasonal climate changes; regulate the installation site temperature making it not to exceed the allowed ambient temperature.
❖ Before plugging-in any power cords, cables and connectors, make sure that the power switches are turned off. Disconnect first any power connection if the power supply module is being removed from the enclosure.
❖ Outlets must be accessible to the equipment.
❖ All external connections should be made using shielded cables and as much as possible should not be performed by bare hand. Using anti-static hand gloves is recommended.
❖ In installing each component, secure all the mounting screws and locks. Make sure that all screws are fully tightened. Follow correctly all the listed procedures in this manual for reliable performance.

Controller Configurations

This RAID subsystem supports single controller configuration.

Packaging, Shipment and Delivery

❖ Before removing the subsystem from the shipping carton, you should visually inspect the physical condition of the shipping carton.
❖ Unpack the subsystem and verify that the contents of the shipping carton are all there and in good condition.
❖ Exterior damage to the shipping carton may indicate that the contents of the carton are damaged.
❖ If any damage is found, do not remove the components; contact the dealer where you purchased the subsystem for further instructions.

The shipping package contains the following:

	RAID Subsystem Unit
	Two (2) power cords
	Two (2) Ethernet LAN cables for single controller Note: Four (4) Ethernet LAN cables for dual controller
	One (1) External null modem cable Note: Two (2) External null modem cables for dual controller
	User Manual

NOTE: If any damage is found, contact the dealer or vendor for assistance.

Chapter 1   Introduction

The RAID Subsystem

Unparalleled Performance & Reliability
- Support Dual-active controllers
- Supports 802.3ad port trunking, Link Aggregation Control Protocol (LACP) with VLAN
- High data bandwidth of system architecture by powerful INTEL 64-bit RAID processor

Unsurpassed Data Availability
- RAID 6 capability provides the highest level of data protection
- Supports Snapshot, Volume cloning, Replication(Option)
- Supports Microsoft Windows Volume Shadow Copy Services (VSS)

Exceptional Manageability Menu-driven front panel display
- Management GUI via serial console, SSH telnet, Web and secure web(HTTPS)
- Event notification via Email and SNMP trap
- Menu-driven front panel display

Features

- 2U 12Bay rack-mount redundant RAID subsystem with SBB compliant controller.
- Supports iSCSI jumbo frame
- Supports Microsoft Multipath I/O (MPIO), MC/S
- Supports RAID levels 0, 1, 0+1, 3, 5, 6, 10, 30, 50, 60 and JBOD
- Local N-way mirror: Extension to RAID 1 level, N copies of the disk
- Global and dedicated hot spare disks
- Write-through or write-back cache policy for different application usage
- Supports greater than 2TB per volume set (64-bit LBA support)
- Supports manual or scheduling volume snapshot (up to 64 snapshot)
- Snapshot rollback mechanism
- On-line volume migration with no system down-time
- Online volume expansion
- Instant RAID volume availability and background initialization
- Supports S.M.A.R.T, NCQ and OOB Staggered Spin-up capable drives
- High efficiency power supply which compliant with 80plus

1.1   Technical Specifications

RAID Controller	iSCSI - 6G SAS
Controller	Single / Dual (Redundant)
Host Interface	Six 1Gb/s Ethernet (per controller)
Disk Interface	6Gb SAS or 6Gb SATA
SAS expansion	One 6Gb SAS (SFF-8088) (per controller)
Processor Type	Intel Xeon processor
Cache Memory	4GB~8GB/8GB~16GB DDR3 ECC SDRAM
Battery Backup	Optional Hot Pluggable BBM
Management Port support	Yes
Monitor Port support	Yes
UPS connection	Yes
RAID level	0, 1, 0+1, 3, 5, 6, 10, 30, 50, 60 and JBOD
Logical volume	Up to 4096
iSCSI Jumbo frame support	Yes
Supports Microsoft Multipath I/O (MPIO)	Yes
802.3ad Port Trunking, LACP Support	Yes
Host connection	Up to 128
Host clustering	Up to 16 for one logical volume
Manual/scheduling volume snapshot	Up to 64
Hot spare disks	Global and dedicated
Host access control	Read-Write & Read-Only
Online Volume Migration	Yes
Online Volume sets expansion	Yes
Configurable stripe size	Yes
Auto volume rebuild	Yes
N-way mirror (N copies of the disk)	Yes
Microsoft Windows Volume Shadow Copy Services (VSS)	Yes
Supports CHAP authentication	Yes
S.M.A.R.T. support	Yes

Snapshot rollback mechanism support	Yes
Platform	Rackmount
Form Factor	2U
# of Hot Swap Trays	12
Tray Lock	Yes
Disk Status Indicator	Access / Fail LED
Backplane	SAS II / SATA III Single BP
# of PS/Fan Modules	460W x 2 w/PFC
# of Fans	2
Power requirements	AC 90V ~ 264V Full Range, 10A ~ 5A, 47Hz ~ 63Hz
Relative Humidity	10% ~ 85% Non-condensing
Operating Temperature	10°C ~ 40°C (50°F ~ 104°F)
Physical Dimension	555 (L) x 482(W) x 88(H) mm
Weight (Without Disk)	14.5/16 Kg

Specification is subject to change without notice.
All company and product names are trademarks of their respective owners.

1.2 Terminology

The document uses the following terms:

|	
RAID	**R**edundant **A**rray of **I**ndependent **D**isks. There are different RAID levels with different degree of 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. A collection of removable media. One RG consists of a set of VDs and owns one RAID level attribute.
VD	**V**irtual **D**isk. Each RD could be divided into several VDs. The VDs from one RG have the same RAID level, but may have different volume capacity.
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 cell	When creating a RAID group with a compound RAID level, such as 10, 30, 50 and 60, this field indicates the number of subgroups in the RAID group. For example, 8 disks can be grouped into a RAID group of RAID 10 with 2 cells, 4 cells. In the 2-cell case, PD {0, 1, 2, 3} forms one RAID 1 subgroup and PD {4, 5, 6, 7} forms another RAID 1 subgroup. In the 4-cells, the 4 subgroups are PD {0, 1}, PD {2, 3}, PD {4, 5} and PD {6,7}.
WT	**W**rite-**T**hrough 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	**W**rite-**B**ack 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 **R**ead-**O**nly.
DS	**D**edicated **S**pare disks. The spare disks are only used by one specific RG. Others could not use these dedicated spare disks for any rebuilding purpose.
GS	**G**lobal **S**pare 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.

DG	**De**Graded 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	**S**mall **C**omputer **S**ystems **I**nterface.
SAS	**S**erial **A**ttached **S**CSI.
S.M.A.R.T.	**S**elf-**M**onitoring **A**nalysis and **R**eporting **T**echnology.
WWN	**W**orld **W**ide **N**ame.
HBA	**H**ost **B**us **A**dapter.
SES	**S**CSI **E**nclosure **S**ervices.
NIC	**N**etwork **I**nterface **C**ard.
BBM	**B**attery **B**ackup **M**odule
iSCSI	**I**nternet **S**mall **C**omputer **S**ystems **I**nterface.
LACP	**L**ink **A**ggregation **C**ontrol **P**rotocol.
MPIO	**M**ulti-**P**ath **I**nput/**O**utput.
MC/S	**M**ultiple **C**onnections per **S**ession
MTU	**M**aximum **T**ransmission **U**nit.
CHAP	**C**hallenge **H**andshake **A**uthentication **P**rotocol. An optional security mechanism to control access to an iSCSI storage system over the iSCSI data ports.
iSNS	**I**nternet **S**torage **N**ame **S**ervice.
SBB	**S**torage **B**ridge **B**ay. The objective of the Storage Bridge Bay Working Group (SBB) is to create a specification that defines mechanical, electrical and low-level enclosure management requirements for an enclosure controller slot that will support a variety of storage controllers from a variety of independent hardware vendors ("IHVs") and system vendors.
Dongle	Dongle board is for SATA II disk connection to the backplane.

1.3 RAID Levels

The subsystem can implement several different levels of RAID technology. RAID levels supported by the subsystem are shown below.

| RAID Level	Description	Min. Drives
0	Block striping is provide, which yields higher performance than with individual drives. There is no redundancy.	1
1	Drives are paired and mirrored. All data is 100% duplicated on an equivalent drive. Fully redundant.	2
N-way mirror	Extension to RAID 1 level. It has N copies of the disk.	N
3	Data is striped across several physical drives. Parity protection is used for data redundancy.	3
5	Data is striped across several physical drives. Parity protection is used for data redundancy.	3
6	Data is striped across several physical drives. Parity protection is used for data redundancy. Requires N+2 drives to implement because of two-dimensional parity scheme	4
0 + 1	Mirroring of the two RAID 0 disk arrays. This level provides striping and redundancy through mirroring.	4
10	Striping over the two RAID 1 disk arrays. This level provides mirroring and redundancy through striping.	4
30	Combination of RAID levels 0 and 3. This level is best implemented on two RAID 3 disk arrays with data striped across both disk arrays.	6
50	RAID 50 provides the features of both RAID 0 and RAID 5. RAID 50 includes both parity and disk striping across multiple drives. RAID 50 is best implemented on two RAID 5 disk arrays with data striped across both disk arrays.	6
60	RAID 60 provides the features of both RAID 0 and RAID 6. RAID 60 includes both parity and disk striping across multiple drives. RAID 60 is best implemented on two RAID 6 disk arrays with data striped across both disk arrays.	8
JBOD	The abbreviation of "Just a Bunch Of Disks". JBOD needs at least one hard drive.	1

1.4   Volume Relationship Diagram
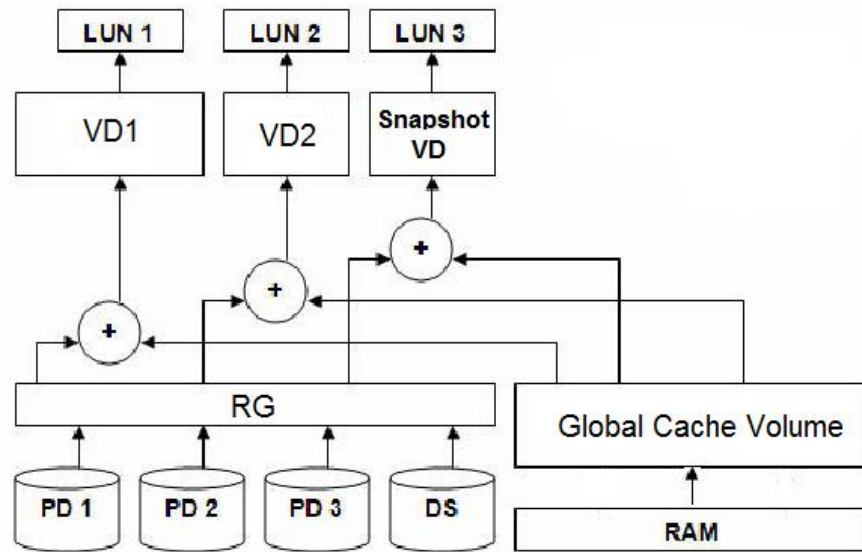
This is the design of volume structure of the RAID subsystem. It describes the relationship of RAID components. One RG (RAID Group) is composed of several PDs (Physical Disks). One RG owns one RAID level attribute. Each RG can be divided into several VDs (Virtual Disks). The VDs in one RG share the same RAID level, but may have different volume capacity. Each VD will be associated with the Global Cache Volume to execute the data transaction. LUN (Logical Unit Number) is a unique identifier, in which users can access through SCSI commands.

Chapter 2   Identifying Parts of the RAID Subsystem

The illustrations below identify the various parts of the subsystem.
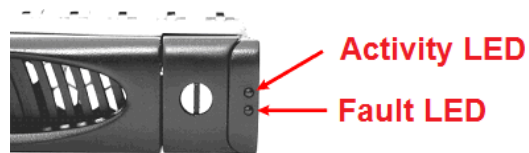
2.1   Main Components

2.1.1   Front View
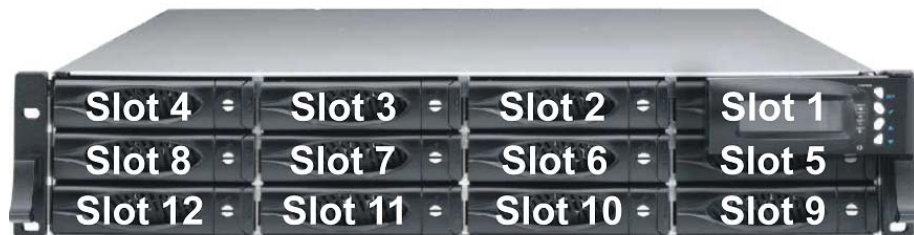
2.1.1.1 Disk Trays


HDD Status Indicator

Part	Function
HDD Activity LED	This LED will blink blue when the hard drive is being accessed.
HDD Fault LED	Green LED indicates power is on and hard drive status is good for this slot. If hard drive is defective or failed, the LED is Red. LED is off when there is no hard drive.

Lock Indicator

Every Disk Tray is lockable and is fitted with a lock indicator to indicate whether or not the tray is locked into the chassis or not. Each tray is also fitted with an ergonomic handle for easy tray removal.

When the Lock Groove is horizontal, this indicates that the Disk Tray is locked. When the Lock Groove is vertical, then the Disk Tray is unlocked.
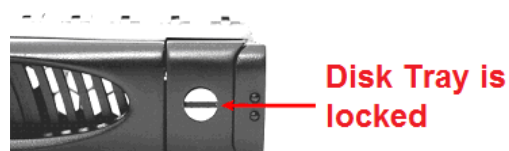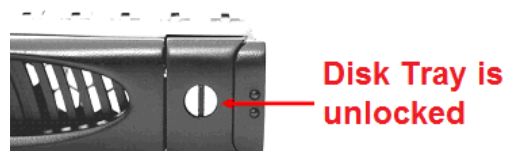
2.1.1.2 LCD Front Panel

Smart Function Front Panel

The smart LCD panel is an option to configure the RAID subsystem. If you are configuring the subsystem using the LCD panel, press the Select button to login and configure the RAID subsystem.

Parts	Function
Up and Down Arrow buttons ▲ ▼	Use the Up or Down arrow keys to go through the information on the LCD screen. This is also used to move between each menu when you configure the subsystem.
Select button ✔	This is used to enter the option you have selected.
Exit button EXIT	Press this button to return to the previous menu.

Environment Status LEDs
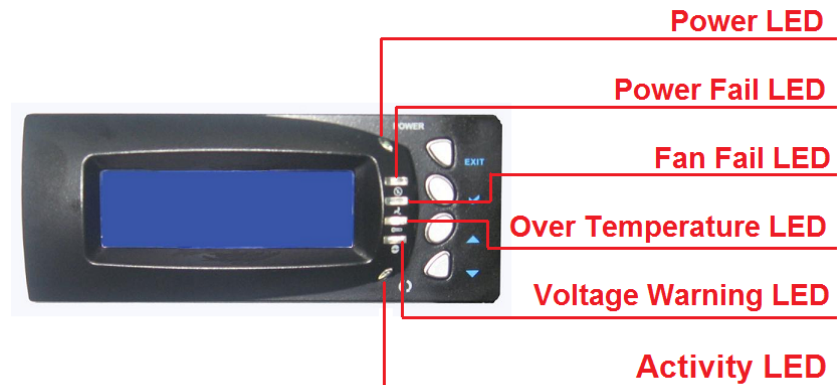
| Parts	Function
Power LED	Green LED indicates power is ON.
Power Fail LED ⊗	If a redundant power supply unit fails, this LED will turn to RED and alarm will sound.
Fan Fail LED	When a fan fails or the fan's rotational speed is below 1500RPM, this LED will turn red and an alarm will sound.
Over Temperature LED	If temperature irregularities in the system occurs (HDD slot temperature over 65°C, Controller temperature over 70°C), this LED will turn RED and alarm will sound.
Voltage Warning LED	An alarm will sound warning of a voltage abnormality and this LED will turn red.
Activity LED	This LED will blink blue when the RAID subsystem is busy or active.

2.1.2 Rear View
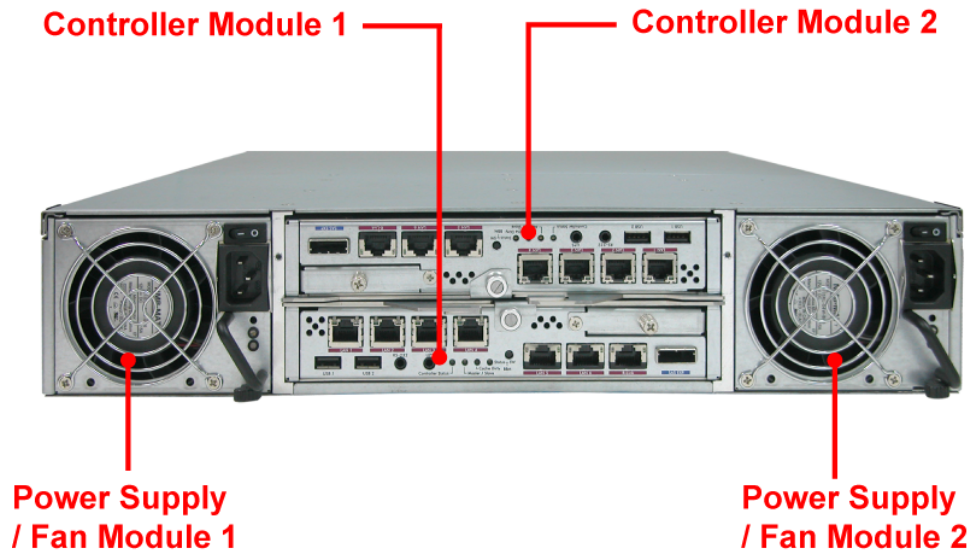
1. Controller Module

The subsystem has one or two controller modules.

2. Power Supply Unit 1 ~ 2

Two power supplies (power supply 1 and power supply 2) are located at the rear of the subsystem. Each PSFM has one Power Supply and one Fan. The PSFM 1 has Power#1, Fan#1. The PSFM 2 has Power#2, Fan#2.

Turn on the power of these power supplies to power-on the subsystem. The "power" LED at the front panel will turn green.

If a power supply fails to function or a power supply was not turned on, the " ⊗ " Power fail LED will turn red and an alarm will sound.

2.2 Controller Module

The RAID system includes single/dual iSCSI-to-6Gb SAS/SATA RAID Controller Module.
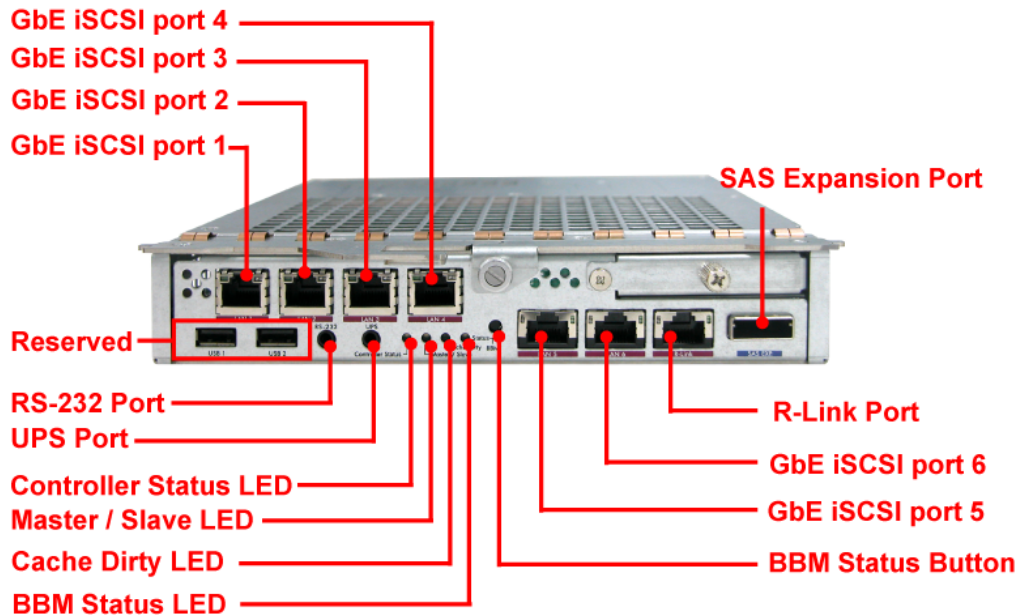
1. GbE iSCSI Ports (Gigabit)

The subsystem is equipped with six LAN data ports (LAN1, LAN2, LAN3, LAN4, LAN5, and LAN6) for iSCSI connection.

2. RS-232 Port (Console port)

3. Uninterrupted Power Supply (UPS) Port (APC Smart UPS only)

The subsystem may come with an optional UPS port allowing you to connect an APC Smart UPS device. Connect the cable from the UPS device to the UPS port located at the rear of the subsystem. This will automatically allow the subsystem to use the functions and features of the UPS.

4. Controller Status LED

- Green: Controller status normal.
- Red: System booting or controller failure.

5. Master/Slave LED (only for dual controllers)

- Green: This is the Master controller.
- Off: This is the Slave controller.

6. **Cache Dirty LED**
   - Orange: Data on the cache waiting for flush to disks.
   - Off: No data on the cache.

7. **BBM Status LED (when status button pressed)**
   - Green: BBM installed and powered.
   - Off: No BBM installed.

8. **SAS Expansion Ports**

   Use for expansion; connect to the SAS In Port of a JBOD subsystem.

9. **R-Link Port: Remote Link through RJ-45 Ethernet for remote management**

   The subsystem is equipped with one 10/100 Ethernet RJ45 LAN port for remote configuration and monitoring. You use web browser to manage the RAID subsystem through Ethernet.

10. **BBM Status Button (Used to check the battery when the power is off.)**

    When the system power is off, press the BBM status button, if the BBM LED is Green, then the BBM still has power to keep data on the cache. If not, then the BBM power is ran out and cannot keep the data on the cache anymore.

2.3   Power Supply / Fan Module (PSFM)

The RAID subsystem contains **two 460W Power Supply / Fan Modules**. All the Power Supply / Fan Modules (PSFMs) are inserted into the rear of the chassis.

2.3.1   PSFM Panel
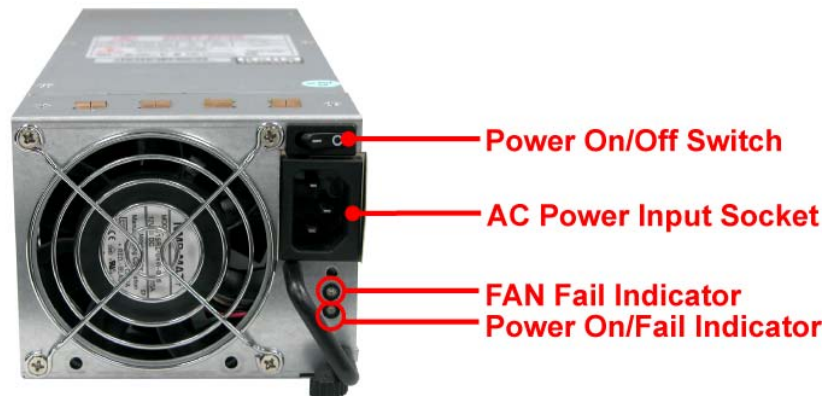
The panel of the Power Supply/Fan Module contains: the Power On/Off Switch, the AC Inlet Plug, FAN fail Indicator, and a Power On/Fail Indicator showing the Power Status LED, indicating ready or fail.

Each fan within a PSFM is powered independently of the power supply within the same PSFM. So if the power supply of a PSFM fails, the fan associated with that PSFM will continue to operate and cool the enclosure.

FAN Fail Indicator
If fan is failed, this LED will turn to RED and alarm will sound.

Power On/Fail Indicator
When the power cord connected from main power source is inserted to the AC Power Inlet, the power status LED becomes RED. When the switch of the PSFM is turned on, the LED will turn GREEN. When the Power On/Fail LED is GREEN, the PSFM is functioning normally.

NOTE: Each PSFM has one Power Supply and one Fan. The PSFM 1 has Power#1 and Fan#1. The PSFM 2 has Power#2 and Fan#2. When the Power Supply of a PSFM fails, the PSFM need not be removed from the slot if replacement is not yet available. The fan will still work and provide necessary airflow inside the enclosure.

NOTE: After replacing the Power Supply Fan Module and turning on the Power On/Off Switch of the PSFM, the Power Supply will not power on immediately. The Fans in the PSFM will spin-up until the RPM becomes stable. When Fan RPM is already stable, the RAID controller will then power on the Power Supply. This process takes more or less 30 seconds. This safety measure helps prevent possible Power Supply overheating when the Fans cannot work.

Chapter 3   Getting Started with the Subsystem

3.1   Powering On

1. Plug in the power cords into the AC Power Input Socket located at the rear of the subsystem.
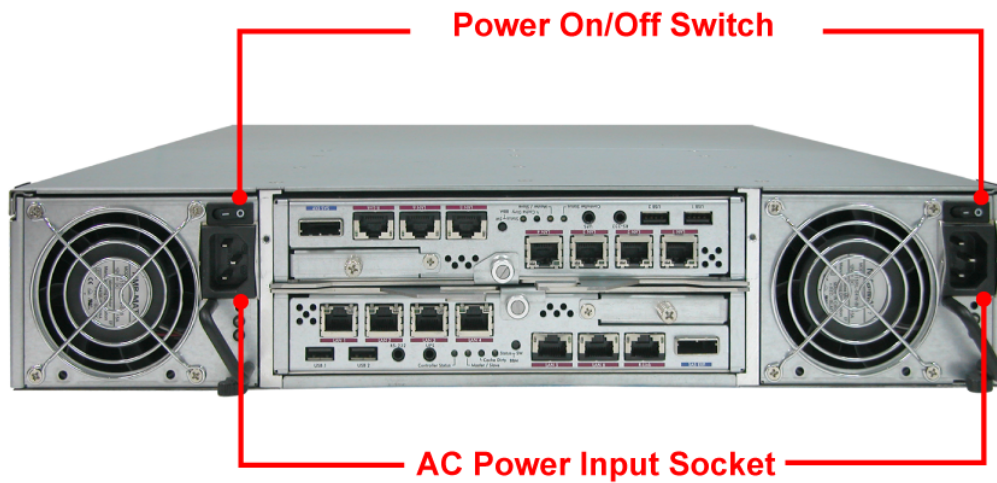
> **NOTE: The subsystem is equipped with redundant, full range power supplies with PFC (power factor correction). The system will automatically select voltage.**

2. Turn on each Power On/Off Switch to power on the subsystem.
3. The Power LED on the front Panel will turn green.

3.2 Disk Drive Installation

This section describes the physical locations of the hard drives supported by the subsystem and give instructions on installing a hard drive. The subsystem supports hot-swapping allowing you to install or replace a hard drive while the subsystem is running.

3.2.1 Installing a SAS Disk Drive in a Disk Tray

1. Unlock the Disk Trays using a flat-head screw driver by rotating the Lock Groove.
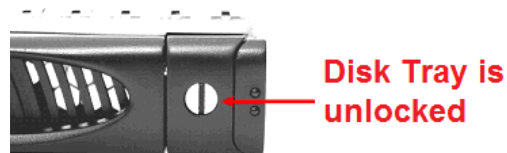
2. Press the Tray Open button and the Disk Tray handle will flip open.
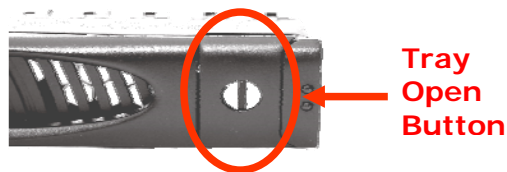
3. Pull out an empty disk tray.

4. Place the hard drive in the disk tray. Turn the disk tray upside down. Align the four screw holes of the SAS disk drive in the four Hole A of the disk tray. To secure the disk drive into the disk tray, tighten four screws on these holes of the disk tray. Note in the picture below where the screws should be placed in the disk tray holes.

Tray Hole A

NOTE: All the disk tray holes are labelled accordingly.

5. Slide the tray into a slot.

6. Press the lever in until you hear the latch click into place. The HDD Fault LED will turn green when the subsystem is powered on and HDD is good.

7. If necessary, lock the Disk Tray by turning the Lock Groove.

3.2.2 Installing a SATA Disk Drive (Dual Controller Mode) in a Disk Tray

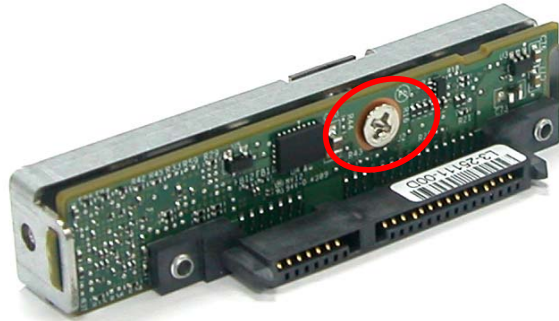1. Remove an empty disk tray from the subsystem.

2. Prepare the dongle board, the Fixed Bracket, and screws.
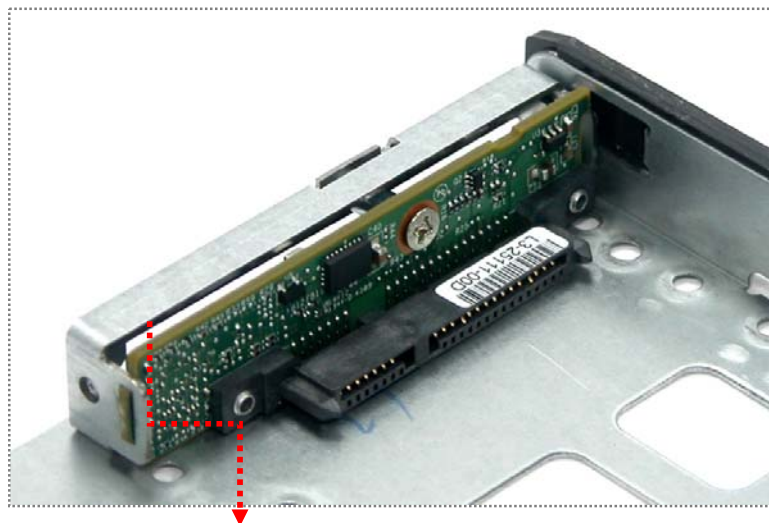
	Fixed Bracket
	Dongle Board
	Screws

3. Attach the dongle board in the Fixed Bracket with a screw.

4. Place the Fixed Bracket with the dongle board in the disk tray as shown.

5. Turn the tray upside down. Align the holes of the Fixed Bracket in the two *Hole d* of the disk tray. Tighten two screws to secure the Fixed Bracket into the disk tray.
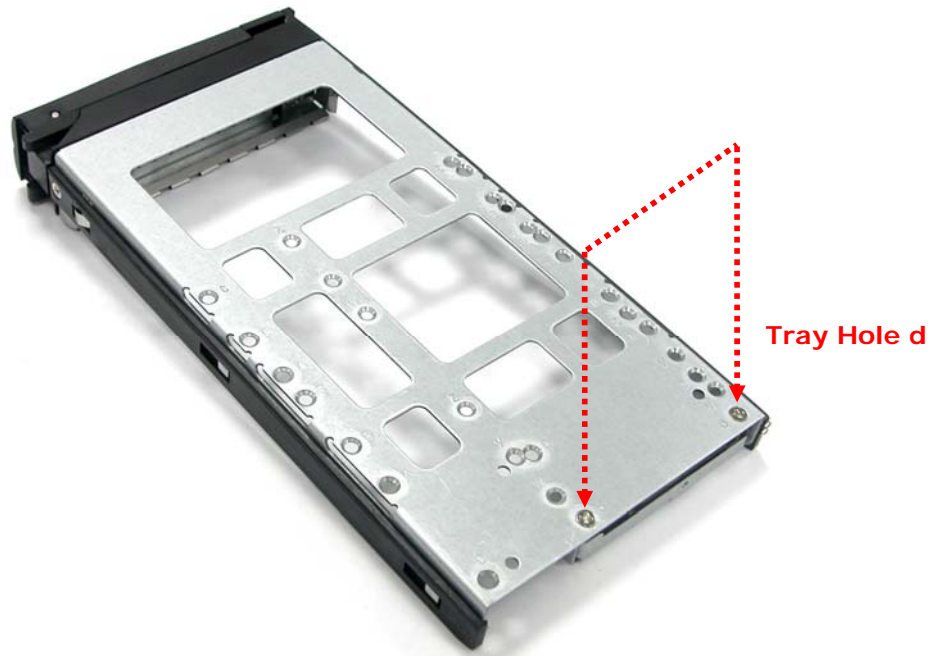
Tray Hole d

   NOTE: All the disk tray holes are labelled accordingly.

6. Place the SATA disk drive into the disk tray. Slide the disk drive towards the dongle board.

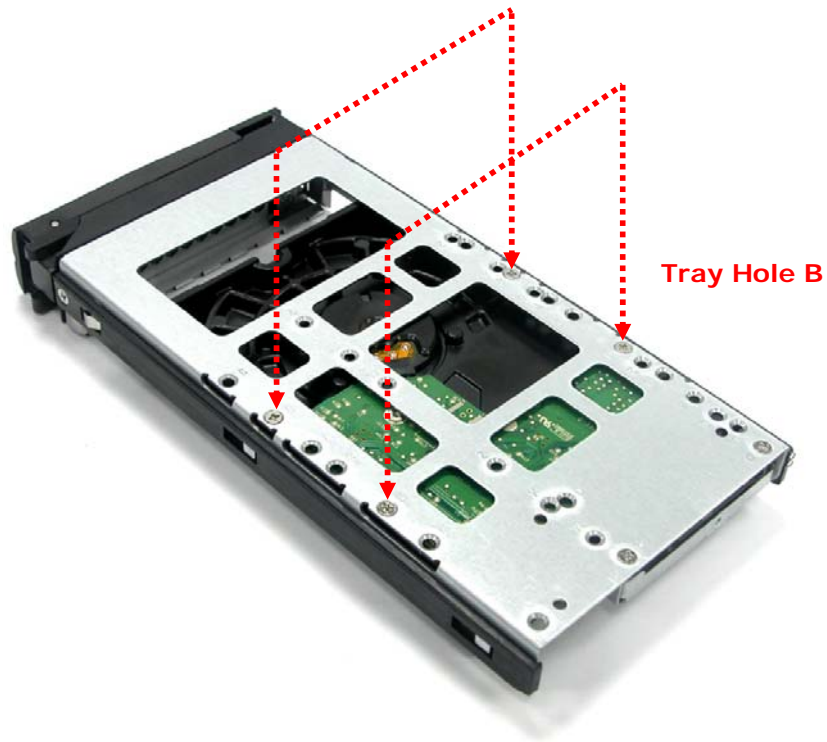7. Turn the disk tray upside down. Align the four screw holes of the SATA disk drive in the four *Hole B* of the disk tray. To secure the disk drive into the disk tray, tighten four screws on these holes of the disk tray. Note in the picture below where the screws should be placed in the disk tray holes.

Tray Hole B

NOTE: All the disk tray holes are labelled accordingly.

8. Insert the disk tray into the subsystem.

3.3 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.
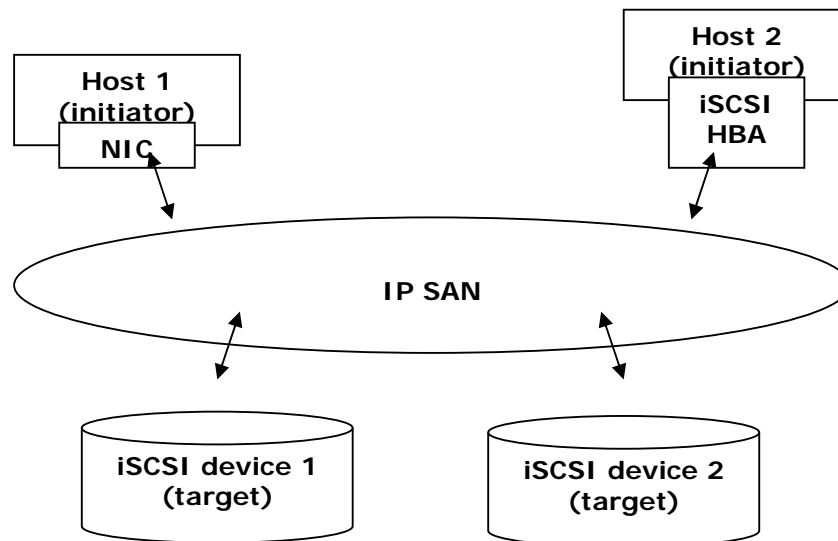
The host side needs an iSCSI initiator. The initiator is a driver which handles the SCSI traffic over iSCSI. The initiator can be software or hardware (HBA). Please refer to the certification list of iSCSI HBA(s) in Appendix A. OS native initiators or other software initiators use the standard TCP/IP 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:

1. 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 D for Microsoft iSCSI initiator installation procedure.

2. Linux iSCSI initiator is also available. For different kernels, there are different iSCSI drivers. If you need 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

3. ATTO iSCSI initiator is available for Mac.
   Website: http://www.attotech.com/xtend.html

4. Solaris iSCSI Initiator
   Version: Solaris 10 u6 (10/08)

Chapter 4   Quick Setup

4.1   Management Interfaces

There are three management methods to manage the RAID subsystem described as follows:

4.1.1   Serial Console Port

Use NULL modem cable to connect console port.

The console settings are on the following:

Baud rate: **115200**, 8 bits, 1 stop bit, and no parity.

Terminal type: **vt100**

Login name: **admin**

Default password: **00000000**

4.1.2   Remote Control – Secure Shell

SSH (secure shell) is required for remote login. 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/

Host name: **192.168.10.50 (Please check your DHCP address for this field.)**

Login name: **admin**

Default password: **00000000**

> **NOTE: This RAID Series only support SSH for remote control. For using SSH, the IP address and the password is required for login.**

4.1.3 LCD Control Module (LCM)

After booting up the system, the following screen shows management port IP and model name:

```
192.168.10.50
Model Name
```

Press "EXIT", the LCM functions **"Alarm Mute"**, **"Reset/Shutdown"**, **"Quick Install"**, **"View IP Setting"**, **"Change IP Config"** and **"Reset to Default"** will rotate by pressing ▲ (up) and ▼ (down).

When there is WARNING or ERROR level of event happening, the LCM also shows the event log to give users event information from front panel.

The following table is the function description of LCM menus.

System Info	Displays System information.
Alarm Mute	Mute alarm when error occurs.
Reset/Shutdown	Reset or shutdown controller.
Quick Install	Quick three steps to create a volume. Please refer to next chapter for operation in web UI.
Volume Wizard	Smart steps to create a volume. Please refer to next chapter for operation in web UI.
View IP Setting	Display current IP address, subnet mask, and gateway.
Change IP Config	Set IP address, subnet mask, and gateway. There are 2 selections, DHCP (Get IP address from DHCP server) or set static IP.
Reset to Default	Reset to default sets password to default: **00000000**, and set IP address to default as DHCP setting.

The following is LCM menu hierarchy.

proIPS ▲▼	[System Info.]	[Firmware Version x.x.x]			
		[RAM Size xxx MB]			
	[Alarm Mute]	[▲Yes　　No▼]			
	[Reset/Shutdown]	[Reset]	[▲Yes No▼]		
		[Shutdown]	[▲Yes No▼]		
	[Quick Install]	RAID 0 RAID 1 RAID 3 RAID 5 RAID 6 RAID 0+1 xxx GB	[Apply The Config]	[▲Yes No▼]	
	[Volume Wizard]	[Local] RAID 0 RAID 1 RAID 3 RAID 5 RAID 6 RAID 0+1	[Use default algorithm]	[Volume Size] xxx GB	[Apply The Config] [▲Yes No▼]
		[JBOD x] ▲▼ RAID 0 RAID 1 RAID 3 RAID 5 RAID 6 RAID 0+1	[new x disk] ▲▼ xxx BG	Adjust Volume Size	[Apply The Config] [▲Yes No▼]
	[View IP Setting]	[IP Config] [Static IP]			
		[IP Address] [192.168.010.050]			
		[IP Subnet Mask] [255.255.255.0]			
		[IP Gateway] [192.168.010.254]			
	[Change IP Config]	[DHCP]	[▲Yes No▼]		
		[Static IP]	[IP Address]	Adjust IP address	
			[IP Subnet Mask]	Adjust Submask IP	
			[IP Gateway]	Adjust Gateway IP	
			[Apply IP Setting]	[▲Yes No▼]	
	[Reset to Default]	[▲Yes　　No▼]			

CAUTION! Before power off, it is better to execute "Shutdown" to flush the data from cache to physical disks.

4.1.4 Web GUI

The RAID subsystem supports graphical user interface (GUI) to operate the system. Be sure to connect the LAN cable. The default IP setting is **DHCP**; open the browser and enter:

http://192.168.10.50 (Please check the DHCP address first on LCM)

Click any function at the first time; it will pop up a dialog window for authentication.

User name: **admin**
Default password: 00000000

After login, you can choose the function blocks on the left side of window to do configuration.

There are seven indicators at the top-right corner.

	RAID light: · **Green** → RAID works well. · **Red** → RAID fails.
	Temperature light: · **Green** → Temperature is normal. · **Red** → Temperature is abnormal.
	Voltage light: · **Green** → voltage is normal. · **Red** → voltage is abnormal.
	UPS light: · **Green** → UPS works well. · **Red** → UPS fails.
	Fan light: · **Green** → Fan works well. · **Red** → Fan fails.
	Power light: · **Green** → Power works well. · **Red** → Power fails.
	Dual controller light: · **Green** → Both controller1 and controller2 are present and well. · **Orange** → The system is degraded and there is only 1 controller alive and well.
	Return to home page.
	Logout the management web UI.
	Mute alarm beeper.

4.2 How to Use the System Quickly

4.2.1 Quick Installation

Please make sure that there are some free drives installed in this system. SAS drivers are recommended. Please check the hard drive details in **"/ Volume configuration / Physical disk"**.

Step 1: Click **"Quick installation"** menu item. Follow the steps to set up system name and date/time.

Step2: Confirm the management port IP address and DNS, and then click **"Next"**.

Step 3: Set up the data port IP and click **"Next"**.

Step 4: Set up the RAID level and volume size and click **"Next"**.

Quick installation

Step 4 : Volume setting

RAID level :
- RAID 0(339 GB) -
  - **RAID 0(339 GB) -**
  - RAID 1(33 GB) -
  - RAID 3(305 GB) -
  - RAID 5(305 GB) -
  - RAID 6(271 GB) -
  - RAID 0+1(169 GB) -

Cancel   << Back   Next >>

Step 5: Check all items, and click **"Finish"**.

Quick installation

Confirm

System name
System name :Model_Name

Network setting
Address :192.168.220.149
Mask :255.255.255.0
Gateway :192.168.220.7
DNS : 8.8.8.8
HTTP port :80, HTTPS port : 443, SSH port : 22

iSCSI IP address
Address : 192.168.1.1
Mask : 255.255.255.0
Gateway : 192.168.1.254

Cancel   << Back   Finish

Step 6: Done.

4.2.2 Volume Creation Wizard

"Volume create wizard" has a smarter policy. When the system is inserted with some HDDs. **"Volume create wizard"** lists all possibilities and sizes in different RAID levels, it will use all available HDDs for RAID level depends on which user chooses. When system has different sizes of HDDs, e.g., 8*200G and 8*80G, it lists all possibilities and combination in different RAID level and different sizes. After user chooses RAID level, user may find that some HDDs are available (free status). It gives user:

1. Biggest capacity of RAID level for user to choose and,
2. The fewest disk number for RAID level / volume size.

E.g., user chooses RAID 5 and the controller has 12*200G + 4*80G HDDs inserted. If we use all 16 HDDs for a RAID 5, and then the maximum size of volume is 1200G (80G*15). By the wizard, we do smarter check and find out the most efficient way of using HDDs. The wizard only uses 200G HDDs (Volume size is 200G*11=2200G), the volume size is bigger and fully uses HDD capacity.

Step 1: Select **"Volume create wizard"** and then choose the RAID level. After the RAID level is chosen, click **"Next"**.

Step 2: Please select the combination of the RG capacity, or **"Use default algorithm"** for maximum RG capacity. After RG size is chosen, click **"Next"**.

Step 3: Decide VD size. User can enter a number less or equal to the default number. Then click **"Next"**.

Step 4: Confirmation page. Click **"Finish"** if all setups are correct. Then a VD will be created.

Step 5: Done. The system is available now.

	Name	Size(GB)	Write	Priority	Bg rate	Type	Clone	Schedule	Status	Health	R %	RAID	#LUN	Snapshot space(GB)	#Snapshot	RG
OP	QUICK71147	1862	WB	HI	4	RAID	N/A	N/A	Online	Optimal		RAID 0	1	0/0	0	QUICK42321

NOTE: A virtual disk of RAID 0 is created and is named by system itself.

Chapter 5   Configuration

5.1   Web GUI Management Interface Hierarchy

The below table is the hierarchy of the management GUI.

System configuration

System setting	→	System name / Date and time / System indication
Network settin g	→	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

NIC	→	Show information for:(Controller 1/ Controller 2) Aggregation / IP settings for iSCSI ports / Become default gateway / Enable jumbo frame / Ping host
Entity property	→	Entity name / iSNS IP
Node	→	Show information for:(Controller 1/ Controller 2) Authenticate / Change portal / Rename alias/ User
Session	→	Show information for:(Controller 1/ Controller 2) List connection / Delete
CHAP account	→	Create / Modify user information / Delete

Volume configuration

Physical disk	→	Set Free disk / Set Global spare / Set Dedicated spare / Upgrade / Disk Scrub / Turn on/off the indication LED / More information
RAID group	→	Create / Migrate / Activate / Deactivate / Parity check / Delete / Set preferred owner /Set disk property / More information
Virtual disk	→	Create / Extend / Parity check / Delete / Set property / Attach LUN / Detach LUN / List LUN / Set clone / Clear clone / Start clone / Stop clone / Schedule clone / Set snapshot space / Cleanup snapshot / Take snapshot / Auto snapshot / List snapshot / More information
Snapshot	→	Set snapshot space / Auto snapshot / Take snapshot / Export / Rollback / Delete/ Cleanup snapshot
Logical unit	→	Attach / Detach/ Session

Enclosure management

Hardware monitor	→	Controller 1 / BPL / Controller 2 / Auto shutdown
UPS	→	UPS Type / Shutdown battery level / Shutdown delay / Shutdown UPS
SES	→	Enable / Disable
S.M.A.R.T.	→	S.M.A.R.T. information **(Only for SATA hard drives)**

Maintenance

System information	→	System information
Event log	→	Download / Mute / Clear
Upgrade	→	Browse the firmware to upgrade
Firmware synchronization	→	Synchronize the slave controller's firmware version with the master's
Reset to factory default	→	Sure to reset to factory default?
Import and export		Import/Export / Import file
Reboot and shutdown	→	Reboot / Shutdown

Quick installation Step 1 / Step 2 / Step 3 / Step 4 / Confirm

Volume creation wizard Step 1 / Step 2 / Step 3 / Confirm

5.2 System Configuration

"System configuration" is designed for setting up the **"System setting"**, **"Network setting"**, **"Login setting"**, **"Mail setting"**, and **"Notification setting"**.
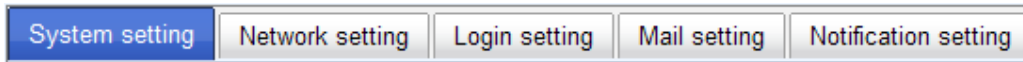
5.2.1 System Setting

"System setting" can be used to set system name and date. Default **"System name"** is composed of model name and serial number of this system.

Check **"Change date and time"** to set up the current date, time, and time zone before using or synchronize time from NTP (Network Time Protocol) server. Click **"Confirm"** in **System indication** to turn on the system indication LED. Click again to turn off.

5.2.2 Network Setting

"Network setting" is for changing IP address for remote administration usage. There are 2 options, DHCP (Get IP address from DHCP server) and static IP. The default setting is DHCP. User can change the HTTP, HTTPS, and SSH port number when the default port number is not allowed on host/server.

5.2.3 Login Setting

"Login setting" can set single admin, auto logout time and Admin/User password. The single admin can prevent multiple users access the same controller at the same time.

1. **Auto logout**: The options are (1) Disable; (2) 5 minutes; (3) 30 minutes; (4) 1 hour. The system will log out automatically when user is inactive for a period of time.
2. **Login lock**: Disable/Enable. When the login lock is enabled, the system allows only one user to login or modify system settings.

System setting	Network setting	Login setting	Mail setting	Notification setting

Setup Login configuration and password.

If Auto logout time is set, the system will log out automatically when user is inactive for a period of time. When the login lock is enabled, the system allows only one user to login or modify system settings.

Login configuration

Auto logout :	- Disable - ▼
Login lock :	- Disable - ▼

Admin password

☐ Change admin password

Old password :

Password :

Confirm :

User password

☐ Change password

Password :

Confirm :

Confirm

Check **"Change admin password"** or **"Change user password"** to change admin or user password. The maximum length of password is 12 characters.

5.2.4 Mail Setting

"Mail setting" can accept at most 3 mail-to address entries for receiving the event notification. 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 or working. User can also select which levels of event logs are needed to be sent via Mail. Default setting only enables ERROR and WARNING event logs. Please also make sure the DNS server IP is well-setup so the event notification mails can be sent successfully.

System setting	Network setting	Login setting	Mail setting	Notification setting

Enter at most 3 mail addresses for receiving the event notification. Some mail servers would check 'Mail-from address' and need authentication for anti-spam.
After information is set, you can click 'Send test mail' to test whether email functions are available.

Mail

Mail-from address :	mailman@yourcompany.com
Mail-to address 1 :	
Send events1 :	☐ INFO ☑ WARNING ☑ ERROR
Mail-to address 2 :	
Send events2 :	☐ INFO ☑ WARNING ☑ ERROR
Mail-to address 3 :	
Send events3 :	☐ INFO ☑ WARNING ☑ ERROR

☐ **SMTP relay** ▾

SMTP server :	
Authentication :	None ▾
Account :	
Password :	
Confirm :	

[Send test mail]

[Confirm]

5.2.5 Notification Setting

"**Notification setting**" can be used to set up SNMP trap for alerting via SNMP, pop-up message via Windows messenger (not MSN), alert via syslog protocol, and event log filter.

"**SNMP**" allows up to 3 SNMP trap addresses. Default community name is set as "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/

Using "**Messenger**", user 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. User can choose the event log levels and default setting enables the WARNING and ERROR event logs.

Using "**System log server**", user 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.

Configuration
The following configuration is a sample for target and log server setting:

Target side
1. Go to \System configuration\Notification setting\System log server.
2. Fill the fields
3. Server IP/hostname: enter the IP address or hostname of system log server.
4. UDP Port: enter the UDP port number on which system log server is listening to. The default port number is 514.
5. Facility: select the facility for event log.
6. Event level: Select the event log options.
7. Click "Confirm" button.

Server side (Linux – RHEL4)
The following steps are used to log RAID subsystem messages to a disk file. In the following, all messages are setup with facility "Local1" and event level "WARNING" or higher are logged to /var/log/raid.log.
1. Flush firewall
2. Add the following line to /etc/syslog.conf
Local1.warn /var/log/raid.log
3. Send a HUP signal to syslogd process, this lets syslogd perform a re-initialization. All open files are closed, the configuration file (default is /etc/syslog.conf) will be reread and the syslog(3) facility is started again.
4. Activate the system log daemon and restart
Note: sysklogd has a parameter "-r" , which will enable sysklogd to receive message from the network using the internet domain socket with the syslog service, this option is introduced in version 1.3 of sysklogd package.
5. Check the syslog port number,
e.g. , 10514
6. Change controller's system log server port number as above
Then, syslogd will direct the selected event log messages to /var/log/raid.log when syslogd receive the messages from RAID subsystem.
For more detail features, please check the syslogd and syslog.conf manpage (e.g.,man syslogd).

Server side (Windows 2003)
Windows doesn't provide system log server, user needs to find or purchase a client from third party, below URL provide evaluation version, you may use it for test first. http://www.winsyslog.com/en/
1. Install winsyslog.exe
2. Open "Interactives Syslog Server"
3. Check the syslog port number, e.g., 10514
4. Change controller's system log server port number as above
5. Start logging on "Interactives Syslog Server"

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/
Most UNIX systems have built-in syslog daemon.

"Event log filter" setting can enable event level on "Pop up events" and "LCM".

5.3 iSCSI Configuration

"iSCSI configuration" is designed for setting up the **"Entity Property"**, **"NIC"**, **"Node"**, **"Session"**, and **"CHAP account"**.
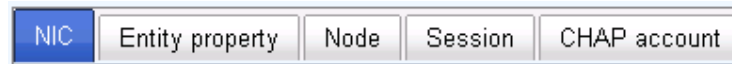
5.3.1 NIC

"NIC" function is used to change the IP addresses of iSCSI data ports. The RAID subsystem has six gigabit LAN ports to transmit data. Each of them must be assigned to one IP address in multi-homed mode unless the link aggregation or trunking mode has been selected. When there are multiple data ports setting up in link aggregation or trunking mode, all the data ports share single address.

Show information for: Controller 1
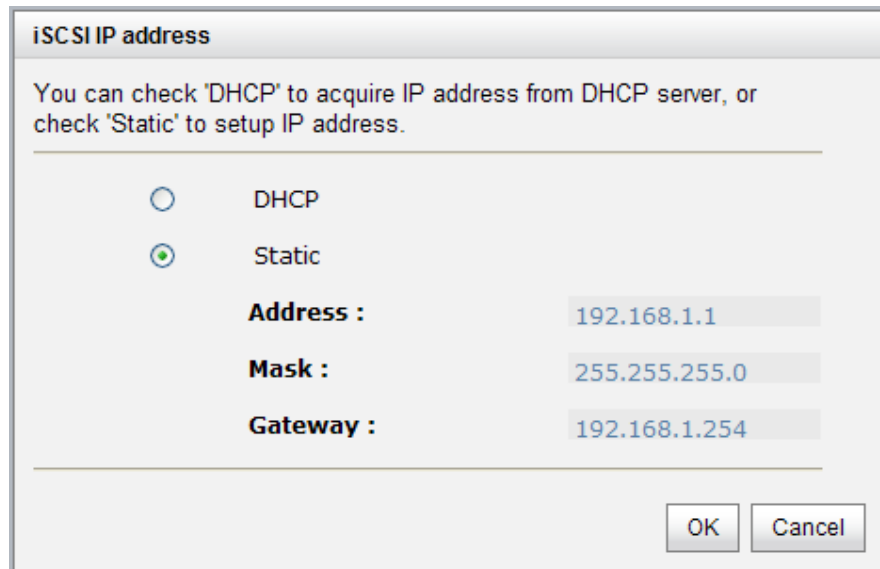
	Name	LAG	LAG No	VLAN ID	DHCP	IP address	Netmask	Gateway	Jumbo frame	MAC address	Link
OP.	LAN1	No	N/A	N/A	No	192.168.1.1	255.255.255.0	192.168.1.254	Disabled	00:13:78:c7:02:d8	Down
OP.	LAN2	No	N/A	N/A	No	192.168.2.1	255.255.255.0	192.168.2.254	Disabled	00:13:78:c7:02:d9	Down
OP.	LAN3	No	N/A	N/A	No	192.168.3.1	255.255.255.0	192.168.3.254	Disabled	00:13:78:c7:02:da	Down
OP.	LAN4	No	N/A	N/A	No	192.168.4.1	255.255.255.0	192.168.4.254	Disabled	00:13:78:c7:02:db	Down
OP.	LAN5	No	N/A	N/A	No	192.168.5.1	255.255.255.0	192.168.5.254	Disabled	00:13:78:c7:02:dc	Down
OP.	LAN6	No	N/A	N/A	No	192.168.6.1	255.255.255.0	192.168.6.254	Disabled	00:13:78:c7:02:dd	Down

Link aggregation
Set VLAN ID
IP settings for iSCSI ports
Become default gateway
Enable jumbo frame
Ping host

There are six iSCSI data ports on each controller. Six data ports are set with static IP.

IP settings:

User can change IP address by moving the mouse to the gray button of LAN port, click **"IP settings for iSCSI ports"**. There are 2 selections, DHCP (Get IP address from DHCP server) or static IP.

iSCSI IP address
You can check 'DHCP' to acquire IP address from DHCP server, or check 'Static' to setup IP address.

○　　DHCP

◉　　Static

Address :　　　192.168.1.1

Mask :　　　255.255.255.0

Gateway :　　　192.168.1.254

OK　Cancel

Default gateway:

Default gateway can be changed by moving the mouse to the gray button of LAN port, click **"Become default gateway"**. There is only one default gateway.

MTU / Jumbo frame:

MTU (**M**aximum **T**ransmission **U**nit) size can be enabled by moving mouse to the gray button of LAN port, click **"Enable jumbo frame"**.

⚠ **WARNING! The MTU size of network switch and HBA on host must be enabled. Otherwise, the LAN connection will not work properly.**

Multi-homed / Trunking / LACP:

The following is the description of multi-homed/trunking/LACP.

1. **Multi-homed**: Default mode. Each of iSCSI data port is connected by itself and is not set to link aggregation and trunking. Selecting this mode can also remove the setting of Trunking/LACP at the same time.

2. **Trunking**: defines the use of multiple iSCSI data ports in parallel to increase the link speed beyond the limits of any single port.

3. **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) increase in bandwidth, and (2) failover when link status fails on a port.

Trunking/LACP setting can be changed by clicking the button **"Aggregation"**.

Select at least two NICs for link aggregation.

For example, LAN1 and LAN2 are set to Trunking mode. To remove Trunking/LACP setting, mouse move to the gray button of LAN port, click **"Delete link aggregation"**. Then it will pop up a message to confirm.

Ping host:

User can ping the corresponding host data port from the target, click **"Ping host"**.

Please input the host IP:

192.168.1.2

Start   Stop

```
Reply from 192.168.1.2: time<1ms
Reply from 192.168.1.2: time<1ms
Reply from 192.168.1.2: time<1ms
Reply from 192.168.1.2: time<1ms
Reply from 192.168.1.2: time<1ms
Reply from 192.168.1.2: time<1ms
```
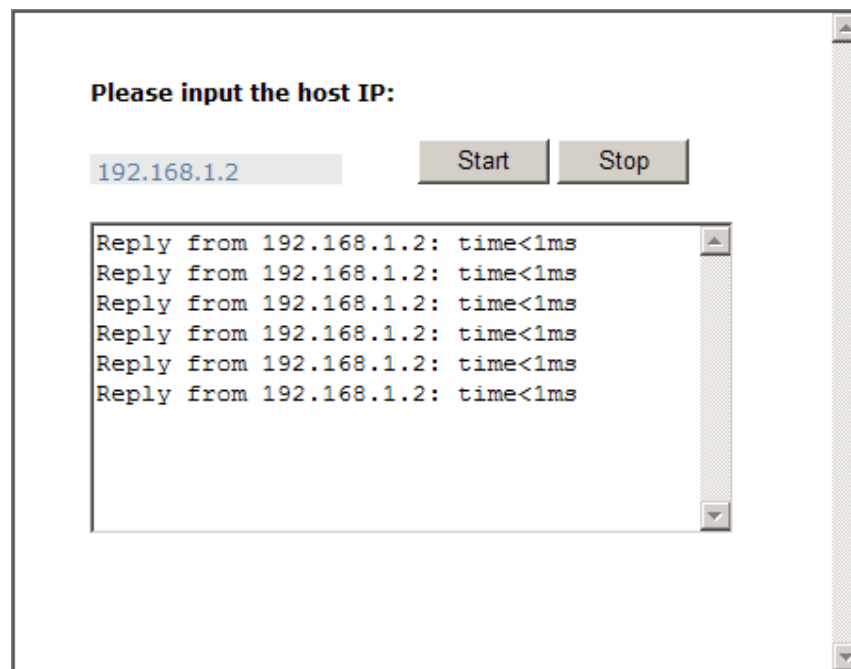
A user can ping host from the target to make sure the data port connection is well.

5.3.2 Entity Property

 "**Entity property**" can view the entity name of the system, and setup **"iSNS IP"** for iSNS (Internet Storage Name Service). iSNS protocol allows automated discovery, management and configuration of iSCSI devices on a TCP/IP network. Using iSNS, it needs to install an iSNS server in SAN. Add an iSNS server IP address into iSNS server lists in order that iSCSI initiator service can send queries. The entity name can be changed.

Setup the entity name and iSNS IP.

iSNS protocol allows automated discovery, management and configuration of iSCSI devices on a TCP/IP network. Add an iSNS server IP address into iSNS server lists in order that iSCSI initiator service can send queries.

Entity name :

iSNS IP :

Confirm

5.3.3 Node

"**Node**" can be used to view the target name for iSCSI initiator. There are 128 default nodes created for each controller.

CHAP:

CHAP is the abbreviation of **C**hallenge **H**andshake **A**uthorization **P**rotocol. CHAP is a strong authentication method used in point-to-point for user login. It's a type of authentication in which the authentication server sends the client a key to be used for encrypting the username and password. CHAP enables the username and password to transmitting in an encrypted form for protection.

To use CHAP authentication, please follow these steps:

1. Select one of 128 default nodes from one controller.
2. Check the gray button of "**OP.**" column, click "**Authenticate**".
3. Select "**CHAP**".

4. Click **"OK"**.

5. Go to **"/ iSCSI configuration / CHAP account"** page to create CHAP account. Please refer to next section for more detail.
6. Check the gray button of **"OP."** column, click **"User"**.
7. Select CHAP user(s) which will be used. It's a multi option; it can be one or more. If choosing none, CHAP cannot work.

8. Click **"OK"**.
9. In **"Authenticate"** of **"OP"** page, select **"None"** to disable CHAP.

Change portal:

Users can change the portals belonging to the device node of each controller.

1. Check the gray button of **"OP."** column next to one device node.
2. Select **"Change portal"**.
3. Choose the portals for the controller.
4. Click **"OK"** to confirm.

Rename alias:

User can create an alias to one device node.

1. Check the gray button of **"OP."** column next to one device node.
2. Select **"Rename alias"**.
3. Create an alias for that device node.
4. Click **"OK"** to confirm.
5. An alias appears at the end of that device node.

NOTE: After setting CHAP, the initiator in host/server should be set the same CHAP account. Otherwise, user cannot login.

5.3.4 Session

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

1. TSIH (target session identifying handle)
2. Host (Initiator Name)
3. Controller (Target Name)
4. InitialR2T(Initial Ready to Transfer)
5. Immed. data(Immediate data)
6. MaxDataOutR2T(Maximum Data Outstanding Ready to Transfer)
7. MaxDataBurstLen(Maximum Data Burst Length)
8. DataSeginOrder(Data Sequence in Order)
9. DataPDUInOrder(Data PDU in Order)
10. Detail of Authentication status and Source IP: port number.

Move the mouse pointer to the gray button of session number, click **"List connection"**. It will list all connection(s) of the session.

No.	Initiator IP	Initiator name	MaxRecvDataSegLen	MaxTransDataSegLen	Authentication
1	192.168.1.2	iqn.1991-05.com.microsoft:win-pgti2lonu8k	16384	65536	CHAP

OK

5.3.5 CHAP Account

"CHAP account" is used to manage CHAP accounts for authentication. This RAID subsystem allows creation of many CHAP accounts.

To setup CHAP account, please follow these steps:

1. Click **"Create"**.
2. Enter **"User"**, **"Secret"**, and **"Confirm"** secret again. **"Node"** can be selected here or later. If selecting none, it can be enabled later in **"/ iSCSI configuration / Node / User"**.

3. Click **"OK"**.

4. Click **"Delete"** to delete CHAP account.

5.4 Volume Configuration

"Volume configuration" is designed for setting up the volume configuration which includes **"Physical disk"**, **"RAID group"**, **"Virtual disk"**, **"Snapshot"**, **"Logical**

unit", and **QReplica** (This option is only visible when QReplica license is enabled.) option tabs.
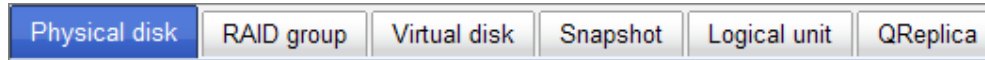
5.4.1 Physical Disk

The **Physical disk** tab provides the status of the hard drives in the system. The two drop-down lists at the top enable you to switch between the local system and any expansion JBOD systems attached. The other is to change the drive size units (MB or GB).

The options are available on this tab:

- **Disk Health Check**: Click the **Disk Health Check** button to check free disks. It can not check the disks which are in used.

- **Disk Check Report**: Click the **Disk Check Report** button to download disk check report.

- **OP.** → **Set Free disk**: Make the selected hard drive be free for use.

- **OP.** → **Set Global spare**: Set the selected hard drive to global spare of all RGs.

- **OP.** → **Set Dedicated spare**: Set a hard drive to dedicated spare of the selected RG.

- **OP.** → **Upgrade**: Upgrade hard drive firmware.

- **OP.** → **Disk Scrub**: Scrub the hard drive.

- **OP.** → **Turn on/off the indication LED**: Turn on the indication LED of the hard drive. Click again to turn off.

- **OP.** → **More information**: Show hard drive detail information.

Take an example to set the fourth PD to dedicated spare disk.

1. Check **OP.** → **Set Dedicated spare** at the fourth PD.

	No.	Name	Total	Free	#PD	#VD	Status	Health	RAID
⊙	1	RG-R5	3725	3725	3	0	Online	Good	RAID 5

Set Dedicated spare

Submit   Cancel

2. If there is any RG which is in protected RAID level and can be set with dedicate spare disk, select one RG, and then click **Submit** button.

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	Related RAID group name.
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. · **"Scrubbing"** → the hard drive is being scrubbed.
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	The usage of hard drive: · **"RAID disk"** → This hard drive has been set to a RAID group. · **"Free disk"** → This hard drive is free for use. · **"Dedicated spare"** → This hard drive has been set as dedicated spare of a RG. · **"Global spare"** → This hard drive has been set as global spare of all RGs.
Vendor	Hard drive vendor.
Serial	Hard drive serial number.
Type	Hard drive type.

	"SATA 1.5G" → SATA disk.
	"SATA 3.0G" → SATA II disk.
	"SATA 6.0G" → Sata III disk.
	"SAS 3.0G" → SAS disk.
	"SAS 6.0G" → SAS 2 disk.
Write cache	Hard drive write cache is enabled or disabled.
Standby	HDD auto spindown function to save power. The default value is disabled.
Readahead	Readahead function of HDD. Default value is enabled
Command Queuing	Command Queue function of HDD. Default value is enabled.

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.
Disk Scrub	Scrub the hard drive.
Turn on/off the indication LED	Turn on the indication LED of the hard drive. Click again to turn off.
More information	Show hard drive detail information.

5.4.2 RAID Group

"RAID group" can view the status of each RAID group, create, and modify RAID groups. The following is an example to create a RG.

Select the traditional RAID group, it displays on the following.

Select the thin provisioning RAID group, it displays on the following. There are two more tables to describe the properties of thin provisioning RAID group, RAID Set and RAID Group Policy.

RG column description:

	The button includes the functions which can be excuted.
Name	RAID group name.
Total(GB)(MB)	Total capacity of this RAID group. The unit can be

	displayed in GB or MB.
Free(GB) (MB)	Free capacity of this RAID group. The unit can be displayed in GB or MB.
Thin **(This option is only visible when Thin is enabled.)**	The status of Thin: • Disabled. • Enabled.
#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. **"Scrubbing"** → 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.
Current owner	The owner of the RAID group. Please refer to next chapter for details.
Preferred owner	The preferred owner of the RAID group. The default owner is controller 1.

RG operations description:

Create	Create a RAID group.
Migrate	Change the RAID level of a RAID group. Please refer to next chapter for details.

Move	Move the member disks of RAID group to totally different physical disks.
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.
Parity Check	Regenerate parity for the RAID group. It supports RAID 3 / 5 / 6 / 30 / 50 / 60.
Delete	Delete a RAID group.
Set preferred owner	Set the RG ownership to the other controller.
Set disk property	Change the disk property of write cache and standby options. Write cache: · **"Enabled"** → Enable disk write cache. (Default) · **"Disabled"** → Disable disk write cache. Standby: · **"Disabled"** → Disable auto spindown. (Default) · **"30 sec / 1 min / 5 min / 30 min"** → Enable hard drive auto spindown to save power when no access after certain period of time. Read ahead: · **"Enabled"** → Enable disk read ahead. (Default) · **"Disabled"** → Disable disk read ahead. Command queuing: · **"Enabled"** → Enable disk command queue. (Default) · **"Disabled"** → Disable disk command queue.
Add Raid set	Add RAID set for thin provisioning RAID group.
Add policy	Add policy for thin provisioning RAID group.
More information	Show RAID group detail information.

Raid set column description:

No	Number of RAID set.
Total size (GB)	Total capacity of this RAID set.

Free size (GB)	Free capacity of this RAID set.
#PD	The number of physical disks in a RAID set.
RAID Cell	The number of RAID cell.
Status	The status of RAID set: • 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. • Scrubbing: the RAID group is being scrubbed.
Health	The health of RAID set: • Good: the RAID group is good. • Failed: the RAID group fails. • Degraded: the RAID group is not healthy and not completed. The reason could be lack of disk(s) or have failed disk

Take an example of creating a RAID group.

1. Click the **Create** button.

2. Enter a **Name** for the RAID group.

3. Use the drop-down list to select a **RAID level**.

4. Click the **Select PD** button to select disks from either local or expansion JBOD systems, and click **OK** to complete the selection. The selected disks are displayed at **RAID PD slot**.

5. Optionally, configure the following:

   ■ **Preferred owner**: This option is only visible when dual controllers are installed. The default value is Auto.

- ■ **Thin provisioning**: This option is only visible when thin provisioning feature is enabled. The default value is Disabled.

- ■ **Write Cache**: It's to enable or disable the write cache option of hard drives. The default value is Disabled.

- ■ **Standby**: It's to enable or disable the auto spindown function of hard drives, when this option is enabled and hard drives have no I/O access after certain period of time, they will spin down automatically. The default value is Disabled.

- ■ **Readahead**: It's to enable or disable the read ahead function. The default value is Enabled.

- ■ **Command queuing**: It's to enable or disable the hard drives' command queue function. The default value is Enabled.

6. Click **OK** button to create the RAID group.

7. At the confirmation message, click **OK** button.

5.4.3   Virtual Disk

"Virtual disk" can view the status of each Virtual disk, create, and modify virtual disks. The following is an example to create a VD.

Step 1: Click **"Create"**, enter **"Name"**, select RAID group from **"RG name"**, enter required **"Capacity (GB)/(MB)"**, **change "Stripe height (KB)"**, change **"Block size (B)"**, change **"Read/Write"** mode, set virtual disk **"Priority"**, select **"Bg rate"** (Background task priority), and change **"Readahead"** option if necessary. **"Erase"** option will wipe out old data in VD to prevent that OS recognizes the old partition. There are three options in "Erase": None (default), erase first 1GB or full disk. Last, select **"Type"** mode for normal or clone usage. Then click **"OK"**.

Create
Name :	VD-01
RG name :	RG-R0 ▼
Capacity :	30	GB ▼
Stripe height (KB) :	64 ▼
Block size (B) :	512 ▼
Read/Write :	○ Write-through cache ◉ Write-back cache ⑫
Priority :	◉ High priority ○ Middle priority ○ Low priority
Bg rate :	4 ▼ ⑫
Readahead :	Enabled ▼ ⑫
AV-media mode :	Disabled ▼
Erase :	None ▼
Type :	RAID ▼
	RAID
	BACKUP
	OK Cancel

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

		Name	Size(GB)	Write	Priority	Bg rate	Type	Clone	Schedule	Status	Health	R %	RAID	#LUN	Snapshot space(GB)	#Snapshot	RG
OP.		VD-01	30	WB	HI	4	RAID	N/A	N/A	Online	Optimal		RAID 0	0	0/0	0	RG-R0
OP.		VD-02	20	WB	HI	4	RAID	N/A	N/A	Initiating	Optimal	44	RAID 5	0	0/0	0	RG-R5

Show size unit as: (GB)

Extend
Parity check
Delete
Set property
Attach LUN
Detach LUN
List LUN
Set clone
Set snapshot space
Cleanup snapshot
Take snapshot
Auto snapshot
List snapshot
More information

Create a VD named "VD-01", from "RG-R0". The second VD is named "VD-02", it's initializing.

Step 3: Done. View **"Virtual disk"** page.

VD column description:

	The button includes the functions which can be executed.
Name	Virtual disk name.
Size (GB) (MB)	Total capacity of the virtual disk. The unit can be displayed in GB or MB.
Right	The right of virtual disk: · **"WT"** → **W**rite **T**hrough. · **"WB"** → **W**rite **B**ack. · **"RO"** → **R**ead **O**nly.
Priority	The priority of virtual disk: · **"HI"** → **HI**gh priority. · **"MD"** → **MiD**dle priority. · **"LO"** → **LO**w priority.
Bg rate	Background task priority: · **"4 / 3 / 2 / 1 / 0"** → Default value is 4. The higher number the background priority of a VD is, 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.
	· **"Scrubbing"** → The virtual disk is being scrubbed.
	· **"Parity checking"** → The virtual disk is being parity check.
Type	The type of virtual disk:
	· **"RAID"** → the virtual disk is normal.
	· **"BACKUP"** → the virtual disk is for clone usage.
Health	The health of virtual disk:
	· **"Optimal"** → the virtual disk is working well and there is no failed disk in the RG.
	· **"Degraded"** → At least one disk from the RG of the Virtual disk is failed or plugged out.
	· **"Failed"** → the RAID group disk of the VD has single or multiple failed disks than its RAID level can recover from data loss.
	· **"Partially optimal"** → the virtual disk has experienced recoverable read errors.
R %	Ratio (%) of initializing or rebuilding.
RAID	RAID level.
#LUN	Number of LUN(s) that virtual disk is attached to.
Snapshot (GB) (MB)	The virtual disk size that is used for snapshot. The number means **"Used snapshot space" / "Total snapshot space"**. The unit can be displayed in GB or MB.
#Snapshot	Number of snapshot(s) that have been taken.
RG name	The RG name of the virtual disk

VD operations description:

Create	Create a virtual disk.
Extend	Extend a Virtual disk capacity.
Parity check	Execute parity check for the virtual disk. It supports RAID 3 / 5 / 6 / 30 / 50 / 60. Regenerate parity: · **"Yes"** → Regenerate RAID parity and write. · **"No"** → Execute parity check only and find mismatches. It will stop checking when mismatches count to 1 / 10 / 20 / … / 100.

Delete	Delete a Virtual disk.
Set property	Change the VD name, right, priority, bg rate and read ahead. Right: · **"WT"** → **W**rite **T**hrough. · **"WB"** → **W**rite **B**ack. (Default) · **"RO"** → **R**ead **O**nly. Priority: · **"HI"** → **HI**gh priority. (Default) · **"MD"** → **MiD**dle priority. · **"LO"** → **LO**w priority. Bg rate: · **"4 / 3 / 2 / 1 / 0"** → Default value is 4. The higher number the background priority of a VD is, the more background I/O will be scheduled to execute. Read ahead: · **"Enabled"** → Enable disk read ahead. (Default) · **"Disabled"** → Disable disk read ahead. AV-media mode: · **"Enabled"** → Enable AV-media mode for optimizing video editing. · **"Disabled"** → Disable AV-media mode. (Default) Type: · **"RAID"** → the virtual disk is normal. (Default) · **"Backup"** → the virtual disk is for clone usage.
Attach LUN	Attach to a LUN.
Detach LUN	Detach to a LUN.
List LUN	List attached LUN(s).
Set Clone	Set the target virtual disk for clone.
Clear Clone	Clear clone function.
Start Clone	Start clone function.
Stop Clone	Stop clone function.
Schedule Clone	Set clone function by schedule.
Set snapshot space	Set snapshot space for executing snapshot. Please refer to next chapter 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.

5.4.4 Snapshot

"Snapshot" can view the status of snapshot, create and modify snapshots. Please refer to next chapter for more detail about snapshot concept. The following is an example to take a snapshot.

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

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

	Name	Size(GB)	Write	Priority	Bg rate	Type	Clone	Schedule	Status	Health	R %	RAID	#LUN	Snapshot space(GB)	#Snapshot	RG
OP.	VD-01	30	WB	HI	4	RAID	N/A	N/A	Online	Optimal		RAID 0	0	1/15	0	RG-R0
OP.	VD-02	20	WB	HI	4	RAID	N/A	N/A	Online	Optimal		RAID 5	0	0/0	0	RG-R5

"VD-01" snapshot space has been created, snapshot space is 15GB, and used 1GB 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: Expose the snapshot VD. Move the mouse pointer to the gray button next to the Snapshot VD number; click **"Expose"**. Enter a capacity for snapshot VD. If 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 snapshots in "VD-01". There are two snapshots in "VD-01". Snapshot VD "SnapVD-01" is exported as read only, "SnapVD-02" is exported as read/write.

Step 5: Attach a LUN for snapshot VD. Please refer to the next section for attaching a LUN.

Step 6: Done. Snapshot VD can be used.

Snapshot column description:

	The button includes the functions which can be executed.
Name	Snapshot VD name.
Used (GB) (MB)	The amount of snapshot space that has been used. The unit can be displayed in GB or MB.
Status	The status of snapshot: · **"N/A"** → The snapshot is normal. · **"Replicated"** → The snapshot is for clone or QReplica usage. · **"Abort"** → The snapshot is over space and abort.
Health	The health of snapshot: · **"Good"** → The snapshot is good. · **"Failed"** → The snapshot fails.
Exposure	Snapshot VD is exposed or not.
Right	The right of snapshot: · **"RW"** → **R**ead / **W**rite. The snapshot VD can be read / write. · **"RO"** → **R**ead **O**nly. The snapshot VD is read only.
#LUN	Number of LUN(s) that snapshot VD is attached.
Created time	Snapshot VD created time.
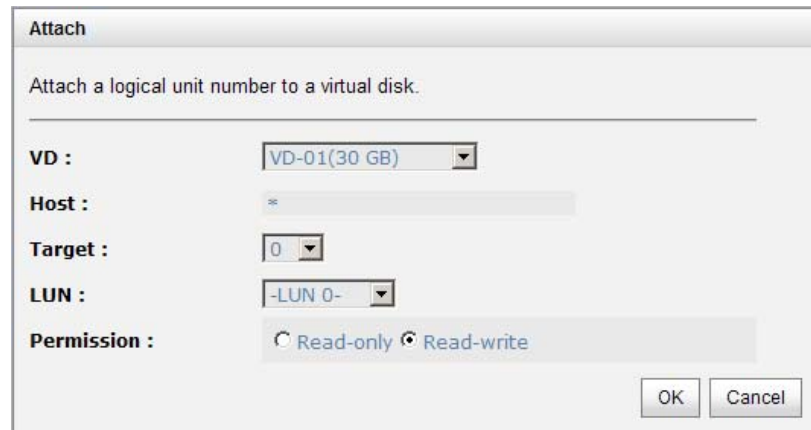
Snapshot operation description:

Expose/ Unexpose	Expose / unexpose the snapshot VD.
Rollback	Rollback the snapshot VD.
Delete	Delete the snapshot VD.
Attach	Attach a LUN.
Detach	Detach a LUN.
List LUN	List attached LUN(s).

5.4.5 Logical Unit

"Logical unit" can view, create, and modify the status of attached logical unit number(s) of each VD.

User can attach LUN by clicking the **"Attach"**. **"Host"** must enter with an iSCSI node name for access control, or fill-in wildcard **"*"**, which means every host can access the volume. Choose LUN number and permission, and then click **"OK"**.

VD-01 is attached to LUN 0 and every host can access. VD-02 is attached to LUN 1 and only initiator node which is named "iqn.1991-05.com.microsoft:win-r6qrvqjd5m7" can access.

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 rule 1.

The access will be denied when there is no matching rule.

5.4.6 Example

The following is an example for creating volumes. Example 1 is to create two VDs and set a global spare disk.

- **Example 1**

Example 1 is to create two VDs in one RG, each VD uses global cache volume. Global cache volume is created after system boots up automatically. So, no action is needed to set CV. Then set a global spare disk. Eventually, delete all of them.

Step 1: Create RG (RAID group).

To create the RAID group, please follow these steps:

1. Select **"/ Volume configuration / RAID group"**.
2. Click "**Create**".
3. Input an RG Name, choose a RAID level from the list, click "**Select PD**" to choose the RAID PD slot(s), then click "**OK**".

4. Check the outcome. Click "**OK**" if all setups are correct.

5. Done. RG has been created.

A RAID 5 RG named "RG-R5" with 3 physical disks is created.

Step 2: Create VD (Virtual disk).

To create a data user volume, please follow these steps.

1. Select **"/ Volume configuration / Virtual disk"**.
2. Click "**Create**".
3. Input a VD name, choose the RG when VD will be created, enter the VD capacity, select the stripe height, block size, read/write mode, set priority, modify Bg rate if necessary, and finally click "**OK**".

4. Done. A VD has been created.
5. Repeat steps 1 to 4 to create another VD.

	Name	Size(GB)	Write	Priority	Bg rate	Type	Clone	Schedule	Status	Health	R %	RAID	#LUN	Snapshot space(GB)	#Snapshot	RG
OP	VD-R5-1	50	WB	HI	4	RAID	N/A	N/A	Initiating	Optimal	9	RAID 5	0	0/0	0	RG-R5
OP	VD-R5-2	64	WB	HI	4	RAID	N/A	N/A	Initiating	Optimal	0	RAID 5	0	0/0	0	RG-R5
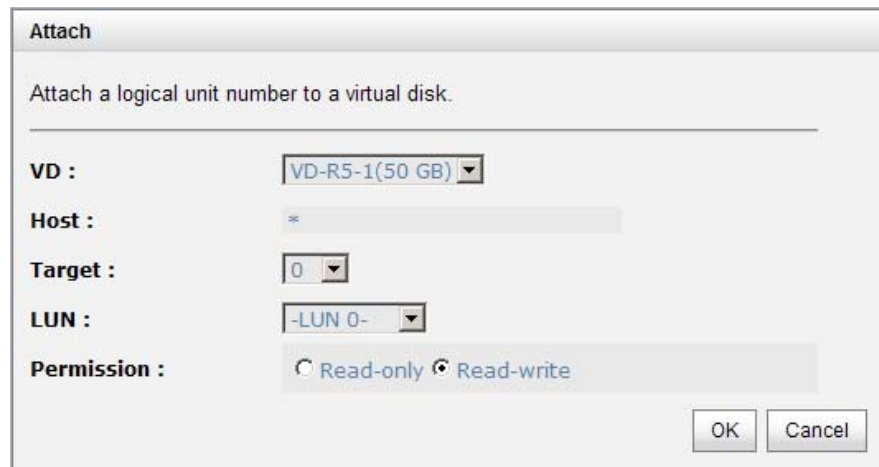
Two VDs, "VD-R5-1" and "VD-R5-2", were created from RG "RG-R5". The size of "VD-R5-1" is 50GB, and the size of "VD-R5-2" is 64GB. There is no LUN attached.

Step 3: Attach LUN to VD.

There are 2 methods to attach LUN to VD.
1. In **"/ Volume configuration / Virtual disk"**, move the mouse pointer to the gray button next to the VD number; click "Attach LUN".
2. In **"/ Volume configuration / Logical unit"**, click "**Attach**".

The steps are as follows:

1. Select a VD.
2. Input **"Host"** name, which is a iqn name for access control, or fill-in wildcard **"*"**, which means every host can access to this volume. Choose LUN and permission, and then click "**OK**".
3. Done.

VD-R5-1 is attached to LUN 0. VD-R5-2 is attached LUN 1.

NOTE: The matching rules of access control are from the LUNs' created time, the earlier created LUN is prior to the matching rules.

Step 4: Set global spare disk.

To set global spare disks, please follow the procedures.

1. Select **"/ Volume configuration / Physical disk"**.
2. Check the gray button next to the PD slot; click **"Set global space"**.
3. **"Global spare"** status is shown in **"Usage"** column.

Slot 4 is set as global spare disk (GS).

Step 5: Done. LUNs can be used as disks.

To delete VDs, RG, please follow the steps listed below.

Step 6: Detach LUN from VD.

In **"/ Volume configuration / Logical unit"**,

1. Move the mouse pointer to the gray button next to the LUN; click **"Detach"**. There will pop up a confirmation page.
2. Choose "OK".
3. Done.

Step 7: Delete VD (Virtual disk).

To delete the Virtual disk, please follow the procedures:

1. Select **"/ Volume configuration / Virtual disk"**.
2. Move the mouse pointer to the gray button next to the VD number; click **"Delete"**. There will pop up a confirmation page, click **"OK"**.
3. Done. Then, the VDs are deleted.

> **NOTE: When deleting VD, the attached LUN(s) related to this VD will be detached automatically.**

Step 8: Delete RG (RAID group).

To delete the RAID group, please follow the procedures:

1. Select **"/ Volume configuration / RAID group"**.
2. Select a RG which all its VD are deleted, otherwise the this RG cannot be deleted.
3. Check the gray button next to the RG number click **"Delete"**.
4. There will pop up a confirmation page, click **"OK"**.
5. Done. The RG has been deleted.

> **NOTE: The action of deleting one RG will succeed only when all of the related VD(s) are deleted in this RG. Otherwise, it will have an error when deleting this RG.**

Step 9: Free global spare disk.

To free global spare disks, please follow the procedures.

1. Select **"/ Volume configuration / Physical disk"**.
2. Check the gray button next to the PD slot; click **"Set Free disk"**.

Step 10: Done, all volumes have been deleted.

5.5 Enclosure Management

"**Enclosure management**" allows managing enclosure information including "**SES configuration**", "**Hardware monitor**", "**S.M.A.R.T.**" and "**UPS**". For the enclosure management, there are many sensors for different purposes, such as temperature sensors, voltage sensors, hard disks, fan sensors, power sensors, and LED status. Due to the different hardware characteristics among these sensors, they 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.
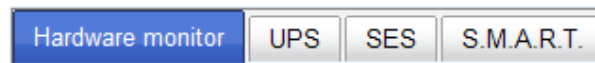
5.5.1 Hardware Monitor

"Hardware monitor" can be used to view the information of current voltage, temperature levels, and fan speed.

If **"Auto shutdown"** has been checked, the system will shutdown automatically when voltage or temperature is out of the normal range. For better data protection, please check **"Auto Shutdown"**.

For better protection and avoiding single short period of high temperature triggering auto shutdown, the RAID controller evaluates multiple conditions for triggering auto shutdown. Below are the details of when the Auto shutdown will be triggered.

1. There are 3 sensors placed on controller for temperature checking, they are on core processor, PCI-X bridge, and daughter board. Controller will check each sensor for every 30 seconds. When one of these sensors is over high temperature value continuously for 3 minutes, auto shutdown will be triggered immediately.
2. The core processor temperature limit is 85°C. The PCI-X bridge temperature limit is 80°C. The daughter board temperature limit is 80°C.
3. If the high temperature situation doesn't last for 3 minutes, controller will not do auto shutdown.

5.5.2 UPS

"**UPS**" is used to set up UPS (**U**ninterruptible **P**ower **S**upply).

Currently, the system only supports and communicates with APC (American Power Conversion Corp.) smart UPS. Please review the details from the website: http://www.apc.com/.

First, connect the system and APC UPS via RS-232 for communication. Then set up the shutdown values (shutdown battery level %) when power is failed. UPS in other companies can work well, but they have no such communication feature with the system.

UPS Type	Select UPS Type. Choose Smart-UPS for APC, None for other vendors or no UPS.
Shutdown	When below the setting level, system will shutdown. Setting level to "**0**" will disable UPS.

Battery Level (%)	
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.

5.5.3 SES

SES represents **S**CSI **E**nclosure **S**ervices, one of the enclosure management standards. "**SES configuration**" can enable or disable the management of SES.

Enable SES in LUN 0, and can be accessed from every host

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

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

5.5.4 Hard Drive S.M.A.R.T. Support

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 in advance. S.M.A.R.T. provides users chances to take actions before possible drive failure.

S.M.A.R.T. measures many attributes of the hard drive all the time and inspects the properties of hard drives which are close to be out of tolerance. The advanced notice of possible hard drive failure can allow users to back up hard drive or replace the hard drive. This is much better than hard drive crash when it is writing data or rebuilding a failed hard drive.

"S.M.A.R.T." can display S.M.A.R.T. information of hard drives. The number is the current value; the number in parenthesis is the threshold value. The threshold values of hard drive vendors are different; please refer to vendors' specification for details.

S.M.A.R.T. only supports SATA drive. SAS drive does not have. It will show N/A in this web page.

Slot	HDD type	Read error	Spin up	Reallocated sector	Seek error	Spin up	Calibration	Temperature
1	SAS	N/A	N/A	N/A	N/A	N/A	N/A	38
2	SAS	N/A	N/A	N/A	N/A	N/A	N/A	39
3	SAS	N/A	N/A	N/A	N/A	N/A	N/A	38
4	SAS	N/A	N/A	N/A	N/A	N/A	N/A	39
5	SAS	N/A	N/A	N/A	N/A	N/A	N/A	38
6	SAS	N/A	N/A	N/A	N/A	N/A	N/A	38
7	SAS	N/A	N/A	N/A	N/A	N/A	N/A	35
8	SAS	N/A	N/A	N/A	N/A	N/A	N/A	33

Self-Monitoring Analysis and Reporting Technology(S.M.A.R.T.). A diagnostic tool for hard drives to deliver warning of drive failures in advance. S.M.A.R.T. provides users chances to take actions before possible drive failure. Show information for: - Local -

| Hardware monitor | UPS | SES | S.M.A.R.T. |

Self-Monitoring Analysis and Reporting Technology(S.M.A.R.T).

A diagnostic tool for hard drives to deliver warning of drive failures in advance.
S.M.A.R.T. provides users chances to take actions before possible drive failure.

Show information for: - Local -

Slot	HDD type	Read error	Spin up	Reallocated sector	Seek error	Spin up	Calibration	Temperature
1	SATA	100(16)	101(24)	100(5)	100(67)	100(60)	N/A	28
2	SATA	100(16)	104(24)	100(5)	100(67)	100(60)	N/A	28
3	SATA	100(16)	98(24)	100(5)	100(67)	100(60)	N/A	27
4	SATA	100(16)	97(24)	100(5)	100(67)	100(60)	N/A	27
5	SATA	100(16)	104(24)	100(5)	100(67)	100(60)	N/A	28
6	SATA	100(16)	100(24)	100(5)	100(67)	100(60)	N/A	27
7	SATA	100(16)	99(24)	100(5)	100(67)	100(60)	N/A	27
8	SATA	100(16)	103(24)	100(5)	100(67)	100(60)	N/A	26

5.6 System Maintenance

"**Maintenance**" allows the operations of system functions which include "**System information**" to show the system version and details, "**Event log**" to view system event logs to record critical events, "**Upgrade**" to the latest firmware, "**Firmware synchronization**" to synchronized firmware versions on both controllers, "**Reset to factory default**" to reset all controller configuration values to factory settings, "**Import and export**" to import and export all controller configuration to a file, and "**Reboot and shutdown**" to reboot or shutdown the system.

| System information | Event log | Upgrade | Firmware synchronization | Reset to factory default | Import and export | Reboot and shutdown |

5.6.1 System Information

The **System information** provides to display system information. It includes CPU type, installed system memory, firmware version, SAS IOC firmware no., SAS expander firmware no., serial numbers of the controller(s), controller hardware no., master controller, backplane ID, serial numbers of the connected JBOD(s), system status and QReplica status.

Item	Information
CPU type	Intel(R) Xeon(R) CPU C3528 @ 1.73GHz
System memory	(Slot 1) ECC Unbuffered DDR-III 4096MB (Slot 2)
Firmware version	
SAS IOC firmware no.	11.00.00.00
SAS expander firmware no.	Controller 1 : 1110 Controller 2 : 1110
Serial number	00172AC700E0 (Controller 1 : 5001378005907280 , Controller 2 : 5001378005906AC0)
Controller HW no.	Controller 1: 1.14 Controller 2: 1.14
Master Controller	Controller 1
Backplane ID	
JBOD serial no.	No JBOD connected
Status	Normal
QReplica	Inactive

Download System Information

Status description:

Normal	Dual controllers are in normal stage.
Degraded	One controller fails or has been plugged out..
Lockdown	The firmware of two controllers is different or the size of memory of two controllers is different.
Single	Single controller mode.

The options are available on this tab:

- **Download System Information**: Download the system information for debug.

5.6.2 Event Log

The **Event log** tab provides a log or event messages. Choose the buttons of INFO, WARNING, or ERROR levels to display those particular events.

The options are available on this tab:

- **Download**: Click **Download** button to save the event log as a text file with file name "log-ModelName-SerialNumber-Date-Time.txt". It will pop up a filter dialog as the following. The default it "Download all event logs".
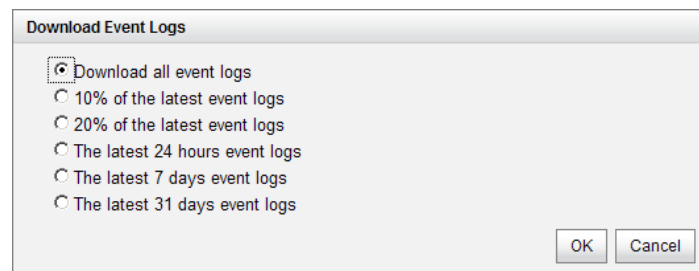
Select event level of displayed event log

| INFO | WARNING | ERROR |

<< first < prev **1** 2 3 4 5 next > last >>

Type	Time	Content
INFO	Tue, 17 Jul 2012 10:31:43	[CTR2] VD 2 completed initialization.
WARNING	Tue, 17 Jul 2012 03:02:14	[CTR1] System temperature(CPU Core 1 : 79.0) is higher.
INFO	Tue, 17 Jul 2012 00:15:37	[CTR1] admin login from 192.168.220.136 via Console UI
INFO	Mon, 16 Jul 2012 23:49:19	[CTR1] VD 1 completed initialization.
INFO	Mon, 16 Jul 2012 22:13:47	[CTR2] iSCSI login from 134 (10.1.26.234:50982) succeeds.
INFO	Mon, 16 Jul 2012 22:13:40	[CTR2] iSCSI login from 134 (10.1.25.234:50981) succeeds.
INFO	Mon, 16 Jul 2012 22:13:28	[CTR1] iSCSI login from 134 (10.1.26.134:50980) succeeds.
INFO	Mon, 16 Jul 2012 22:13:16	[CTR1] iSCSI login from 134 (10.1.25.134:50979) succeeds.
INFO	Mon, 16 Jul 2012 22:13:00	[CTR2] iSCSI logout from 134 (10.1.25.234:50921) was received, reason [close the session].
INFO	Mon, 16 Jul 2012 22:13:00	[CTR2] iSCSI logout from 134 (10.1.26.234:50923) was received, reason [close the session].
INFO	Mon, 16 Jul 2012 22:13:00	[CTR1] iSCSI logout from 134 (10.1.25.134:50917) was received, reason [close the session].
INFO	Mon, 16 Jul 2012 22:12:50	[CTR2] iSCSI login from 133 (10.1.26.233:50888) succeeds.
INFO	Mon, 16 Jul 2012 22:12:41	[CTR2] iSCSI login from 133 (10.1.25.233:50887) succeeds.
INFO	Mon, 16 Jul 2012 22:12:28	[CTR1] iSCSI login from 133 (10.1.26.133:50886) succeeds.
INFO	Mon, 16 Jul 2012 22:12:18	[CTR1] iSCSI login from 133 (10.1.25.133:50885) succeeds.
INFO	Mon, 16 Jul 2012 22:12:05	[CTR2] iSCSI logout from 133 (10.1.25.233:50881) was received, reason [close the session].
INFO	Mon, 16 Jul 2012 22:12:05	[CTR2] iSCSI logout from 133 (10.1.26.233:50883) was received, reason [close the session].
INFO	Mon, 16 Jul 2012 22:12:06	[CTR1] iSCSI logout from 133 (10.1.26.133:50882) was received, reason [close the session].
INFO	Mon, 16 Jul 2012 22:12:06	[CTR1] iSCSI logout from 133 (10.1.25.133:50880) was received, reason [close the session].
INFO	Mon, 16 Jul 2012 22:10:27	[CTR2] iSCSI login from 134 (10.1.26.234:50923) succeeds.

<< first < prev **1** 2 3 4 5 next > last >>

| Download | Mute | Clear |

The event log is displayed in reverse order which means the latest event log is on the first page. The event logs are actually saved in the first four hard drives; each hard drive has one copy of event log. For one controller, there are four copies of event logs to make sure users can check event log any time when there is/are failed disk(s).

NOTE: Please plug-in any of the first four hard drives, then event logs can be saved and displayed in next system boot up. Otherwise, the event logs would disappear.

5.6.3 Upgrade

The **Upgrade** tab is used to upgrade controller firmware, JBOD firmware, change operation mode, and activate QReplica license. Before upgrade, it's better to use **Export** function to backup all configurations to a file.

RAID Controller/System(s)		
Browse the firmware to upgrade :		Browse...
Confirm		

JBOD Controller/System(s)		
Choose a JBOD:	▾	
Browse the firmware to upgrade:		Browse...
Confirm		

Controller Mode		
Enter the MAC address for the mode setting:		
Operation mode:	Dual ▾	
Confirm		

QReplica license		
Select the license file to activate QReplica:		Browse...
Confirm		

The options are available on this tab:

- **Controller firmware upgrade**: Please prepare new controller firmware file named "xxxx.bin" in local hard drive, then click **Browse** to select the file. Click **Confirm** button, it will pop up a warning message, click **OK** button to start upgrading the firmware.

> ？ Upgrade system now?
>
> If you want to downgrade to the previous FW later, please export your system configuration first!
>
> [OK]   [Cancel]
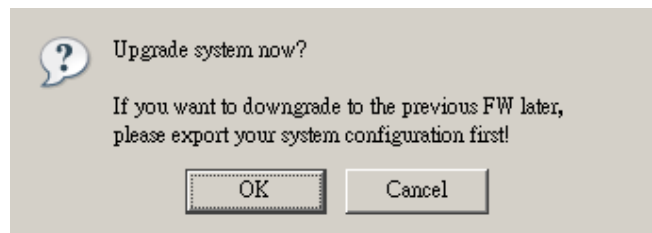
  When upgrading, there is a progress bar running. After finished upgrading, the system must reboot manually to make the new firmware took effect.

- **JBOD firmware upgrade**: To upgrade JBOD firmware, the steps are the same as controller firmware but choosing number of JBOD first.

- **Controller mode**: This option can be modified to dual or single here. If the system installs only one controller, switch this mode to **Single**. This mode indicates single upgradable. Enter the MAC address displayed in **System configuration** → **Network setting** such as 001378xxxxxx (case-insensitive), and then click **Confirm** button.

- **QReplica license**: This option can activate QReplica function if there is a license here. Select the license file, and then click **Confirm** button.

NOTE: Please contact your vendor for the latest firmware.
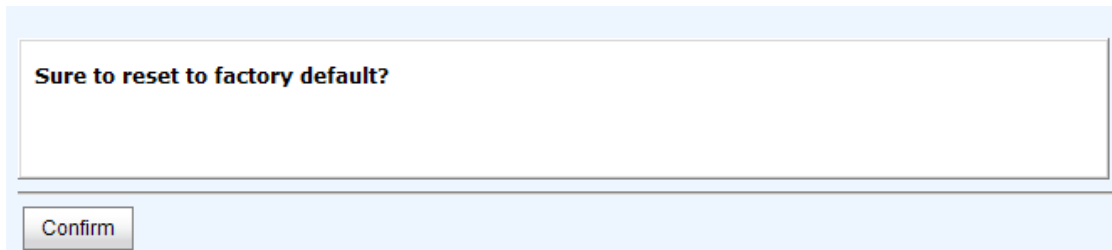
5.6.4 Firmware Synchronization

The **Firmware synchronization** tab is used on dual controller systems to synchronize the controller firmware versions when the firmware of the master controller and the slave controller are different. The firmware of slave controller is always changed to match the firmware of the master controller. It doesn't matter if the firmware version of slave controller is newer or older than that of the master.

The firmware versions are the same between two controllers.
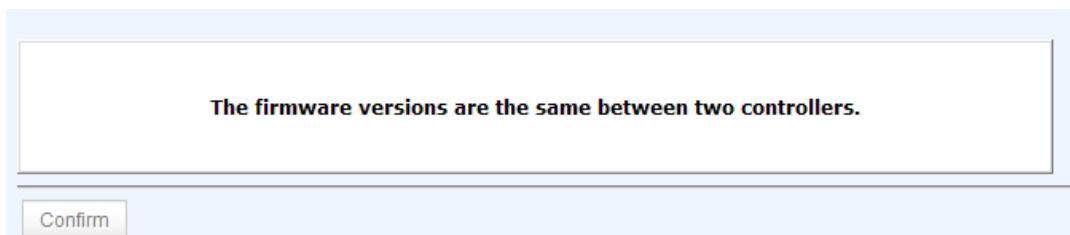
Confirm

5.6.5 Reset to Factory Default

"Reset to factory default" allows user to reset controller to factory default setting.

Reset to default value, the password is: **00000000**, and IP address to default DHCP.

5.6.6 Import and Export

"Import and export" allows user to save system configuration values: export, and apply all configuration: import. For the volume configuration setting, the values are available in export and not available in import which can avoid confliction / date-deleting between two controllers which mean if one system already has valuable volumes in the disks and user may forget and overwrite it. Use import could return to original configuration. If the volume setting was also imported, user's current volumes will be overwritten with different configuration.

1. **Import:** Import all system configurations excluding volume configuration.
2. **Export:** Export all configurations to a file.

⚠️ **WARNING: "Import" will import all system configurations excluding volume configuration; the current configurations will be replaced.**

5.6.7 Reboot and Shutdown

"**Reboot and shutdown**" displays "**Reboot**" and "**Shutdown**" buttons. Before power off, it's better to execute "**Shutdown**" to flush the data from cache to physical disks. The step is necessary for data protection.
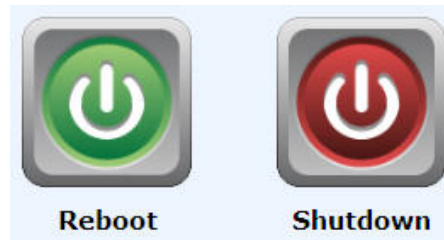
The Reboot function has three options, reboot both controllers, controller 1 only or controller 2 only.
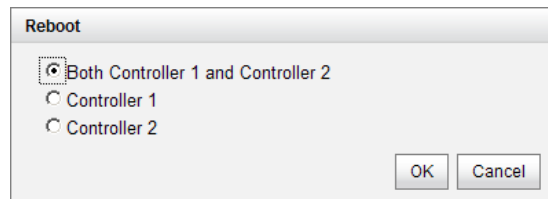
5.7 Home/Logout/Mute

In the right-upper corner of web UI, there are 3 individual icons, "**Home**", "**Logout**", and "**Mute**".
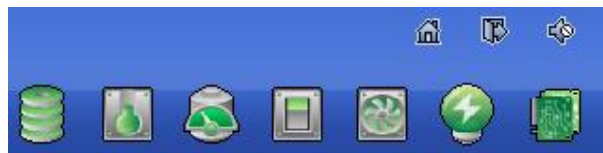
5.7.1 Home

Click "**Home**" to return to home page

5.7.2 Logout

For security reason, please use "**Logout**" to exit the web UI. To re-login the system, please enter username and password again.

5.7.3 Mute

Click "**Mute**" to stop the alarm when error occurs.

Chapter 6 Advanced Operations

6.1 Volume Rebuild

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

The RAID subsystem supports Auto-Rebuild. The following is the scenario:

Take RAID 6 for example:

1. 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. It is recommended for users not to rebuild in the failed disk for better data protection.

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

3. 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 completing the rebuilding process, the status will become "Online". RG will become complete or normal.

NOTE: "Set dedicated spare" is not available if there is no RG, or if RG is set to RAID 0 or 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.

6.2   RG Migration

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

1. Select **"/ Volume configuration / RAID group"**.
2. Check 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 **"OK "** to go back to setup page. When doing migration to lower RAID level, such as the original RAID level is RAID 6 and user wants to migrate to RAID 0, system 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 **"OK"**.
5. Finally a confirmation page shows the detail of RAID information. If there is no problem, click **"OK"** 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%"**.

A RAID 0 with 3 physical disks migrates to RAID 5 with 4 physical disks.

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.
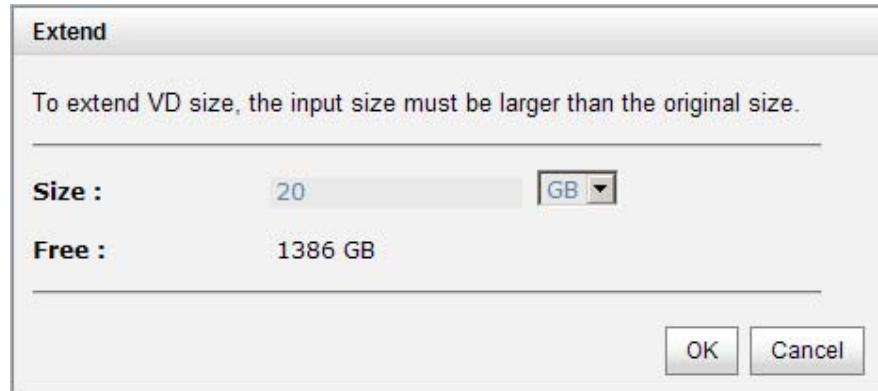
IMPORTANT! RG Migration cannot be executed during rebuild or VD extension.

6.3 VD Extension

To extend VD size, please follow the procedures.

1. Select **"/ Volume configuration / Virtual disk"**.
2. Check 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 "**OK**" to start extension.

4. Extension starts. If VD needs initialization, it will display **"Initiating"** in **"Status"** and the completed percentage of initialization in **"R%"** column.

   NOTE: The size of VD extension must be larger than original.

   IMPORTANT! VD Extension cannot be executed during rebuild or migration.

6.4 Snapshot / Rollback

Snapshot-on-the-box captures the instant state of data 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 to 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. Please refer to the figure below for the snapshot concept.
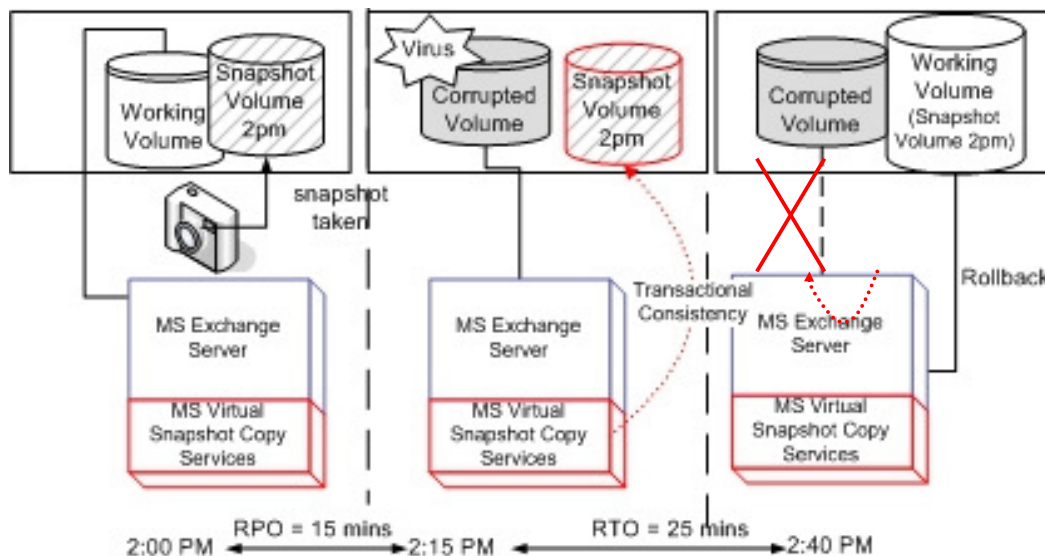
> ⚠️ **IMPORTANT! Snapshot / rollback features need at least 1 GB controller cache RAM. Please also refer to RAM certification list in Appendix A.**

6.4.1 Create Snapshot Volume

To take a snapshot of the data, please follow the procedures.

1. Select **"/ Volume configuration / Virtual disk"**.
2. Check 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 "**OK**". 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 are **"Used snapshot space"** and **"Total snapshot space"**.
4. There are two methods to take snapshot. In **"/ Volume configuration / Virtual disk"**, move the mouse pointer 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 "**OK**". A snapshot VD is created.
6. Select **"/ Volume configuration / Snapshot"** to display all snapshot VDs related to the VD

7. Check gray button next to the Snapshot VD number; click **"Export"**. Enter a capacity for snapshot VD. If 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 the previous chapter for attaching a LUN.
9. Done. It can be used as a disk.

This is the snapshot list of "VD-01". There are two snapshots. Snapshot VD "SnapVD-01" is exposed as read-only, "SnapVD-02" is exposed as read-write.

1. There are two methods to clean all snapshots. In **"/ Volume configuration / Virtual disk"**, move the mouse pointer to the gray button next to the VD

number; click **"Cleanup snapshot"**. Or in **"/ Volume configuration / Snapshot"**, click "**Cleanup**".

2. "**Cleanup snapshot**" will delete all snapshots related to the VD and release snapshot space.

Snapshot has some constraints such as the following:

1. Minimum RAM size for enabling snapshot is **1GB**.
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 cannot be taken by manual because system does not know which snapshot VDs can be deleted.

6.4.2 Auto Snapshot

The snapshot copies can be taken manually or by schedule such as hourly or daily.

Please follow the procedures.

1. There are two methods to set auto snapshot. In **"/ Volume configuration / Virtual disk"**, move the mouse pointer 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.

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

6.4.3 Rollback

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

1. Select **"/ Volume configuration / Snapshot"**.
2. Check 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 original VD.

Rollback has some constraints as described in the following:

1. Minimum RAM size required for enabling rollback is **1GB**.
2. When making a rollback, the original VD cannot be accessed for a while. At the same time, the system connects to original VD and snapshot VD, and then starts rollback.
3. During rollback, data from snapshot VD to 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) cannot be accessed.
4. After rollback, the other snapshot VD(s) after the VD which is doing rollback will be deleted.

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

6.5 Disk Roaming

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 these steps:

1. Select "**/ Volume configuration / RAID group**".
2. Check the gray button next to the RG number; click **"Deactivate"**.
3. Move all PDs related to the RG to another system.
4. In the web GUI of the other system, check the gray button next to the RG number; click **"Activate"**.
5. Done.

Disk roaming has some constraints as described in the following:

1. Check the firmware of two systems first. It is better that both systems have the same firmware version or newer.
2. 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-2.

6.6 VD Clone

The user can use VD clone function to backup data from source VD to target VD, set up backup schedule, and deploy the clone rules.

The procedures of VD clone are on the following:

1. Copy all data from source VD to target VD at the beginning (full copy).
2. Use Snapshot technology to perform the incremental copy afterwards. Please be fully aware that the incremental copy needs to use snapshot to compare the data difference. Therefore, the enough snapshot space for VD clone is very important.

The following contents will take an example of a RAID 5 virtual disk (SourceVD_Raid5) clone to RAID 6 virtual disk (TargetVD_Raid6).

- **Start VD clone**

1. Create a RAID group (RG) in advance.

	Name	Total(GB)	Free(GB)	#PD	#VD	Status	Health	RAID	Current owner	Preferred owner
OP.	RG-R5	931	931	3	0	Online	Good	RAID 5	Controller 1	Controller 1
OP.	RG-R6	931	931	4	0	Online	Good	RAID 6	Controller 1	Controller 1

Show size unit as: (GB)

2. Create two virtual disks (VD) "SourceVD_R5" and "TargetVD_R6". The raid type of backup target needs to be set as **"BACKUP"**.

3. Here are the objects, a Source VD and a Target VD. Before starting clone process, it needs to deploy the VD Clone rule first. Click **"Configuration"**.

4. There are three clone configurations, describe on the following.
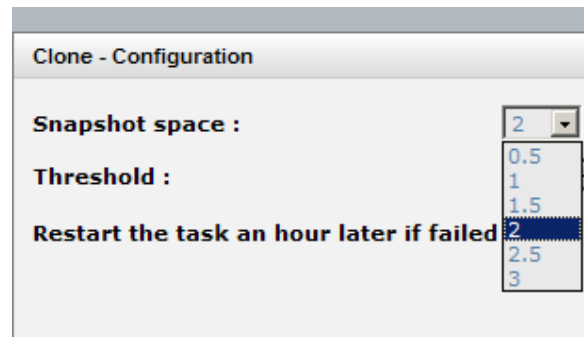
· **Snapshot space:**

This setting is the ratio of source VD and snapshot space. The default ratio is 2 to 1. It means when the clone process is starting, the system will automatically use the free RG space to create a snapshot space which capacity is double the source VD.

· **Threshold: (The setting will be effective after enabling schedule clone)**
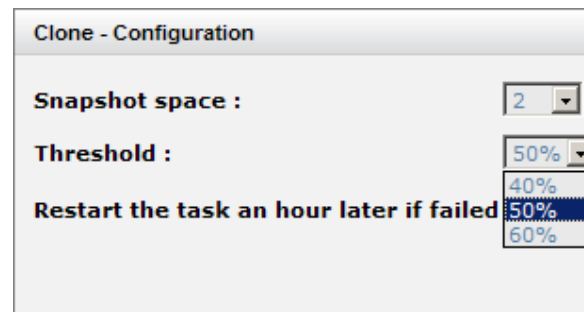
The threshold setting will monitor the usage amount of snapshot space. When the used snapshot space achieves its threshold, system will automatically take a clone snapshot and start VD clone process. The purpose of threshold could prevent the incremental copy fail immediately when running out of snapshot space.

For example, the default threshold is 50%. The system will check the snapshot space every hour. When the snapshot space is used over 50%, the system will synchronize the source VD and target VD automatically. Next time, when the rest snapshot space has been used 50%, in other words, the total snapshot space has been used 75%, the system will synchronize the source VD and target VD again.

· **Restart the task an hour later if failed: (The setting will be effective after enabling schedule clone)**
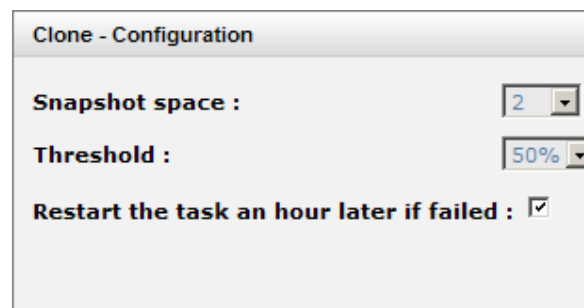
When running out of snapshot space, the VD clone process will be stopped because there is no more available snapshot space. If this option has been checked, system will clear the snapshots of clone in order to release snapshot space automatically, and the VD clone will restart the task after an hour. This task will start a full copy.

5. After deploying the VD clone rule, the VD clone process can be started now. Firstly, Click **"Set clone"** to set the target VD at the VD name "SourceVD_R5".

6. Select the target VD. Then click **"Confirm"**.

7. Now, the clone target "TargetVD_R6" has been set.

8.   Click **"Start clone"**, the clone process will start.

9.   The default setting will create a snapshot space automatically which the capacity is double size of the VD space. Before starting clone, system will initiate the snapshot space.

10. After initiating the snapshot space, it will start cloning.

11. Click **"Schedule clone"** to set up the clone by schedule.

12. There are **"Set Clone schedule"** and **"Clear Clone schedule"** in this page. Please remember that **"Threshold"** and **"Restart the task an hour later if failed"** options in VD configuration will take effect after clone schedule has been set.

- **Run out of snapshot space while VD clone**

While the clone is processing, the increment data of this VD is over the snapshot space. The clone will complete, but the clone snapshot will fail. Next time, when trying to start clone, it will get a warning message "This is not enough of snapshot space for the operation". At this time, the user needs to clean up the snapshot space in order to operate the clone process. Each time the clone snapshot failed, it means that the system loses the reference value of incremental data. So it will start a full copy at next clone process.

When running out of snapshot space, the flow diagram of VD clone procedure will be like the following.

```
                        ( VD Clone )
                             |
                             v
        Yes <--- < Schedule clone > ---> NO
         |                                |
         v                                v
  [Check threshold              [Manually start
   every hour]                   clone by user]
         |                                |
         v                                v
  [Run out of                   [Run out of
   snapshot space]               snapshot space]
         |                                |
         v                                v
  [Auto delete old              [Manually release
   clone snapshot]               snapshot space]
         |                                |
         v                                v
  [Auto restart an              [Restart clone
   hour later]                   by user]
         |                                |
         +----> / Start clone <-----------+
                  process with
                  fully copy /
                       |
                       v
                   ( Done )
```
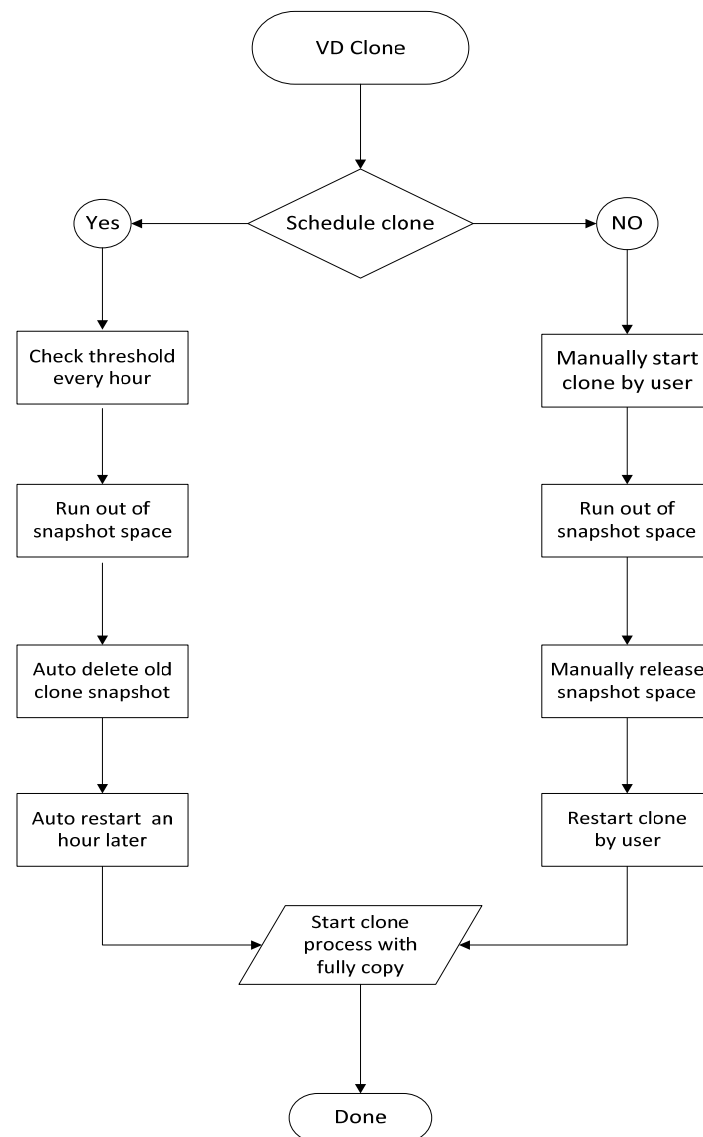
6.7 SAS JBOD Expansion

6.7.1 Connecting JBOD

The RAID controller suports SAS JBOD expansion to connect extra SAS dual JBOD controller. When connecting a dual JBOD controller which can be detected in RAID Subsystem management GUI, it will be displayed in **"Show PD for:"** under **"/ Volume configuration / Physical disk" menu**. For example, Local, JBOD 1, JBOD 2, …etc. Local means disks located in local RAID subsystem, JBOD 1 means disks located in first JBOD subsystem, and so on. The hard drives in JBOD can be used as local disks.

	Slot							Serial	Type	Write cache	Standby	Readahead	Command queuing
OP	1	558	r50-1	Online	Good	RAID disk	WDC	WD-WXM1E60RW203	SATA2	Enabled	Disabled	Enabled	Disabled
OP	3	465	r6-3	Online	Good	RAID disk	WDC	WD-WCASY3223587	SATA2	Enabled	Disabled	Enabled	Disabled
OP	4	465	r6-3	Online	Good	RAID disk	WDC	WD-WMAYP0015736	SATA2	Enabled	Disabled	Enabled	Disabled
OP	5	558	r50-1	Online	Good	RAID disk	WDC	WD-WXM1E6070999	SATA2	Enabled	Disabled	Enabled	Disabled
OP	7	232		Online	Good	Free disk	Seagate	9QE6T6DW	SATA2	Enabled	Disabled	Enabled	Disabled
OP	8	465	r6-3	Online	Good	RAID disk	WDC	WD-WMAYP0015949	SATA2	Enabled	Disabled	Enabled	Disabled
OP	9	558	r50-1	Online	Good	RAID disk	WDC	WD-WXM1E6070513	SATA2	Enabled	Disabled	Enabled	Disabled
OP	12	465	r6-3	Online	Good	RAID disk	WDC	WD-WMAYP0014684	SATA2	Enabled	Disabled	Enabled	Disabled
OP	13	558	r50-1	Online	Good	RAID disk	WDC	WD-WXM1E6071038	SATA2	Enabled	Disabled	Enabled	Disabled
OP	15	232		Online	Good	Free disk	Seagate	5QE5FK6D	SATA2	Enabled	Disabled	Enabled	Disabled
OP	16	465	r6-3	Online	Good	RAID disk	WDC	WD-WMAYP0015624	SATA2	Enabled	Disabled	Enabled	Disabled

"/ Enclosure management / Hardware monitor" can display the hardware status of SAS JBODs.

| Hardware monitor | UPS | SES | S.M.A.R.T. |

Show information for: [- JBOD 1 (proIPS EP-3164JD-S6S6 v1.0.1) 5001378004B50190 - ▼]

Controller 1 (50013780049007BD)

<< first < prev | 1 | 2 next > last >>

Type	Item	Value	Status
Temperature	Location 13(R6R)	26.0 (C)	OK
Temperature	Location 14(R6R)	24.0 (C)	OK
Temperature	Location 15(R6R)	26.0 (C)	OK
Temperature	Location 16(R6R)	28.0 (C)	OK
Temperature	Onboard 1	71.0 (C)	OK
Temperature	Onboard 2	40.0 (C)	OK
Temperature	Onboard 3	37.0 (C)	OK
Power Supply	PSU 1	N/A	OK
Power Supply	PSU 2	N/A	OK
Cooling	FAN 1	4380 RPM	OK
Cooling	FAN 2	4380 RPM	OK
Cooling	FAN 3	4440 RPM	OK
Cooling	FAN 4	3970 RPM	OK

<< first < prev | 1 | 2 next > last >>

Controller 2 (500137800490057D)

<< first < prev 1 | 2 | next > last >>

Type	Item	Value	Status
Voltage	PSU +3.3V(R6R)	3.38 V	OK
Voltage	PSU +5V(R6R)	5.10 V	OK
Voltage	PSU +12V(R6R)	12.31 V	OK
Voltage	+1.0V (Onboard)	1.01 V	OK
Voltage	+1.8V (Onboard)	1.84 V	OK
Voltage	+3.3V (Onboard)	3.36 V	OK
Voltage	+5V (Onboard)	5.12 V	OK
Voltage	+12V (Onboard)	12.27 V	OK
Temperature	Location 1(R6R)	26.0 (C)	OK
Temperature	Location 2(R6R)	25.0 (C)	OK
Temperature	Location 3(R6R)	26.0 (C)	OK
Temperature	Location 4(R6R)	26.0 (C)	OK
Temperature	Location 5(R6R)	26.0 (C)	OK
Temperature	Location 6(R6R)	24.0 (C)	OK
Temperature	Location 7(R6R)	26.0 (C)	OK
Temperature	Location 8(R6R)	27.0 (C)	OK
Temperature	Location 9(R6R)	26.0 (C)	OK
Temperature	Location 10(R6R)	24.0 (C)	OK
Temperature	Location 11(R6R)	26.0 (C)	OK
Temperature	Location 12(R6R)	27.0 (C)	OK

<< first < prev 1 | 2 | next > last >>

"/ Enclosure management / S.M.A.R.T." can display S.M.A.R.T. information of all PDs, including Local and all SAS JBODs.

Hardware monitor	UPS	SES	**S.M.A.R.T.**							

Self-Monitoring Analysis and Reporting Technology(S.M.A.R.T.).
A diagnostic tool for hard drives to deliver warning of drive failures in advance.
S.M.A.R.T. provides users chances to take actions before possible drive failure.

Show information for: - JBOD 1 (proIPS EP-3164JD-S6S6 v1.0.1) 5001378004B50190 - ▾
- Local -
- JBOD 1 (proIPS EP-3164JD-S6S6 v1.0.1) 5001378004B50190 -
- JBOD 2 (proIPS EP-3164JD-S6S6 v1.0.1) 5001378004B50380 -
- JBOD 3 (proIPS EP-3164JD-S6S6 v1.0.1) 5001378004B501E0 -

Slot	HDD type				Seek error (rate)	Spin up (retries)	Calibration (retries)	Temperature (C)
1	SATA2	200(51)	100(21)	200(140)	200(0)	100(0)	100(0)	28
3	SATA2	200(51)	160(21)	200(140)	200(0)	100(0)	100(0)	33
4	SATA2	200(51)	141(21)	200(140)	200(0)	100(0)	100(0)	29
5	SATA2	200(51)	100(21)	200(140)	200(0)	100(0)	100(0)	27
7	SATA2	114(6)	97(0)	100(36)	83(30)	100(97)	N/A	33
8	SATA2	200(51)	141(21)	200(140)	200(0)	100(0)	100(0)	30
9	SATA2	200(51)	100(21)	200(140)	200(0)	100(0)	100(0)	28
12	SATA2	200(51)	137(21)	200(140)	200(0)	100(0)	100(0)	29
13	SATA2	200(51)	100(21)	200(140)	200(0)	100(0)	100(0)	28
15	SATA2	108(6)	97(0)	100(36)	87(30)	100(97)	N/A	33
16	SATA2	200(51)	137(21)	200(140)	200(0)	100(0)	100(0)	30

SAS JBOD expansion has some constraints as described in the followings:

1   User can create RAID group among multiple chassis/enclosures; the maximum number of disks in a single RAID group is 64.

2   Global spare disk can support all RAID groups which can be located in the different chassis/enclosure.

3   When support SATA drives for the redundant JBOD model, the SAS-SATA Bridge board is required. The SATA Dongle board does not apply to this model.

6.8 MPIO and MC/S

These features come from iSCSi initiator. They can be setup from iSCSI initiator to establish redundant paths for sending I/O from the initiator to the target.

1. **MPIO**: In Microsoft Windows server base system, Microsoft MPIO driver allows initiators to login multiple sessions to the same target and aggregate the duplicate devices into a single device. Each session to the target can be established using different NICs, network infrastructure and target ports. If one session fails, then another session can continue processing I/O without interruption to the application.
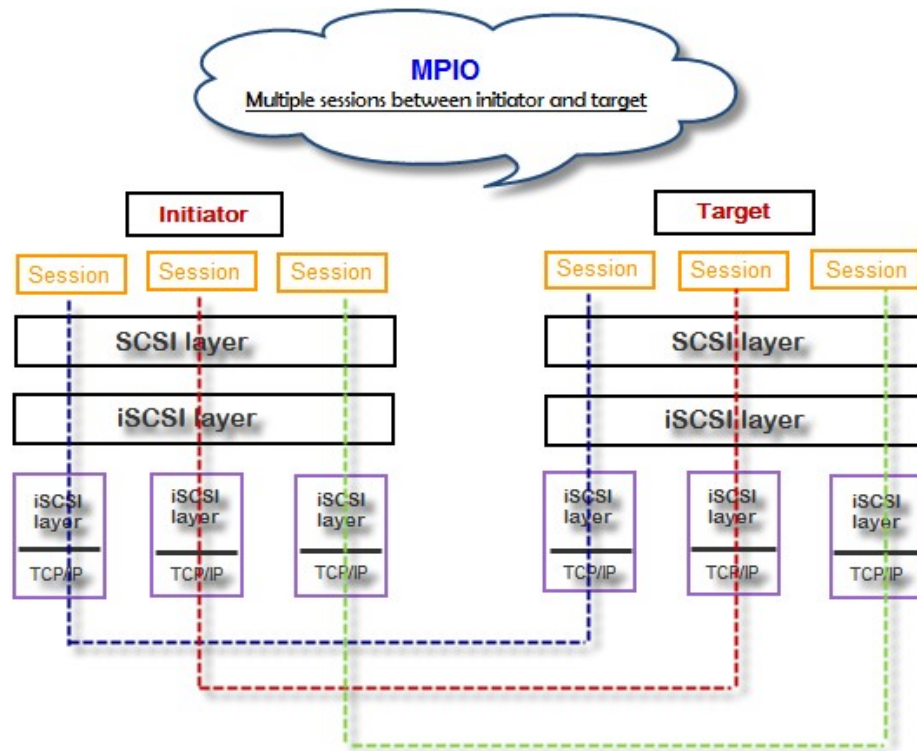
2. **MC/S**: MC/S (Multiple Connections per Session) is a feature of iSCSI protocol, which allows combining several connections inside a single session for performance and failover purposes. In this way, I/O can be sent on any TCP/IP connection to the target. If one connection fails, another connection can continue processing I/O without interruption to the application.
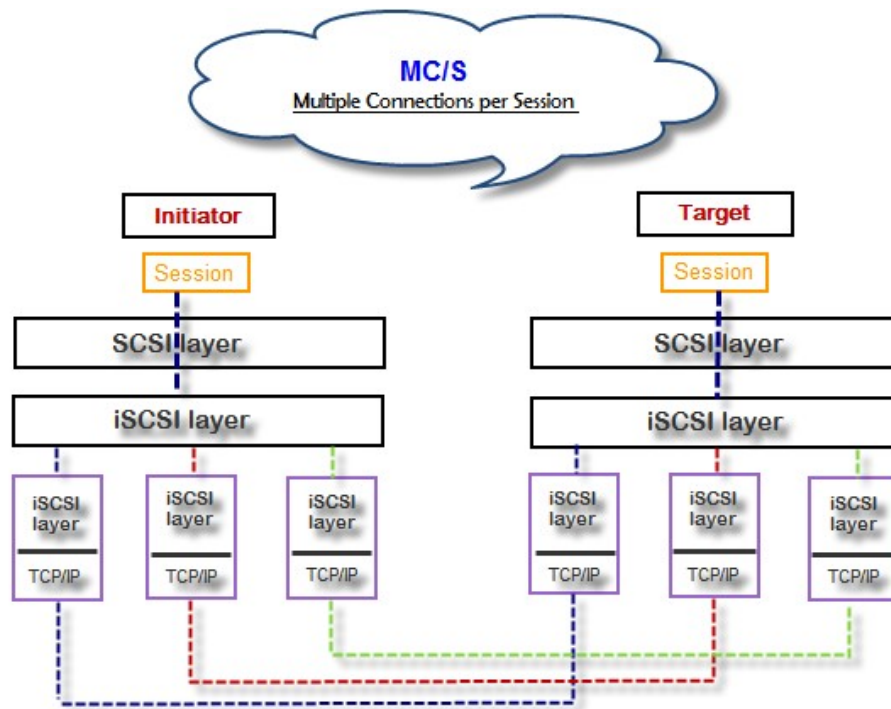
Difference:

MC/S is implemented on iSCSI level, while MPIO is implemented on the higher level. Hence, all MPIO infrastructures are shared among all SCSI transports, including Fiber Channel, SAS, etc. MPIO is the most common usage across all OS vendors. The primary difference between these two is which level the redundancy is maintained. MPIO creates multiple iSCSI sessions with the target storage. Load balance and failover occurs between the multiple sessions. MC/S creates multiple connections within a single iSCSI session to manage load balance and failover. Notice that iSCSI connections and sessions are different than TCP/IP connections and sessions. The above figures describe the difference between MPIO and MC/S.

There are some considerations when user chooses MC/S or MPIO for multipathing.

1. If user uses hardware iSCSI off-load HBA, then MPIO is the only one choice.
2. If user needs to specify different load balance policies for different LUNs, then MPIO should be used.
3. If user installs anyone of Windows XP, Windows Vista or Windows 7, MC/S is the only option since Microsoft MPIO is supported Windows Server editions only.
4. MC/S can provide higher throughput than MPIO in Windows system, but it consumes more CPU resources than MPIO.

6.9 Trunking and LACP

Link aggregation is the technique of taking several distinct Ethernet links to let them appear as a single link. It has a larger bandwidth and provides the fault tolerance ability. Beside the advantage of wide bandwidth, the I/O traffic remains operating until all physical links fail. If any link is restored, it will be added to the link group automatically. The RAID subsystem implements link aggregation as LACP and Trunking.

1. **LACP (IEEE 802.3ad)**: The Link Aggregation Control Protocol (LACP) is a part of IEEE specification 802.3ad. It allows bundling several physical ports together to form a single logical channel. A network switch negotiates an automatic bundle by sending LACP packets to the peer. Theoretically, LACP port can be defined as active or passive. iSCSI controller implements it as active mode which means that LACP port sends LACP protocol packets automatically. Please notice that using the same configurations between iSCSI controller and gigabit switch.

   The usage occasion of LACP:
   A. It's necessary to use LACP in a network environment of multiple switches. When adding new devices, LACP will separate the traffic to each path dynamically.
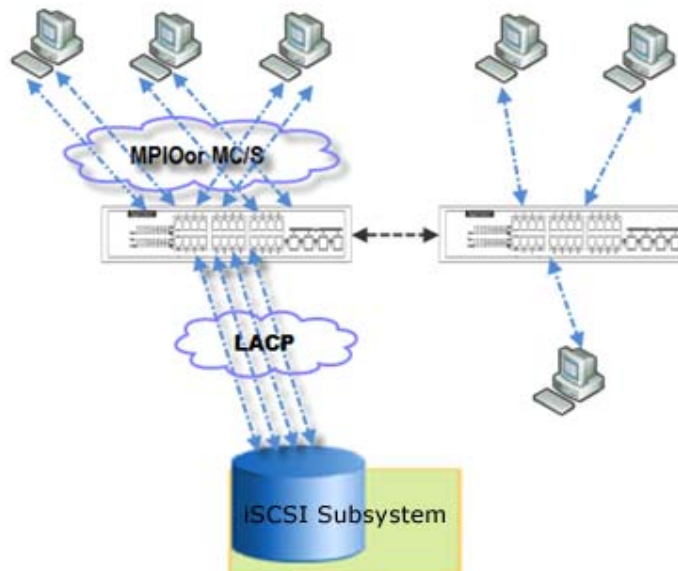
2. **Trunking (Non-protocol)**: Defines the usage of multiple iSCSI data ports in parallel to increase the link speed beyond the limits of any single port.

   The usage occasion of Trunking:
   A. This is a simple SAN environment. There is only one switch to connect the server and storage. And there is no extra server to be added in the future.
   B. There is no idea of using LACP or Trunking, uses Trunking first.
   C. There is a request of monitoring the traffic on a trunk in switch.
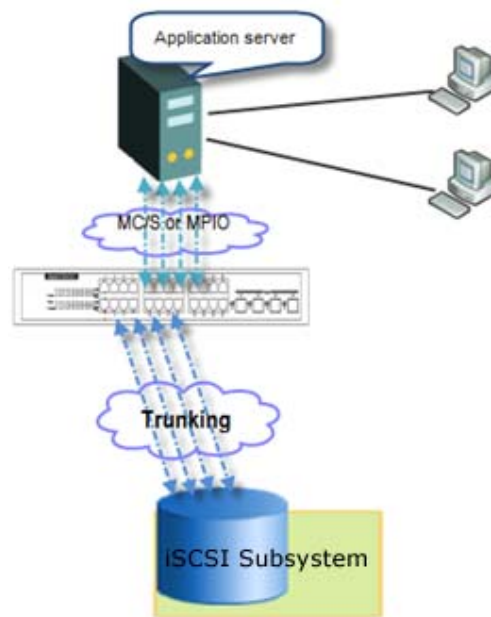
> **IMPORTANT!** Before using trunking or LACP, he gigabit switch must support trunking or LACP and enabled. Otherwise, host cannot connect the link with storage device.

6.10   Dual Controllers

6.10.1   Perform I/O

Please refer to the following topology and have all the connections ready. To perform I/O on dual controllers, server/host should setup MPIO. MPIO policy will keep I/O running and prevent fail connection with single controller failure.
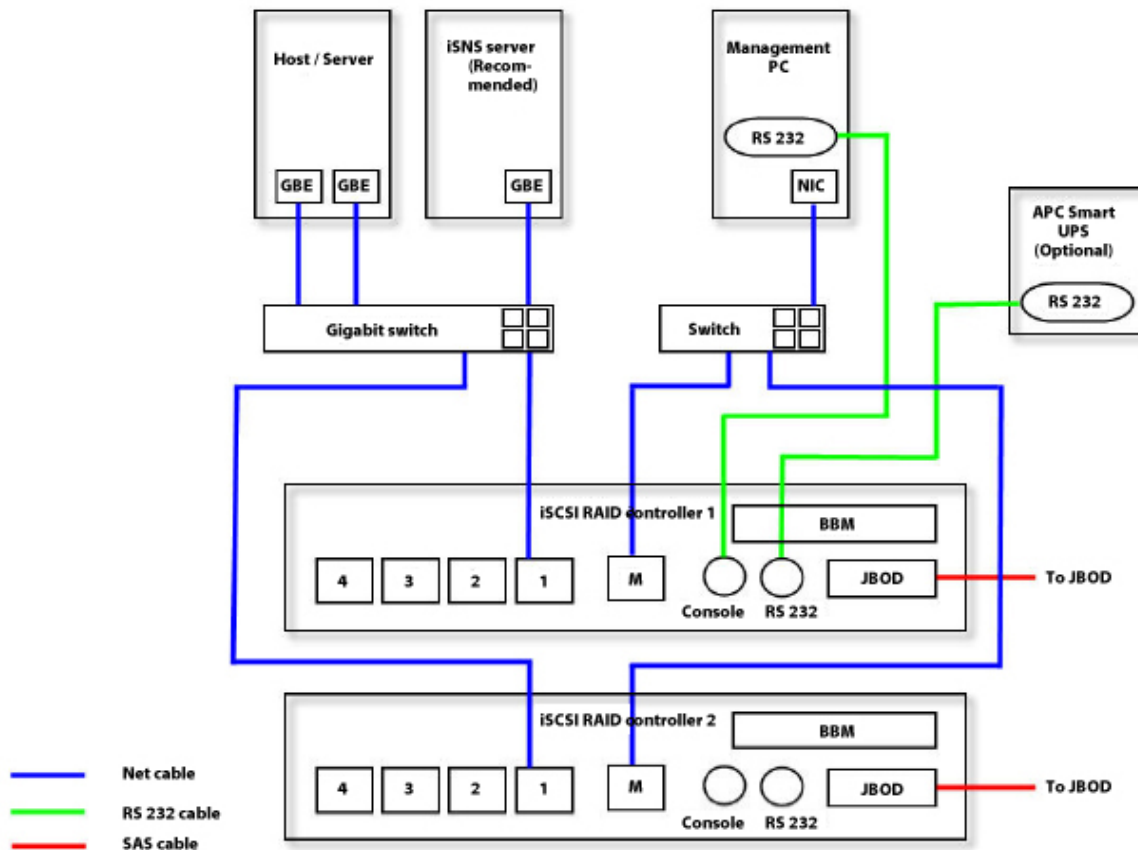
6.10.2 Ownership

When creating RG, it will be assigned with a prefered owner, the default owner is controller 1. To change the RG ownership, please follow the procedures.

1. Select "**/ Volume configuration / RAID group**".
2. Check the gray button next to the RG name; click "**Set preferred owner**".
3. The ownership of the RG will be switched to the other controller.
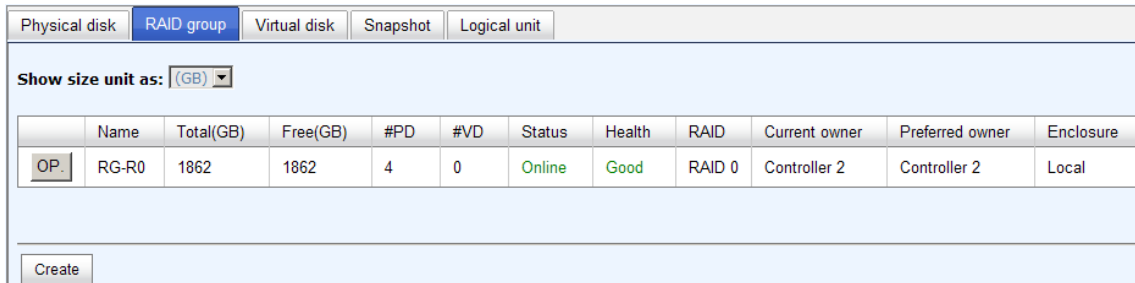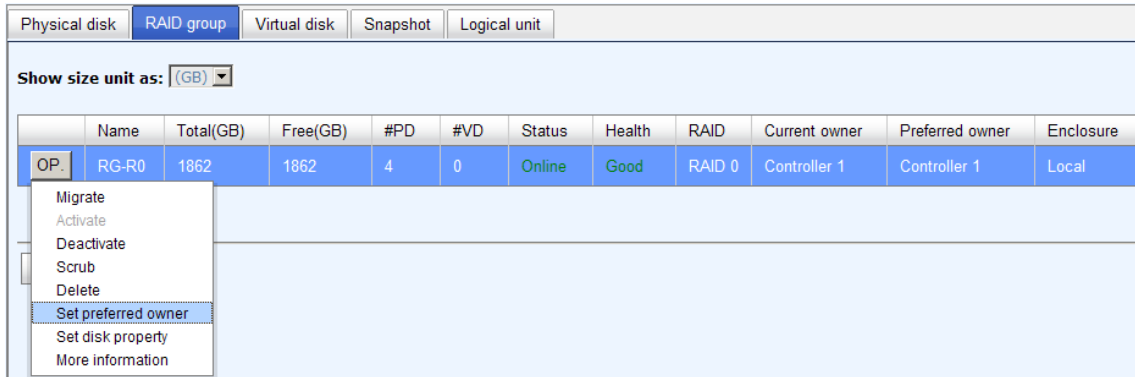
The RG ownership is changed to the other controller.

6.10.3 Controller Status

There are four statuses described on the following. It can be found in "**/ System maintenance / System information**".

1. **Normal**: Dual controller mode. Both of controllers are functional.

2. **Degraded**: Dual controller mode. When one controller fails or has been plugged out, the system will turn to degraded. In this stage, I/O will force to write through for protecting data and the ownership of RG will switch to good one. For example: if controller 1 which owns the RG1 fails accidently, the ownership of RG1 will be switched to controller 2 automatically. And the system and data can keep working well. After controller 1 is fixed or replaced, The current owner of all RGs will be asigned back to their prefered owner.

3. **Lockdown**: Dual controller mode. The firmware of two controllers is different or the size of memory of two controllers is different. In this stage, only master controller can work and I/O will force to write through for protecting data.

4. **Single**: Single controller mode. In the stage, the controller must stay in slot A. Boards for SATA drives are not necessary. The differences between single and degraded are described on the following. There is no error message for inserted one controller only. I/O will not force to write through. And there is no ownership of RG. Single controller mode can be upgraded to dual controller mode, please contact the distributor for upgradable.

In addition, iSNS server is recommended. It's important for keeping I/O running smoothly when RG ownership is switching or single controller is failed. Without iSNS server, when controller 1 fails, the running I/O from host to controller 1 may fail because the time which host switches to the new portal is slower than I/O time out. With iSNS server, this case would not happen.

NOTE: iSNS server is recommended for dual controller system.

6.11 QReplica (Optional)

QReplica function will help users to replicate data easily through LAN or WAN from one subsystem to another.

The procedures of QReplica are on the following:

1. Copy all data from source VD to target VD at the beginning (full copy).
2. Use Snapshot technology to perform the incremental copy afterwards. Please be fully aware that the incremental copy needs to use snapshot to compare the data difference. Therefore, the enough snapshot space for VD clone is very important.

- **Activate the license key**

User needs to obtain a license key and download it to the RAID subsystem to activate the **QReplica** function. Each license key is unique and dedicated to a specific subsystem. It means that the license key for subsystem A cannot be used on another subsystem. To obtain the license key, please contact sales for assistance.

- **Setup the QReplica port on the source subsystem**

The **QReplica** uses the last iSCSI port on the controller to replicate the data. The iSCSI is configured as **QReplica** port, it is no longer available for the host to connected as iSCSI port until it is configured as the normal iSCSI port again.

1. In the operation menu of the last iSCSI port on the controller, select **"Enable QRepica"** to set this port as the **QReplica** port. The last iSCSI port on controller 2 will also be set as the **QReplica** port automatically at the same time.

	Name	LAG	LAG No	DHCP	IP address	Netmask
OP.	LAN1	No	N/A	No	192.168.1.1	255.255.255.0
OP.	LAN2	No	N/A	No	192.168.2.1	255.255.255.0
OP.	LAN3	No	N/A	No	192.168.3.1	255.255.255.0
OP.	LAN4	No	N/A	No	192.168.4.1	255.255.255.0

Show information for: Controller 1

Link aggregation or Multi-homed
IP settings for iSCSI ports
Become default gateway
Enable jumbo frame
Ping host
Enable QReplica
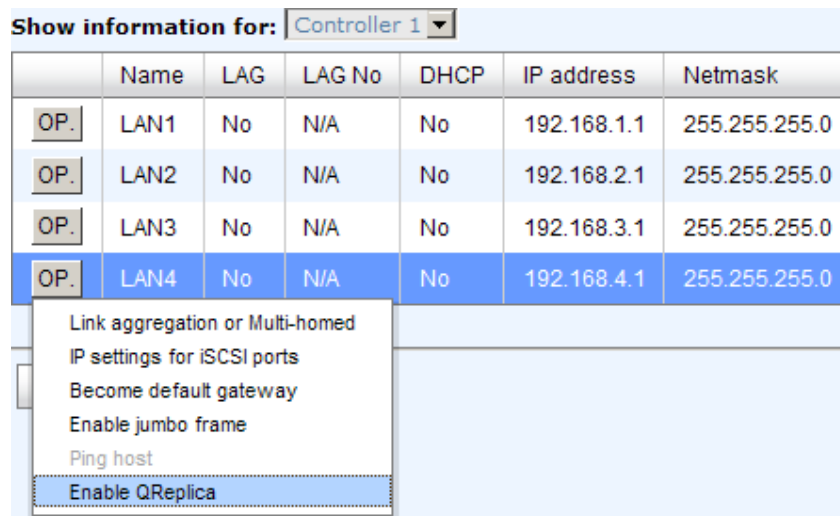
2. The setting can be reverted by select **"Disable QReplica"** in the operation menu.

- **Create backup VD on the target subsystem**

1. Before creating the replication job on the source subsystem, user has to create a virtual disk on the target subsystem and set the type of the VD as **"Backup"**.

2. The backup VD needs to be attached to a LUN ID first before creating replication job.

- **Create replication job on the source subsystem**

1. If the license key is activated on the subsystem correctly, a new **QReplica** tab will be added on the Web UI. Click **"Create"** to create a new replication job.
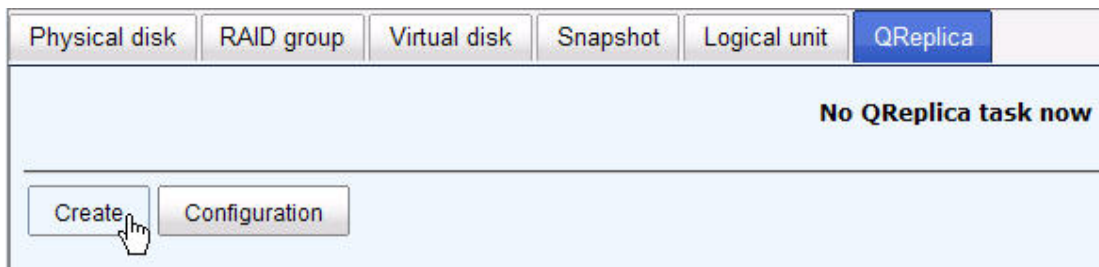
2. Select the source VD which will be replicated to the target subsystem and click **"Next"**.

NOTE: If the message displays that there is not enough space for creation, please refer to the section of *Configure the snapshot space* below for solution.

3. Enter the IP address of iSCSI port on controller 1 of the target subsystem. Click **"Next"** to continue.

4. The QReplica uses standard iSCSI protocol for data replication. User has to log on the iSCSI node to create the iSCSI connection for the data transmission. Enter the **CHAP** information if necessary and select the target node to log no. Click **"Next"** to continue.

5. Choose the backup VD and click **"Next"**.

6. A new replication job is created and listed on the **QReplica** page.

- **Run the replication job**

1. Click the **"OP"** button on the replication job to open operation menu. Click **"Start"** to run the replication job.

2. Click **"Start"** again to confirm the execution of the replication job.

Start QReplica

Sure to start QReplica for task 1?

[Start]   [Close]
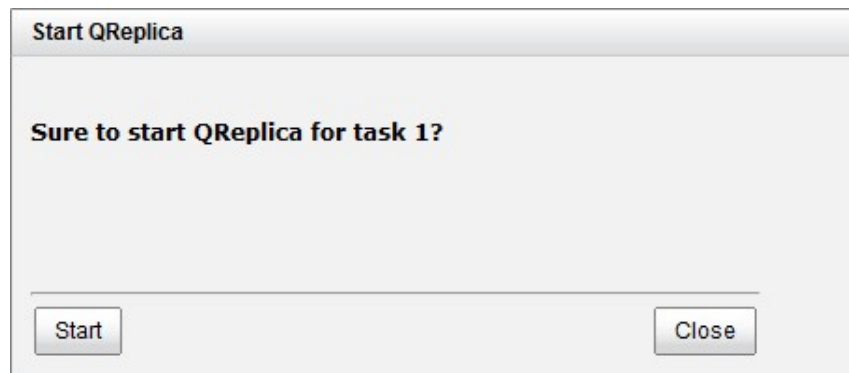
3. User can monitor the replication job from the **"Status"** information and the progress is expressed by percentage.

	No.	VD name	Current owner	Target Name	Target IP	LUN	Name	Size(MB)	Size(GB)	Status	%
OP.	1	source	Controller 1	iqn.1997-05.tw.com.proware:proips-000902298:dev0.ctr1	192.168.15.1	1	target	307200	300	Replicating	0

[Create] [Configuration]

- **Create multi-path on the replication job**

1. Click the **"Create multi-path"** in the operation menu of the replication job.

	No.	VD name	Current owner	Target Name	Target IP
OP.	1	source	Controller 1	iqn.1997-05.tw.com.proware:proips-000902298:dev0.ctr1	192.168.15.1

Start
Stop
Refresh
Create multi-path
Delete multi-path
Schedule
Delete
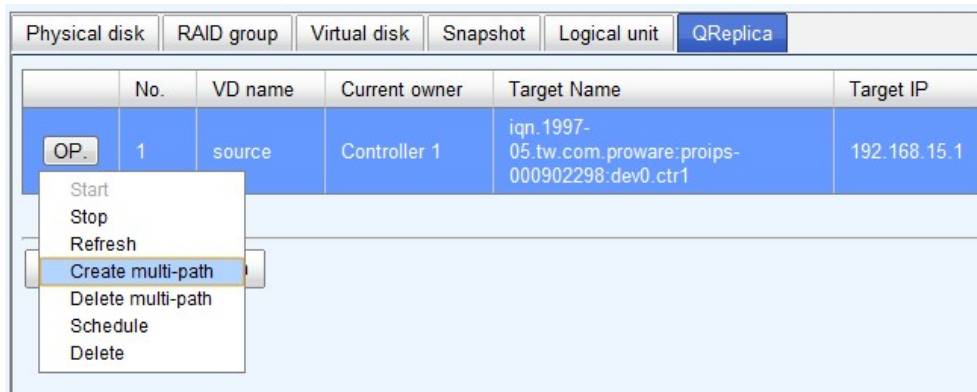
2. Enter the IP of iSCSI port on controller 2 of the target subsystem.

3. Select the iSCSI node to log on and click **"Next"**.

4. Choose the same target VD and click **"Next"**.

5. A new target will be added in this replication job as a redundancy path.

- **Configure the replication job to run by schedule**

1. Click **"Schedule"** in the operation menu of the replication job.

2. The replication job can be scheduled to run by day, by week or by month. The execution time can be configurable per user's need.

- **Configure the snapshot space**

The **QReplica** uses Snapshot. The snapshot technique helps user to replicate the data without stop accessing to the source VD. If the snapshot space is not configured on the source VD in advance, the subsystem will allocate snapshot space for the source VD automatically when the replication job is created. The default snapshot space allocated by the subsystem is double size of the source VD. If the free space of the RG which the source VD resides in is less than double size of the source VD, the replication job will fail and pops up the error message.

To prevent this problem, user has to make sure the RG has enough free space for the snapshot space of source VD, or user has to configure the snapshot space of the source VD manually before the replication job is created.

1. To configure the snapshot space settings of QReplica, click the **"configuration"** button.

There are three settings in the **QReplica configuration** menu,

The **Snapshot space** specifies the ratio of snapshot space allocated to the source VD automatically when the snapshot space is not configured in advance. The default ratio is 2 to 1. It means when the replication job is creating, the subsystem will automatically use the free space of RG to create a snapshot space which size is double of the source VD.

The **Threshold** setting will monitor the utilization of snapshot space. When the used snapshot space achieves the threshold, the subsystem will automatically take a new snapshot and start the replication job. The purpose of threshold is to prevent the incremental copy fail immediately when running out of snapshot space. For example, the default threshold is 50%, and the system will check the snapshot space every hour. When the snapshot space is used over 50%, the subsystem will automatically replicate data from the source VD to the target VD. Next time, when the rest snapshot space has been used over 50%, in other words, the total snapshot space has been used over 75%, the subsystem will start the replication job again.

The **Restart the task an hour later if failed** setting is used when running out of snapshot space, the replication job will stop because there is no more available snapshot space. If this option has been check, the subsystem will automatically clear the snapshots to release snapshot space, and the replication job will restart the task after an hour.

> **IMPORTANT! These two settings, *Threshold* and *Restart the task an hour later if failed*, will take effect only when the replication job is configured to run the schedule.**

6.12 Thin provisioning

Nowadays thin provisioning is a hot topic people talk about in IT management and storage industry. To make contrast to thin provisioning, it naturally brings to our minds with the opposite term - fat provisioning, which is the traditional way IT administrators allocate storage space to each logical volume that is used by an application or a group of users. When it comes to the point to decide how much space a logical volume requires for three years or for the lifetime of an application, it's really hard to make the prediction correctly and precisely. To avoid the complexity of adding more space to the volumes frequently, IT administrators might as well allocate more storage space to each logical volume than it needs in the beginning. This is why it's called "fat" provisioning. Usually it turns out that a lot of free space is sitting around idle. This stranded capacity is wasted, which equals to waste of investment and inefficiency. Various studies indicate that as much as 75% of the storage capacity in small and medium enterprises or large data centers is allocated but unused. And this is where thin provisioning kicks in.

Volume A

Actual data

Physical space

Available space

Volume B

Whole
System
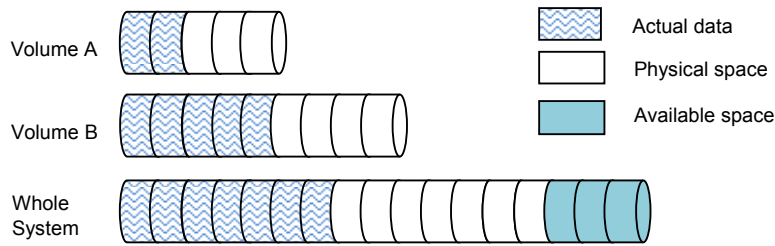
Traditional Fat Provisioning

Thin provisioning sometimes is known as just-in-time capacity or over allocation. As the term explains itself, it provides storage space by requests dynamically. Thin provisioning presents more storage space to the hosts or servers connecting to the storage system than is actually available on the storage system. Put it in another way. Thin provisioning allocates storage space that does not exist. The whole idea is actually another way of virtualization. Virtualization is always about a logical pool of physical assets and provides better utilization over those assets. Here the virtualization mechanism behind thin provisioning is storage pool. The capacity of the storage pool is shared by all volumes. When write requests come in, the space will be drawn dynamically from this storage pool to meet the needs.

Volume A

Actual data

Physical space

Thin provisioning space

Available space

Volume B

Whole
System

Disks not purchased
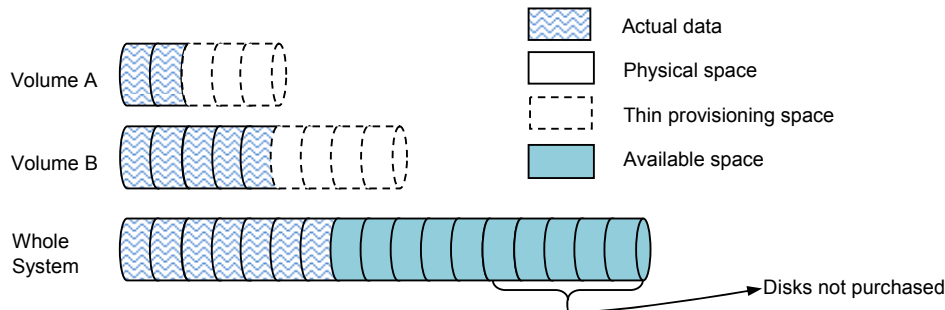
Thin Provisioning

The Benefits of Thin Provisioning

- Less disk purchase is needed initially when setting up a new storage system.

  You don't need to buy more capacity to meet your future data growth at present time. Usually hard drive price declines as time progresses. You can buy the same hard drives with cheaper price at a later time. Why not save money upfront while you can?

- No stranded storage capacity, better utilization efficiency and lower total cost of ownership.

  Thin Provisioning can make full use of the stranded capacity that traditional provisioning can't. All free capacity can be made available to other hosts. A single storage system can serve more hosts and servers to achieve high consolidation ratio. Thin Provisioning can help you achieve the same level of services with less hard drives

purchased upfront, which can significantly reduce your total cost of ownership.

- Scalability: storage pool can grow on demand.

    When the storage pool (RAID group) has reached the threshold you set before. Up to 32 RAID sets can be added to the RAID group to increase the capacity on demand without interrupting I/O. Each RAID set can have up to 64 physical disks.

- Automatic space reclamation mechanism to recycle unused blocks.

    The view of host file system about storage usage can be quite different from that of the storage system. Because deleting a file in the host file system doesn't necessarily mean that the storage system will be informed about the deletion of the file and certain blocks need to be released back to the unused storage pool. If there is no space reclamation function in place, in general the storage system tends to allocate more and more space until the LUN reaches it maximum size, at which point it is the same as if you are using traditional fat provisioning.

- An eco-friendly green feature that helps to reduce energy consumption.

    Hard drive is the top power consumer in a storage system. Because you can use less hard drives to achieve the same amount of work, this translates directly to a huge reduction of power consumption and more green in your pocket.

Features Highlight

1. Downward firmware compatibility with existing array firmware.

    You can upgrade your current storage system to Thin-enabled firmware with no problem. Certain steps need to be followed to ensure a smooth transition to thin provision enabled environment.

2. Write on demand or allocate on demand.

    This is the most distinctive function in thin provisioning. You can see from the screenshots below that figure 1 shows there are two RAID groups created. "Fat_RG" is using traditional provisioning without Thin enabled and its size is 136GB. "Thin-RG" is Thin-enabled and its size is 272GB.

Figure 1: No virtual disk is created

Let's create a Virtual Disk on each RAID group with the same size of 60GB respectively in figure 2 and see what happen.

Figure 2: Virtual disks are created.

In figure 3, the free space of "FAT_RG" immediately reduces to 76GB. 60GB is taken away by the virtual disk. However, the free space of "Thin-RG" is still 272GB even though the same size of virtual disk is created from the RAID group. Nothing is written to the virtual disk yet, so no space is allocated. The remaining 272GB can be used to create other virtual disks. This is storage efficiency.

Figure 3: Write on demand

3. Expand capacity on demand without downtime.

    Extra RAID set can be added to the thin RAID group to increase the size of free storage pool. A thin RAID group can have up to 32 RAID sets with each RAID set containing up to 64 physical hard drives. The maximum size of each RAID set is 64TB. Figure 4 shows that "Thin-RG" consists of two RAID sets.

Figure 4: Scalable RAID group size

4. Allocation unit (granularity) is 1GB. This is a number that demands careful balance between efficiency and performance. The smaller it is, the better the efficiency and the worse the performance becomes, and vice versa.

5. Thin provisioned snapshot space and it is writeable.

   Snapshot space sits at the same RAID group of the volume that the snapshot is taken against. Therefore when you expose the snapshot into a virtual disk, it becomes a thin-provisioned virtual disk. It will only take up the just the right amount of space to store the data, not the full size of the virtual disk.

6. Convert traditional VD to Thin VD and vice versa.

   You can enjoy the benefits of Thin right now and right this moment. Upgrade your systems to Thin-enabled firmware. Move all your existing fat-provisioned virtual disks to thin-provisioned ones. VD cloning functions can be performed on both directions - fat to thin and thin-to-fat, depending on your application needs. Figure 5 shows cloning a fat virtual disk to a thin one.

Figure 5: VD cloning between thin VD and fat VD

7. Threshold settings and capacity policies.

   These are designed to simplify the management and better monitoring the storage usage. You can set as many as 16 policies for each RAID group. When space usage ratio grows over the

threshold set in the policy, the action will be taken and event log will be generated.

Figure 6: Capacity policy settings

8. Automatic space reclamation to recycle unused space and increase utilization rate.

Automatic space reclamation can be set through capacity policy. You can set as many as 16 policies. When space usage ratio grows over the threshold set in the policy, space reclamation will be enabled automatically at the background with the lowest priority or when the I/O is low. The resource impact is reduced to minimum. Space reclamation can also be enabled manually in the functions of Virtual Disk.

Figure 7: Space reclamation

What scenarios does Thin Provisioning fit well?

We suggest that you apply Thin to non-critical production applications first. Thin provisioning works well when the data written is thin-friendly, which means that the data written is not completely spread across the whole volume. Applications that spread metadata across the entire volume will obviate the advantages of thin provisioning. Some applications that expect the data to be contiguous at block level are not good candidates for thin provisioning as well.

Thin works well with email system, web-based archive, or regular file archive system. When the number of supported volumes grows larger, the benefits of Thin will become more apparent.

Chapter 7   Troubleshooting

7.1   System Buzzer

The system buzzer features are listed below:
1.   The system buzzer alarms 1 second when system boots up successfully.
2.   The system buzzer alarms continuously when there is error occurred. The alarm will be stopped after error resolved or be muted.
3.   The alarm will be muted automatically when the error is resolved. E.g., when RAID 5 is degraded and alarm rings immediately, user changes / adds one physical disk for rebuilding. When the rebuilding is done, the alarm will be muted automatically.

7.2 Event Notifications

- **PD events**

Level	Type	Description
INFO	PD inserted	Disk <slot> is inserted into system
WARNING	PD removed	Disk <slot> is removed from system
ERROR	HDD read error	Disk <slot> read block error
ERROR	HDD write error	Disk <slot> write block error
ERROR	HDD error	Disk <slot> is disabled
ERROR	HDD IO timeout	Disk <slot> gets no response
INFO	PD upgrade started	PD [<string>] starts upgrading firmware process.
INFO	PD upgrade finished	PD [<string>] finished upgrading firmware process.
WARNING	PD upgrade failed	PD [<string>] upgrade firmware failed.

- **HW events**

Level	Type	Description
WARNING	ECC single	Single-bit ECC error is detected at <address>
ERROR	ECC multiple	Multi-bit ECC error is detected at <address>
INFO	ECC dimm	ECC memory is installed
INFO	ECC none	Non-ECC memory is installed
INFO	SCSI bus reset	Received SCSI Bus Reset event at the SCSI Bus <number>
ERROR	SCSI host error	SCSI Host allocation failed
ERROR	SATA enable device fail	Failed to enable the SATA pci device
ERROR	SATA EDMA mem fail	Failed to allocate memory for SATA EDMA
ERROR	SATA remap mem fail	Failed to remap SATA memory io spcae
ERROR	SATA PRD mem fail	Failed to init SATA PRD memory manager
ERROR	SATA revision id fail	Failed to get SATA revision id
ERROR	SATA set reg fail	Failed to set SATA register
ERROR	SATA init fail	Core failed to initialize the SATA adapter
ERROR	SATA diag fail	SATA Adapter diagnostics failed
ERROR	Mode ID fail	SATA Mode ID failed
ERROR	SATA chip count error	SATA Chip count error
INFO	SAS port reply error	SAS HBA port <number> reply terminated abnormally
INFO	SAS unknown	SAS frontend reply terminated abnormally

	port reply error	
INFO	FC port reply error	FC HBA port <number> reply terminated abnormally
INFO	FC unknown port reply error	FC frontend reply terminated abnormally

- **EMS events**

Level	Type	Description
INFO	Power install	Power(<string>) is installed
ERROR	Power absent	Power(<string>) is absent
INFO	Power restore	Power(<string>) is restored to work.
ERROR	Power fail	Power(<string>) is not functioning
WARNING	Power detect	PSU signal detection(<string>)
INFO	Fan restore	Fan(<string>) is restored to work.
ERROR	Fan fail	Fan(<string>) is not functioning
INFO	Fan install	Fan(<string>) is installed
ERROR	Fan not present	Fan(<string>) is not present
ERROR	Fan over speed	Fan(<string>) is over speed
WARNING	Thermal level 1	System temperature(<string>) is higher.
ERROR	Thermal level 2	System Overheated(<string>)!!!
ERROR	Thermal level 2 shutdown	System Overheated(<string>)!!! The system will auto-shutdown immediately.
ERROR	Thermal level 2 CTR shutdown	The controller will auto shutdown immediately, reason [Overheated(<string>)].
WARNING	Thermal ignore value	Unable to update thermal value on <string>
WARNING	Voltage level 1	System voltage(<string>) is higher/lower.
ERROR	Voltage level 2	System voltages(<string>) failed!!!
ERROR	Voltage level 2 shutdown	System voltages(<string>) failed!!! The system will auto-shutdown immediately.
ERROR	Voltage level 2 CTR shutdown	The controller will auto shutdown immediately, reason [Voltage abnormal(<string>)].
INFO	UPS OK	Successfully detect UPS
WARNING	UPS fail	Failed to detect UPS
ERROR	UPS AC loss	AC loss for system is detected
ERROR	UPS power low	UPS Power Low!!! The system will auto-shutdown immediately.
WARNING	SMART T.E.C.	Disk <slot> S.M.A.R.T. Threshold Exceed Condition occurred for attribute <string>
WARNING	SMART fail	Disk <slot>: Failure to get S.M.A.R.T information
WARNING	RedBoot failover	RedBoot failover event occurred
WARNING	Watchdog shutdown	Watchdog timeout shutdown occurred
WARNING	Watchdog	Watchdog timeout reset occurred

	reset	

- **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
INFO	Log clear	All event logs are cleared
WARNING	Send mail fail	Failed to send event to \<email\>.

- **LVM events**

Level	Type	Description
INFO	RG create OK	RG \<name\> has been created.
INFO	RG create fail	Failed to create RG \<name\>.
INFO	RG delete	RG \<name\> has been deleted.
INFO	RG rename	RG \<name\> has been renamed as \<name\>.
INFO	VD create OK	VD \<name\> has been created.
INFO	VD create fail	Failed to create VD \<name\>.
INFO	VD delete	VD \<name\> has been deleted.
INFO	VD rename	Name of VD \<name\> has been renamed to \<name\>.
INFO	VD read only	Cache policy of VD \<name\> has been set as read only.
INFO	VD write back	Cache policy of VD \<name\> has been set as write-back.
INFO	VD write through	Cache policy of VD \<name\> has been set as write-through.
INFO	VD extend	Size of VD \<name\> extends.
INFO	VD attach LUN OK	VD \<name\> has been LUN-attached.
INFO	VD attach LUN fail	Failed to attach LUN to VD \<name\>.
INFO	VD detach LUN OK	VD \<name\> has been detached.
INFO	VD detach LUN fail	Failed to attach LUN from bus \<number\>, SCSI ID \<number\>, lun \<number\>.
INFO	VD init started	VD \<name\> starts initialization.
INFO	VD init finished	VD \<name\> completes initialization.
WARNING	VD init 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 migrate	VD \<name\> starts migration.

	started	
INFO	VD migrate finished	VD <name> completes migration.
ERROR	VD migrate failed	Failed to complete migration of VD <name>.
INFO	VD scrub started	Parity checking on VD <name> starts.
INFO	VD scrub finished	Parity checking on VD <name> completes with <address> parity/data inconsistency found.
INFO	VD scrub aborted	Parity checking on VD <name> stops with <address> parity/data inconsistency found.
INFO	RG migrate started	RG <name> starts migration.
INFO	RG migrate finished	RG <name> completes migration.
INFO	RG move started	RG <name> starts move.
INFO	RG move finished	RG <name> completes move.
INFO	VD move started	VD <name> starts move.
INFO	VD move finished	VD <name> completes move.
ERROR	VD move failed	Failed to complete move of VD <name>.
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 <name> starts.
INFO	VD rewrite finished	Rewrite at LBA <address> of VD <name> completes.
WARNING	VD rewrite failed	Rewrite at LBA <address> of VD <name> failed.
WARNING	RG degraded	RG <name> is in degraded mode.
WARNING	VD degraded	VD <name> is in degraded mode.
ERROR	RG failed	RG <name> is failed.
ERROR	VD failed	VD <name> is failed.
ERROR	VD IO fault	I/O failure for stripe number <address> in VD <name>.
WARNING	Recoverable read error	Recoverable read error occurred at LBA <address>-<address> of VD <name>.
WARNING	Recoverable write error	Recoverable write error occurred at LBA <address>-<address> of VD <name>.
ERROR	Unrecoverable read error	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>.
ERROR	Config read fail	Config read failed at LBA <address>-<address> of PD <slot>.
ERROR	Config write fail	Config write failed at LBA <address>-<address> of PD <slot>.
ERROR	CV boot error adjust global	Failed to change size of the global cache.
INFO	CV boot global	The global cache is ok.
ERROR	CV boot error	Failed to create the global cache.

	create global	
INFO	PD dedicated spare	Assign PD <slot> to be the dedicated spare disk of RG <name>.
INFO	PD global spare	Assign PD <slot> to Global Spare Disks.
WARNING	PD read error	Read error occurred at LBA <address>-<address> of PD <slot>.
WARNING	PD write error	Write error occurred at LBA <address>-<address> of PD <slot>.
WARNING	Scrub wrong parity	The parity/data inconsistency is found at LBA <address>-<address> when checking parity on VD <name>.
WARNING	Scrub data recovered	The data at LBA <address>-<address> is recovered when checking parity on VD <name>.
WARNING	Scrub recovered data	A recoverable read error occurred at LBA <address>-<address> when checking parity on VD <name>.
WARNING	Scrub parity recovered	The parity at LBA <address>-<address> is regenerated when checking parity on VD <name>.
INFO	PD freed	PD <slot> has been freed 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.
INFO	PD scrub started	PD <slot> starts disk scrubbing process.
INFO	Disk scrub finished	PD <slot> completed disk scrubbing process.
INFO	Large RG created	A large RG <name> with <number> disks included is created
INFO	Weak RG created	A RG <name> made up disks across <number> chassis is created
INFO	RG size shrunk	The total size of RG <name> shrunk
INFO	VD erase finished	VD <name> finished erasing process.
WARNING	VD erase failed	The erasing process of VD <name> failed.
INFO	VD erase started	VD <name> starts erasing process.

- **Snapshot events**

Level	Type	Description
WARNING	Snap mem	Failed to allocate snapshot memory for VD <name>.
WARNING	Snap space overflow	Failed to allocate snapshot space for VD <name>.
WARNING	Snap threshold	The snapshot space threshold of VD <name> has been reached.

INFO	Snap delete	The snapshot VD <name> has been deleted.
INFO	Snap auto delete	The oldest snapshot VD <name> has been deleted to obtain extra snapshot space.
INFO	Snap take	A snapshot on VD <name> has been taken.
INFO	Snap set space	Set the snapshot space of VD <name> to <number> MB.
INFO	Snap rollback started	Snapshot rollback of VD <name> has been started.
INFO	Snap rollback finished	Snapshot rollback of VD <name> has been finished.
WARNING	Snap quota reached	The quota assigned to snapshot <name> is reached.
INFO	Snap clear space	The snapshot space of VD <name> is cleared

- **iSCSI events**

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

- **Battery backup events**

Level	Type	Description
INFO	BBM start syncing	Abnormal shutdown detected, start flushing battery-backed data (<number> KB).
INFO	BBM stop syncing	Abnormal shutdown detected, flushing battery-backed data finished
INFO	BBM installed	Battery backup module is detected
INFO	BBM status good	Battery backup module is good
INFO	BBM status charging	Battery backup module is charging
WARNING	BBM status fail	Battery backup module is failed
INFO	BBM enabled	Battery backup feature is <string>.
INFO	BBM inserted	Battery backup module is inserted
INFO	BBM removed	Battery backup module is removed

- **JBOD events**

Level	Type	Description
INFO	PD upgrade started	JBOD <name> PD [<string>] starts upgrading firmware process.
INFO	PD upgrade finished	JBOD <name> PD [<string>] finished upgrading firmware process.
WARNING	PD upgrade	JBOD <name> PD [<string>] upgrade

	failed	firmware failed.
INFO	PD freed	JBOD <name> PD <slot> has been freed from RG <name>.
INFO	PD inserted	JBOD <name> disk <slot> is inserted into system.
Warning	PD removed	JBOD <name> disk <slot> is removed from system.
ERROR	HDD read error	JBOD <name> disk <slot> read block error
ERROR	HDD write error	JBOD <name> disk <slot> write block error
ERROR	HDD error	JBOD <name> disk <slot> is disabled.
ERROR	HDD IO timeout	JBOD <name> disk <slot> gets no response
INFO	JBOD inserted	JBOD <name> is inserted into system
WARNING	JBOD removed	JBOD <name> is removed from system
WARNING	SMART T.E.C	JBOD <name> disk <slot>: S.M.A.R.T. Threshold Exceed Condition occurred for attribute <string>
WARNING	SMART fail	JBOD <name> disk <slot>: Failure to get S.M.A.R.T information
INFO	PD dedicated spare	Assign JBOD <name> PD <slot> to be the dedicated spare disk of RG <name>.
INFO	PD global spare	Assign JBOD <name> PD <slot> to Global Spare Disks.
ERROR	Config read fail	Config read error occurred at LBA <address>-<address> of JBOD <name> PD <slot>.
ERROR	Config write fail	Config write error occurred at LBA <address>-<address> of JBOD <name> PD <slot>.
WARNING	PD read error	Read error occurred at LBA <address>-<address> of JBOD <name> PD <slot>.
WARNING	PD write error	Write error occurred at LBA <address>-<address> of JBOD <name> PD <slot>.
INFO	PD scrub started	JBOD <name> PD <slot> starts disk scrubbing process.
INFO	PD scrub completed	JBOD <name> PD <slot> completed disk scrubbing process.
WARNING	PS fail	Power Supply of <string> in JBOD <name> is FAIL
INFO	PS normal	Power Supply of <string> in JBOD <name> is NORMAL
WARNING	FAN fail	Cooling fan of <string> in JBOD <name> is FAIL
INFO	FAN normal	Cooling fan of <string> in JBOD <name> is NORMAL
WARNING	Volt warn OV	Voltage of <string> read as <string> in JBOD <name> is WARN OVER
WARNING	Volt warn UV	Voltage of <string> read as <string> in JBOD <name> is WARN UNDER
WARNING	Volt crit OV	Voltage of <string> read as <string> in JBOD <name> is CRIT OVER
WARNING	Volt crit UV	Voltage of <item> read as <string> in JBOD <name> is CRIT UNDER
INFO	Volt recovery	Voltage of <string> in JBOD <string> is NORMAL
WARNING	Therm warn	Temperature of <string> read as <string> in

	OT	JBOD <name> is OT WARNING
WARNING	Therm warn UT	Temperature of <string> read as <string> in JBOD <name> is UT WARNING
WARNING	Therm fail OT	Temperature of <string> read as <string> in JBOD <name> is OT FAILURE
WARNING	Therm fail UT	Temperature of <string> read as <string> in JBOD <name> is UT FAILURE
INFO	Therm recovery	Temperature of <string> in JBOD <name> is NORMAL

- **System maintenance events**

Level	Type	Description
INFO	System shutdown	System shutdown.
INFO	System reboot	System reboot.
INFO	System console shutdown	System shutdown from <string> via Console UI
INFO	System web shutdown	System shutdown from <string> via Web UI
INFO	System button shutdown	System shutdown via power button
INFO	System LCM shutdown	System shutdown via LCM
INFO	System console reboot	System reboot from <string> via Console UI
INFO	System web reboot	System reboot from <string> via Web UI
INFO	System LCM reboot	System reboot via LCM
INFO	FW upgrade start	System firmware upgrade starts.
INFO	FW upgrade success	System firmware upgrade succeeds.
WARNING	FW upgrade failure	System firmware upgrade is failed.
ERROR	IPC FW upgrade timeout	System firmware upgrade timeout on another controller
INFO	Config imported	<string> config imported

- **HAC events**

Level	Type	Description
INFO	RG owner changed	The preferred owner of RG <name> has been changed to controller <number>.
INFO	Force CTR write through	Controller <number> forced to adopt write-through mode on failover.
INFO	Restore CTR cache mode	Controller <number> restored to previous caching mode on failback.
INFO	Failover	All volumes in controller <number> completed

	complete	failover process.
INFO	Failback complete	All volumes in controller <number> completed failback process.
INFO	CTR inserted	Controller <number> is inserted into system
ERROR	CTR removed	Controller <number> is removed from system
ERROR	CTR timeout	Controller <number> gets no response
ERROR	CTR lockdown	Controller <number> is locked down
ERROR	CTR memory NG	Memory size mismatch
ERROR	CTR firmware NG	Firmware version mismatch
ERROR	CTR lowspeed NG	Low speed inter link is down
ERROR	CTR highspeed NG	High speed inter link is down
ERROR	CTR backend NG	SAS expander is down
ERROR	CTR frontend NG	FC IO controller is down
INFO	CTR reboot FW sync	Controller reboot, reason [Firmware synchronization completed]

- **Clone events**

Level	Type	Description
INFO	VD clone started	VD <name> starts cloning process.
INFO	VD clone finished	VD <name> finished cloning process.
WARNING	VD clone failed	The cloning in VD <name> failed.
INFO	VD clone aborted	The cloning in VD <name> was aborted.
INFO	VD clone set	The clone of VD <name> has been designated.
INFO	VD clone reset	The clone of VD <name> is no longer designated.
WARNING	Auto clone error	Auto clone task: <string>.
WARNING	Auto clone no snap	Auto clone task: Snapshot <name> is not found for VD <name>.

- **QReplica events**

Level	Type	Description
INFO	Qrep portal enabled	LAN<number> is enabled for QReplica portal
INFO	Qrep portal disabled	QReplica portal is disabled
INFO	VD replicate started	VD <name> starts replication process.
INFO	VD replicate finished	VD <name> finished replication process.
WARNING	VD replicate	The replication in VD <name> failed.

		failed	
INFO	VD replicate aborted	The replication in VD <name> was aborted.
INFO	VD set as replica	VD <name> has been configured as a replica.
INFO	VD set as RAID	VD <name> has been configured as a RAID volume.
INFO	VD replica set	The replica of VD <name> has been designated.
INFO	VD replica reset	The replica of VD <name> is no longer designated.
WARNING	Auto qrep not enable	Auto QReplica task: QReplica is not enabled for VD <name>.
WARNING	Auto qrep error	Auto QReplica task: <string>.
WARNING	Auto qrep no snap	Auto QReplica task: Snapshot <name> is not found for VD <name>.
INFO	Source replicate started	Remote VD <name> starts replicating to VD <name>.
INFO	Source replicate finished	Remote VD <name> finished replication to VD <name>.
INFO	Source replicate failed	Remote VD <name> failed replication to VD <name>.
INFO	Source replicate aborted	Remote VD <name> aborted replication to VD <name>.