

Enteroc iS1030 iSCSI RAID Storage System

User Manual

Revision 1.0

Table of Contents

Preface	7
Before You Begin	8
Safety Guidelines	8
Controller Configurations	8
Packaging, Shipment and Delivery	8
Chapter 1 Introduction.....	10
1.1 Technical Specifications.....	12
1.2 Terminology	14
1.3 RAID Levels.....	16
1.4 Volume Relationship Diagram.....	17
1.5 iSCSI Concepts	17
Chapter 2 Identifying Parts of the RAID Subsystem.....	18
2.1 Main Components	18
2.1.1 Front View	18
2.1.1.1 Disk Trays	19
2.1.1.2 LCD Front Panel.....	20
2.1.2 Rear View	21
2.2 Controller Module	22
2.3 Power Supply / Fan Module (PSFM).....	24
2.3.1 PSFM Panel.....	24
Chapter 3 Getting Started with the Subsystem.....	26
3.1 Powering On	26
3.2 Disk Drive Installation	26
3.2.1 Installing a SAS Disk Drive in a Disk Tray	27
3.2.2 Installing a SATA Disk Drive (Dual Controller Mode) in a Disk Tray	29
Chapter 4 Quick Setup	33
4.1 Management Interfaces.....	33
4.1.1 Serial Console Port.....	33
4.1.2 Remote Control – Secure Shell	33

4.1.3	LCD Control Module (LCM)	34
4.1.4	Web GUI	37
4.2	How to Use the System Quickly.....	39
4.2.1	Quick Installation	39
4.2.2	Volume Creation Wizard.....	43
Chapter 5	Configuration	46
5.1	Web GUI Management Interface Hierarchy.....	46
5.2	System Configuration.....	49
5.2.1	System Setting	49
5.2.2	Network Setting.....	50
5.2.3	Login Setting.....	51
5.2.4	Email Notification Settings.....	52
5.2.5	Log and Alert Settings.....	53
5.3	Host Port / iSCSI Configuration.....	55
5.3.1	Network Setup	55
5.3.2	Entity and iSCSI Settings.....	58
5.3.3	iSCSI Node.....	58
5.3.4	Active Session.....	62
5.3.5	CHAP Account.....	63
5.3.6	Fibre Channel.....	64
5.4	Volume Configuration.....	66
5.4.1	Physical Disk.....	66
5.4.2	RAID Group	69
5.4.3	Virtual Disk.....	72
5.4.4	Snapshot.....	77
5.4.5	Logical Unit.....	80
5.5	Enclosure Management.....	82
5.5.1	Hardware Monitor	83
5.5.2	UPS.....	84
5.5.3	SES.....	86
5.5.4	S.M.A.R.T.	86
5.6	System Maintenance	87
5.6.1	System Information.....	87

5.6.2	Event Log.....	88
5.6.3	Upgrade	89
5.6.4	Firmware Synchronization (Only available in Dual controller models).....	91
5.6.5	Reset to Factory Default	92
5.6.6	Configuration Backup.....	92
5.6.7	Volume Restoration	93
5.6.8	Reboot and Shutdown.....	94
5.7	Performance Monitor	95
5.7.1	Disk	95
5.7.2	iSCSI.....	96
5.7.3	Fibre Channel.....	96
Chapter 6	Advanced Operations.....	97
6.1	Volume Rebuild	97
6.2	Migrate and Move RAID Groups.....	99
6.3	Extend Virtual Disks	101
6.4	Thin provisioning	102
6.4.1	The Benefits of Thin provisioning	103
6.4.2	Features Highlight	104
6.4.3	Thin provisioning Options.....	106
6.4.4	Thin Provisioning Case	107
6.5	Disk Roaming.....	107
6.6	JBOD Expansion.....	108
6.6.1	Connecting JBOD	108
6.6.2	Upgrade Firmware	108
6.7	MPIO and MC/S	109
6.7.1	MPIO	109
6.7.2	MC/S.....	110
6.7.3	Difference	110
6.8	Trunking and LACP.....	111
6.8.1	LACP	111
6.8.2	Trunking.....	112
6.9	Dual Controllers.....	113
6.9.1	Perform I/O.....	113

6.9.2	Ownership	114
6.9.3	Controller Status.....	114
6.9.4	Change Controller Mode.....	115
6.9.5	Recommend iSNS Server	115
6.10	Snapshot / Rollback	116
6.10.1	Take a Snapshot.....	117
6.10.2	Cleanup Snapshots	118
6.10.3	Schedule Snapshots	119
6.10.4	Rollback	119
6.10.5	Snapshot Constraint.....	120
6.11	Clone.....	122
6.11.1	Setup Clone	122
6.11.2	Start and Stop Clone	124
6.11.3	Schedule Clone.....	125
6.11.4	Cloning Options.....	126
6.11.5	Clear Clone.....	127
6.11.6	Clone Constraint	127
6.12	QReplicas	128
6.12.1	Create QReplica Task.....	128
6.12.2	Start and Stop QReplica Task	133
6.12.3	MPIO.....	134
6.12.4	MC/S	134
6.12.5	Task Shaping	135
6.12.6	Schedule QReplica Task.....	136
6.12.7	QReplica Options.....	137
6.12.8	Delete QReplica Task.....	138
6.12.9	Clone Transfers to QReplica	138
6.13	Fast Rebuild	141
6.13.1	Solution.....	141
6.13.2	Configuration	142
6.13.3	Constraint	142
6.14	SSD Caching	143
6.14.1	Solution.....	143

6.14.2	Methodology.....	143
6.14.3	Populating the Cache	144
6.14.4	Read/Write Cache Cases	144
6.14.5	I/O Type.....	147
6.14.6	Configuration	149
6.14.7	Constraint	149
Chapter 7	Troubleshooting	150
7.1	System Buzzer	150
7.2	Event Notifications	150
Appendix		159
A.	Microsoft iSCSI initiator	159

Preface

About this manual

This manual provides information regarding the quick installation and hardware features of the Enteroc iS1030 series **RAID subsystem**. This document also describes how to use the storage management software. Information contained in the manual has been reviewed for accuracy, but not for product warranty because of the various environment/OS/settings. Information and specifications will be changed without further notice.

This manual uses section numbering for every topics being discussed for easy and convenient way of finding information in accordance with the user's needs. The following icons are being used for some details and information to be considered in going through with this manual:



NOTES:

These are notes that contain useful information and tips that the user must give attention to in going through with the subsystem operation.



IMPORTANT!

These are the important information that the user must remember.



WARNING!

These are the warnings that the user must follow to avoid unnecessary errors and bodily injury during hardware and software operation of the subsystem.



CAUTION:

These are the cautions that user must be aware to prevent damage to the equipment and its components.

Copyright

2017 Rocstor. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording or otherwise, without the prior written consent.

Trademarks

All products and trade names used in this document are trademarks Rocstor or registered trademarks of their respective holders.

Changes

The material in this document is for information only and is subject to change without notice.

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°C. 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 both single controller and dual controller configurations. The single controller can be configured depending on the user's requirements. On the other side, these controllers can be both configured and be active to increase system efficiency and to improve performance.

This manual will discuss both single and dual 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
	One (1) Ethernet LAN cable for single controller Note: Two (2) Ethernet LAN cables for dual controller
	One (1) LC-LC Fibre Optical Cable for single controller Note: Two(2) LC-LC Fibre Optical 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(Optional)
- 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

- 3U 16Bay 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
- Automatic synchronization of firmware version in the dual-active mode
- Supports S.M.A.R.T, NCQ and OOB Staggered Spin-up capable drives
- Supports fast rebuild
- High efficiency power supply which compliant with 80plus

1.1 Technical Specifications

RAID Controller	iSCSI - 6G SAS
Controller	Single / Dual (Redundant)
Host Interface	2 x 10GbE + 2 x 1GbE (per Controller)
Disk Interface	6Gb SAS or 6Gb SATA
SAS expansion	One 6Gb SAS (SFF-8088) (per controller)
Processor Type	Intel S1200 Series
Cache Memory	4GB~8GB/8GB~16GB DDR3 ECC SDRAM
Battery Backup	Optional Hot Pluggable BBM
Expansion Disk No.	Up to 256 Disks
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 2048
iSCSI Jumbo frame support	Yes
Supports Microsoft Multipath I/O (MPIO)	Yes
802.3ad Port Trunking, LACP Support	Yes
Host connection	Up to 64
Host clustering	Up to 16 for one logical volume
Manual/scheduling volume snapshot	Up to 64
Hot spare disks	Global, local 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

Thin Provision	Yes
Local Clone	Yes
Remote Replication	Yes
VAAI (vStorage APIs for Array Integration)	Yes
S.M.A.R.T. support	Yes
Snapshot rollback mechanism support	Yes
Platform	Rackmount
Form Factor	3U
# of Hot Swap Trays	16
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 131(H) mm
Weight (Without Disk)	19/20.5 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	Redundant Array of Independent Disks. There are different RAID levels with different degree of data protection, data availability, and performance to host environment.
PD	The Physical Disk belongs to the member disk of one specific RAID group.
RG	Raid Group. A collection of removable media. One RG consists of a set of VDs and owns one RAID level attribute.
VD	Virtual Disk. 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	Logical Unit Number. A logical unit number (LUN) is a unique identifier which enables it to differentiate among separate devices (each one is a logical unit).
GUI	Graphic User Interface.
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	Write-Through cache-write policy. A caching technique in which the completion of a write request is not signaled until data is safely stored in non-volatile media. Each data is synchronized in both data cache and accessed physical disks.
WB	Write-Back cache-write policy. A caching technique in which the completion of a write request is signaled as soon as the data is in cache and actual writing to non-volatile media occurs at a later time. It speeds up system write performance but needs to bear the risk where data may be inconsistent between data cache and the physical disks in one short time interval.
RO	Set the volume to be Read-Only .
DS	Dedicated Spare disks. The spare disks are only used by one specific RG. Others could not use these dedicated spare disks for any rebuilding purpose.
GS	Global Spare disks. GS is shared for rebuilding purpose. If some RGs need to use the global spare disks for rebuilding, they could get the spare disks out from the common spare disks pool for such requirement.

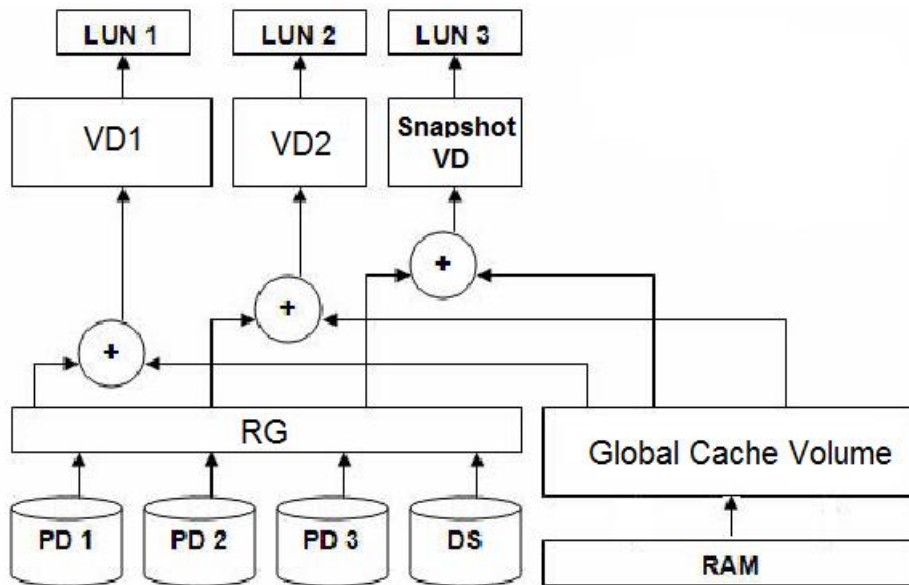
DG	DeGraded mode. Not all of the array's member disks are functioning, but the array is able to respond to application read and write requests to its virtual disks.
SCSI	S mall C omputer S ystems I nterface.
SAS	S erial A ttached SCSI .
S.M.A.R.T.	S elf- M onitoring A nalysis and R eporting T echnology.
WWN	W orld W ide N ame.
HBA	H ost B us A dapter.
SES	SCSI 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.

1.5 iSCSI Concepts

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.

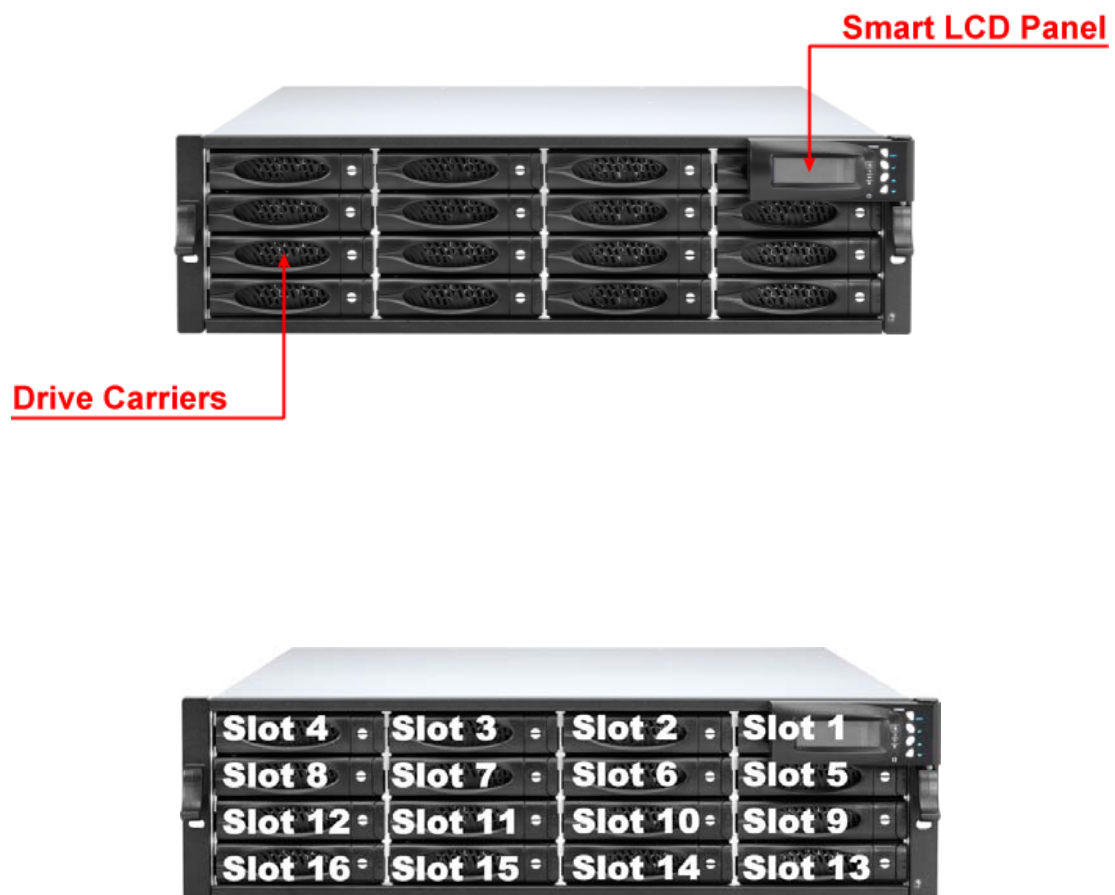
IP SANs are true SANs (Storage Area Networks) which allow several servers to attach to an infinite number of storage volumes by using iSCSI over TCP/IP networks. IP SANs can scale the storage capacity with any type and brand of storage system. In addition, it can be used by any type of network (Ethernet, Fast Ethernet, Gigabit Ethernet, and 10 Gigabit Ethernet) and combination of operating systems (Microsoft Windows, Linux, Solaris, Mac, etc.) within the SAN network. IP-SANs also include mechanisms for security, data replication, multi-path and high availability.

Chapter 2 Identifying Parts of the RAID Subsystem

The illustrations below identify the various parts of the subsystem.

2.1 Main Components

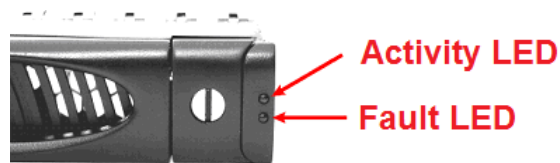
2.1.1 Front View



2.1.1.1 Disk Trays



HDD Status Indicator

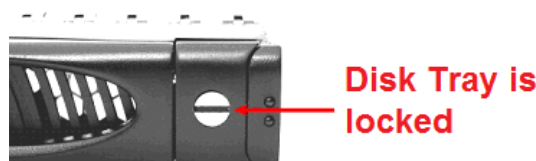
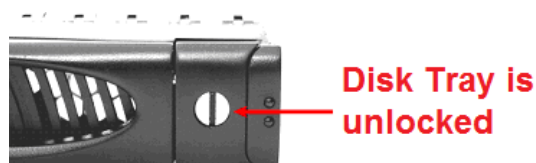


Part	Function
HDD Activity LED	This LED will blink blue when the hard drive is being accessed.
HDD Fault LED	Green LED indicates power is on and hard drive status is good for this slot. If hard drive is defective or failed, the LED is Red. LED is off when there is no hard drive.

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

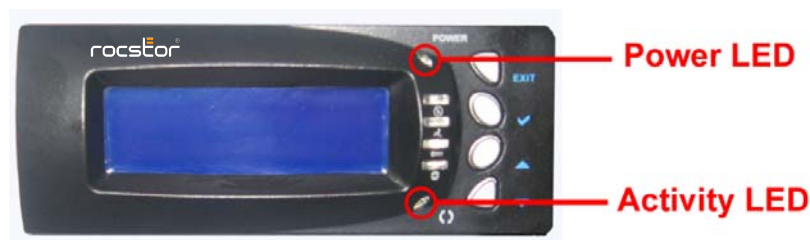



Smart Function Front Panel

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.

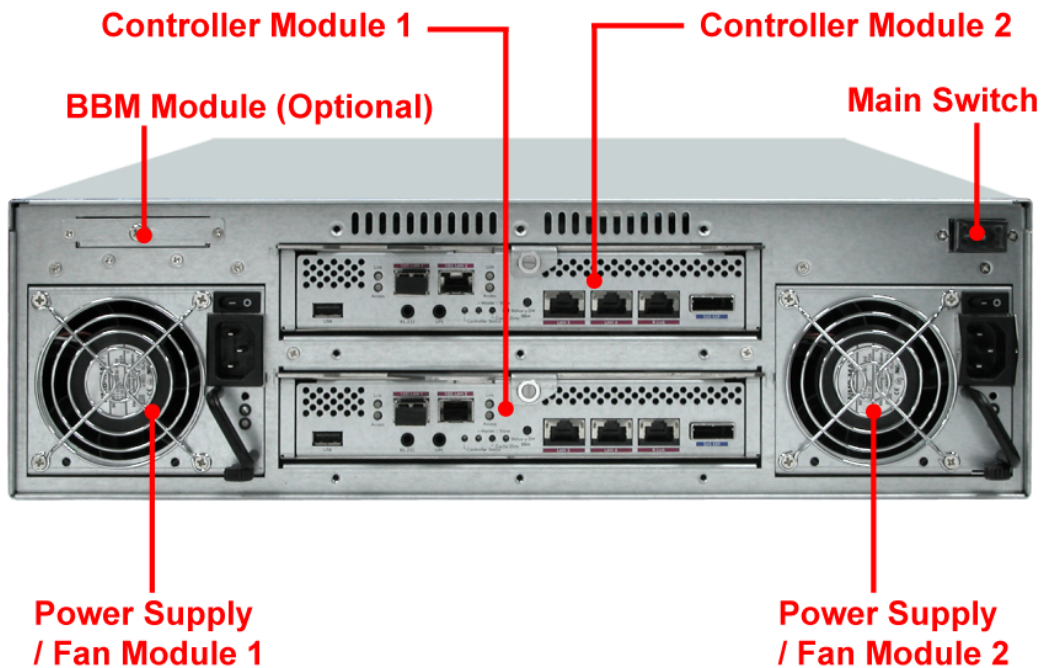
Parts	Function
Up and Down Arrow buttons 	Use the Up or Down arrow keys to go through the information on the LCD screen. This is also used to move between each menu when you configure the subsystem.
Select button 	This is used to enter the option you have selected.
Exit button EXIT	Press this button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

Status LEDs



Parts	Function
Power LED	Green LED indicates power is ON.
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 / two controller modules.

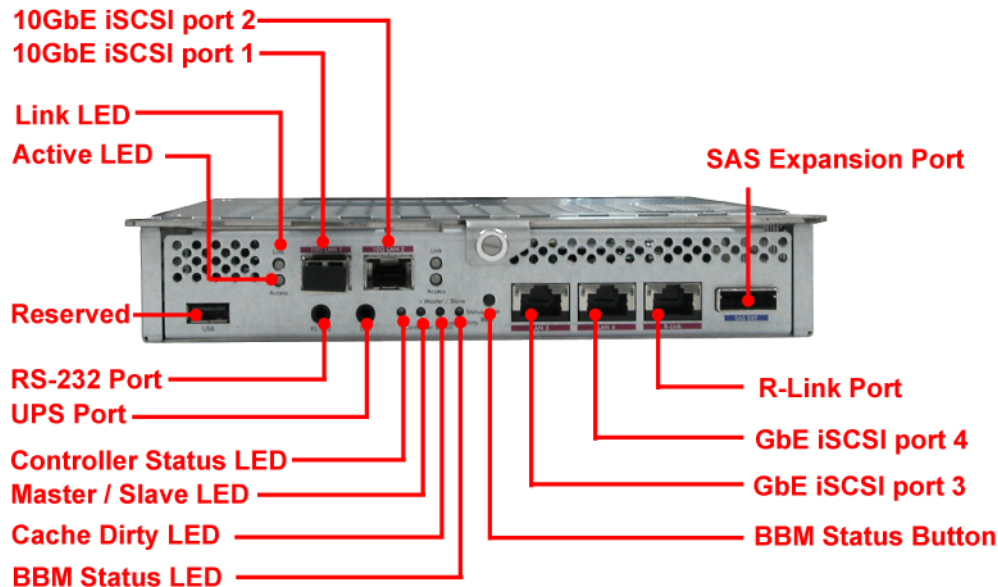
2. Power Supply Unit 1 ~ 2

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.

2.2 Controller Module

The RAID system includes single/dual iSCSI-to-6Gb SAS/SATA RAID Controller Module.



1. 10GbE iSCSI Ports (10 Gigabit)

Each controller is equipped with two 10GbE LAN data ports (LAN1 and LAN2) 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. BBM Status Button (Used to check the battery when the power is off.)

When the system shut down abnormally, 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.

9. GbE iSCSI Ports (Gigabit)

Each controller is equipped with two LAN data ports (LAN3, and LAN4) for iSCSI connection.

10.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.

11.SAS Expansion Ports

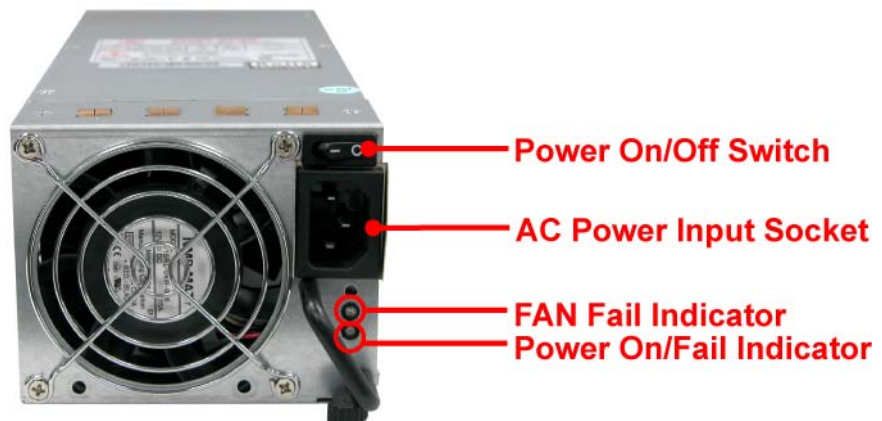
Use for expansion; connect to the SAS In Port of a JBOD subsystem.

2.3 Power Supply / Fan Module (PSFM)

The RAID subsystem contains **two 460W Power Supply / Fan Modules**. All the Power Supply / Fan Modules (PSFM) 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.

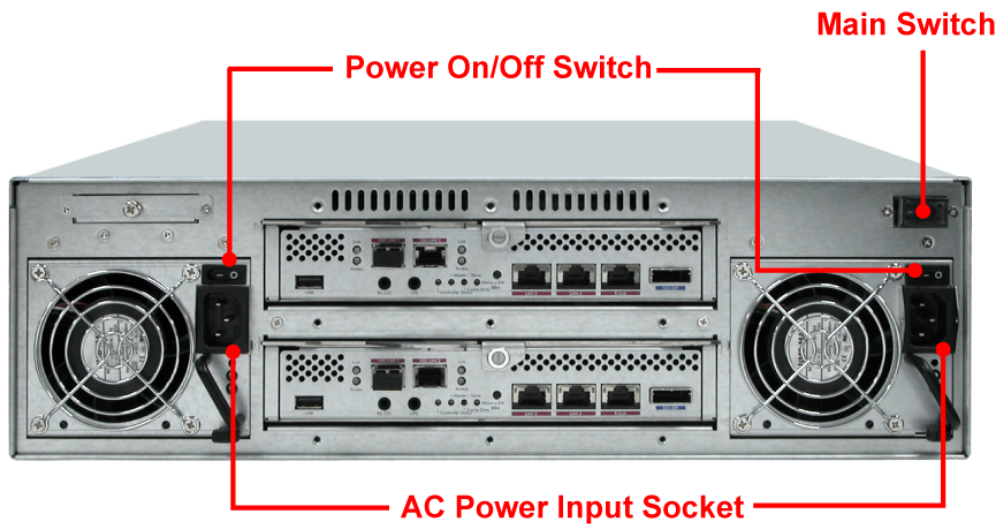


NOTE: After replacing the Power Supply Fan Module and turning on the Power On/Off Switch of the PSFM, the Power Supply will not power on immediately. The Fans in the PSFM will spin-up until the RPM becomes stable. When Fan RPM is already stable, the RAID controller will then power on the Power Supply. 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.

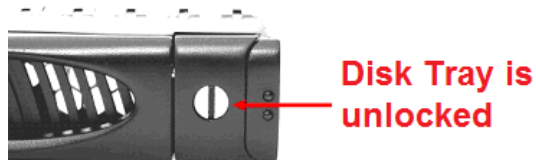
2. Turn on each Power On/Off Switch.
3. Turn on the main switch to power on the subsystem.
4. The Power LED on the front Panel will turn green.

3.2 Disk Drive Installation

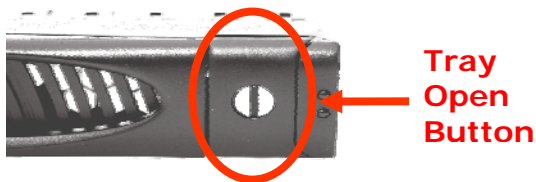
This section describes the physical locations of the hard drives supported by the subsystem and give instructions on installing a hard drive. The subsystem supports hot-swapping allowing you to install or replace a hard drive while the subsystem is running.

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.



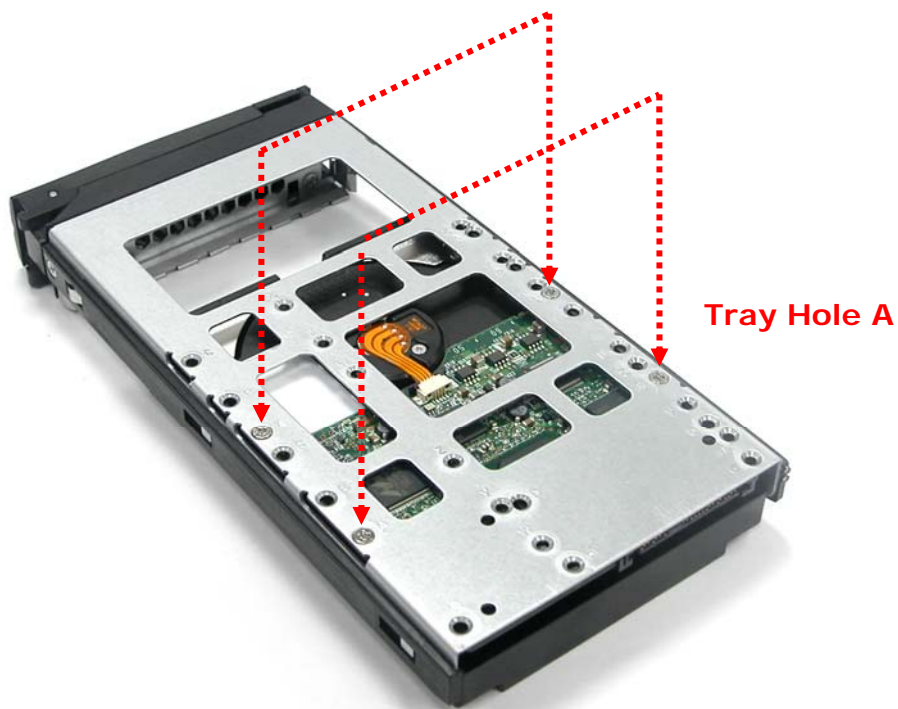
2. Press the Tray Open button and the Disk Tray handle will flip open.



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.



NOTE: All the disk tray holes are labelled accordingly.

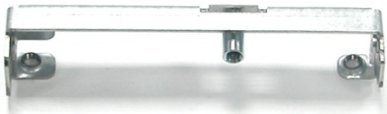


5. Slide the tray into a slot.
6. Press the lever in until you hear the latch click into place. The HDD Fault LED will turn green when the subsystem is powered on and HDD is good.
7. If necessary, lock the Disk Tray by turning the Lock Groove.

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

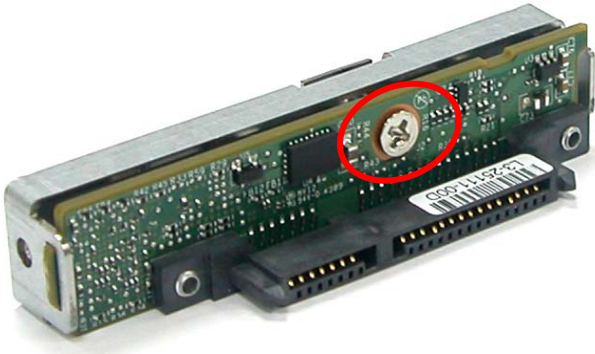
1. Remove an empty disk tray from the subsystem.



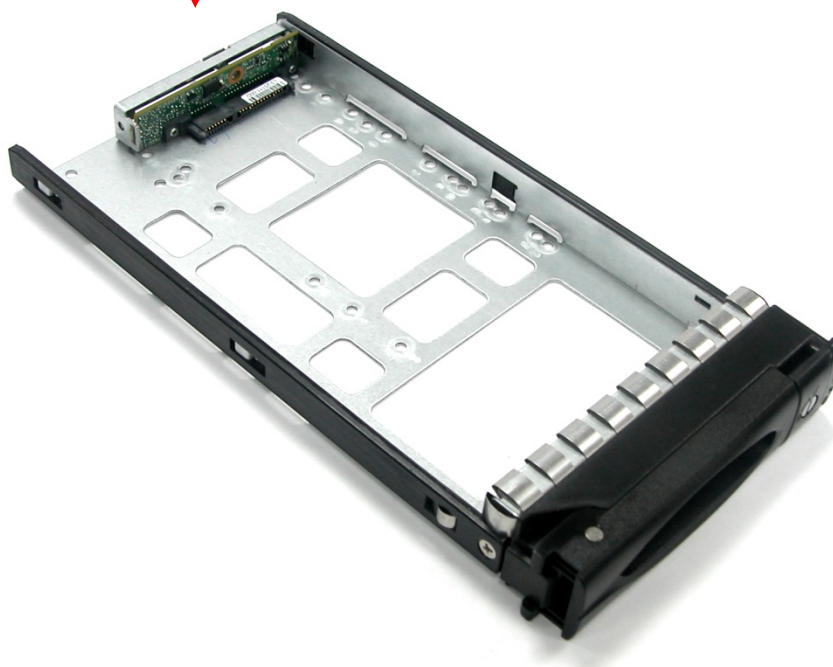
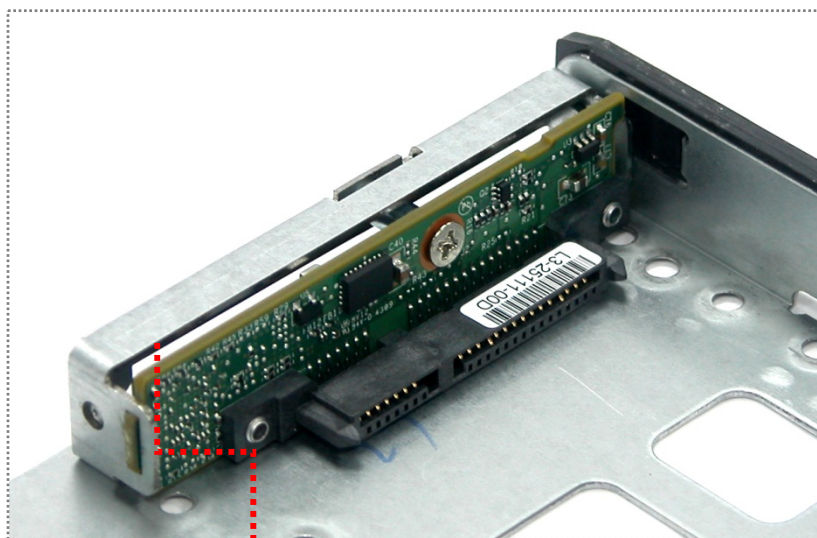
2. Prepare the dongle board, the Fixed Bracket, and screws.

	Fixed Bracket
	Dongle Board
	Screws

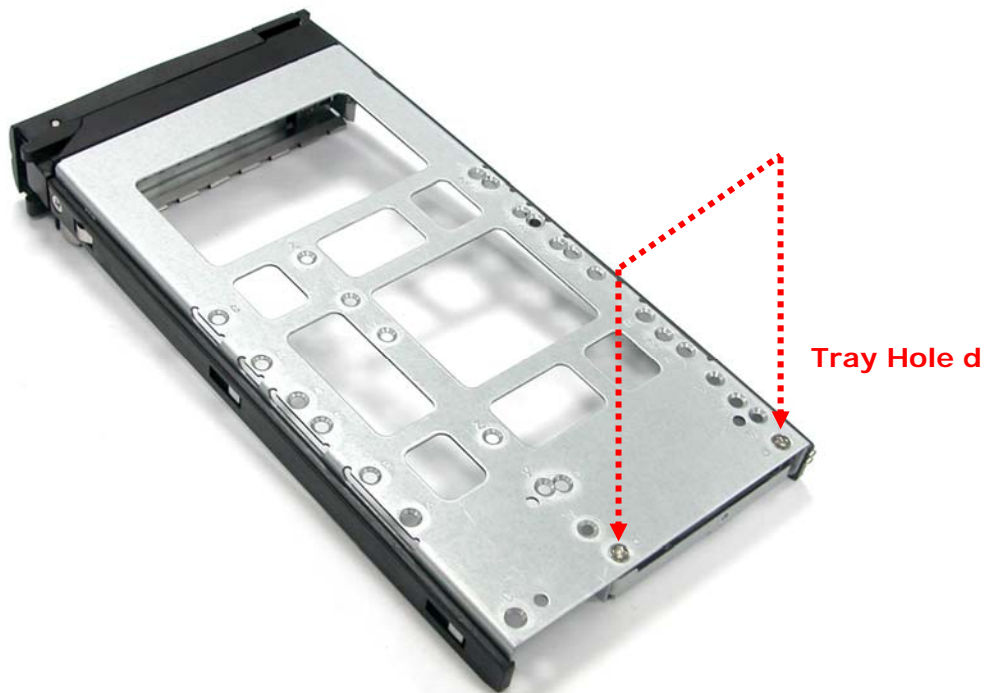
3. Attach the dongle board in the Fixed Bracket with a screw.



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.

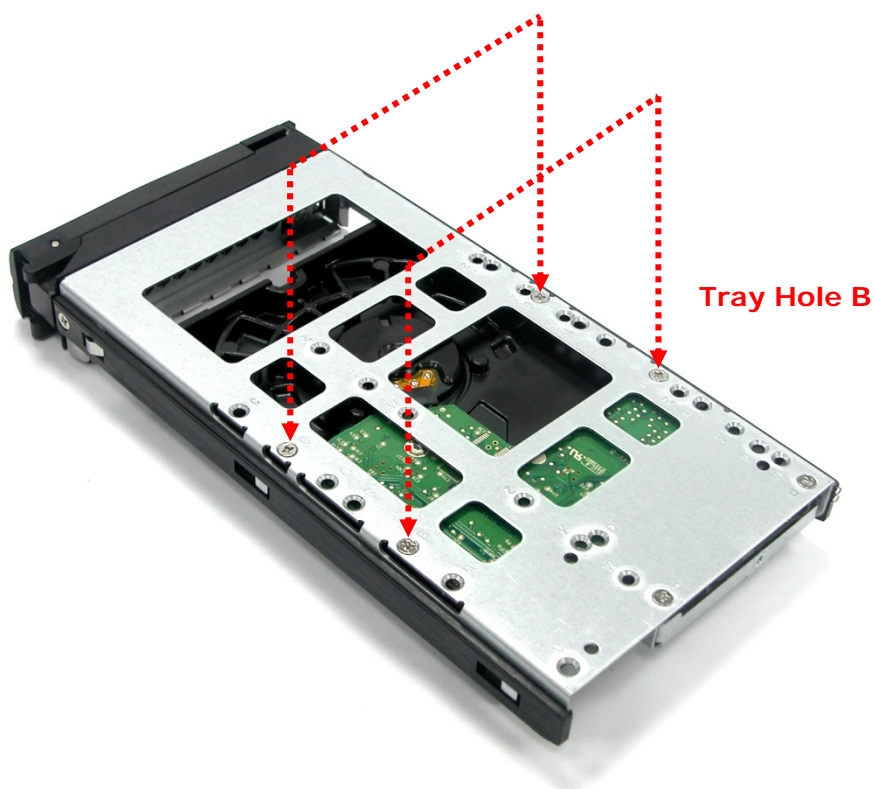


NOTE: All the disk tray holes are labelled accordingly.

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.



NOTE: All the disk tray holes are labelled accordingly.

8. Insert the disk tray into the subsystem.

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.

WARNING or ERROR events displayed on the LCM are automatically filtered by the LCM default filter. The filter setting can be changed in the Web UI under System Configuration -> Log and Alert Settings.

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▼]		
		[BOOTP]	[▲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▼]	

	[Enc. Management]	Phy. Disk Temp.	Local Slot <n>: <nn> (C)		
		Cooling	Local FAN<n>: <nnnn> RPM		
		Power Supply	Local PSU<n>: <status>		
	[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

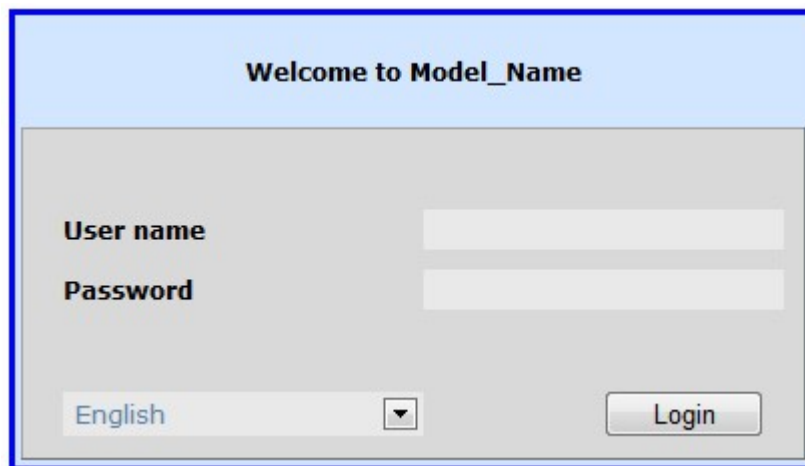
The RAID subsystem supports graphical user interface (GUI) to operate the system. Be sure to connect the LAN cable. The default IP setting is **DHCP**; open the browser and enter:

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.



Note: The Host Port Configuration menu bar option is only visible when the controller has multiple interfaces. The iSCSI Configuration menu bar option is only visible when the controller has iSCSI ports.

There are up to seven indicators and three icons at the top-right corner. The last indicator (Dual controller) is only visible when two controllers are installed.



	<p>RAID light:</p> <ul style="list-style-type: none"> ● Green → RAID works well. ● Red → RAID fails.
	<p>Temperature light:</p> <ul style="list-style-type: none"> ● Green → Temperature is normal. ● Red → Temperature is abnormal.
	<p>Voltage light:</p> <ul style="list-style-type: none"> ● Green → voltage is normal. ● Red → voltage is abnormal.
	<p>UPS light:</p> <ul style="list-style-type: none"> ● Green → UPS works well. ● Red → UPS fails.
	<p>Fan light:</p> <ul style="list-style-type: none"> ● Green → Fan works well. ● Red → Fan fails.
	<p>Power light:</p> <ul style="list-style-type: none"> ● Green → Power works well. ● Red → Power fails.
	<p>Dual controller light:</p> <ul style="list-style-type: none"> ● 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

To help users get started quickly, two guided configuration tools are available in the Web UI and LCM. Quick Installation guides you a easy way to create a volume. Volume Creation Wizard provides a smarter policy to help users to create a volume. If you are an advanced user, you can skip these steps.

4.2.1 Quick Installation

This tool guides you through the process of setting up basic array information, configuring network settings, and the creation of a volume on the storage system. Please make sure that it has some free hard drives installed in the system. SAS drivers are recommended.

Physical Disks

RAID Groups

Virtual Disks

Snapshots

Logical Units

QReplicas

Show disk for: Local Show disk size in: GB

	Slot	Size (GB)	RAID Group	RAID Set	Status	Health	Usage	Vendor	Serial Number	Rate	Write Cache	Standby	Read-Ahead	Command Queuing
	1	1862		N/A	Online	Good	Free	WDC	WD-WCAVY4158095	SATA 6.0Gb/s	Disabled	Disabled	Enabled	Enabled
	2	1862		N/A	Online	Good	Free	WDC	WD-WCAVY3924333	SATA 6.0Gb/s	Disabled	Disabled	Enabled	Enabled
	3	1862		N/A	Online	Good	Free	WDC	WD-WCAVY4118479	SATA 6.0Gb/s	Disabled	Disabled	Enabled	Enabled

Disk Health Check

Disk Check Report

1. Click **Quick Installation** from the menu bar.
2. Enter a **System Name** and set up the **Date and Time**. Click **Next** button to proceed.

Quick Installation

Step 1: System Settings

System Name

System Name:

Date and Time

☒ Change Date and Time

Current Time:

2014/1/17 10:41:5

Time Zone:

(GMT+08:00) Taipei

☒ Setup Date and Time Manually

Date:

2014 / 1 / 17

Time:

10 : 39 : 50

☐ NTP

Server:

Next >>

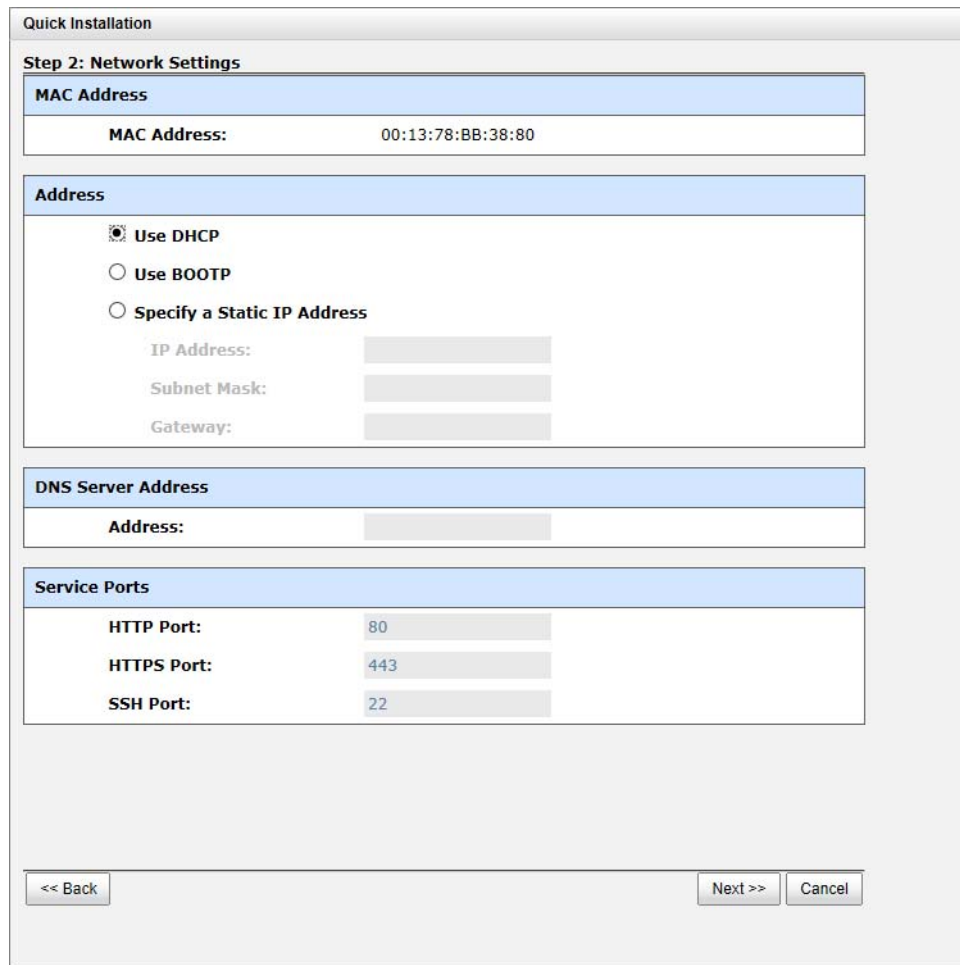
Cancel

rocstor®

User Manual

39

3. Confirm or change the management port IP address and DNS server. If you don't want to use the default DHCP setting, choose either BOOTP or specify a Static IP address. If the default HTTP, HTTPS, and SSH port numbers are not allowed on your network, they can be changed here as well.



The image shows a 'Quick Installation' window titled 'Step 2: Network Settings'. It contains several sections for configuring network parameters:

- MAC Address:** A section with a label 'MAC Address:' and a text field containing '00:13:78:BB:38:80'.
- Address:** A section with three radio buttons: 'Use DHCP' (selected), 'Use BOOTP', and 'Specify a Static IP Address'. Below these are three text fields for 'IP Address:', 'Subnet Mask:', and 'Gateway:'.
- DNS Server Address:** A section with a label 'Address:' and a text field.
- Service Ports:** A section with three rows: 'HTTP Port:' with value '80', 'HTTPS Port:' with value '443', and 'SSH Port:' with value '22'.

At the bottom of the window are three buttons: '<< Back', 'Next >>', and 'Cancel'.

4. For iSCSI Configurations, use this step to set up the data port iSCSI IP address, and then click **Next** button.

Quick Installation

Step 3: iSCSI IP Address Settings

LAN1:

☐ Use DHCP

☒ Specify a Static IP Address

Address: 10.0.0.1

Mask: 255.255.255.0

Gateway: 10.0.0.254

<< Back Next >> Cancel

5. Choose a **RAID Level**. The number in the brackets is the maximum capacity at the RAID level. This step utilizes all drives in the storage system as well as any JBOD expansion arrays present. This option allows the selection of the RAID type and the number of drives in each array.

Quick Installation

Step 4: Volume Settings

Enclosure: Local

RAID Level:

- RAID 0 (5588 GB) -
- RAID 1 (1862 GB) -
- RAID 3 (3725 GB) -
- RAID 5 (3725 GB) -

<< Back Next >> Cancel

6. Verify all items, and then click **Finish** button to complete the quick installation.

The image shows a 'Quick Installation' window with a 'Confirm' tab. It displays various system settings organized into sections: General, Date and Time, Network Settings, iSCSI IP Address Settings, and Volume Settings. At the bottom, there are three buttons: '<< Back', 'Finish', and 'Cancel'.

Confirm	
General	
System Name:	
Date and Time	
Time zone:	(GMT+08:00) Taipei
Date:	2014/1/17
Time:	10:39:50
Network Settings	
Address:	Using-DHCP
HTTP Port:	80
HTTPS Port:	443
SSH Port:	22
DNS Server Address:	
iSCSI IP Address Settings	
Address:	10.0.0.1
Mask:	255.255.255.0
Gateway:	10.0.0.254
Volume Settings	
RAID Level:	RAID 0 on Local enclosure
RAID Size:	5588

<< Back Finish Cancel

The iSCSI information is only displayed when iSCSI controllers are used. Use **Back** button to return to a previous page to change any setting.

4.2.2 Volume Creation Wizard

The **Volume Creation Wizard** provides a smarter policy to determine all possibilities and volume sizes in the different RAID levels that can be created using the existing free drives. It provides:

- Biggest capacity of RAID level for user to choose.
- The fewest disk number for RAID level / volume size.

This way, after choosing RAID level, you may find that some drives are still available (free status). This phenomenon is the result of using smart design. Take an example, user chooses the RAID 5 level and the system has 12*200GB + 4*80GB free drives inserted. Generally, if using all 16 drives for a RAID 5 group, the maximum size of volume is $(16-1)*80\text{GB} = 1200\text{GB}$. This wizard provides a smarter check and searches the most efficient way of using free drives. It uses 200GB drives only to provide $(12-1)*200\text{GB} = 2200\text{GB}$ capacity, the volume size is larger and less drives.

1. Click **Volume Creation Wizard** from the menu bar.
2. Choose a **RAID Level**. The number in the brackets is the maximum capacity at the RAID level.

Volume Creation Wizard

Step 1
The dropdown list below contains the levels and the amount of storage that will be available using that RAID method.
Please select the option that best suits your storage needs.

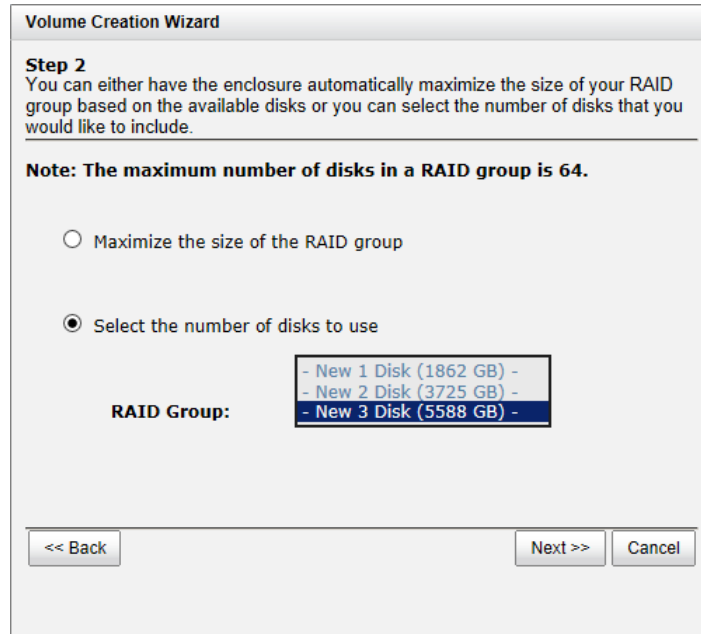
Enclosure: Local

RAID Level:

- RAID 0 (5588 GB) -
- RAID 1 (1862 GB) -
- RAID 3 (3725 GB) -
- RAID 5 (3725 GB) -

Next >> Cancel

3. Select the default option **Maximize the size of the RAID group** or manual option **Select the number of disks to use**. From the drop-down list, select either the RAID Group capacity combination desired. Click **Next** button to proceed.



Volume Creation Wizard

Step 2
You can either have the enclosure automatically maximize the size of your RAID group based on the available disks or you can select the number of disks that you would like to include.

Note: The maximum number of disks in a RAID group is 64.

☐ Maximize the size of the RAID group

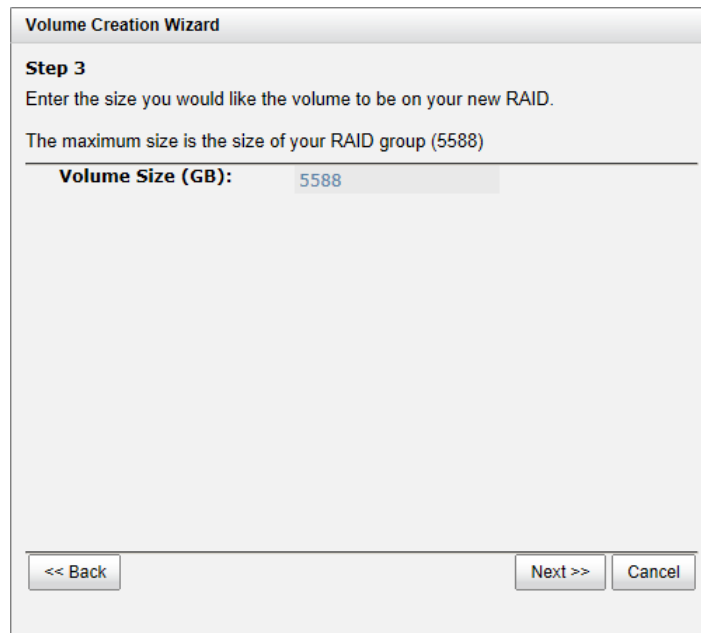
☒ Select the number of disks to use

RAID Group:

- New 1 Disk (1862 GB) -
- New 2 Disk (3725 GB) -
- New 3 Disk (5588 GB) -

<< Back Next >> Cancel

4. Enter the **Volume Size (GB)** desired that is less than or equal to the default available size shown. Then click **Next** button.



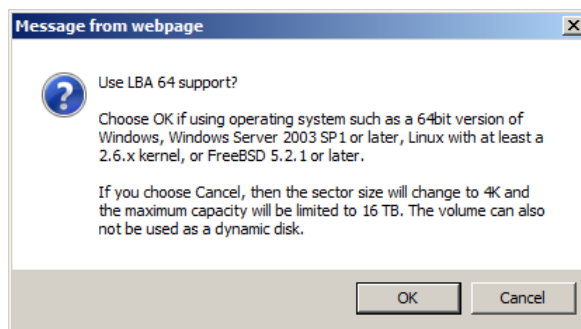
Volume Creation Wizard

Step 3
Enter the size you would like the volume to be on your new RAID.
The maximum size is the size of your RAID group (5588)

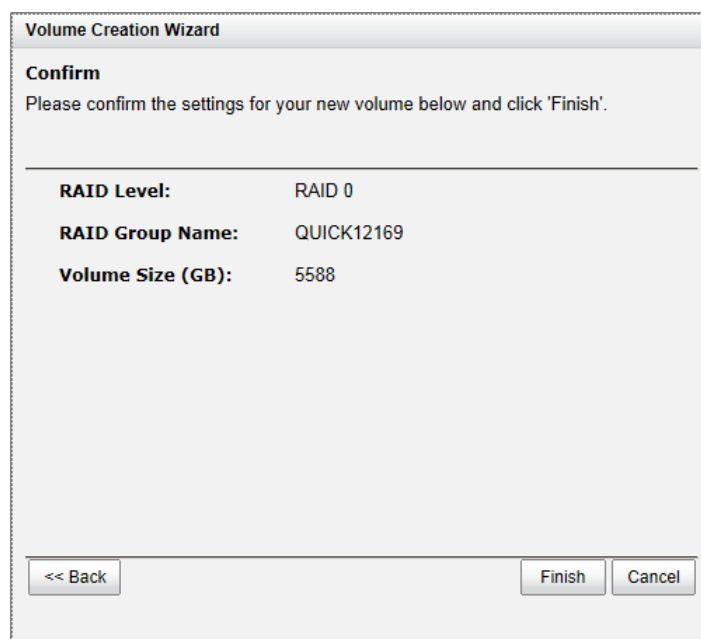
Volume Size (GB): 5588

<< Back Next >> Cancel

5. Use LBA 64 support? It depends on the operation system.



6. Finally, verify the selections and click **Finish** button if they are correct.



The volume is created and named by the system automatically. It is now available to use.

Chapter 5 Configuration

5.1 Web GUI Management Interface Hierarchy

The below table is the hierarchy of the management GUI.

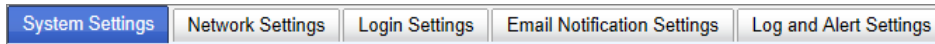
Menu Bar	L1	L2, Button or Menu
System Configuration	System Settings	System Name / Date and Time / System Indication
	Network Settings	MAC Address / IP Address / DNS Server Address / Service Ports
	Login Settings	Login Options / Admin Password / User Password
	Email Notification Settings	Email Settings / Send Test Mail
	Log and Alert Settings	SNMP Trap Settings / Windows Messenger / Syslog Server Settings / Admin Interface and Front Display Alerts / Device Buzzer
iSCSI Configuration (This option is only visible when the controller has iSCSI ports.)	Network Setup	Show information for: < Controller 1 Controller 2 > Options: [iSCSI Bonding Settings Delete iSCSI Bonding] / Set VLAN ID / iSCSI IP Address Settings / Make Default Gateway / [Enable Disable] Jumbo Frames / Ping Host / Reset Port
	Entity and iSNS Settings	Entity Name / iSNS IP Address
	iSCSI Node	Show information for: < Controller 1 Controller 2 > Options: Authentication Method / Change Portal / Rename Alias / Users
Host Configuration (This option is only visible when the controller has multiple interfaces.)	Active Sessions	Show information for: < Controller 1 Controller 2 > Connection Details / Disconnect
	CHAP Accounts	Create User Options: Modify User Information / Delete User
	Fibre Channel (This option is only visible when the controller has FC ports.)	Show information for: < Controller 1 Controller 2 > Options: Change Link speed / Change Connection Mode / Node Configuration / Clear Counters
Volume	Physical Disks	Show disk for: < -Local- -JBODn- >

Configuration		Show disk size in: < (GB) (MB) > Disk Health Check / Disk Check Report Options: Set Free Disk / Set Global Spare / Set Local Spare / Set Dedicated Spare / Upgrade / Disk Scrub / Read Error Cleared / Turn [on off] the Indication LED / More information
	RAID Groups	Show RAID size in: < (GB) (MB) > Create Options: Migrate RAID Level / Move RAID Level / Activate / Deactivate / Verify Parity / Delete / Change Preferred Controller / Change RAID Options / Add RAID Set / Add Policy / More information RAID Set options: Remove / Move RAID Level / List Disks RAID Group Policy options: Delete / Modify
	Virtual Disks	Create / Cloning Options Options: Extend / Verify Parity / Delete / Set Properties / Space Reclamation / Attach LUN / Detach LUNs / List LUNs / Set Clone / Set Snapshot Space / Cleanup Snapshots / Take a Snapshot / Scheduled Snapshots / List Snapshots / More information
	Snapshots	Set Snapshot Space / Scheduled Snapshots / Take a Snapshot / Cleanup Snapshots Options: Set Quota / Rollback / Delete
	Logical Units	Attach LUN Options: Detach LUN
	QReplicas	Create / Rebuild / QReplica Options / Shaping Setting Configuration Options: Start / Stop / Set Task Shaping / Add Path / Delete Path / Schedule / Delete / Add Connection / Delete Connection
	Hardware Monitor	Show information for: < -Local- -JBODn- > Temperature (Internal)/(Case): < (C) / (F) > Controller 1 Monitors / Controller 2 Monitors / Backplane Options: Auto Shutdown
Enclosure Management	UPS	UPS Type / Shutdown Battery Level (%) / Shutdown Delay (Seconds) / Shutdown UPS / UPS Status / UPS Battery Level
	SES	[Enable Disable]
	S.M.A.R.T.	Show information for: < -Local- -JBODn- >

Temperature (Internal)/(Case): < (C) / (F) >		
System Maintenance	System information	Download System Information
	Event log	Event Log Level to Show: < Information Warning Error > Download / Mute Buzzer / Clear
	Upgrade	Controller Module Firmware Update / JBOD Firmware Update / Controller Mode
	Firmware Synchronization	Apply (This option is only visible when dual controllers are inserted.)
	Reset to Factory Default	Reset
	Configuration Backup	Import or Export / Import File
	Volume Restoration	Options: Restore
	Reboot and Shutdown	Reboot / Shutdown Reboot options: Both Controller 1 and Controller 2 / Controller 1 / Controller 2
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

The **System Configuration** menu option is for accessing the **System Settings**, **Network Settings**, **Login Settings**, **Email Notification Settings** and **Log and Alert Settings** option tabs.



5.2.1 System Setting

The **System Settings** tab is used to setup the system name and date. The default system name is composed of the model name and the serial number of this system.

Change General System Settings
On this screen you can change the name of the device, set the current date and time manually or automatically using an NTP (Network Time Protocol) server, and identify the device by flashing an indicator.

System Name

System Name:

Date and Time

☐ **Change Date and Time**

Current Time:

Time Zone:

☒ **Setup Date and Time Manually**

Date: / /

Time: : :

☒ **NTP**

Server:

The options are available on this tab:

- **System Name:** Change the System Name, highlight the old name and type in a new one.
- **Date and Time:** Change the current date, time and time zone settings, check **Change Date and Time**. The changes can be done manually or synchronized from an NTP (Network Time Protocol) server.

When it is done, click **Apply** button.

5.2.2 Network Setting

The **Network Settings** tab is used to view the MAC address and change basic network settings.

Change Network Settings
 On this screen change the network settings for the administration port.

☐ **Enable dual management ports**

MAC Address

MAC Address:	00:13:78:BB:38:80
---------------------	-------------------

IP Address

☐ Use DHCP
☐ Use BOOTP
☒ **Specify a Static IP Address**

IP Address:	192.168.1.234
Subnet Mask:	255.255.0.0
Gateway:	192.168.1.254

DNS Server Address

Address:	8.8.8.8
-----------------	---------

Service Ports

HTTP Port:	80
HTTPS Port:	443
SSH Port:	22

The options are available on this tab:

- **Enable dual management ports:** This is for dual controller models. Check it to enable dual management ports.
- **MAC Address:** Display the MAC address of the management port in the system.
- **IP Address:** The option can change IP address for remote administration usage. There are three options: DHCP, BOOTP and Specify a Static IP Address. The default setting is DHCP.
- **DNS Server Address:** If necessary, the IP address of DNS server can be entered or changed here.
- **Service Ports:** If the default port numbers of HTTP, HTTPS and SSH are not allowed on the network, they can be changed here.

When it is done, click Apply button.

5.2.3 Login Setting

The **Login Settings** tab is used to control access to the storage system. For the security reason, set the auto logout option or set the limit access of one administrator at a time. The other options can change the Admin and User passwords.

Change Login Options and Passwords
 When the auto logout option is enabled, you will be logged out of the admin interface after the time specified.
 The login lock option prevents multiple people from administering the storage server at the same time.

Login Options

Auto Logout:	- Disable -	▼
Login Lock:	- Disable -	
	- Enable -	

Admin Password
☐ **Change Admin Password**

Current Password:	
New Password:	
Re-type New Password:	

User Password
☐ **Change User Password**

New Password:	
Re-type New Password:	

Apply

The options are available on this tab:

- **Auto Logout:** When the auto logout option is enabled, you will be logged out of the admin interface after the time specified. There are Disable (default), 5 minutes, 30 minutes and 1 hour options.
- **Login Lock:** When the login lock is enabled, the system allows only one user to login to the web UI at a time. There are Disable (default) and Enable options.
- **Change Admin Password:** Check it to change administrator password. The maximum length of password is 12 alphanumeric characters.
- **Change User Password:** Check it to change user password. The maximum length of password is 12 alphanumeric characters.

When it is done, click Apply button.

5.2.4 Email Notification Settings

The Email Notification Settings tab is used to enter up to three email addresses for receiving the event notifications. Fill in the necessary fields and click Send Test Email button to test whether it is available. Some email servers will check the mail-from address and need the SMTP relay settings for authentication.



Note: Please make sure the DNS server IP is well-setup in System Configuration -> Network Settings. So the event notification emails can be sent successfully.

You can also select which levels of event logs which you would like to receive. The default setting only includes **Warning** and **Error** event logs.

Configure Email Notification Settings
 You can specify up to three email addresses for email notifications. You should use the SMTP server option to specify a specific email server that you would like to use for sending email notifications (required if your network will not allow this device to send the email directly).
 After the information is set, you can click 'Send test mail' to test whether email functions are available.

Email Settings	
From Email Address:	mailman@QsanTechnology.com
To Email Address #1:	
Alert Levels To Send1:	<input type="checkbox"/> Information <input checked="" type="checkbox"/> Warning <input checked="" type="checkbox"/> Error
To Email Address #2:	
Alert Levels To Send2:	<input type="checkbox"/> Information <input checked="" type="checkbox"/> Warning <input checked="" type="checkbox"/> Error
To Email Address #3:	
Alert Levels To Send3:	<input type="checkbox"/> Information <input checked="" type="checkbox"/> Warning <input checked="" type="checkbox"/> Error
<input type="checkbox"/> Specify a SMTP Server ▾	
SMTP Server Address:	
Use Authentication:	No ▾
User Name:	
Password:	
Re-type Password:	
Send Test Email	

Apply

When it is done, click **Apply** button.

5.2.5 Log and Alert Settings

The **Log and Alert Settings** tab is used to setup SNMP traps (for alerting via SNMP), pop-up messages via Windows messenger (not MSN or Skype), alerts via the syslog protocol, the pop-up alerts and alerts on the front display. The device buzzer is also managed here.

SNMP Trap Settings ▾	
Host Address #1:	<input type="text"/>
Host Address #2:	<input type="text"/>
Host Address #3:	<input type="text"/>
Community:	<input type="text" value="public"/>
SNMP MIB File Download:	<input type="button" value="Download"/>
Alert Levels To Send:	<input checked="" type="checkbox"/> Information <input checked="" type="checkbox"/> Warning <input checked="" type="checkbox"/> Error
Windows Messenger ▾	
Host Address #1:	<input type="text"/>
Host Address #2:	<input type="text"/>
Host Address #3:	<input type="text"/>
Alert Levels To Send:	<input type="checkbox"/> Information <input checked="" type="checkbox"/> Warning <input checked="" type="checkbox"/> Error
Syslog Server Settings ▾	
Host Address or Name:	<input type="text"/>
UDP Port:	<input type="text" value="514"/>
Facility:	<input type="text" value="User"/> ▾
Alert Levels To Log:	<input type="checkbox"/> Information <input checked="" type="checkbox"/> Warning <input checked="" type="checkbox"/> Error
Admin Interface and Front Display Alerts ▾	
Admin Interface Popup Alerts:	<input type="checkbox"/> Information <input type="checkbox"/> Warning <input type="checkbox"/> Error
Alerts to Show on Front Display:	<input type="checkbox"/> Information <input checked="" type="checkbox"/> Warning <input checked="" type="checkbox"/> Error
Device Buzzer ▾	
Disable the Device Buzzer:	<input type="checkbox"/>
<input type="button" value="Apply"/>	

The options are available on this tab:

- SNMP Trap Settings:** It allows up to three SNMP trap addresses. The default community setting is public. You can check the alert levels which you would like to receive. The default setting only includes Warning and Error event logs. If necessary, click Download to get the MIB file for importing to the SNMP client tool. There are many SNMP tools available on the internet.
 SNMPc: <http://www.snmpc.com/>
 Net-SNMP: <http://net-snmp.sourceforge.net/>
- Windows Messenger:** You must enable the Messenger service in Windows (Start -> Control Panel -> Administrative Tools -> Services -> Messenger). It allows up to three host addresses. The same, you can check the alert levels which you would like to receive.

- **System Server Settings:** Fill in the host address and the facility for syslog service. The default UDP port is 514. You can also check the alert levels here.
There are some syslog server tools available on the internet for Windows.
WinSyslog: <http://www.winsyslog.com/>
Kiwi Syslog Daemon: <http://www.kiwisyslog.com/>
Most UNIX systems build in syslog daemon.
- **Admin Interface and Front Display Alerts:** You can check the alert levels which you would like to have pop-up message in the Web UI and show on front display. The default setting for admin interface is none while the default setting for shown on the front display includes Warning and Error event logs.
- **Device Buzzer:** Check it to disable the device buzzer. Uncheck it to activate the device buzzer.

When it is done, click Apply button.

5.3 Host Port / iSCSI Configuration

The **Host port / iSCSI Configuration** menu option is for accessing the **Network Setup, Entity and iSNS Settings, iSCSI Nodes, Active Sessions, CHAP Account and Fibre Channel** (This option is only visible when the controller has Fibre Channel ports) option tabs.



5.3.1 Network Setup

These network ports must be assigned IP addresses then they can be used. For better performance or fault tolerance reason, they can be bonding as Trunking or LACP. These bonding network ports share a single IP address. The following example shows the 1 GB series (6 x GbE iSCSI ports).

Show information for: **Controller 1**

	Name	LAG	LAG No	VLAN ID	Use DHCP	IP Address	Netmask	Gateway	Jumbo Frames	MAC Address	Link
▼	LAN1	No	N/A	N/A	No	10.0.0.1	255.255.255.0	10.0.0.254	Disabled	00:13:78:bb:38:82	1 Gbps
▼	LAN2	No	N/A	N/A	No	10.0.0.2	255.255.255.0	10.0.0.254	Disabled	00:13:78:bb:38:83	Down
▼	LAN3	No	N/A	N/A	No	10.0.0.3	255.255.255.0	10.0.0.254	Disabled	00:13:78:bb:38:84	Down
▼	LAN4	No	N/A	N/A	No	10.0.0.4	255.255.255.0	10.0.0.254	Disabled	00:13:78:bb:38:85	Down
▼	LAN5	No	N/A	N/A	No	10.0.0.5	255.255.255.0	10.0.0.254	Disabled	00:13:78:bb:38:86	Down
▼	LAN6	No	N/A	N/A	No	10.0.0.6	255.255.255.0	10.0.0.254	Disabled	00:13:78:bb:38:87	Down

iSCSI Bonding Settings
 Set VLAN ID
 iSCSI IP Address Settings
 Make Default Gateway
 Enable Jumbo Frames
 Ping Host
 Reset Port

This figure shows six iSCSI data ports. These data ports are set up with a static IP address. For the other controllers, that can be set up the same way.

The options are available on this tab:

- ▼ **iSCSI Bonding Settings:** The default mode of each iSCSI data port is individually connected without any bonding. Trunking and LACP (Link Aggregation Control Protocol) settings can be setup here. At least two iSCSI data ports must be checked for iSCSI bonding.

Network Bonding Settings

Select the network interfaces that you would like to bond together.

Bonding Method: ☒ Trunking ☐ LACP

IP Address: 10.0.0.1

Subnet Mask: 255.255.255.0

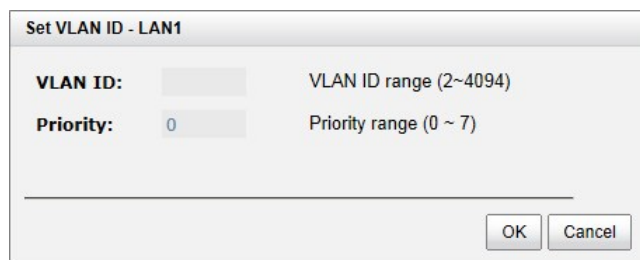
Gateway: 10.0.0.254

Network Setup: ☒ LAN1 ☒ LAN2 ☐ LAN3 ☐ LAN4 ☐ LAN5 ☐ LAN6

OK Cancel

- ◆ **Trunking:** Configures multiple iSCSI ports to be grouped together into one in order to increase the connection speed beyond the limit of a single iSCSI port.

- ◆ **LACP:** The Link Aggregation Control Protocol is part of IEEE specification 802.3ad that allows bonding 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 that it increases bandwidth usage and it automatically performs a failover when the link status fails on a port.
- ▼ **Set VLAN ID:** VLAN is a logical grouping mechanism implemented on switch device. VLANs are collections of switching ports that comprise a single broadcast domain. It allows network traffic to flow more efficiently within these logical subgroups. Please consult your network switch user manual for VLAN setting instructions. Most of the work is done at the switch part. All you need to do is to make sure that your iSCSI port's VLAN ID matches that of switch port. If your network environment supports VLAN, you can use this function to change the configurations. Fill in VLAN ID and Priority settings to enable VLAN.



The dialog box titled "Set VLAN ID - LAN1" contains two input fields. The first is labeled "VLAN ID:" with a text box next to it, and to its right is the text "VLAN ID range (2~4094)". The second is labeled "Priority:" with a text box containing the value "0", and to its right is the text "Priority range (0 ~ 7)". At the bottom right of the dialog are "OK" and "Cancel" buttons.

- ◆ **VLAN ID:** VLAN ID is a 12-bit number. Its range is from 2 to 4094, while 0, 1, and 4095 are reserved for special purposes.
- ◆ **Priority:** The PCP (Priority Code Point) is a 3-bit number and reserved for QoS. The definition complies with IEEE 802.1p protocol, ranging from 0 to 7, with 0 as the default value. In normal cases, you don't need to set this value. Using the default will do just fine.



NOTE: If iSCSI ports are assigned with VLAN ID before creating aggregation takes place, aggregation will remove VLAN ID. You need to repeat the steps to set VLAN ID for the aggregation group.

- ▼ **iSCSI IP Address Settings:** It can assign an iSCSI IP address of the iSCSI data port. There are two options: **Use DHCP** to acquire an IP address automatically or **Specify a Static IP Address** to set the IP address manually.



The dialog box titled "iSCSI IP Address Settings" contains a message: "You can select 'DHCP' to acquire an IP address automatically or select 'Static' to specify an IP address manually." Below this are two radio buttons. The first is labeled "Use DHCP" and is unselected. The second is labeled "Specify a Static IP Address" and is selected. Below the radio buttons are three text fields: "IP Address:" with the value "10.0.0.1", "Subnet Mask:" with the value "255.255.255.0", and "Gateway:" with the value "10.0.0.254". At the bottom right of the dialog are "OK" and "Cancel" buttons.

- **Make Default Gateway:** Set the gateway of the IP address as default gateway. There can be only one default gateway. To remove the default gateway, click ▼ **Remove Default Gateway**.
- **Enable jumbo frames:** It can enable the MTU (Maximum Transmission Unit) size. The maximum jumbo frame size is **3900** bytes. To disable jumbo frames, click ▼ **Disable Jumbo Frames**.

**CAUTION:**

VLAN ID, jumbo frames for both the switching hub and HBA on host must be enabled. Otherwise, the LAN connection cannot work properly.

- **Ping host:** It can verify the port connection from a target to the corresponding host data port. Input the host's IP address and click **Start** button. The system will display the ping result. Or click **Stop** button to stop the test.

Please input the host's IP address:

192.168.55.2 Start Stop

```

Reply from 192.168.55.2: time<1ms
Reply from 192.168.55.2: time<1ms
Reply from 192.168.55.2: time<1ms
Reply from 192.168.55.2: time<1ms
Reply from 192.168.55.2: time<1ms
Reply from 192.168.55.2: time<1ms
Reply from 192.168.55.2: time<1ms
Reply from 192.168.55.2: time<1ms
  
```

- **Reset Port:** If the behavior of the port is abnormal, try to reset port to make it normal.

5.3.2 Entity and iSCSI Settings

The **Entity and iSCSI Settings** tab is used to view the entity name of the system, and setup iSNS IP for the iSNS (Internet Storage Name Service) protocol. It allows automated discovery, management and configuration of iSCSI devices on a TCP/IP network. To use iSNS, an iSNS server needs to be added to the SAN. When this is done, the iSNS server IP address must be added to the storage system for iSCSI initiator service to send queries to it.

Entity Name and iSNS Configuration Information

The entity name is for a device or gateway that is accessible from the network. The iSNS protocol allows automated discovery, management, and configuration of iSCSI devices on a TCP/IP network.

Entity Name:	<input type="text"/>
iSNS IP Address:	<input type="text"/>

To make changes, enter the Entity Name and the iSNS IP Address, and then click Apply.

5.3.3 iSCSI Node

iSCSI Node can be used to view the target name for iSCSI initiator.

Show information for: Controller 1

<< first < prev **1** 2 3 4 5 6 7 8 9 10 next > last >>

	ID	Auth	Name	Portal	Alias
<input type="button" value="OP."/>	0	None	iqn:dev0.ctr1	192.168.1.1:3260, 192.168.3.1:3260, 192.168.4.1:3260, 192.168.5.1:3260, 192.168.6.1:3260	
<input type="button" value="OP."/>	1	None	iqn:dev1.ctr1	192.168.1.1:3260, 192.168.3.1:3260, 192.168.4.1:3260, 192.168.5.1:3260, 192.168.6.1:3260	
<input type="button" value="OP."/>	2	None	iqn:dev2.ctr1	192.168.1.1:3260, 192.168.3.1:3260, 192.168.4.1:3260, 192.168.5.1:3260, 192.168.6.1:3260	
<input type="button" value="OP."/>	3	None	iqn:dev3.ctr1	192.168.1.1:3260, 192.168.3.1:3260, 192.168.4.1:3260, 192.168.5.1:3260, 192.168.6.1:3260	
<input type="button" value="OP."/>	4	None	iqn:dev4.ctr1	192.168.1.1:3260, 192.168.3.1:3260, 192.168.4.1:3260, 192.168.5.1:3260, 192.168.6.1:3260	
<input type="button" value="OP."/>	5	None	iqn:dev5.ctr1	192.168.1.1:3260, 192.168.3.1:3260, 192.168.4.1:3260, 192.168.5.1:3260, 192.168.6.1:3260	
<input type="button" value="OP."/>	6	None	iqn:dev6.ctr1	192.168.1.1:3260, 192.168.3.1:3260, 192.168.4.1:3260, 192.168.5.1:3260, 192.168.6.1:3260	
<input type="button" value="OP."/>	7	None	iqn:dev7.ctr1	192.168.1.1:3260, 192.168.3.1:3260, 192.168.4.1:3260, 192.168.5.1:3260, 192.168.6.1:3260	
<input type="button" value="OP."/>	8	None	iqn:dev8.ctr1	192.168.1.1:3260, 192.168.3.1:3260, 192.168.4.1:3260, 192.168.5.1:3260, 192.168.6.1:3260	
<input type="button" value="OP."/>	9	None	iqn:dev9.ctr1	192.168.1.1:3260, 192.168.3.1:3260, 192.168.4.1:3260, 192.168.5.1:3260, 192.168.6.1:3260	
<input type="button" value="OP."/>	10	None	iqn:dev10.ctr1	192.168.1.1:3260, 192.168.3.1:3260, 192.168.4.1:3260, 192.168.5.1:3260, 192.168.6.1:3260	
<input type="button" value="OP."/>	11	None	iqn:dev11.ctr1	192.168.1.1:3260, 192.168.3.1:3260, 192.168.4.1:3260, 192.168.5.1:3260, 192.168.6.1:3260	

<< first < prev **1** 2 3 4 5 6 7 8 9 10 next > last >>

The options are available on this tab:

- **Authentication Method:** CHAP (Challenge Handshake Authentication Protocol) 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 transmit in an encrypted form for protection.



NOTE: A CHAP account must be added before you can use this authentication method. Please refer to CHAP Accounts session to create an account if none exists.

To use CHAP authentication, please follow the procedures.

- ◆ Select one of nodes from one controller.
- ◆ Click ▼ Authentication Method.
- ◆ Select CHAP from the drop-down list.

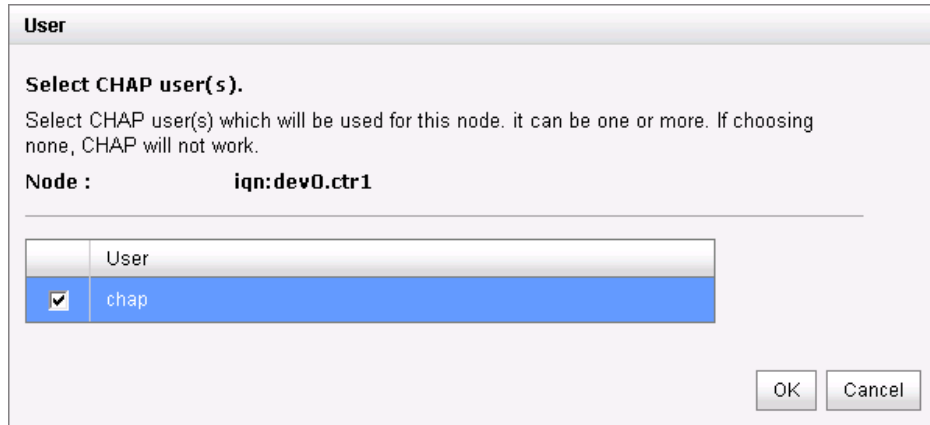
- ◆ Click **OK** button.

Show information for: Controller 1

<< first < prev 1 2 3 4 5 6 7 8 9 10 next > last >>

	ID	Auth	Name	Portal	Alias
OP.	0	CHAP	iqn:dev0.ctr1	192.168.1.1:3260, 192.168.3.1:3260, 192.168.4.1:3260, 192.168.5.1:3260, 192.168.6.1:3260	
OP.	1	None	iqn:dev1.ctr1	192.168.1.1:3260, 192.168.3.1:3260, 192.168.4.1:3260, 192.168.5.1:3260, 192.168.6.1:3260	
OP.	2	None	iqn:dev2.ctr1	192.168.1.1:3260, 192.168.3.1:3260, 192.168.4.1:3260, 192.168.5.1:3260, 192.168.6.1:3260	
OP.	3	None	iqn:dev3.ctr1	192.168.1.1:3260, 192.168.3.1:3260, 192.168.4.1:3260, 192.168.5.1:3260, 192.168.6.1:3260	

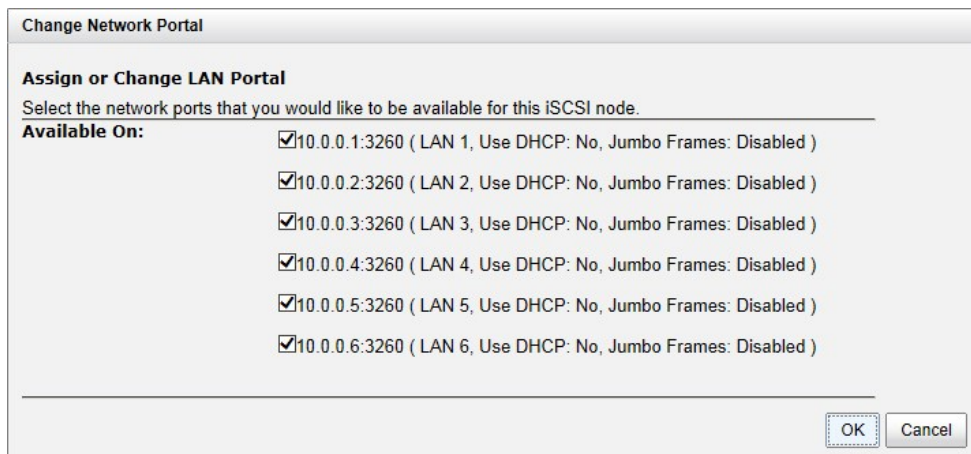
- ◆ Click ▼ User.
- ◆ Select CHAP user(s) which will be used. It can be more than one, but it must be at least one CHAP to enable on the node.



- ◆ Click OK button.

To disable CHAP authentication, please follow the procedures.

- ◆ Select the node which wants to disable CHAP.
 - ◆ Click ▼ Authentication Method.
 - ◆ Change it to None from the drop-down list.
 - ◆ Click OK button
- **Change Portal:** Use this iSCSI node option to change the network ports available.
 - ◆ Select one of nodes from one controller.
 - ◆ Click ▼ Change Portal.
 - ◆ Select the network ports that you would like to be available for this iSCSI node.



- ◆ Click OK button.

- **Rename Alias:** Use this option to add or change iSCSI alias.
 - ◆ Select one of nodes from one controller.
 - ◆ Click ▼ **Rename Alias**.
 - ◆ Enter the Alias Name. Leave it empty to remove the alias.
 - ◆ Click **OK** button.

iSCSI Alias

Add or change iSCSI alias.
 To add or change the alias name, enter the name below and press OK. To remove an alias, clear out the current name and press OK.

Alias Name:

After creating an alias, it is displayed at the end of the portal information.

Show information for: Controller 1 ▼

<< first < prev 1 2 3 4 5 6 7 8 9 10 next > last >>

	ID	Auth	Name	Portal	Alias
OP.	0	CHAP	iqn:dev0.ctr1	192.168.1.1:3260, 192.168.2.1:3260, 192.168.3.1:3260, 192.168.4.1:3260, 192.168.5.1:3260, 192.168.6.1:3260	dev0.ctr1
OP.	1	None	iqn:dev1.ctr1	192.168.1.1:3260, 192.168.2.1:3260, 192.168.3.1:3260, 192.168.4.1:3260, 192.168.5.1:3260, 192.168.6.1:3260	
OP.	2	None	iqn:dev2.ctr1	192.168.1.1:3260, 192.168.2.1:3260, 192.168.3.1:3260, 192.168.4.1:3260, 192.168.5.1:3260, 192.168.6.1:3260	



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

5.3.4 Active Session

The **Active Session** tab is used to display all currently active iSCSI sessions and their connection information.

	No.	TSIH	Initiator Name	Target Name	InitialR2T	Immed. Data	MaxOutR2T	MaxDataBurstLen	DataSeqInOrder	DataPDUInOrder
▼	0	0x0201	iqn.1991-05.com.microsoft.win-eebjh1nigp	iqn.entity.name:000927fc0.dev0.ctr1	Yes	Yes	1	262144	Yes	Yes

This table shows the column descriptions. Most of the options are standard parameters used in the negotiation between the initiator and target when an iSCSI connection is created.

Column Name	Description
TSIH	TSIH (Target Session Identifying Handle) is used for this active session.
Initiator Name	It displays the host computer name.
Target Name	It displays the controller name.
InitialR2T	InitialR2T (Initial Ready to Transfer) is used to turn off either the use of a unidirectional R2T command or the output part of a bidirectional command. The default value is Yes.
Immed. data	Immed. data (Immediate Data) sets the support for immediate data between the initiator and the target. Both must be set to the same setting. The default value is Yes.
MaxDataOutR2T	MaxDataOutR2T (Maximum Data Outstanding Ready to Transfer) determines the maximum number of outstanding ready to transfer per task. The default value is 1.
MaxDataBurstLen	MaxDataBurstLen (Maximum Data Burst Length) determines the maximum SCSI data payload. The default value is 256kb.
DataSeqInOrder	DataSeqInOrder (Data Sequence in Order) determines if the PDU (Protocol Data Units) are transferred in continuously non-decreasing sequence offsets. The default value is Yes.
DataPDU InOrder	DataPDU InOrder (Data PDU in Order) determines if the data PDUs within sequences are to be in order and overlays forbidden. The default value is Yes.

The options are available on this tab:

- Click ▼ **Connection Details**: It can list all connection(s) of the selected session.

Connection					
No.	Initiator IP	Initiator Name	MaxRecvDataSegLen	MaxTransDataSegLen	Authentication
1	192.168.1.131	iqn.1991-05.com.microsoft.win-eebjh1nigp	16384	65536	No

OK

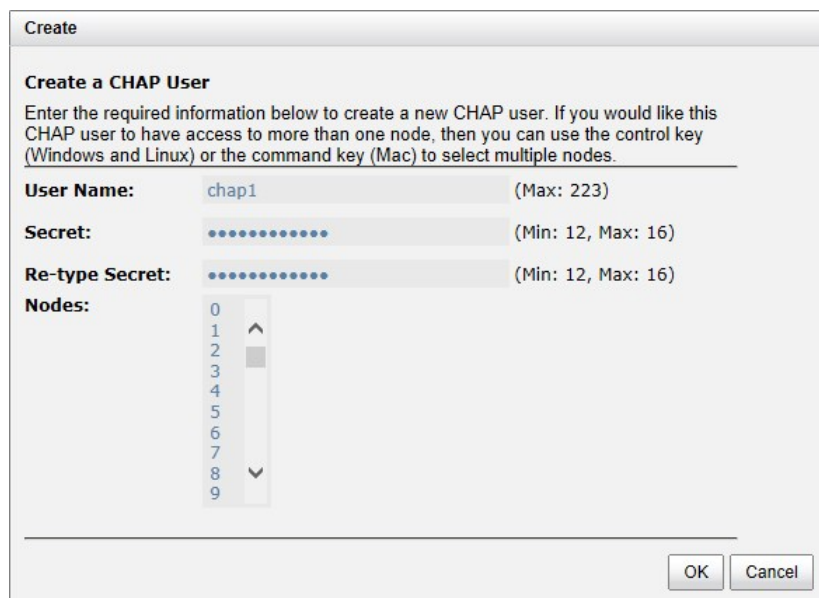
- Disconnect**: Disconnect the selected session, click OK button to confirm.

5.3.5 CHAP Account

The CHAP Account tab is used to manage the CHAP accounts on the system.

The options are available on this tab:

- **Create User:** Create a CHAP user.



Create

Create a CHAP User

Enter the required information below to create a new CHAP user. If you would like this CHAP user to have access to more than one node, then you can use the control key (Windows and Linux) or the command key (Mac) to select multiple nodes.

User Name: chap1 (Max: 223)

Secret: (Min: 12, Max: 16)

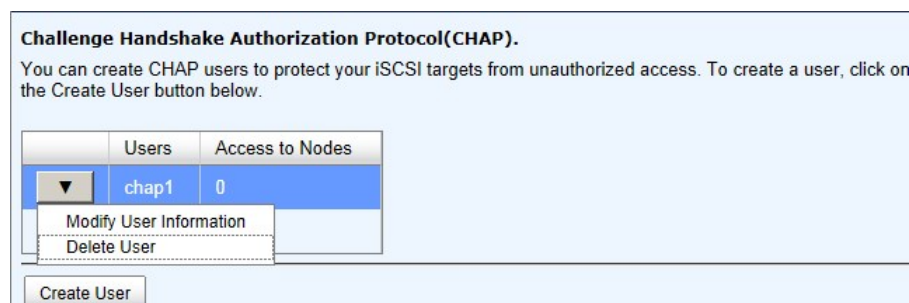
Re-type Secret: (Min: 12, Max: 16)

Nodes:

- 0
- 1
- 2
- 3
- 4
- 5
- 6
- 7
- 8
- 9

OK Cancel

- ◆ Enter the required information for **User Name**, **Secret**, and **Re-type Secret**.
- ◆ If you would like this CHAP user to have access, select one or multiple nodes. If selecting none, you can add it later by **iSCSI Configuration iSCSI Nodes Users**.
- ◆ Click **OK** button.



Challenge Handshake Authorization Protocol(CHAP).

You can create CHAP users to protect your iSCSI targets from unauthorized access. To create a user, click on the Create User button below.

	Users	Access to Nodes
▼	chap1	0

Modify User Information
Delete User

Create User

- **Modify User Information:** Modify the selected CHAP user information.
- **Delete User:** Delete the selected CHAP user.

5.3.6 Fibre Channel



NOTE:

This option is only visible when the controller has FC ports.

The **Fibre Channel** tab is used view the fibre channel information, and change the link speed of FC. It displays the Port ID, Connection Mode, Data Rate, WWNN (World Wide Node Name), WWPNN (World Wide Port Name) , error count and the link status.

Show information for: **Controller 1** ▼

	Name	Port ID	Connection Mode	Data Rate	WWNN/WWPN	Loss of Signal	Loss of Sync	Link Failure	Invalid CRC	Link
▼	Port 1	1	Arbitrated Loop	8 Gb/s	WWNN: 2000001378F70030 WWPN: 2100001378F70030	0	0	0	0	Up
▼	Port 2	1	Arbitrated Loop	8 Gb/s	WWNN: 2000001378F70030 WWPN: 2200001378F70030	0	0	0	0	Up
▼	Port 3	1	Arbitrated Loop	8 Gb/s	WWNN: 2000001378F70030 WWPN: 2300001378F70030	0	0	0	0	Up
▼	Port 4	1	Arbitrated Loop	8 Gb/s	WWNN: 2000001378F70030 WWPN: 2400001378F70030	0	0	0	0	Up

Clear All Counters

The options are available on this tab:

- **Clear All Counters:** Clear all counters of all fibre channels.
- **Change Link Speed:** There are **Automatic / 2 Gb/s / 4 Gb/s / 8 Gb/s** options. The default and recommended setting is to automatically detect the data rate.

Data Rate

Select the data rate for Port 4 on Controller 1 below. The default and recommended setting is for the array to automatically detect the data rate.

Data Rate: Automatic ▼

Automatic
2 Gb/s
4 Gb/s
8 Gb/s

OK Cancel

- **Change Connection Mode:** There are **Loop / Point-to-Point / Fabric** options.

Connection Mode

Change Connection Mode

Connection Mode : Point-to-Point ▼

Point-to-Point
Loop
Fabric

OK Cancel

- ◆ **Point-to-Point (FC-P2P):** Two devices are connected directly to each other. This is the simplest topology, with limited connectivity.
- ◆ **Loop (Arbitrated Loop)(FC-AL):** In this design, all devices are in a loop or ring, similar to token ring networking. Adding or removing a device from the loop causes all activity on the loop to be interrupted. The failure of one device causes a break in the ring. Fibre Channel hubs exist to connect multiple devices together and may bypass failed ports. A loop may also be made by cabling each port to the next in a ring.

- ◆ **Fabric (Switched Fabric)(FC-SW):** All devices or loops of devices are connected to Fibre Channel switches, similar conceptually to modern Ethernet implementations. Advantages of this topology over FC-P2P or FC-AL include.
- **Node Configuration:** Set the selected fibre channel for multi-nodes configuration. Check the nodes which can be accessed by the host.

Node Configuration

Node List : ☐ All

<input checked="" type="checkbox"/> Node 1	<input checked="" type="checkbox"/> Node 2	<input checked="" type="checkbox"/> Node 3	<input checked="" type="checkbox"/> Node 4
<input checked="" type="checkbox"/> Node 5	<input checked="" type="checkbox"/> Node 6	<input checked="" type="checkbox"/> Node 7	<input checked="" type="checkbox"/> Node 8
<input checked="" type="checkbox"/> Node 9	<input checked="" type="checkbox"/> Node 10	<input checked="" type="checkbox"/> Node 11	<input checked="" type="checkbox"/> Node 12
<input checked="" type="checkbox"/> Node 13	<input checked="" type="checkbox"/> Node 14	<input checked="" type="checkbox"/> Node 15	<input checked="" type="checkbox"/> Node 16
<input checked="" type="checkbox"/> Node 17	<input checked="" type="checkbox"/> Node 18	<input checked="" type="checkbox"/> Node 19	<input checked="" type="checkbox"/> Node 20
<input checked="" type="checkbox"/> Node 21	<input checked="" type="checkbox"/> Node 22	<input checked="" type="checkbox"/> Node 23	<input checked="" type="checkbox"/> Node 24
<input checked="" type="checkbox"/> Node 25	<input checked="" type="checkbox"/> Node 26	<input checked="" type="checkbox"/> Node 27	<input checked="" type="checkbox"/> Node 28
<input checked="" type="checkbox"/> Node 29	<input checked="" type="checkbox"/> Node 30	<input checked="" type="checkbox"/> Node 31	<input checked="" type="checkbox"/> Node 32
<input checked="" type="checkbox"/> Node 33	<input checked="" type="checkbox"/> Node 34	<input checked="" type="checkbox"/> Node 35	<input checked="" type="checkbox"/> Node 36
<input checked="" type="checkbox"/> Node 37	<input checked="" type="checkbox"/> Node 38	<input checked="" type="checkbox"/> Node 39	<input checked="" type="checkbox"/> Node 40
<input checked="" type="checkbox"/> Node 41	<input checked="" type="checkbox"/> Node 42	<input checked="" type="checkbox"/> Node 43	<input checked="" type="checkbox"/> Node 44
<input checked="" type="checkbox"/> Node 45	<input checked="" type="checkbox"/> Node 46	<input checked="" type="checkbox"/> Node 47	<input checked="" type="checkbox"/> Node 48
<input checked="" type="checkbox"/> Node 49	<input checked="" type="checkbox"/> Node 50	<input checked="" type="checkbox"/> Node 51	<input checked="" type="checkbox"/> Node 52
<input checked="" type="checkbox"/> Node 53	<input checked="" type="checkbox"/> Node 54	<input checked="" type="checkbox"/> Node 55	<input checked="" type="checkbox"/> Node 56
<input checked="" type="checkbox"/> Node 57	<input checked="" type="checkbox"/> Node 58	<input checked="" type="checkbox"/> Node 59	<input checked="" type="checkbox"/> Node 60
<input checked="" type="checkbox"/> Node 61	<input checked="" type="checkbox"/> Node 62	<input checked="" type="checkbox"/> Node 63	<input checked="" type="checkbox"/> Node 64
<input checked="" type="checkbox"/> Node 65	<input checked="" type="checkbox"/> Node 66	<input checked="" type="checkbox"/> Node 67	<input checked="" type="checkbox"/> Node 68
<input checked="" type="checkbox"/> Node 69	<input checked="" type="checkbox"/> Node 70	<input checked="" type="checkbox"/> Node 71	<input checked="" type="checkbox"/> Node 72
<input checked="" type="checkbox"/> Node 73	<input checked="" type="checkbox"/> Node 74	<input checked="" type="checkbox"/> Node 75	<input checked="" type="checkbox"/> Node 76
<input checked="" type="checkbox"/> Node 77	<input checked="" type="checkbox"/> Node 78	<input checked="" type="checkbox"/> Node 79	<input checked="" type="checkbox"/> Node 80
<input checked="" type="checkbox"/> Node 81	<input checked="" type="checkbox"/> Node 82	<input checked="" type="checkbox"/> Node 83	<input checked="" type="checkbox"/> Node 84
<input checked="" type="checkbox"/> Node 85	<input checked="" type="checkbox"/> Node 86	<input checked="" type="checkbox"/> Node 87	<input checked="" type="checkbox"/> Node 88
<input checked="" type="checkbox"/> Node 89	<input checked="" type="checkbox"/> Node 90	<input checked="" type="checkbox"/> Node 91	<input checked="" type="checkbox"/> Node 92
<input checked="" type="checkbox"/> Node 93	<input checked="" type="checkbox"/> Node 94	<input checked="" type="checkbox"/> Node 95	<input checked="" type="checkbox"/> Node 96
<input checked="" type="checkbox"/> Node 97	<input checked="" type="checkbox"/> Node 98	<input checked="" type="checkbox"/> Node 99	<input checked="" type="checkbox"/> Node 100
<input checked="" type="checkbox"/> Node 101	<input checked="" type="checkbox"/> Node 102	<input checked="" type="checkbox"/> Node 103	<input checked="" type="checkbox"/> Node 104
<input checked="" type="checkbox"/> Node 105	<input checked="" type="checkbox"/> Node 106	<input checked="" type="checkbox"/> Node 107	<input checked="" type="checkbox"/> Node 108
<input checked="" type="checkbox"/> Node 109	<input checked="" type="checkbox"/> Node 110	<input checked="" type="checkbox"/> Node 111	<input checked="" type="checkbox"/> Node 112
<input checked="" type="checkbox"/> Node 113	<input checked="" type="checkbox"/> Node 114	<input checked="" type="checkbox"/> Node 115	<input checked="" type="checkbox"/> Node 116
<input checked="" type="checkbox"/> Node 117	<input checked="" type="checkbox"/> Node 118	<input checked="" type="checkbox"/> Node 119	<input checked="" type="checkbox"/> Node 120
<input checked="" type="checkbox"/> Node 121	<input checked="" type="checkbox"/> Node 122	<input checked="" type="checkbox"/> Node 123	<input checked="" type="checkbox"/> Node 124

OK Cancel

- **Clear Counters:** Clear the counters of the selected fibre channel.

**CAUTION:**

The connection mode Point-to-Point does not support multi-node

5.4 Volume Configuration

The **Volume configuration** menu option is for accessing the **Physical Disks**, **RAID Groups**, **Virtual Disks**, **Snapshots**, **Logical Units**, and **QReplicas** option tabs.



5.4.1 Physical Disk

The **Physical Disks** 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).

Show disk for: <input type="button" value="Local"/> Show disk size in: <input type="button" value="GB"/>														
Slot	Size (GB)	RAID Group	RAID Set	Virtual Disk	Status	Health	Usage	Vendor	Serial Number	Rate	Write Cache	Standby	Read-Ahead	Command Queuing
1	1862		N/A	N/A	Online	Good	Free	WDC	WD-WCAVY4158095	SATA 6.0Gb/s	Disabled	Disabled	Enabled	Enabled
2	1862		N/A	N/A	Online	Good	Free	WDC	WD-WCAVY3924333	SATA 6.0Gb/s	Disabled	Disabled	Enabled	Enabled
3	446		N/A	N/A	Online	Good	Free	INTEL	CVWL414500UJ480QGN	SATA SSD 6.0Gb/s	Enabled	Disabled	Enabled	Enabled

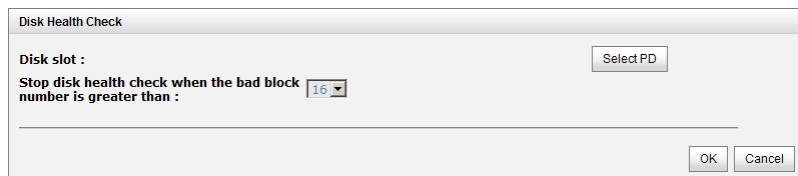
This table shows the column descriptions.

Column Name	Description
Slot	The position of a hard drive. The button next to the number of slot shows the functions which can be executed.
Size (GB) or (MB)	Capacity of hard drive. The unit can be displayed in GB or MB.
RAID Group	RAID group name.
RAID Set	<p>The number of RAID Set:</p> <ul style="list-style-type: none"> ● N/A: The RAID group is traditional provisioning. ● Number: The RAID group is the number of RAID set of thin provisioning.
Status	<p>The status of the hard drive:</p> <ul style="list-style-type: none"> ● Online: the hard drive is online. ● Rebuilding: the hard drive is being rebuilt. ● Transitioning: the hard drive is being migrated or is replaced by another disk when rebuilding occurs. ● Scrubbing: the hard drive is being scrubbed.

Health	<p>The health of the hard drive:</p> <ul style="list-style-type: none"> ● 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	<p>The usage of the hard drive:</p> <ul style="list-style-type: none"> ● RAID: This hard drive has been set to a RAID group. ● Free: This hard drive is free for use. ● Dedicated Spare: This hard drive has been set as dedicated spare of a RAID group. ● Local Spare: This hard drive has been set as local spare of the enclosure. ● Global Spare: This hard drive has been set as global spare of whole system.
Vendor	Hard drive vendor.
Serial Number	Hard drive serial number.
Rate	<p>Hard drive rate:</p> <ul style="list-style-type: none"> ● SAS 6.0Gb/s. ● SAS 3.0Gb/s. ● SATA 6.0Gb/s. ● SATA 3.0Gb/s. ● SATA 1.5Gb/s. ● SAS SSD 6.0Gb/s. ● SATA SSD 6.0Gb/s.
Write Cache	Hard drive write cache is enabled or disabled. The default value is Enabled.
Standby	HDD auto spindown to save power. The default value is Disabled.
Read-Ahead	This feature makes data be loaded to disk's buffer in advance for further use. The default value is Enabled.
Command Queuing	Newer SATA and most SCSI disks can queue multiple commands and handle one by one. The default value is Enabled.

The options are available on this tab:

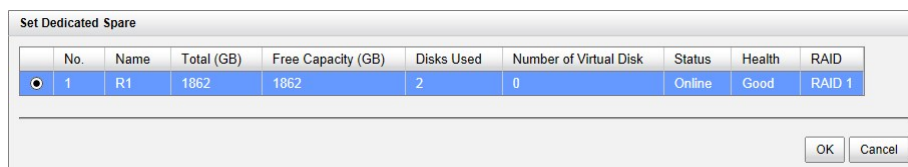
- **Disk Health Check:** Check the health of the selected disks. It cannot check the disks which are in used.



- **Disk Check Report:** Download the disk check report. It's available after executing Disk Health Check.
- **Set Free Disk:** Make the selected hard drive be free for use.
- **Set Global Spare:** Set the selected hard drive to global spare of all RIAD groups.
- **Set Local Spare:** Set the selected hard drive to local spare of the RIAD groups which locates in the same enclosure.
- **Set Dedicated Spare:** Set a hard drive to dedicated spare of the selected RAID group.
- **Upgrade:** Upgrade the firmware of the hard drive.
- **Disk Scrub:** Scrub the hard drive. It's not available when the hard drive is in used.
- **Read Error Cleared:** Clean the read error of 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:** Display hard drive detail information.

Take an example to set the physical disk to dedicated spare disk.

1. **Set Dedicated Spare** at one physical disk.



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

5.4.2 RAID Group

The **RAID Groups** tab provides to create, modify, delete, or view the status of the RAID groups. Use the drop-down list at the top to change the drive size units (MB or GB).

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

Show RAID size in: GB

	Name	Total (GB)	Free Capacity (GB)	Available Size (GB)	Thin Provisioning	Disks Used	Number of Virtual Disk	Status	Health	RAID	Current Controller	Preferred Controller
	R0	1862	1862	1862	Disabled	1	0	Online	Good	RAID 0	Controller 1	Controller 1
	R1	1862	1862	1862	Enabled	2	0	Online	Good	RAID 1	Controller 1	Controller 1

Create

This table shows the column descriptions.

Column Name	Description
Name	RAID group name.
Total (GB) or (MB)	Total capacity of the RAID group. The unit can be displayed in GB or MB.
Free Capacity (GB) or (MB)	Free capacity of the RAID group. The unit can be displayed in GB or MB.
Available Size (GB) or (MB)	Available capacity of the RAID group. The unit can be displayed in GB or MB.
Thin Provisioning	The status of Thin provisioning: <ul style="list-style-type: none"> ● Disabled. ● Enabled.
Disks Uses	The number of physical disks in the RAID group.
Number of Virtual Disk	The number of virtual disks in the RAID group.
Status	The status of the RAID group: <ul style="list-style-type: none"> ● Online: the RAID group is online. ● Offline: the RAID group is offline. ● Rebuilding: the RAID group is being rebuilt. ● Migrating: the RAID group is being migrated. ● Scrubbing: the RAID group is being scrubbed.
Health	The health of the RAID group: <ul style="list-style-type: none"> ● 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
RAID	The RAID level of the RAID group.

Current

Controller

(This option is only visible when dual controllers are installed.)

The controller of the RAID group. The default is controller 1.

Preferred

Controller

(This option is only visible when dual controllers are installed.)

The preferred controller of the RAID group. The default is controller 1.

The options are available on this tab:

- **Create:** Create a RAID group.

The options are available after creating a RAID group:

- **Migrate RAID Level :** Change the RAID level of a RAID group. Please refer to next chapter for details.
- **Move RAID Level :** Move the member disks of RAID group to totally different physical disks.
- **Activate/Deactivate :** Activate or deactivate the RAID group after disk roaming. Activate can be executed when the RAID group status is offline. Conversely, Deactivate can be executed when the status is online. These are for online disk roaming purpose.
- **Verify Parity :** Regenerate parity for the RAID group. It supports the RAID level 3 / 5 / 6 / 30 / 50 / 60.
- **Delete :** Delete the RAID group.
- **Change Preferred Controller :** Set the RAID group ownership to the other controller.
- **Change RAID Options :** Change the RAID property options.
 - ◆ Write Cache:
 - Enabled: When the write cache is enabled, data transfer operations are written to fast cache memory instead of being written directly to disk. This may improve performance but may take the data lost risk when losing power if there is no BBM protection.
 - Disabled: Disable disk write cache. (Default)

- ◆ Standby:
 - Disabled: Disable auto spin down. (Default)
 - 30 sec / 1 min / 5 min / 30 min: The hard drives will be spun down for power saving when the disk is idle for the period of time specified.
- ◆ Read-Ahead:
 - Enabled: The system will discern what data will be needed next based on what was just retrieved from disk and then preload this data into the disks buffer. This feature will improve performance when the data being retrieved is sequential. (Default)
 - Disabled: Disable disk read ahead.
- ◆ Command Queuing:
 - Enabled: Sends multiple commands at once to a disk to improve performance.
 - Disabled: Disable disk command queuing.

5.4.3 Virtual Disk

The Virtual Disks tab provides to create, modify, delete, or view the status of the virtual disk. Use the drop-down list at the top to change the drive size units (MB or GB).

This table shows the column descriptions.

Column Name	Description
Name	Virtual disk name.
Size (GB) or (MB)	Total capacity of the virtual disk. The unit can be displayed in GB or MB.
Write	The right of virtual disk: <ul style="list-style-type: none"> ● WT: Write Through. ● WB: Write Back. ● RO: Read Only.
Priority	The priority of virtual disk: <ul style="list-style-type: none"> ● HI: High priority. ● MD: Middle priority. ● LO: Low priority.
Bg Rate	Background task priority: <ul style="list-style-type: none"> ● 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.
Type	The type of the virtual disk: <ul style="list-style-type: none"> ● RAID: the virtual disk is normal. ● BACKUP: the virtual disk is for backup usage.
Clone	The clone target name of the virtual disk.
Schedule Clone	The clone schedule of the virtual disk.
Status	The status of the virtual disk: <ul style="list-style-type: none"> ● Online: The virtual disk is online. ● Offline: The virtual disk is offline. ● Initiating: The virtual disk is being initialized. ● Rebuilding: The virtual disk is being rebuilt. ● Migrating: The virtual disk is being migrated. ● Rollback: The virtual disk is being rolled back. ● Parity checking: The virtual disk is being parity check.
Health	The health of virtual disk: <ul style="list-style-type: none"> ● 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.

	<ul style="list-style-type: none"> ● 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. After passing parity check, the health will become Optimal.
R %	Ratio (%) of initializing or rebuilding.
RAID	RAID level.
LUN #	Number of LUN(s) that virtual disk is attached.
Snapshot space (GB) or (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.
RAID Group	The RAID group name of the virtual disk

The options are available on this tab:

- **Create** : Create a virtual disk.
- **Cloning Options** : Set the clone options.

The options are available after creating a virtual disk:

- **Extend** : Extend the virtual disk capacity.
- **Set SSD Caching**: Set SSD caching for the virtual disk.
- **Verify Parity** : Execute parity check for the virtual disk. It supports RAID 3 / 5 / 6 / 30 / 50 / 60. The options are:
 - ◆ Verify and repair data inconsistencies.
 - ◆ Only verify for data inconsistencies. Stop verifying when 1 10 20 30 40 50 60 70 80 90 100 inconsistencies have been found.
- **Delete**: Delete the virtual disk.
- **Set Properties**: Change the virtual disk name, Cache mode, priority, bg rate and read ahead.
 - ◆ Cache Mode:
 - **Write-through Cache**: 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.
 - **Write-back Cache**: 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 nonvolatile 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. (Default)
 - **Read-Only**: Set the volume to be read-only, any write request is forbidden.
 - ◆ Priority:
 - High Priority (Default)

- Medium Priority.
- Low Priority.
- ◆ Bg Rate:
 - 4 / 3 / 2 / 1 / 0: Default value is 4. The higher number the background priority of a virtual disk has, the more background I/O will be scheduled to execute.
- ◆ Read-Ahead:
 - Enabled: The system will discern what data will be needed next based on what was just retrieved from disk and then preload this data into the disks buffer. This feature will improve performance when the data being retrieved is sequential. (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 Target: The virtual disk is used for clone or QReplica usage.
- **Space Reclamation:** Reclaim space for the virtual disk.
- **Attach LUN:** Attach a logical unit number to the virtual disk.
- **Detach LUNs:** Detach a logical unit number from the virtual disk.
- **List LUNs:** List all of the attached logical unit numbers.
- **Set Clone:** Set the target virtual disk for clone.
- **Clear Clone:** Clear the clone function.
- **Start Clone:** Start the clone function.
- **Stop Clone:** Stop the clone function.
- **Change QReplica Options:** Change the clone to QReplica relationship.
- **Schedule Clone:** Set the clone function by schedule.
- **Set Snapshot Space:** Set snapshot space for preparing to take snapshots.
- **Cleanup Snapshots:** Clean all snapshots of the virtual disk and release the snapshot space.
- **Take a Snapshot:** Take a snapshot on the virtual disk.
- **Schedule Snapshots:** Set the snapshots by schedule.
- **List Snapshots:** List all snapshots of the virtual disk.
- **More Information:** Show the detail information of the virtual disk.

Take an example of creating a virtual disk.

1. Click Create button.

Create a Virtual Disk

Virtual Disk Name: VD-01

Data Storage: R5

Size: 30 GB

Stripe Size (KB): 64

Block Size (Bytes): 512

Cache Mode: ☐ Write-through Cache ☒ Write-back Cache

Priority: ☒ High Priority ☐ Medium Priority ☐ Low Priority

Bg Rate: 4

Read-Ahead: Enabled

AV-Media Mode: Disabled

Space Reclaim: Enabled

Disk Type: RAID
Backup Target

OK Cancel

2. Enter a **Virtual Disk Name** for the virtual disk.
3. Select a **Data Storage** from the drop-down list.
4. Enter required **Size**.
5. Optionally, configure the following:
 - **Stripe Size (KB):** The options are 4KB, 8KB, 16KB, 32KB, 64KB. The default value is 64KB.
 - **Block Size (Bytes):** The options are 512 to 65536. The default value is 512 bytes.
 - **Cache Mode:** The options are Write-through Cache and Write-back Cache. The default value is Write-back Cache.
 - **Priority:** The options are High, Medium and Low Priority. The default value is High priority.
 - **Bg Rate:** Background task priority. The higher number the background priority of a virtual disk has, the more background I/O will be scheduled to execute. The options are 0 to 4. The default value is 4.
 - **Read-Ahead:** The system will discern what data will be needed next based on what was just retrieved from disk and then preload this data into the disks buffer. This feature will improve performance when the data being retrieved is sequential. The default value is Enabled.
 - **AV-Media Mode:** Optimize for video editing. The default value is Disabled.
 - **Erase:** This option is available when the RAID group is not thin provisioning. This option will wipe out old data in virtual disk to prevent that OS recognizes the old partition. The options are Do Not Erase, erase First 1GB or Full Disk. The default value is Don Not Erase.

- **Space Reclaim:** This option is available when the RAID group is thin provisioning. There are Enabled or Disabled. The default value is Enabled.
 - **Disk Type:** Select type for normal or backup usage. The options are RAID (for general usage) and Backup Target (for Clone or QReplica). The default value is RAID.
6. Click OK button to create the virtual disk.
 7. At the confirmation message, click OK button.

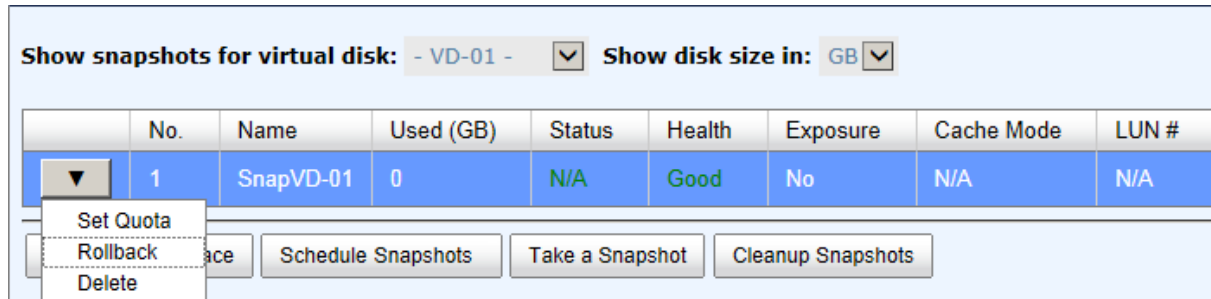


CAUTION:

If shutdown or reboot the system when creating a virtual disk, the erase process will stop.

5.4.4 Snapshot

The **Snapshots** tab provides to create, modify, delete, or view the status of snapshot. The two drop-down lists at the top enable you to switch the virtual disks. The other is to change the drive size units (MB or GB)



This table shows the column descriptions.

Column Name	Description
No.	Number.
Name	Snapshot name.
Used (GB) or (MB)	The amount of the snapshot space that has been used. The unit can be displayed in GB or MB.
Status	The status of the snapshot: <ul style="list-style-type: none"> ● 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 the snapshot: <ul style="list-style-type: none"> ● Good: The snapshot is good. ● Failed: The snapshot fails.
Exposure	The snapshot is exposed or not.
Cache Mode	The cache mode of the snapshot: <ul style="list-style-type: none"> ● N/A: Unknown when the snapshot is unexposed. ● Read-write: The snapshot can be read / write. ● Read-only: The snapshot is read only.
LUN #	Number of LUN(s) that snapshot is attached.
Time Created	The created time of the snapshot.

The options are available on this tab:

- **Set Snapshot Space:** Set snapshot space for preparing to take snapshots.
- **Schedule Snapshots:** Set the snapshots by schedule.

Take a Snapshot: Take a snapshot on the virtual disk.

Cleanup Snapshots: Clean all snapshots of the virtual disk and release the snapshot space.

The options are available after taking a snapshot:

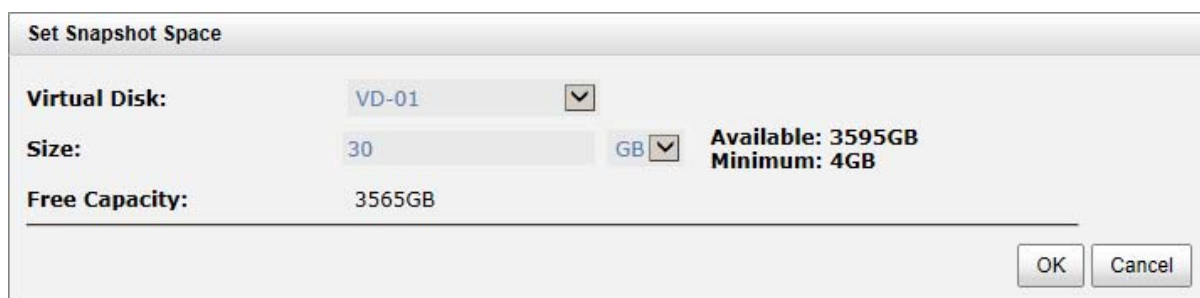
- **Set Quota** : Set the snapshot quota.
- **Rollback** : Rollback the snapshot.
- **Delete** : Delete the snapshot.

The options are available after setting the quota of the snapshot:

- **Unexpose** : Unexpose the snapshot VD.
- **Attach LUN** : Attach a logical unit number to the snapshot.
- **Detach LUNs** : Detach a logical unit number from the virtual disk.
- **List LUNs** : List all of the attached logical unit numbers.

Take an example of taking a snapshot.

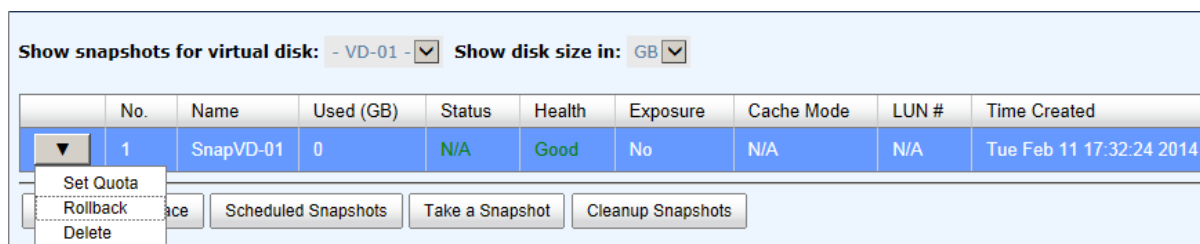
1. Before taking a snapshot, it must reserve some storage space for saving variant data. Click **Set Snapshot Space** button.



The 'Set Snapshot Space' dialog box contains the following fields and controls:

- Virtual Disk:** A dropdown menu showing 'VD-01'.
- Size:** A text input field containing '30'.
- Unit:** A dropdown menu showing 'GB'.
- Available:** 3595GB
- Minimum:** 4GB
- Free Capacity:** 3565GB
- Buttons:** 'OK' and 'Cancel' at the bottom right.

2. Select a **Virtual Disk** from the drop-down list.
3. Enter a **Size** which is reserved for the snapshot space.
4. Click **OK**. The snapshot space is created.
5. Click **Take a Snapshot** button.
6. Use the drop-down list to select a **Virtual Disk**.
7. Enter a **Snapshot Name**.
8. Click **OK**. The snapshot is taken.



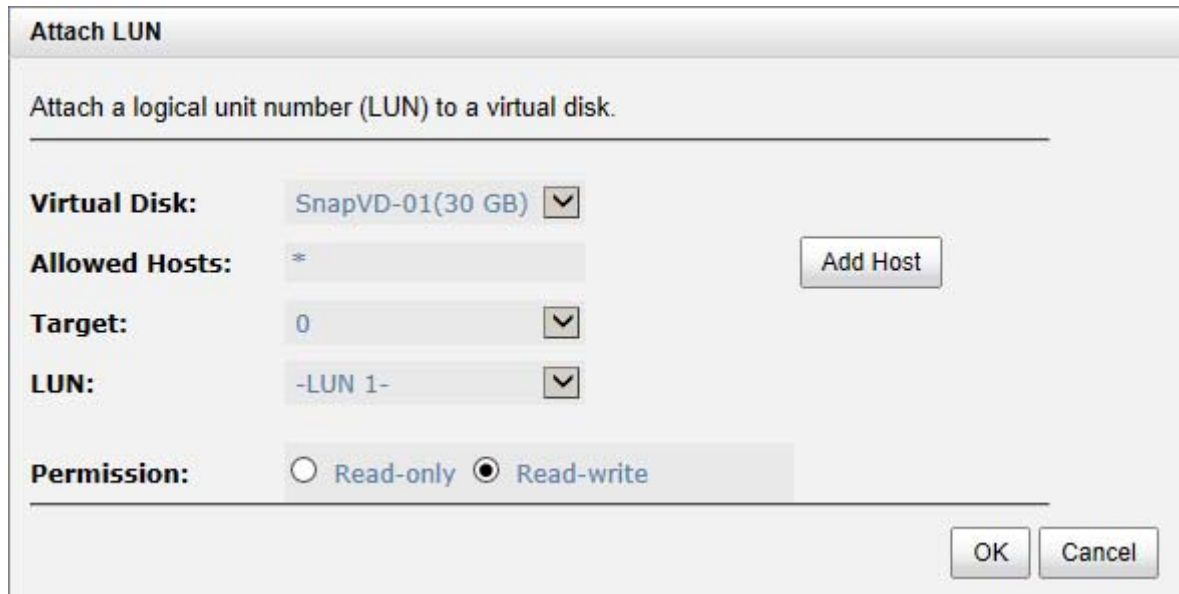
The interface shows a table of snapshots for virtual disk 'VD-01'.

No.	Name	Used (GB)	Status	Health	Exposure	Cache Mode	LUN #	Time Created
1	SnapVD-01	0	N/A	Good	No	N/A	N/A	Tue Feb 11 17:32:24 2014

Below the table, there is a context menu with options: 'Set Quota', 'Rollback', and 'Delete'. At the bottom, there are buttons: 'Scheduled Snapshots', 'Take a Snapshot', and 'Cleanup Snapshots'.

9. Set quota to expose the snapshot. Click ▼ -> **Set Quota** option.

10. Enter a size which is reserved for the snapshot. If the size is zero, the exposed snapshot will be read only. Otherwise, the exposed snapshot can be read / written, and the size will be the maximum capacity for writing.
11. Attach LUN to the snapshot.



The image shows a dialog box titled "Attach LUN". Inside the dialog, there is a header that says "Attach a logical unit number (LUN) to a virtual disk." Below this header, there are several fields and controls:




- Virtual Disk:** A dropdown menu showing "SnapVD-01(30 GB)".
- Allowed Hosts:** A text field containing an asterisk (*). To the right of this field is a button labeled "Add Host".
- Target:** A dropdown menu showing "0".
- LUN:** A dropdown menu showing "-LUN 1-".
- Permission:** Two radio buttons. The first is labeled "Read-only" and is unselected. The second is labeled "Read-write" and is selected (indicated by a filled circle).

At the bottom right of the dialog, there are two buttons: "OK" and "Cancel".

12. Done. The Snapshot can be used.

5.4.5 Logical Unit

The Logical Units tab provides to attach, detach or view the status of logical unit numbers for each virtual disk.

	Allowed Hosts	Target	LUN	Permission	Virtual Disk	Number of Session
	*	0	0	Read-write	VD-01	0
	iqn.1991-05.com.microsoft	0	1	Read-only	VD-02	0
						

This table shows the column descriptions.

Column Name	Description
Allowed Hosts	The FC node name / iSCSI node name for access control or a wildcard (*) for access by all hosts.
Target	The number of the target.
LUN	The number of the LUN assigned.
Permission	The permission level: <ul style="list-style-type: none"> ● Read-write. ● Read-only.
Virtual Disk	The name of the virtual disk assigned to this LUN.
Number of Session (This option is only visible when the controller has iSCSI ports.)	The number of the active connection linked to the logical unit.

The options are available on this tab:

- **Attach LUN** : Attach a logical unit number to the virtual disk.

The options are available after attaching LUN:

- **Detach LUNs** : Detach a logical unit number from the virtual disk.

Take an example of attaching a LUN

1. Click the **Attach LUN** button.

2. Select the **Protocol**. (FC models only)
3. Select a **Virtual Disk** from the drop-down list.
4. Enter the **Allowed Hosts** with semicolons (;) or click **Add Host** button to add one by one. Fill-in wildcard (*) for access by all hosts.
5. Select a **Target** number from the drop-down list.
6. Select a **LUN** from the drop-down list.
7. Check the **Permission** level.
8. Click **OK** button.

The matching rules of access control are followed from created time of the LUNs. The earlier created LUN is prior to the matching rules. For example: there are 2 LUN rules for the same VD, one is "*", LUN 0; and the other is "iqn.host1", LUN 1. The host "iqn.host2" can login successfully because it matches the rule 1.

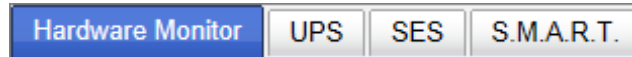
Wildcard "*" and "?" are allowed in this field. "*" can replace any word. "?" can replace only one character. For example:

- "iqn.host?" -> "iqn.host1" and "iqn.host2" are accepted.
- "iqn.host*" -> "iqn.host1" and "iqn.host12345" are accepted.

This field cannot accept comma, so "iqn.host1, iqn.host2" stands a long string, not 2 iqns.

5.5 Enclosure Management

The **Enclosure Management** menu option is for accessing the **Hardware Monitor**, **UPS**, **SES**, and **S.M.A.R.T.** option tabs.



For the enclosure management, there are many sensors for different purposes, such as temperature sensors, voltage sensors, hard disk status, 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 the polling time intervals:

- Temperature sensors: 1 minute.
- Voltage sensors: 1 minute.
- Hard disk sensors: 10 minutes.
- Fan sensors: 10 seconds . When there are 3 errors consecutively, system sends ERROR event log.
- Power sensors: 10 seconds, when there are 3 errors consecutively, system sends ERROR event log.
- 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.

Show information for: - Local - Temperature (Internal)/(Case): (C)

Controller 1 Monitors

Type	Item	Value	Status
Voltage	On Board Vcore	+0.99 V (min = +0.75 V, max = +1.35 V)	OK
Voltage	Onboard +3.3V	+3.34 V (min = +3.10 V, max = +3.50 V)	OK
Voltage	Onboard +5V	+5.00 V (min = +4.60 V, max = +5.40 V)	OK
Voltage	Onboard +12V	+12.04 V (min = +11.04 V, max = +12.96 V)	OK
Voltage	On Board Vddr	+1.50 V (min = +1.39 V, max = +1.60 V)	OK
Temperature	CPU Core 0	+48.0 (C) (hyst = +5.0 (C), high = +79.0 (C))	OK
Temperature	CPU Core 1	+46.0 (C) (hyst = +5.0 (C), high = +79.0 (C))	OK
Temperature	iSCSI NIC 1	+36.0 (C) (hyst = +0.0 (C), high = +65.0 (C))	OK
Temperature	iSCSI NIC 2	+36.0 (C) (hyst = +0.0 (C), high = +65.0 (C))	OK
Temperature	System Board	+40.0 (C) (hyst = +5.0 (C), high = +65.0 (C))	OK
Temperature	SAS Expander	+63.0 (C) (hyst = +5.0 (C), high = +90.0 (C))	OK
Temperature	Location BBM	N/A	Not installed

Backplane

Type	Item	Value	Status
Voltage	PSU +5V	+5.07 V (min = +4.60 V, max = +5.40 V)	OK
Voltage	PSU +12V	+12.08 V (min = +11.04 V, max = +12.96 V)	OK
Voltage	PSU +3.3V	+3.38 V (min = +3.04 V, max = +3.56 V)	OK
Temperature	Location 1	+26.0 (C) (hyst = +0.0 (C), high = +55.0 (C))	OK
Temperature	Location 2	+29.0 (C) (hyst = +0.0 (C), high = +55.0 (C))	OK
Temperature	Location 3	+26.0 (C) (hyst = +0.0 (C), high = +55.0 (C))	OK
Temperature	Location 4	+25.0 (C) (hyst = +0.0 (C), high = +55.0 (C))	OK
Temperature	Location 5	+26.0 (C) (hyst = +0.0 (C), high = +55.0 (C))	OK
Temperature	Location 6	+25.0 (C) (hyst = +0.0 (C), high = +55.0 (C))	OK
Temperature	Location 7	+25.0 (C) (hyst = +0.0 (C), high = +55.0 (C))	OK
Temperature	Location 8	+25.0 (C) (hyst = +0.0 (C), high = +55.0 (C))	OK
Power Supply	PSU1	N/A	OK
Power Supply	PSU2	N/A	OK
Cooling	FAN1	3375 RPM	OK
Cooling	FAN2	3590 RPM	OK
Cooling	FAN3	3515 RPM	OK
Cooling	FAN4	3515 RPM	OK

Auto Shutdown: ☒

If auto shutdown is enabled, the system will shut down automatically when the internal power

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 that could trigger an automatic shutdown, the system uses to gauge if a shutdown is needed. This is done using several sensors placed on key systems that the system checks every 30 seconds for present temperatures.

When one of these sensors reports a temperature above the threshold for three continuous minutes, the system shuts down automatically.

5.5.2 UPS

The UPS is used to set up UPS (Uninterruptible Power Supply).

The system supports Smart-UPS made by APC, and Megatec series UPS.
 Choose Smart-UPS for APC products, Megatec-UPS for Megatec series products, or none if you are using a UPS

UPS Type:	Smart-UPS (SNMP) ▼
Shutdown Battery Level (%):	20 ▼
Shutdown Delay (Seconds):	0 ▼
Shutdown UPS:	OFF ▼
IP address:	<input style="width: 100%;" type="text"/>
Community:	<input style="width: 100%;" type="text"/>
UPS Status:	<div style="width: 20px; height: 10px; background-color: #ccc; border: 1px solid #ccc;"></div>
UPS Battery Level:	<div style="width: 100%; height: 15px; background: linear-gradient(to right, blue 0%, blue 10%, gray 10%, gray 100%); position: relative;"> <div style="position: absolute; right: 0; top: 0; color: #666;">0%</div> </div>

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/>.



NOTE:
Connection with other vendors of UPS can work well, but they have no such communication features with the system.

Now we support the traditional UPS via serial port and network UPS via **SNMP**. If using the UPS with serial port, connect the system to UPS via the included cable for communication. (The cable plugs into the serial cable that comes with the UPS.) Then set up the shutdown values for when the power goes out.

This table shows the available options and their descriptions.

Options	Description
UPS Type	Select UPS Type: <ul style="list-style-type: none"> ● None: No UPS or other vendors. ● Smart-UPS (Serial port): APC UPS with serial port. ● Smart-UPS (SNMP): APC UPS with network function. ● Megatec-UPS: Megatec UPS.
Shutdown Battery Level (%)	When below the setting level, the system will shutdown. Setting level to "0" will disable UPS.
Shutdown Delay (Seconds)	If power failure occurs and system power cannot recover after the time setting, the system will shutdown. Setting delay to "0" will disable the function.
Shutdown UPS	Select ON, when power is gone, UPS will shut down by itself after the system shutdown successfully. After power comes back, UPS will start working and notify system to boot up. OFF will not.
IP Address (This option is only visible when the UPS type is Smart-UPS (SNMP).)	The IP address of the network UPS.
Community (This option is only visible when the UPS type is Smart-UPS (SNMP).)	The SNMP community of the network UPS.
Status	The status of UPS: <ul style="list-style-type: none"> ● 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 power percentage of battery level.

The system will shutdown either **Shutdown Battery level (%)** or **Shutdown Delay (Seconds)** reaches the condition. User should set these values carefully.

5.5.3 SES

The **SES** (SCSI Enclosure Services, one of the enclosure management standards) tab is used to enable or disable the management of SES.

The options are available on this tab:

- **Enable:** Click the Enable button to enable SES.
- **Disable:** Click the Disable button to disable SES.

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

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

5.5.4 S.M.A.R.T.

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

Self-Monitoring Analysis and Reporting Technology (S.M.A.R.T.)												
Below is the current S.M.A.R.T. information for the drives attached to this device. S.M.A.R.T. provides users with an opportunity to take action before possible drive failure.												
Show information for: <input type="button" value="- Local -"/> Temperature (Internal)/(Case): <input type="button" value="(C)"/> <input type="button" value="F"/>												
Slot	HDD Rate	Media Wea	Reallocated Sec	Erase Fail (Unexpected Pc	Uncorrectable	Temperatur	Read Error	Spin Up (Time)	Seek Error #R	Spin Up (Ret	Calibration (Re
1	SATA 6.0Gb/s	N/A	200(140)	N/A	N/A	N/A	N/A	200(51)	177(21)	200(0)	100(0)	100(0)
2	SATA 6.0Gb/s	N/A	200(140)	N/A	N/A	N/A	N/A	200(51)	161(21)	200(0)	100(0)	100(0)
3	SATA 6.0Gb/s	N/A	200(140)	N/A	N/A	N/A	N/A	200(51)	166(21)	200(0)	100(0)	100(0)

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.

5.6 System Maintenance

The **System Maintenance** menu option is accessing the **System Information**, Event Log, Upgrade, Firmware Synchronization (This option is only visible when dual controllers is installed.), **Reset to Factory Defaults**, **Configuration Backup**, **Volume Restoration**, and **Reboot and Shutdown** option tabs.

System Information	Event Log	Upgrade	Firmware Synchronization	Reset to Factory Defaults	Configuration Backup	Volume Restoration	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., MAC/SAS Address, Controller Hardware No., Master Controller, Backplane ID, JBOD MAC/SAS Address, Status, Error Message (This item is only visible when the system status is Degraded or Lockdown.), QReplica, QThin, and SSD Caching status.

Item	Information
CPU Type	
System Memory	
Firmware Version	
SAS IOC Firmware No.	17.00.01.00
SAS Expander Firmware No.	Local Controller 1 : 1120 Controller 2 : 1120
MAC/SAS Address	001378BB3880 (Controller 1 : 5001378005900CC0 , Controller 2 : 5001378005900640)
Controller HW No.	Controller 1: 1.14 Controller 2: 1.14
Master Controller	Controller 1
Backplane ID	
JBOD MAC/SAS Address	No JBOD is connected.
Status	Normal
QReplica	Activated
QThin	Activated
SSD Caching	Activated
Get System Information	

Status description:

Status	Description
Normal	Dual controllers and JBODs are in normal stage.
Degraded	One controller or JBOD 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:

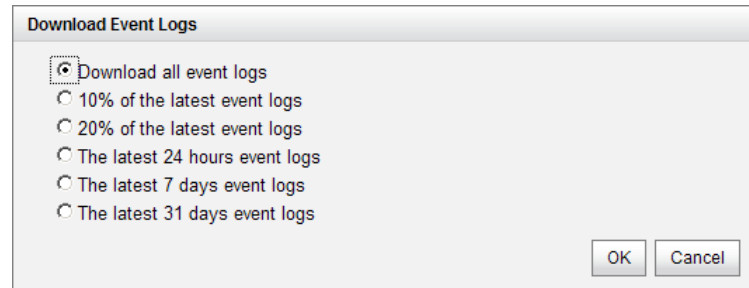
- **Download System Information:** Download the system information for debug.

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.




A dialog box titled "Download Event Logs" with a list of radio button options and "OK" and "Cancel" buttons.

Download Event Logs

- ☒ Download all event logs
- ☐ 10% of the latest event logs
- ☐ 20% of the latest event logs
- ☐ The latest 24 hours event logs
- ☐ The latest 7 days event logs
- ☐ The latest 31 days event logs

OK Cancel

- **Mute Buzzer:** Stop alarm if the system alerts.
- **Clear:** Clear all event logs.



An interface titled "Event Log Level to Show" with buttons for "Information", "Warning", and "Error". Below the buttons is a table of event logs with columns "Type", "Time", and "Content". At the bottom are buttons for "Download", "Mute Buzzer", and "Clear".

Event Log Level to Show

Information Warning Error

<< first < prev 1 2 3 4 5 6 7 8 9 10 next > last >>

Type	Time	Content
Information	Mon, 17 Feb 2014 18:35:56	[CTR1] Disk 1 has been freed from RAID group 'R5'.
Information	Mon, 17 Feb 2014 18:35:56	[CTR1] Virtual disk 'VD-02' has been deleted.
Information	Mon, 17 Feb 2014 18:35:56	[CTR1] Virtual disk 'SnapVD-01' has been deleted.
Information	Mon, 17 Feb 2014 18:35:56	[CTR1] Virtual disk 'VD-01' has been deleted.
Information	Mon, 17 Feb 2014 18:35:56	[CTR1] RAID group 'R5' has been deleted.
Information	Mon, 17 Feb 2014 18:35:42	[CTR1] LUN 1 is attached to virtual disk 'VD-01'.
Information	Mon, 17 Feb 2014 18:35:34	[CTR1] Disk 2 has been freed from RAID group 'R5'.
Error	Mon, 17 Feb 2014 18:35:34	[CTR1] Virtual disk 'VD-02' has failed.
Error	Mon, 17 Feb 2014 18:35:34	[CTR1] Virtual disk 'VD-01' has failed.
Error	Mon, 17 Feb 2014 18:35:34	[CTR1] RAID group 'R5' has failed.
Information	Mon, 17 Feb 2014 18:35:26	[CTR1] Disk 3 has been freed from RAID group 'R5'.
Warning	Mon, 17 Feb 2014 18:35:26	[CTR1] RAID group 'R5' is in degraded mode.
Information	Mon, 17 Feb 2014 18:23:47	[CTR1] admin login from 192.168.8.231 via web UI.
Information	Sat, 15 Feb 2014 20:54:24	[CTR1] admin login from 92.242.203.131 via web UI.
Information	Fri, 14 Feb 2014 15:42:28	[CTR1] admin login from 59.125.120.109 via web UI.
Information	Fri, 14 Feb 2014 15:01:17	[CTR1] admin login from 203.117.200.77 via web UI.
Information	Thu, 13 Feb 2014 11:46:00	[CTR1] admin login from 192.168.135.1 via web UI.
Information	Wed, 12 Feb 2014 21:57:00	[CTR1] Virtual disk 'VD-02' has completed rebuilding.
Information	Wed, 12 Feb 2014 21:42:25	[CTR1] Virtual disk 'VD-02' has started rebuilding.
Information	Wed, 12 Feb 2014 21:42:25	[CTR1] Virtual disk 'VD-01' has completed rebuilding.

<< first < prev 1 2 3 4 5 6 7 8 9 10 next > last >>

Download Mute Buzzer Clear

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



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, and change operation mode. Before upgrade, it recommends to use **Configuration Backup** tab to export all configurations to a file.

Controller Module Firmware Update	
Select the firmware file for the upgrade:	<input type="text"/> <input type="button" value="Browse..."/>
<input type="button" value="Apply"/>	
JBOD Firmware Update	
Choose an JBOD:	<input type="text"/> <input type="button" value="v"/>
Select the firmware file for the upgrade:	<input type="text"/> <input type="button" value="Browse..."/>
<input type="button" value="Apply"/>	
Controller Mode	
Operation Mode:	<input type="text" value="Dual"/> <input type="button" value="v"/>
<input type="button" value="Apply"/>	
SSD Caching License	
Select the license file to activate SSD Caching:	<input type="text"/> <input type="button" value="Browse..."/>
<input type="button" value="Apply"/>	

The options are available on this tab:

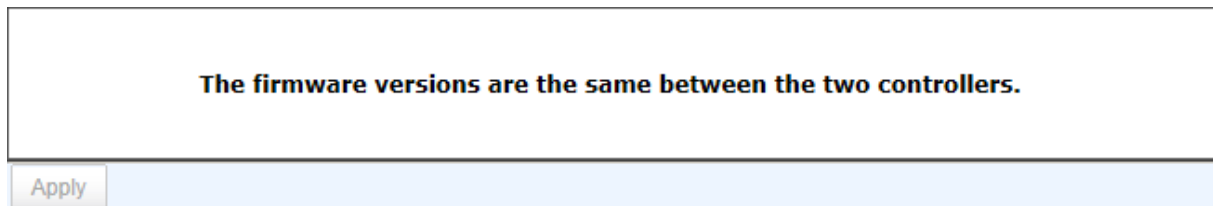
- **Controller Module Firmware Update:** Please prepare new controller firmware file named "xxxx.bin" in local hard drive, then click **Browse** to select the firmware file. Click **Apply** button, it will pop up a warning message, click OK button to start upgrading the firmware.

When upgrading, there is a progress bar running. After finished upgrading, the system must reboot manually to make the new firmware take effect.

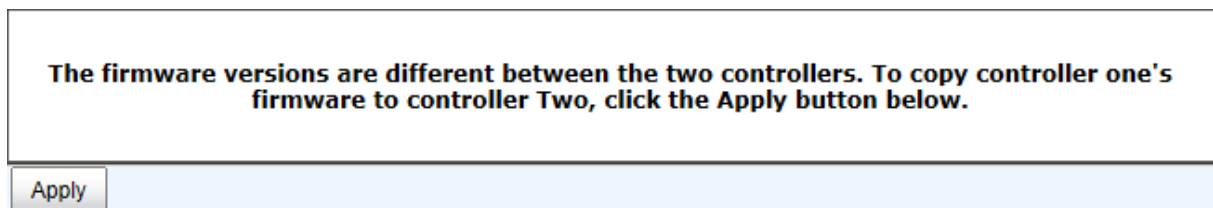
- **JBOD firmware upgrade:** To upgrade JBOD firmware, the steps are the same as controller firmware but choosing number of JBOD first.
- **Controller mode:** This option can be modified to dual or single here. If the system installs only one controller, switch this mode to Single. This mode indicates single upgradable. Enter the MAC address displayed in System configuration Network setting such as 001378xxxxxx (case-insensitive), and then click Confirm button.
- **SSD Caching license:** This option can activate SSD caching function if there is a license here. Select the license file, and then click Apply button. Each license key is unique and dedicated to a specific system. To obtain the license key, please contact sales for assistance.

5.6.4 Firmware Synchronization (Only available in Dual controller models)

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. Normally, the firmware versions in both controllers are the same.



If the firmware versions between two controllers are different, it will display the following message. Click **Apply** button to synchronize.



NOTE:

This tab is only visible when the dual controllers are installed. A single controller system does not have this option.

5.6.5 Reset to Factory Default

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

Click the Reset button below to reset the system to the factory defaults.

Reset

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

5.6.6 Configuration Backup

The **Configuration Backup** is used to either save system configuration (export) or apply a saved configuration (import).

Import or Export:

Import File:

Import
Export

Browse...

Apply

While the volume configuration settings are available for exporting, to prevent conflicts and overwriting existing data, they cannot be imported.

The options are available on this tab:

- **Import:** Import all system configurations excluding volume configuration.
- **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 Volume Restoration

The **Volume Restoration** can restore the volume configuration from the volume creation history. It is used for RAID group corrupt and tries to recreate the volume. When trying to do data recovery, the same volume configurations as original must be set and all member disks must be installed by the same sequence as original. Otherwise, data recovery will fail. The volume restoration does not guarantee that the lost data can be restored. Please get help from the expert before executing the function.

Restore the Volume Configuration

The volume restoration can restore your previous volume configurations when a RAID group corruption or a mis-delete occurs. Before restoration, please make sure that all the member disks are in place and guarantee all the lost data will be recovered. Please contact for support before using this function.

<< first < prev 1 2 3 4 5 6 7 8 next > last >>

	RAID Group Name	RAID	Virtual Disk	Volume Size (GB)	Disks Used	Disk Slot	Time	Event Log
▼	1	RAID 5	3	300	3	Local: 1, 2, 3	2014/02/17 18:52:41 CST	The virtual disk is created.
Restore		RAID 5	2	200	3	Local: 1, 2, 3	2014/02/17 18:52:35 CST	The virtual disk is created.
▼	1	RAID 5	1	100	3	Local: 1, 2, 3	2014/02/17 18:52:29 CST	The virtual disk is created.
▼	R5	RAID 5	VD-02	50	1	Local: 1	2014/02/17 18:35:34 CST	Physical disk is removed from the system.
▼	R5	RAID 5	VD-01	30	1	Local: 1	2014/02/17 18:35:34 CST	Physical disk is removed from the system.
▼	R5	RAID 5	VD-02	50	2	Local: 1, 2	2014/02/17 18:35:26 CST	Physical disk is removed from the system.
▼	R5	RAID 5	VD-01	30	2	Local: 1, 2	2014/02/17 18:35:26 CST	Physical disk is removed from the system.
▼	R5	RAID 5	VD-02	50	3	Local: 1, 2, 3	2014/02/11 17:03:30 CST	The snapshot space has initialized.
▼	R5	RAID 5	VD-02	50	3	Local: 1, 2, 3	2014/02/11 17:03:08 CST	The virtual disk is created.
▼	R5	RAID 5	VD-01	30	3	Local: 1, 2, 3	2014/02/11 17:02:45 CST	The snapshot space has initialized.
▼	R5	RAID 5	VD-01	30	3	Local: 1, 2, 3	2014/02/11 17:00:04 CST	The virtual disk is created.
▼	QUICK13645	RAID 5	QUICK21222	3725	3	Local: 3, 2, 1	2014/02/11 14:46:51 CST	The virtual disk is created.

<< first < prev 1 2 3 4 5 6 7 8 next > last >>

This table shows the column descriptions.

Column Name	Description
RAID Group Name	The original RAID group name.
RAID	The original RAID level.
Virtual Disk	The original virtual disk name.
Volume Size (GB)	The original capacity of the virtual disk.
Disks Used	The original physical disk number of the RAID group.
Disk slot	The original physical disk locations.
Time	The last action time of the virtual disk.
Event Log	The last event of the virtual disk.

The options are available on this tab:

- **Restore:** Restore the virtual disk of the RAID group.



NOTE: When trying to do data recovery, the same volume configurations as original must be set and all member disks must be installed by the same sequence as original. Otherwise, data recovery will fail.



CAUTION:

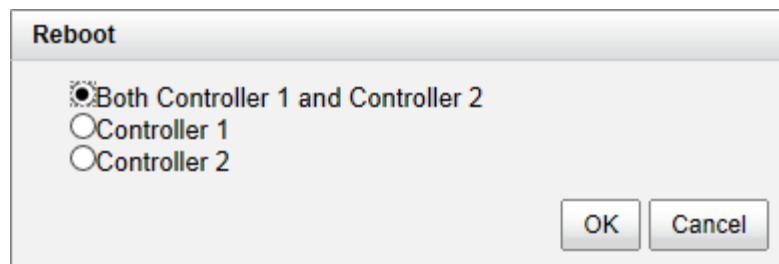
The data recovery does not guarantee that the lost data can be restored 100%. It depends on the real operation and the degree of physical damages on disks. Users will take their own risk to do these procedures.

5.6.8 Reboot and Shutdown

The Reboot and Shutdown function is used to reboot or shutdown the system. Before powering off the system, it is highly recommended to execute Shutdown function to flush the data from cache onto the physical disks. The step is important for data protection.



The Reboot function has three options, reboot both controllers, controller 1 only or controller 2 only.



5.7 Performance Monitor

The Performance Monitor menu option is accessing the Disk, iSCSI, and Fibre Channel (This option is only visible when it is fibre channel model.) option tabs.



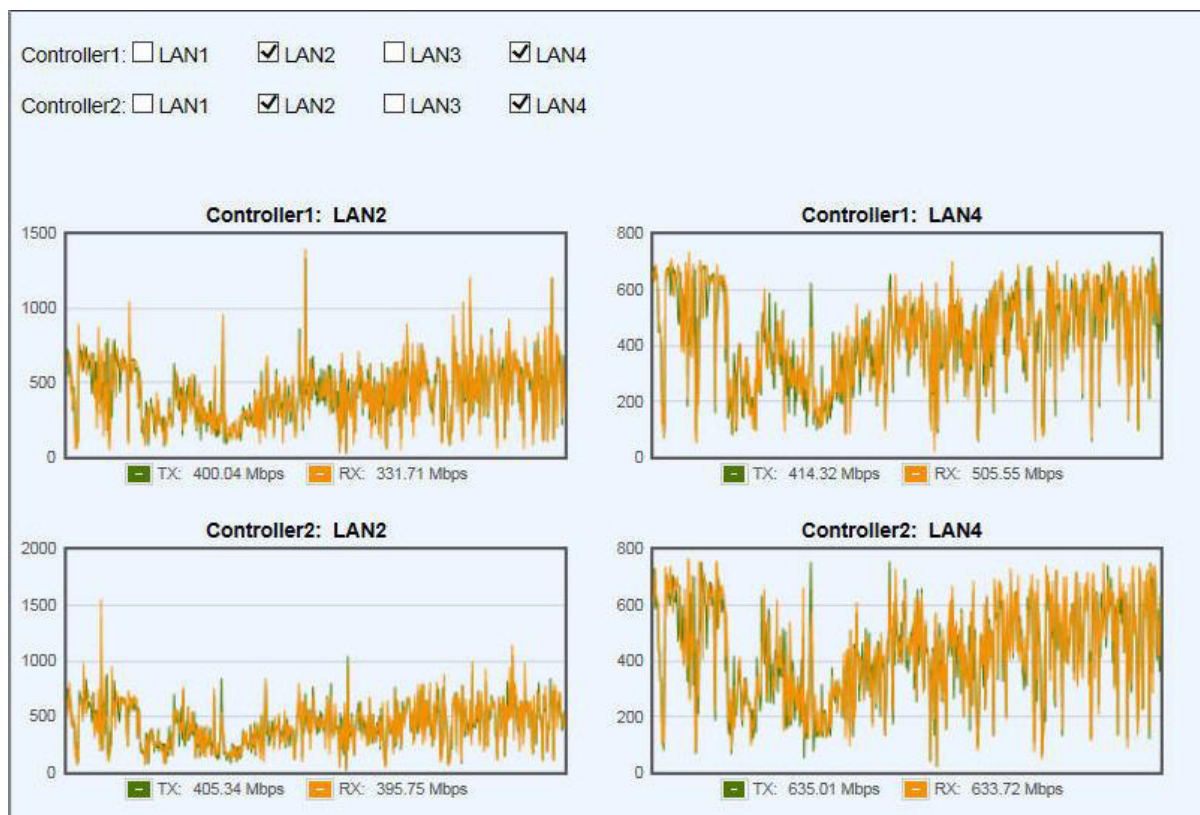
5.7.1 Disk

The Disk provides to display the throughput and latency of the physical disk. Check the slots which you want to monitor.



5.7.2 iSCSI

The iSCSI provides to display TX (Transmission) and RX (Reception) of the iSCSI ports. Check the interfaces which you want to monitor.



5.7.3 Fibre Channel



NOTE:

This option is only visible when the controller has FC ports.

The Fibre Channel provides to display TX (Transmission) and RX (Reception) of the fibre channels.

Check the interfaces which you want to monitor.

Chapter 6 Advanced Operations

6.1 Volume Rebuild

If one physical disk of the RAID group which is set as protected RAID level (e.g.: RAID 5, or RAID 6) fails or has been removed, then the status of RAID group will be changed to degraded mode. At the same time, the system will search the spare disk to execute volume rebuild the degraded RAID group into complete one.

There are three types of spare disks which can be set in **Physical Disks**:

- **Dedicated Spare**: The hard drive has been set as dedicated spare of a RAID group.
- **Local Spare**: The hard drive has been set as local spare of the enclosure.
- **Global Spare**: The hard drive has been set as global spare of whole system.

The detection sequence is the dedicated spare disk as the rebuild disk first, then local spare disk and global spare disk.

The following examples are scenarios for a RAID 6.

1. When there is no global spare disk or dedicated spare disk in the system, The RAID group will be in degraded mode and wait until there is one disk assigned as spare disk, or the failed disk is removed and replaced with new clean disk, and then the Auto-Rebuild starts.
2. When there are spare disks for the degraded array, system starts Auto-Rebuild immediately. In RAID 6, if there is another disk failure occurs during rebuilding, system will start the above Auto-Rebuild process as well. Auto-Rebuild feature only works at that the status of RAID group is Online. Thus, it will not conflict with the online roaming feature.
3. In degraded mode, the health of the RAID group is **Degraded**. When rebuilding, the status of RAID group and virtual disk will display **Rebuilding**, the column **R%** in virtual disk will display the ratio in percentage. After complete rebuilding, the status will become **Online**.



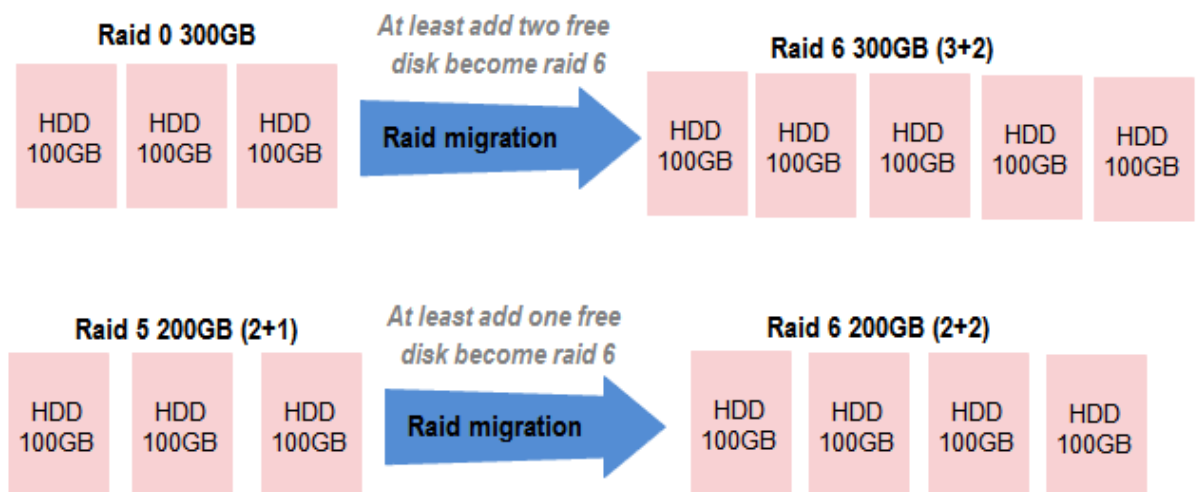
NOTE: The dedicated spare cannot be set if there is no RAID group or only RAID groups with RAID 0 or JBOD level.

Sometimes, rebuild is called recover; they are the same meaning. The following table is the relationship between RAID levels and rebuild.

Operation	Description
RAID 0	Disk striping. No protection for data. RAID group 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 60 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 Migrate and Move RAID Groups

Migrate RAID Level function changes the RAID group to different RAID level or adds the member disks of the RAID group for larger capacity. Usually, the RAID group migrates to higher RAID level for better protection. To do migration, the total size of RAID group must be larger than or equal to the original RAID group. The limitation is that it's not allowed expanding the same RAID level with the same physical disks of the original RAID group. There is a similar function **Move RAID Level** which will move the member disks of the RAID group to totally different physical disks. In addition, thin provision RAID group cannot execute migrate or move, it uses **Add RAID Set** to enlarge capacity. Describe more detail in the Thin Provision section.



There are some limitations when a RAID group is being migrated or moved. System would reject these operations:

1. Add dedicated spare.
2. Remove a dedicated spare.
3. Create a new virtual disk.
4. Delete a virtual disk.
5. Extend a virtual disk.
6. Scrub a virtual disk.
7. Perform another migration operation.
8. Scrub entire RAID group.
9. Take a snapshot.
10. Delete a snapshot.
11. Expose a snapshot.
12. Rollback to a snapshot.



NOTE: Migrate function will migrate the member disks of RAID group to the same physical disks but it should increase the number of disks or it should be different RAID level. Move function will move the member disks of RAID group to totally different physical disks.



CAUTION:
RAID group migration or moving cannot be executed during rebuilding or virtual disk extension.

Take an example of migrate the RAID group.

1. Select **Volume Configuration -> RAID Groups**.
2. Select a RAID group, and then click ▼ -> **Migrate RAID Level**.
3. Select a **RAID Level** from the drop-down list.
4. Click the **Select Disks** button to select disks from either local or expansion JBOD systems, and click **OK** to complete the selection. The selected disks are displayed at **Disks Used**.

5. At the confirmation dialog, click **OK** button to execute migration.
6. Migration starts and the status of Physical Disks, RAID Groups and Virtual Disks are changing. The complete percentage of migration is displayed in R%.

Show disk for: Local Show disk size in: GB

	Slot	Size (GB)	RAID Group	RAID Set	Status	Health	Usage	Vendor	Serial Number	Rate	Write Cache	Standby	Read-Ahead	Command Queuing
▼	1	1862	R0->R5	N/A	Transitioning	Good	RAID	WDC	WD-WCAVY4158095	SATA 6.0Gb/s	Disabled	Disabled	Enabled	Enabled
▼	2	1862	R0->R5	N/A	Transitioning	Good	RAID	WDC	WD-WCAVY3924333	SATA 6.0Gb/s	Disabled	Disabled	Enabled	Enabled
▼	3	1862	R0->R5	N/A	Online	Good	RAID	WDC	WD-WCAVY4118479	SATA 6.0Gb/s	Disabled	Disabled	Enabled	Enabled

Disk Health Check Disk Check Report

	Name	Total (GB)	Free Capacity (GB)	Available Size (GB)	Thin Provisioning	Disks Used	Number of Virtual Disk	Status	Health	RAID	Current Controller	Preferred Controller
▼	R0->R5	3725	3625	3625	Disabled	3	1	Migrating	Good	RAID 5	Controller 1	Controller 1

Create

Show disk size in: GB

<< first < prev 1 next > last >>

	Name	Size (GB)	Write	Priority	Bg Rate	Type	Clone	Schedule Clone	Status	Health	R %	RAID	LUN #	Snapshot Space (GB)	Snapshot #	RAID Group
▼	VD-01	5	WB	HI	4	RAID	N/A	N/A	Migrating	Optimal	0	RAID 5	0	0/0	0	R0->R5

<< first < prev 1 next > last >>

Create Cloning Options

Move RAID Level usage is the same as **Migrate RAID Level** except it cannot change the RAID level.

6.3 Extend Virtual Disks

Extend function extend the size of the virtual disk if there is enough free space.

Take an example of extending the virtual disk.

1. Select **Volume Configuration -> Virtual Disks**.
2. Select a virtual disk, and then click ▼ -> **Extend**.
3. Change the virtual disk size. The size must be larger than the current, and then click **OK** button to start extension.



4. Extension starts. If the virtual disk needs initialization, it will display the status Initiating and the complete percentage of initialization in **R%**.



NOTE: The extension size must be larger than the current size of the virtual disk.

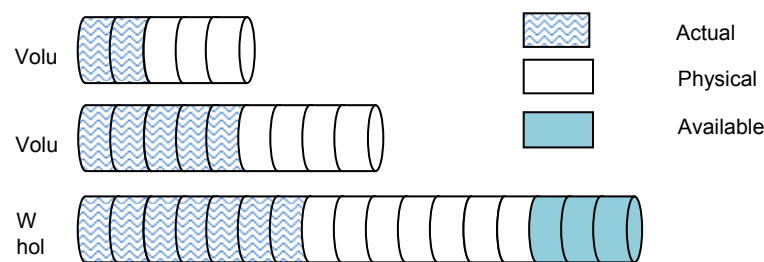


IMPORTANT! Extension cannot be executed during rebuilding or migration.

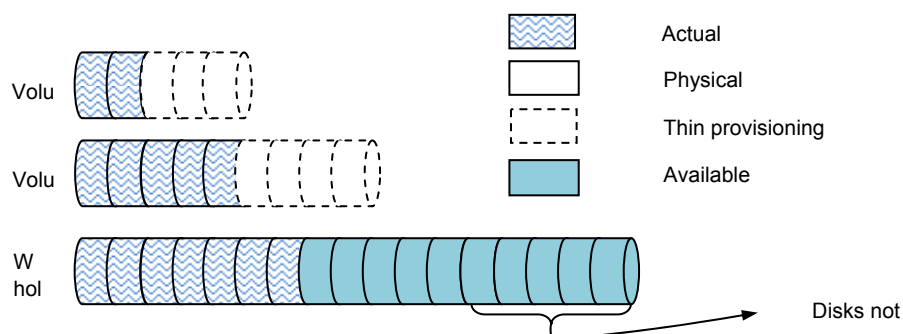
6.4 Thin provisioning

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.



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 may or may 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.



6.4.1 The Benefits of Thin provisioning

The benefits of Thin provisioning are described on the following.

- 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 technology used here is called zero reclamation. When a thin RG is created, the initialization process will try to fill out all the storage pool space with zero. This process will run in background with low priority in order not to impact the I/O performance. This is the reason why when there is no I/O traffic from the hosts, the hard drive LED will keep blinking as if there are I/O activities. The purpose of zero reclamation is that when the actual user data happens to have all zero in a basic allocation unit (granularity), the storage system will treat it as free space and recycle it. Until the next time there is data update to this reclaimed all zero basic unit, the storage system can swiftly return a basic unit from the free storage pool because it's already filled with zero.
- 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.

6.4.2 Features Highlight

The following describes the comparison with Fat and Thin provisioning.

- Write on demand or allocate on demand.

This is the most distinctive function in thin provisioning. You can see from the screenshots below. Figure 1 shows there are two RAID groups created. "Fat-RG" is using traditional provisioning without Thin provisioning enabled and its size is 1862GB. "Thin-RG" is Thin provisioning -enabled and its size is the same.



	Name	Total (GB)	Free Capacity (GB)	Available Size (GB)	Thin Provisioning
	Fat-RG	1862	1862	1862	Disabled
	Thin-RG	1862	1862	1862	Enabled

Figure 1: No virtual disk is created

Let's create a Virtual Disk on each RAID group with the same size of 1000GB respectively in Figure 2 and see what happen.



	Name	Size (GB)	Write	Priority	Bg Rate	Type	Clone
	Fat-VD	1000	WB	HI	4	RAID	N/A
	Thin-VD	1000	WB	HI	4	RAID	N/A

Figure 2: Virtual disks are created.

In Figure 3, the free space of "Fat-RG" immediately reduces to 862GB. 1000GB is taken away by the virtual disk. However, the free space of "Thin-RG" is still 1862GB 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 1862GB can be used to create other virtual disks. This is storage efficiency.



	Name	Total (GB)	Free Capacity (GB)	Available Size (GB)	Thin Provisioning
	Fat-RG	1862	862	862	Disabled
	Thin-RG	1862	1862	1862	Enabled

Figure 3: Write on demand

- 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.

Show RAID size in: GB

	Name	Total (GB)	Free Capacity (GB)	Available Size (GB)	Thin Provisioning	Disks Used
▼	Fat-RG	1862	862	862	Disabled	1
▼	Thin-RG	3724	3724	3724	Enabled	2

RAID Set:

	No	Total Size (GB)	Free Size (GB)	Disks Used	RAID Cell	Status	Health
▼	1	1862	1862	1	1	Online	Good
▼	2	1862	1862	1	1	Online	Good

Figure 4: Scalable RAID group size

- 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.
- 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.
- Convert traditional virtual disk to Thin and vice versa.
You can enjoy the benefits of Thin provisioning right now and right this moment. Move all your existing fat-provisioned virtual disks to thin-provisioned ones. Virtual disk clone function 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.

	Name	Size (GB)	Write	Priority	Bg Rate	Type	Clone	Schedule Clone	Status	Health
▼	Fat-VD	1000	WB	HI	4	RAID	N/A	N/A	Online	Optimal
▼	Thin-VD	1000	WB	HI	4	BACKUP	N/A	N/A	Online	Optimal

<< first < prev 1 next >

Create Cloning Options

Select a Virtual Disk Target

<< first < prev 1 next > last >>

Name	Size (GB)	Status	Health	RAID	RAID Group
<input checked="" type="radio"/> Thin-VD	1000	Online	Optimal	RAID 0	Thin-RG

<< first < prev 1 next > last >>

OK Cancel

Figure 5: Clone between thin virtual disk and fat one

6.4.3 Thin provisioning Options

The following describes the thin provisioning options.

- 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.

	Name	Total (GB)	Free Capacity (GB)	Available Size (GB)	Thin Provisioning	Disks Used
▼	Fat-RG	1862	360	360	Disabled	1
▼	Thin-RG	3724	3722	3724	Enabled	2

RAID Set:

	No	Total Size (GB)	Free Size (GB)	Disks Used	RAID Cell	Status	Health
▼	1	1862	1862	1	1	Online	Good
▼	2	1862	1860	1	1	Online	Good

RAID Group Policy:
 << first < prev 1 next > last >>

	No	Threshold	Level	Action
▼	1	60%	Information	Take no Action
▼	2	70%	Information	Take no Action
▼	3	80%	Information	Take no Action
▼	4	85%	Warning	Reclaim Space
▼	5	90%	Warning	Delete Snapshots
▼	6	95%	Warning	De-activate RAID Group

Figure 6: Capacity policy settings

- Automatic space reclamation to recycle unused space and increase utilization rate. Automatic space reclamation will be automatically activated in RAID group initialization process or it can be set manually 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.

Modify RAID Group Policy

Level: Information ▼

Action:

Take no Action
 Reclaim Space
 Delete Snapshots
 De-activate RAID Group

OK Cancel

Figure 7: Space reclamation

6.4.4 Thin Provisioning Case

We suggest that you apply QThin 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.

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

6.5 Disk Roaming

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

1. In **Volume Configuration -> RAID Group** tab, selects a RAID group. And then click ▼ -> **Deactivate**.
2. Click OK to apply. The **Status** changes to **Offline**.
3. Move all physical disks of the RAID group to another system.
4. In **Volume Configuration -> RAID Group** tab, selects a **RAID group**. And then click ▼ -> **Activate**.
5. Click **OK** to apply. The **Status** changes to **Online**.

Disk roaming has some constraints as described in the followings:

1. Check the firmware version of two systems first. It is better that either systems have the same firmware version or the firmware version of the system-2 is newer.
2. All physical disks of the RAID group should be moved from system-1 to system-2 together. The configuration of both RAID group and virtual disk will be kept but LUN configuration will be cleared in order to avoid conflict with the current setting of the system-2.

6.6 JBOD Expansion

The storage space can be expanded by adding JBOD expansion system.

6.6.1 Connecting JBOD

The storage systems support expansion systems with SAS connections. When connecting to an expansion system, it will be displayed at the Show disk for: drop-down list in Volume Configuration -> Physical Disks tab.

In **Enclosure Management** -> **Hardware monitor** tab, select the enclosure at the Show information for: drop-down list, it can display the hardware status of SAS JBODs.

In **Enclosure Management** -> **S.M.A.R.T.** tab, select the enclosure at the **Show information** for: drop-down list, it can display the SMART information of the disks in JBODs.

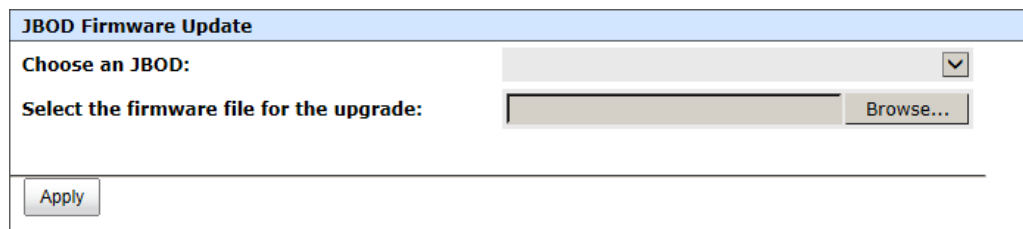
SAS JBOD expansion has some constraints as described in the followings:

1. User could create RAID group among multiple chassis.
2. Local spare disk can support the RAID groups which located in the local chassis.
3. Global spare disk can support all RAID groups which located in the different chassis.
4. When support SATA drives for the redundant JBOD model, the 6G MUX board is required. The 3G MUX board does not apply to this model.
5. The following table is the maximum JBOD numbers and maximum HDD numbers with different chassis can be cascaded.

6.6.2 Upgrade Firmware

Before upgrade, it recommends to use System maintenance -> Configuration Backup tab to export all configurations to a file. To upgrade the firmware of JBOD, please follow the procedures.

1. In **System Maintenance** -> **Upgrade** tab, choose an JBOD first, and then click **Browse** to select the firmware file.



The image shows a 'JBOD Firmware Update' dialog box. It has a title bar with the text 'JBOD Firmware Update'. Inside the dialog, there are two main sections. The first section is labeled 'Choose an JBOD:' and contains a dropdown menu with a downward arrow. The second section is labeled 'Select the firmware file for the upgrade:' and contains a text input field followed by a 'Browse...' button. At the bottom left of the dialog is an 'Apply' button.

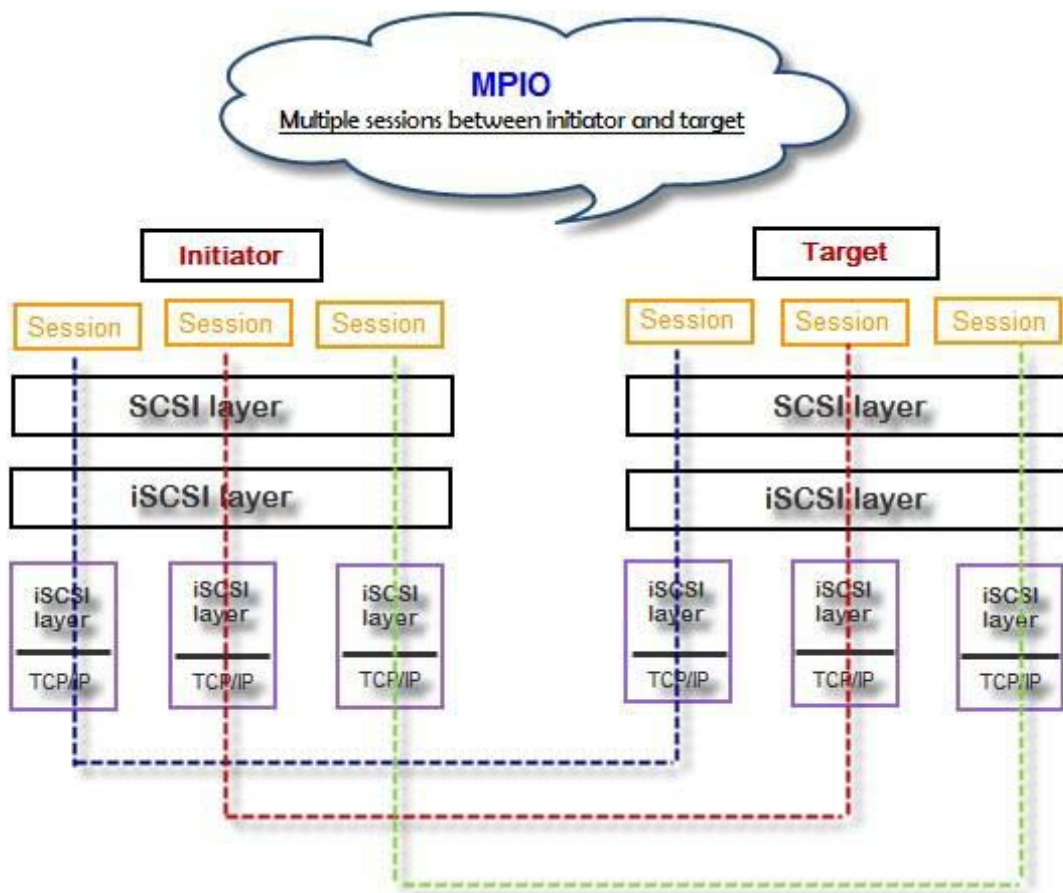
2. Click **Apply** button, it will pop up a warning message, click **OK** button to start upgrading the JBOD firmware.
3. After finished upgrading, the JBOD system must reboot manually to make the new firmware took effect.

6.7 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.

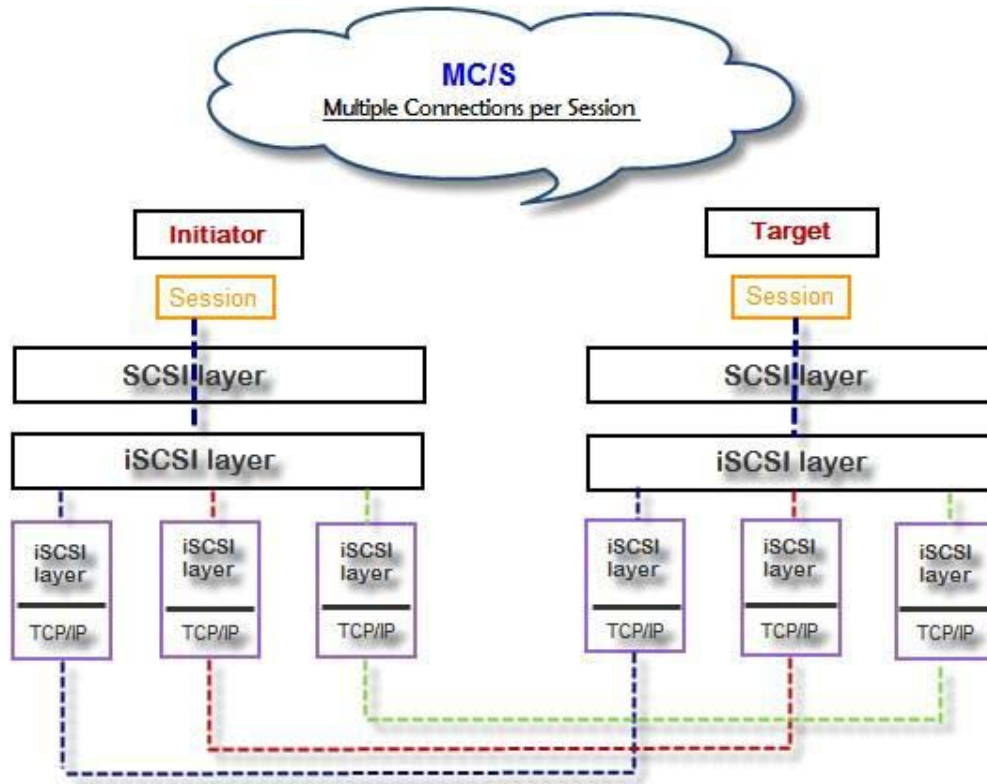
6.7.1 MPIO

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.



6.7.2 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.



6.7.3 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 multi-path.

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.

6.8 Trunking and LACP

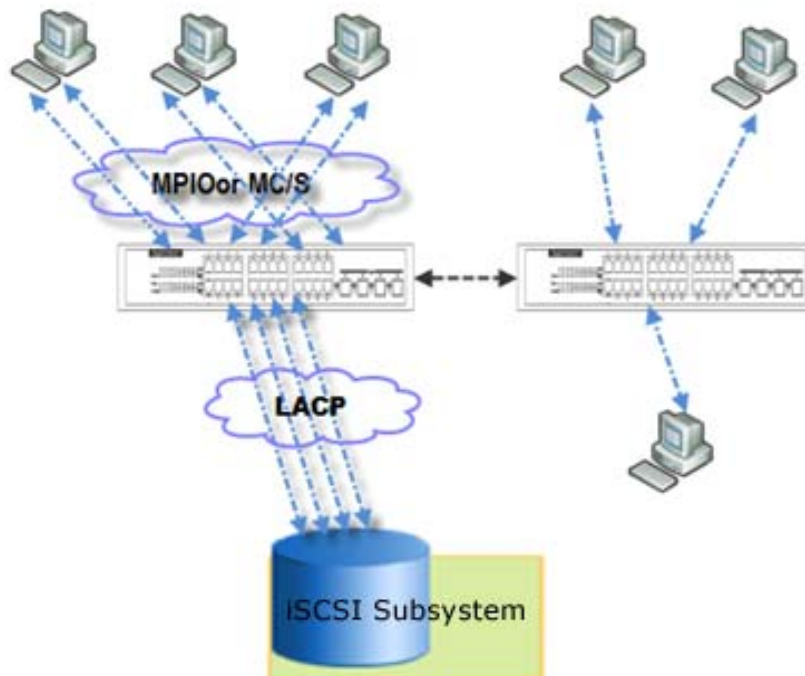
Link aggregation is the technique of taking several distinct Ethernet links to let them appear as a single link. It has a larger bandwidth and provides the fault tolerance ability. Beside the advantage of wide bandwidth, the I/O traffic remains operating until all physical links fail. If any link is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

6.8.1 LACP

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. The controller implements it as active mode which means that LACP port sends LACP protocol packets automatically. Please notice that using the same configurations between The controller and gigabit switch.

The usage occasion of LACP:

- 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.

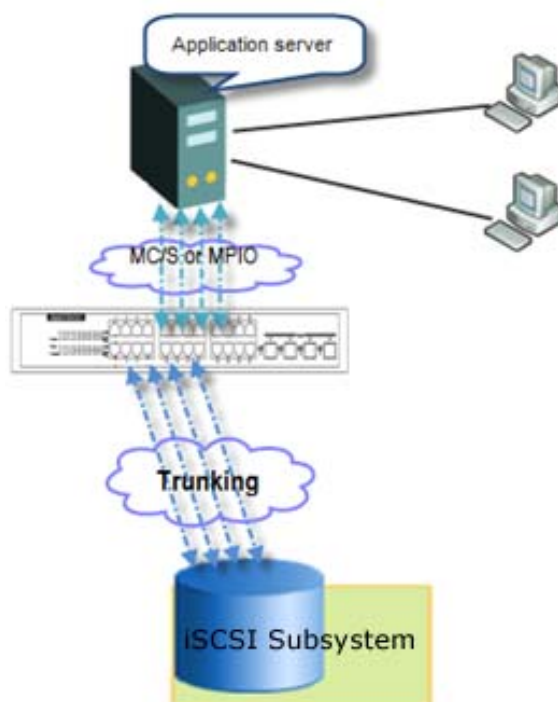


6.8.2 Trunking

Trunking is not a standard protocol. It 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:

- 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.
- There is no idea of using LACP or Trunking, uses Trunking first.
- There is a request of monitoring the traffic on a trunk in switch.



CAUTION:

Before using trunking or LACP, the gigabit switch must support either trunking or LACP. Otherwise, host cannot connect the link with storage device.

6.9 Dual Controllers

The storage system supports dual controllers of the same type for redundancy. Controller 1 (CTRL 1) is the master controller and controller 2 (CTRL 2) is the slave by default.

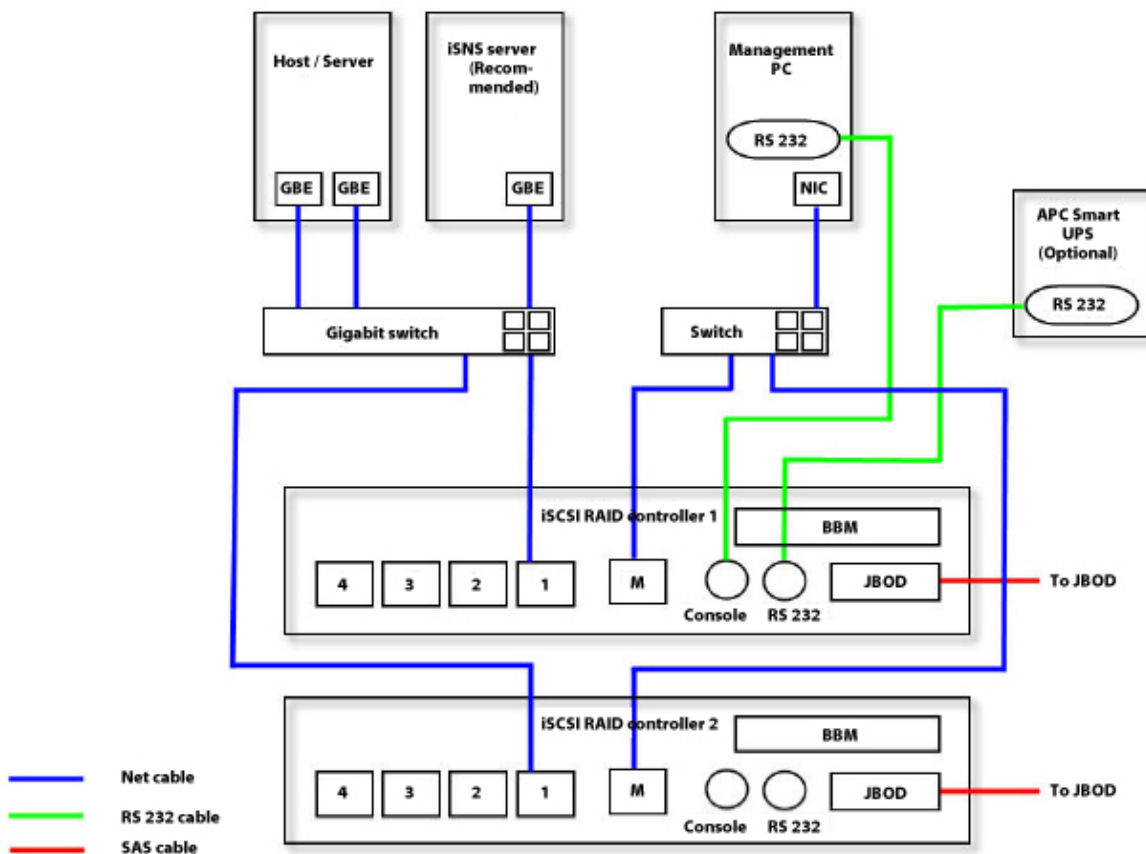


CAUTION:

- If you try to increase the system memory and running in dual controller mode, please make sure both controllers have the same DIMM on each corresponding memory slot. Failing to do so will result in controller malfunction, which will not be covered by warranty.
- Be aware that when the LED of the Controller Health is in RED, please DO NOT unplug the controller from the system or turn off the power suddenly. This may cause unrecoverable damage, which will not be covered by warranty.

6.9.1 Perform I/O

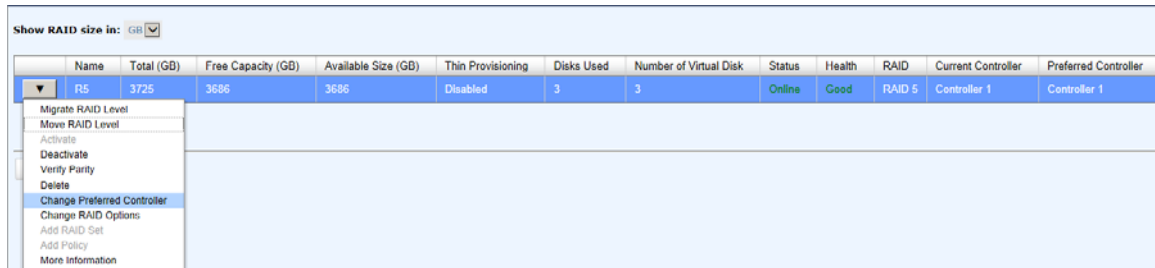
Please refer to the following topology and have all the connections ready. To perform I/O on dual controllers, server/host should setup MPIO. MPIO policy will keep I/O running and prevent fail connection with single controller failure.



6.9.2 Ownership

When creating a RAID group, it will be assigned with a preferred owner, the default owner is controller 1. To change the ownership of the RAID group, please follow the procedures.

1. In **Volume Configuration -> RAID Group** tab, selects a RAID group. And then click ▼ -> **Change Preferred Controller**.



2. Click **OK** to apply. The ownership of the RG will be switched to the other controller.

6.9.3 Controller Status

There are four statuses in dual controller. It is displayed at Status column in **System Maintenance - > System Information**. Describe on the following.

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 RAID group will switch to good one. For example: if controller 1 which owns the RAID group 1 fails accidentally, the ownership of RAID group 1 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 RAID groups will be assigned back to their preferred 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 and MUX 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 RAID group.

6.9.4 Change Controller Mode

The operation mode can be changed from Single to Dual or vice versa. Here is the procedures.

1. In **System Maintenance** -> **Upgrade** tab, choose **Single** or **Dual** in the drop-down list.

Controller Mode	
Operation Mode:	Dual <input type="button" value="v"/>
<input type="button" value="Apply"/>	

2. Click **Apply** button, it will pop up a warning message, click OK button to confirm.

6.9.5 Recommend iSNS Server

In addition, iSNS server is recommended. It's important for keeping I/O running smoothly when the ownership of the RAID group is switching or one of the dual controllers fails. For example of without iSNS server, when the controller 1 fails, the running I/O from host to controller 1 may fail because the host switches to new portal is slower at the moment and it may cause I/O time out. With iSNS server, this case would not happen.

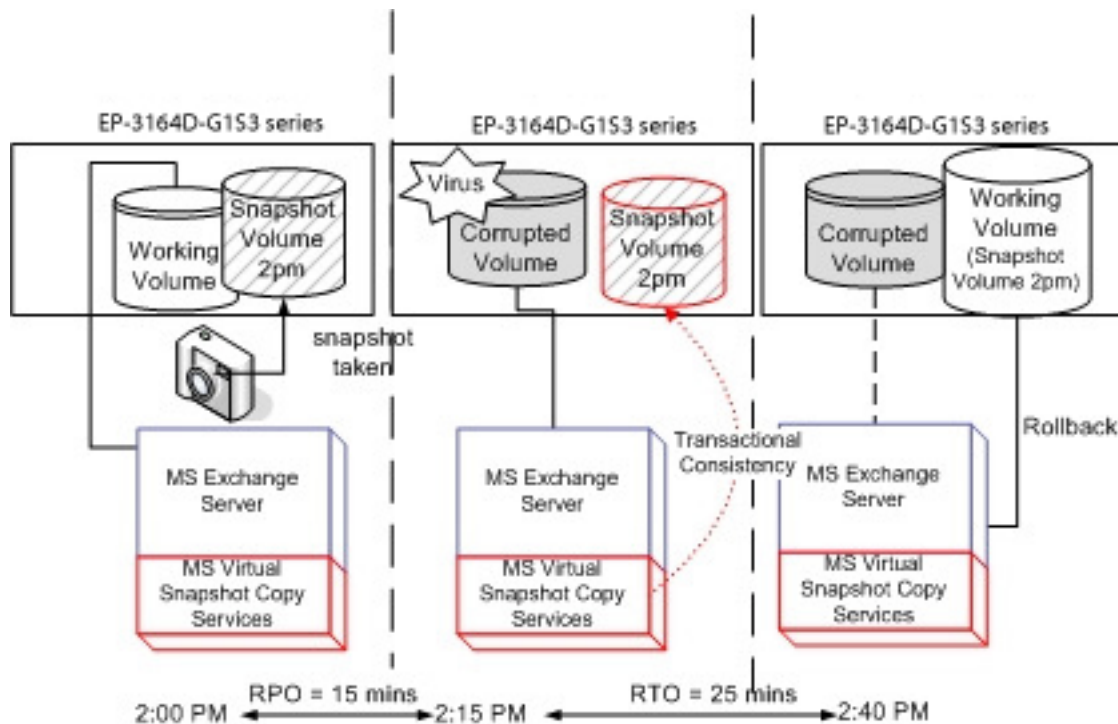


NOTE:

iSNS server is recommended for dual controller system of iSCSI interfaces.

6.10 Snapshot / Rollback

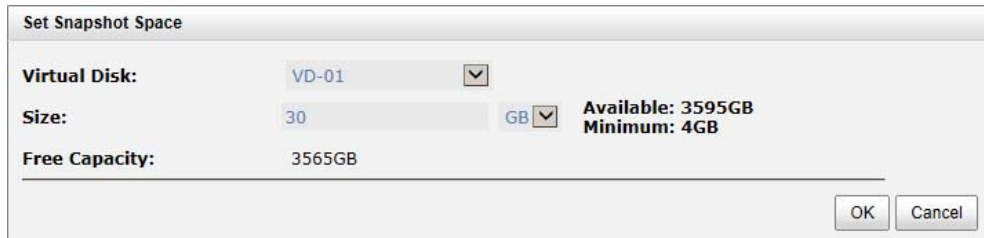
Snapshot-on-the-box captures the instant state of data in the target volume in a logical sense. The underlying logic is Copy-on-Write -- moving out the data which would be written to certain location where a write action occurs since the time of data capture. The certain location, named as Snap VD, is 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.



6.10.1 Take a Snapshot

Take an example of taking a snapshot.

1. Before taking a snapshot, it must reserve some storage space for saving variant data. There are two methods to set snapshot space. In **Virtual Disks** tab, selects a virtual disk. And then click ▼ -> **Set Snapshot Space** or in Snapshots tab, click **Set Snapshot Space** button.

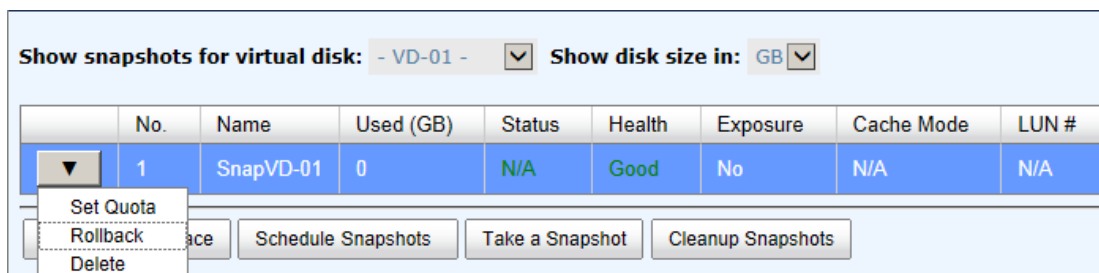


The 'Set Snapshot Space' dialog box shows the following fields:

- Virtual Disk:** VD-01 (selected from a dropdown)
- Size:** 30 (input field) GB (unit dropdown)
- Free Capacity:** 3565GB
- Available:** 3595GB
- Minimum:** 4GB

Buttons: OK, Cancel

2. Enter a **Size** which is reserved for the snapshot space, and then click **OK** button. The minimum size is suggested to be 20% of the virtual disk size. Now there are two numbers in **Snapshot Space (GB)** column in **Virtual Disks** tab. They mean used snapshot space and total snapshot space.
3. There are two methods to take snapshot. In Virtual Disks tab, selects a virtual disk. And then click ▼ -> **Take a Snapshot** or in Snapshots tab, click **Take a Snapshot** button.
4. Enter a Snapshot Name, and then click OK button. The snapshot is taken.



The Snapshots tab interface shows the following:

- Show snapshots for virtual disk:** - VD-01 - (dropdown)
- Show disk size in:** GB (dropdown)

	No.	Name	Used (GB)	Status	Health	Exposure	Cache Mode	LUN #
▼	1	SnapVD-01	0	N/A	Good	No	N/A	N/A

Buttons: Set Quota, Rollback, Delete, Schedule Snapshots, Take a Snapshot, Cleanup Snapshots

5. Set quota to expose the snapshot. Click ▼ -> **Set Quota** option.



The 'Set Quota' dialog box shows the following fields:

- Size:** 26 (input field) × GB (unit dropdown)
- Available Space:** 26 GB

Buttons: OK, Cancel

6. Enter a size which is reserved for the snapshot. If the size is zero, the exposed snapshot will be read only. Otherwise, the exposed snapshot can be read / written, and the size will be the maximum capacity for writing.
7. Attach LUN to the snapshot.

8. Done. The Snapshot can be used.

6.10.2 Cleanup Snapshots

To cleanup all the snapshots, please follow the procedures.

1. There are two methods to cleanup snapshots. In **Virtual Disks** tab, selects a virtual disk. And then click ▼ -> **Cleanup Snapshots** or in Snapshots tab, click **Cleanup Snapshots** button.
2. Click **OK** to apply. It will delete all snapshots of the virtual disk and release the snapshot space.

6.10.3 Schedule Snapshots

The snapshots can be taken by schedule such as hourly or daily. Please follow the procedures.

1. There are two methods to set schedule snapshots. In Virtual Disks tab, selects a virtual disk. And then click ▼ -> Schedule Snapshots or in Snapshots tab, click Schedule Snapshots button.
2. Check the schedules which you want. They can be set by monthly, weekly, daily, or hourly. Check Auto Mapping to attach LUN automatically when the snapshot is taken. And the LUN is allowed to access by Allowed Hosts.
3. Click OK to apply.



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

6.10.4 Rollback

The data in snapshot can rollback to the original virtual disk. Please follow the procedures.

1. In Snapshots tab, selects a snapshot. And then click ▼ -> Schedule Rollback.
2. Click OK to apply.



CAUTION:

Before executing rollback, it is better that the disk is unmounted on the host computer for flushing data from cache.

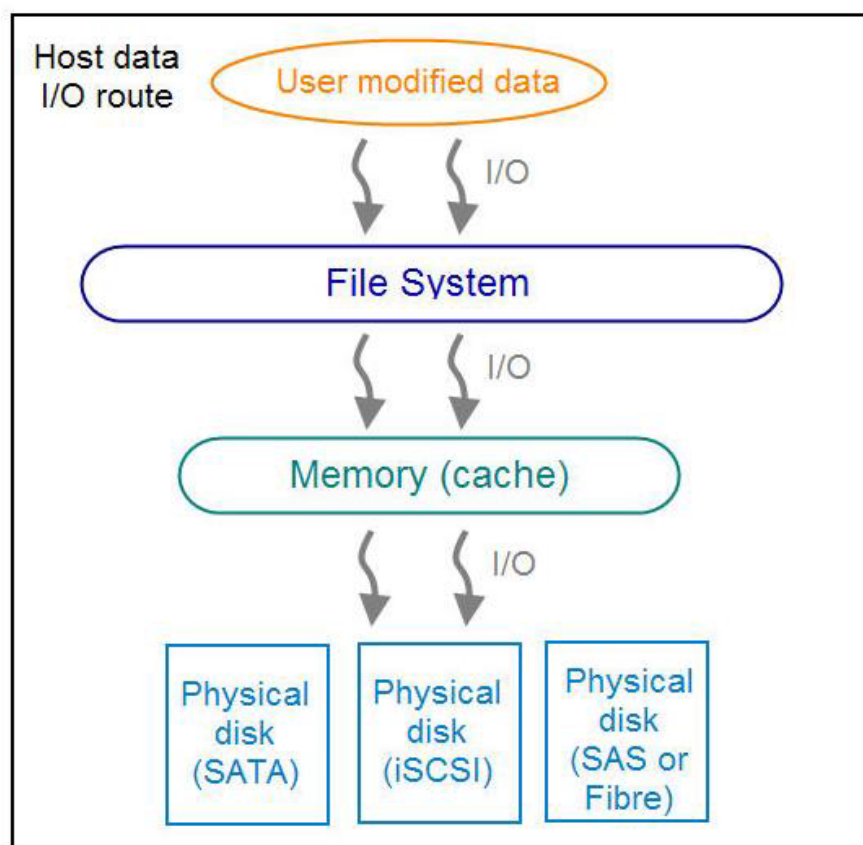
6.10.5 Snapshot Constraint

Snapshot function applies Copy-on-Write technique on virtual disk and provides a quick and efficient backup methodology. When taking a snapshot, it does not copy any data at first time until a request of data modification comes in. The snapshot copies the original data to snapshot space and then overwrites the original data with new changes. With this technique, snapshot only copies the changed data instead of copying whole data. It will save a lot of disk space.

- Create a data-consistent snapshot

Before using snapshot, user has to know why sometimes the data corrupts after rollback of snapshot. Please refer to the following diagram.

When user modifies the data from host, the data will pass through file system and memory of the host (write caching). Then the host will flush the data from memory to physical disks, no matter the disk is local disk (IDE or SATA), DAS (SCSI or SAS), or SAN (fibre or iSCSI). From the viewpoint of storage device, it cannot control the behavior of host side. This case maybe happens. If a snapshot is taken, some data is still in memory and not flush to disk. Then the snapshot may have an incomplete image of original data. The problem does not belong to the storage device. To avoid this data inconsistent issue between snapshot and original data, user has to make the operating system flush the data from memory of host (write caching) into disk before taking snapshot.



On Linux and UNIX platform, a command named sync can be used to make the operating system flush data from write caching into disk. For Windows platform, Microsoft also provides a tool – sync, which can do exactly the same thing as the sync command in Linux/UNIX. It will tell the OS to flush the data on demand. For more detail about sync tool, please refer to: <http://technet.microsoft.com/en-us/sysinternals/bb897438.aspx>

Besides the sync tool, Microsoft develops VSS (volume shadow copy service) to prevent this issue. VSS is a mechanism for creating consistent point-in-time copies of data known as shadow copies. It is a coordinator between backup software, application (SQL or Exchange...) and storages to make sure the snapshot without the problem of data-inconsistent. For more detail about the VSS, please refer to <http://technet.microsoft.com/enus/library/cc785914.aspx>. The storage system can support Microsoft VSS.

- What if the snapshot space is over?

Before using snapshot, a snapshot space is needed from RAID group capacity. After a period of working snapshot, what if the snapshot size over the snapshot space of user defined? There are two different situations:

1. If there are two or more snapshots existed, the system will try to remove the oldest snapshots (to release more space for the latest snapshot) until enough space is released.
2. If there is only one snapshot existed, the snapshot will fail. Because the snapshot space is run out.

For example, there are two or more snapshots existed on a virtual disk and the latest snapshot keeps growing. When it comes to the moment that the snapshot space is run out, the system will try to remove the oldest snapshot to release more space for the latest snapshot usage. As the latest snapshot is growing, the system keeps removing the old snapshots. When it comes that the latest snapshot is the only one in system, there is no more snapshot space which can be released for incoming changes, then snapshot will fail.

- How many snapshots can be created on a virtual disk?

There are up to 64 snapshots can be created per virtual disk. What if the 65th snapshot has been taken? There are two different situations:

1. If the snapshot is configured as schedule snapshot, the latest one (the 65th snapshot) will replace the oldest one (the first snapshot) and so on.
2. If the snapshot is taken manually, when taking the 65th snapshot will fail and a warning message will be showed on Web UI.

- Rollback and delete snapshot

When a snapshot has been rollbacked, the related snapshots which are earlier than it will also be removed. But the rest snapshots will be kept after rollback. If a snapshot has been deleted, the other snapshots which are earlier than it will also be deleted. The space occupied by these snapshots will be released after deleting.

6.11 Clone

Clone function can backup data from the source virtual disk to target. Here is the clone operation. At the beginning, copy all data from the source virtual disk to target. It is also called full copy. Afterwards, use snapshot technology to perform the incremental copy. Please be fully aware that the incremental copy needs to use snapshot to compare the data difference. Therefore, the enough snapshot space for the virtual disk is very important. Of course, clone job can also be set as schedule.

6.11.1 Setup Clone

Take an example of clone the virtual disk.

1. Before cloning, it must prepare backup target virtual disk. In Virtual Disks tab, click Create button. And then select Disk Type to Backup Target.

Create a Virtual Disk

Virtual Disk Name: SourceVD

Data Storage: R5

Size: 10 GB

Stripe Size (KB): 64

Block Size (Bytes): 512

Cache Mode: ☐ Write-through Cache ☒ Write-back Cache

Priority: ☒ High Priority ☐ Medium Priority ☐ Low Priority

Bg Rate: 4

Read-Ahead: Enabled

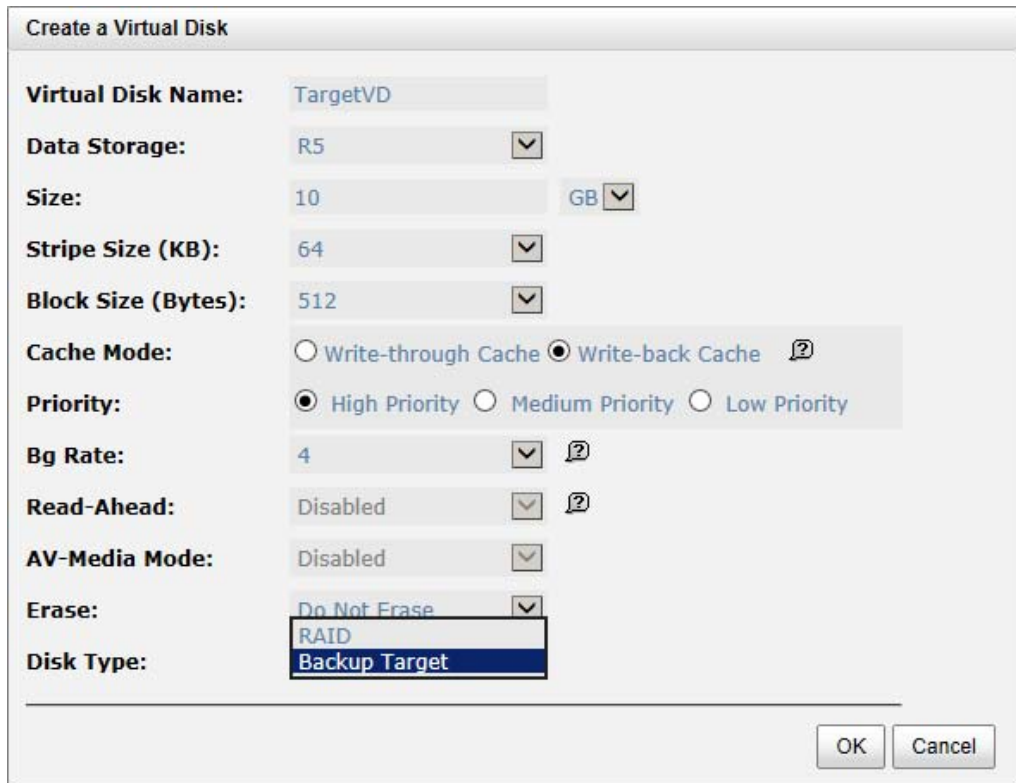
AV-Media Mode: Disabled

Erase: Do Not Erase

Disk Type: RAID, Backup Target

OK Cancel

Figure 1: Source side



Create a Virtual Disk

Virtual Disk Name: TargetVD

Data Storage: R5

Size: 10 GB

Stripe Size (KB): 64

Block Size (Bytes): 512

Cache Mode: ☐ Write-through Cache ☒ Write-back Cache

Priority: ☒ High Priority ☐ Medium Priority ☐ Low Priority

Bg Rate: 4

Read-Ahead: Disabled

AV-Media Mode: Disabled

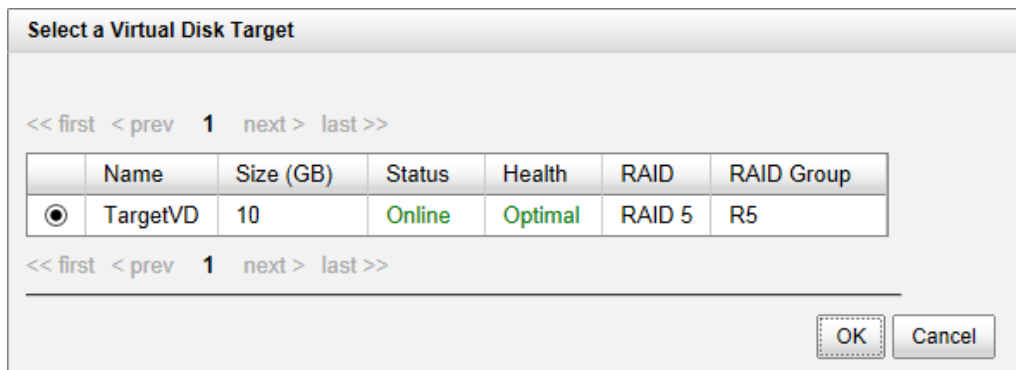
Erase: Do Not Erase

Disk Type: RAID
Backup Target

OK Cancel

Figure 2: Target side

2. Select the source virtual disk, and then click ▼ -> Set Clone.
3. Select a target virtual disk, and then click OK button.



Select a Virtual Disk Target

<< first < prev 1 next > last >>

	Name	Size (GB)	Status	Health	RAID	RAID Group
<input checked="" type="radio"/>	TargetVD	10	Online	Optimal	RAID 5	R5

<< first < prev 1 next > last >>

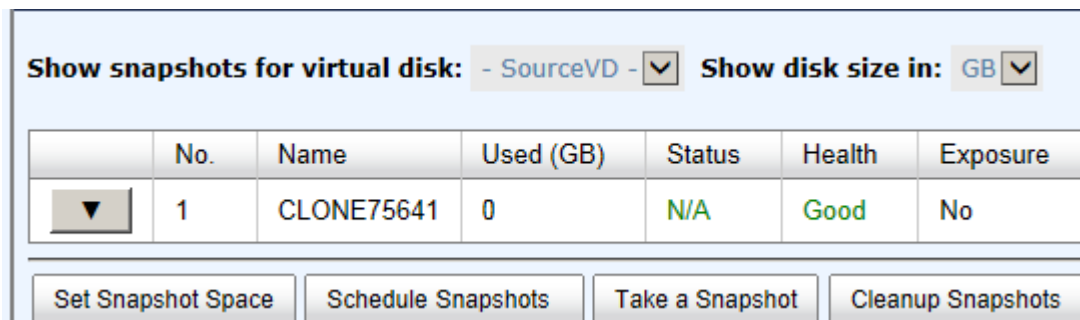
OK Cancel

4. At this time, if the source virtual disk has no snapshot space, it will be allocated snapshot space for clone usage automatically. The size will depend on the parameter of Cloning Options.

6.11.2 Start and Stop Clone

To start clone, please follow the procedures.

1. Select the source virtual disk, and then click ▼ -> **Start Clone**.
2. Click **OK** button. The source virtual disk will take a snapshot, and then start cloning.



Show snapshots for virtual disk: - SourceVD - ▼ Show disk size in: GB ▼

	No.	Name	Used (GB)	Status	Health	Exposure
▼	1	CLONE75641	0	N/A	Good	No

Set Snapshot Space Schedule Snapshots Take a Snapshot Cleanup Snapshots

To stop clone, please follow the procedures.

1. Select the source virtual disk, and then click ▼ -> **Stop Clone**.
2. Click **OK** button to stop cloning.

6.11.3 Schedule Clone

The clone job can be set by schedule such as hourly or daily. Please follow the procedures.

1. Select the source virtual disk, and then click ▼ -> **Schedule Clone**.
2. Check the schedules which you want. They can be set by monthly, weekly, daily, or hourly. Click **OK** to apply.

Clone - Set Clone Schedule

Set Clone Schedule: SourceVD

Months in the Year:

☐ All
☐ 01 ☐ 02 ☐ 03 ☐ 04
☐ 05 ☐ 06 ☐ 07 ☐ 08
☐ 09 ☐ 10 ☐ 11 ☐ 12

Weeks in the Month:

☐ All
☐ 1 ☐ 2 ☐ 3 ☐ 4
☐ 5

Days of the Week:

☐ All
☐ Sun ☐ Mon ☐ Tue ☐ Wed
☐ Thu ☐ Fri ☐ Sat

Hours in the Day:

☐ All
☐ 00 ☐ 01 ☐ 02 ☐ 03
☐ 04 ☐ 05 ☐ 06 ☐ 07
☐ 08 ☐ 09 ☐ 10 ☐ 11
☐ 12 ☐ 13 ☐ 14 ☐ 15
☐ 16 ☐ 17 ☐ 18 ☐ 19
☐ 20 ☐ 21 ☐ 22 ☐ 23

Minutes in the Hour:

☐ All
☐ 00 ☐ 15 ☐ 30 ☐ 45

OK

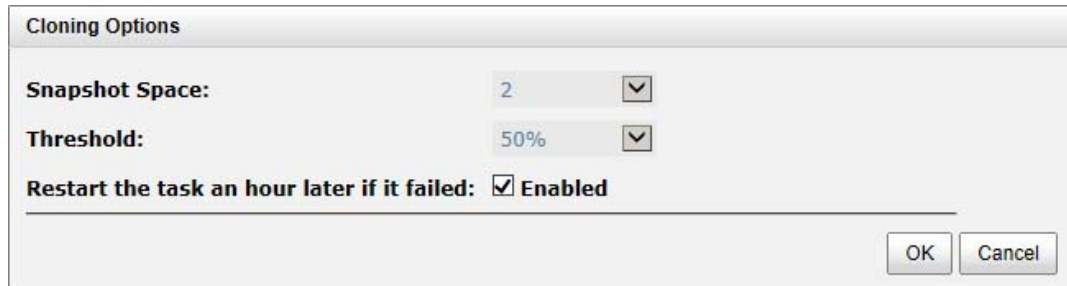
Cancel



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

6.11.4 Cloning Options

There are three clone options, described on the following.



The image shows a 'Cloning Options' dialog box with the following settings:

- Snapshot Space:** A dropdown menu set to '2'.
- Threshold:** A dropdown menu set to '50%'.
- Restart the task an hour later if it failed:** A checkbox labeled 'Enabled' that is checked.

At the bottom right of the dialog are 'OK' and 'Cancel' buttons.

- **Snapshot Space:** This setting is the ratio of the source virtual disk and snapshot space. If the ratio sets to 2, it means when the clone process is starting, the system will book the free RAID group space to set as the snapshot space which capacity is double the source virtual disk automatically. The options are 0.5 ~ 3.
- **Threshold:** The setting will be effective after enabling schedule clone. The threshold will monitor the usage amount of the snapshot space. When the used snapshot space achieves the threshold, system will take a snapshot and start clone process automatically. The purpose of threshold could prevent the incremental copy failure immediately when running out of the 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 start clone job automatically. And then continue monitoring the snapshot space. When the rest snapshot space has been used 50%, in other words, the total snapshot space has been used 75%, the system will start clone job again.
- **Restart the task an hour later if failed:** The setting will be effective after enabling schedule clone. When running out of the snapshot space, the virtual disk clone process will be stopped because there is no more available snapshot space. If this option is checked, the system will clear the snapshots of clone in order to release snapshot space automatically, and the clone task will be restarted after an hour. This task will start a full copy.



CAUTION:

The default snapshot space allocated by the system is two times the size of source virtual disk. That is the best value of our suggestion. If user sets snapshot space by manually and lower than the default value, user should take the risk if the snapshot space is not enough and the clone job will fail.

6.11.5 Clear Clone

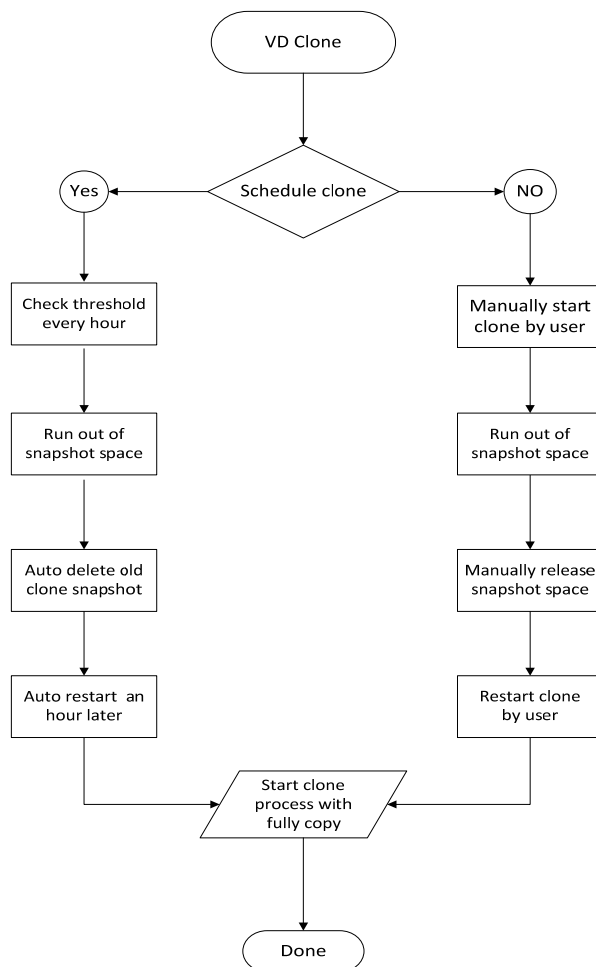
To clear the clone job, please follow the procedures.

1. Select the source virtual disk, and then click ▼ -> **Clear Clone**.
2. Click **OK** button to clear clone job.

6.11.6 Clone Constraint

While the clone is processing manually, the increment data of the virtual disk is over the snapshot space. The clone will complete the task, but the clone snapshot will fail. At the next time, when trying to start clone, it will get a warning message "This is not enough of snapshot space for the operation". 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 the next clone process.

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



6.12 QReplicas

QReplicas function can replicate data easily through LAN or WAN from one system to another. Here is the replication operation. At the beginning, copy all data from the source virtual disk to target. It is also called full copy. Afterwards, use snapshot technology to perform the incremental copy. Please be fully aware that the incremental copy needs to use snapshot to compare the data difference. Therefore, the enough snapshot space for the virtual disk is very important. Of course, replication task can also be set as schedule.

6.12.1 Create QReplica Task

Take an example of creating the QReplica task.

1. Before replication, it must prepare backup target virtual disk. In Virtual Disks tab of the target side, click Create button. And then select Disk Type to Backup Target.

Create a Virtual Disk

Virtual Disk Name: SourceVD

Data Storage: R5

Size: 10 GB

Stripe Size (KB): 64

Block Size (Bytes): 512

Cache Mode: ☐ Write-through Cache ☒ Write-back Cache

Priority: ☒ High Priority ☐ Medium Priority ☐ Low Priority

Bg Rate: 4

Read-Ahead: Enabled

AV-Media Mode: Disabled

Erase: Do Not Erase

Disk Type: RAID, Backup Target

OK Cancel

Figure 1: Source Side

Figure 2: Target Side

2. After creating the target virtual disk, please also setup snapshot space. The snapshot of the source virtual disk can replicate to the target virtual disk. In Virtual Disks tab, selects the backup virtual disk. And then click ▼ -> Set Snapshot Space.
3. Enter a Size which is reserved for the snapshot space, and then click OK button.
4. Attach LUN of the source and target virtual disk separately.

	Name	Size (GB)	Write	Priority	Bg Rate	Type
▼	SourceVD	10	WB	HI	4	RAID

Figure 3: Source Side

	Name	Size (GB)	Write	Priority	Bg Rate	Type
▼	TargetVD	10	WB	HI	4	BACKUP

Figure 4: Target Side

5. In QReplicas tab of the source side, click Create.

6. Select a target virtual disk, and then click Next button.

QReplica - Select a Source Virtual Disk

<< first < prev 1 next > last >>

	Name	Size (GB)	Status	RAID	LUN #	Snapshot #	RAID Group
<input checked="" type="radio"/>	SourceVD	10	Online	RAID 5	1	0	R5

<< first < prev 1 next > last >>

Next >> Cancel

7. Select the Source Port and input the Target IP, and then click Next button.

QReplica - Select Target IP Address

Source Port: LAN1

Target IP: 10.0.0.2

<< Back Next >> Cancel

8. Choose Authentication Method and input the CHAP user if needed. Select a Target Node, and then click Next button.

QReplca - Set iSCSI Authentication Information

Choose Authentication Method

☒ **No Authentication Method**

☐ CHAP

Users: (Max: 223)

Secret: (Min: 12, Max: 16)

Select a Target Node

	No.	Name
<input checked="" type="radio"/>	1	iqn.

<< Back Next >> Cancel

9. Select a Target LUN. When a replication job completes, it will take a snapshot on its target virtual disk. Please make sure the snapshot space of the backup virtual disk on the target side is properly configured. Finally, click Finish button.

QReplca - Select a Target LUN

When a replication job completes, it will take a snapshot on its target virtual disk. Please make sure the snapshot space of the backup virtual disk on the target side is properly configured.

	No.	LUN	Virtual Disk	Size (GB)	Vendor	Model	Serial Number
<input checked="" type="radio"/>	1	1	TargetVD	10			

<< Back Finish Cancel

10. The replication task is created.

Show disk size in: GB

Task:

	No.	Source Virtual Disk	Status	%	Shaping	Speed (MB)	Target Virtual Disk	Size (GB)
<input type="button" value="v"/>	1	SourceVD	Online		N/A	0	TargetVD	10

Task 'SourceVD' Path:

	No.	Source NIC	Target IP	Target Name	LUN	Status
<input type="button" value="v"/>	1	LAN1	10.0.0.2	iqn.	1	Connected

11. At this time, if the source virtual disk has no snapshot space, it will be allocated snapshot space for replication usage automatically. The size will depend on the parameter of QReplica Options.

6.12.2 Start and Stop QReplica Task

To start replication task, please follow the procedures.

1. In QReplicas tab of the source side, select the source virtual disk, and then click ▼ -> **Start**.
2. Click **OK** button. The source and target virtual disks will take snapshots, and then start replication.

Show disk size in: GB ▼

Task:

	No.	Source Virtual Disk	Status	%	Shaping	Speed (MB)	Target Virtual Disk	Size (GB)
▼	1	SourceVD	Online		N/A	0	TargetVD	10

Task 'SourceVD' Path:

	No.	Source NIC	Target IP	Target Name	LUN	Status
▼	1	LAN1	10.0.0.2	iqn.	1	Connected

Create Rebuild QReplica Options Shaping Setting Configuration

Figure 5: Source side

Show snapshots for virtual disk: - TargetVD - ▼ Show disk size in: GB ▼

	No.	Name	Used (GB)	Status	Health	Exposure
▼	1	QREP309461	0	N/A	Good	No

Set Snapshot Space Scheduled Snapshots Take a Snapshot Cleanup Snapshots

Figure 6: Target side

To stop replication task, please follow the procedures.

1. In **QReplicas** tab of the source side, select the source virtual disk, and then click ▼ -> **Stop**.
2. Click **OK** button to stop replication.

6.12.3 MPIO

To setup MPIO (Multi Path Input/Output) of the replication task, please follow the procedures.

1. Select the task in QReplicas tab, and then click ▼ -> Add Path.
2. Next steps are the same as the procedure of creating a new replication task.

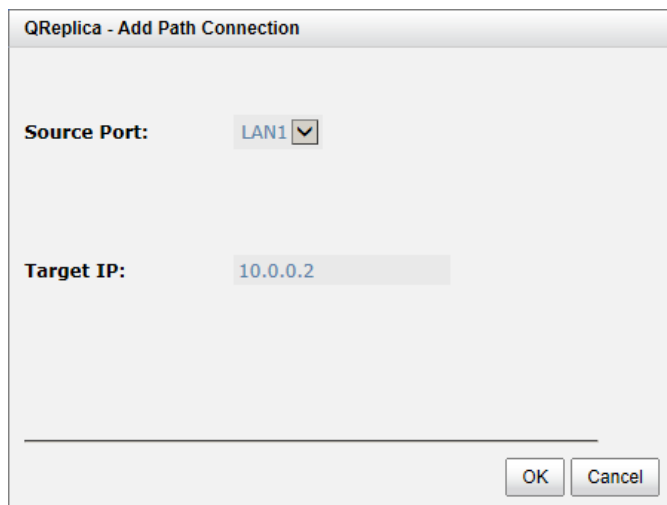
To delete multi path of the replication task, please follow the procedures.

1. Select the task in QReplicas tab, and then click ▼ -> Delete Path.
2. Select the path(s) which want to be deleted, and then click OK button.
3. The multi path(s) are deleted.

6.12.4 MC/S

To setup MC/S (Multiple Connections per Session) of the replication task path, please follow the procedures.

1. Select the task path in QReplicas tab, and then click ▼ -> Add Connection.



The screenshot shows a dialog box titled "QReplica - Add Path Connection". Inside the dialog, there are two main input areas. The first is labeled "Source Port:" and has a dropdown menu currently set to "LAN1". The second is labeled "Target IP:" and has a text input field containing the IP address "10.0.0.2". At the bottom right of the dialog, there are two buttons: "OK" and "Cancel".

2. Select the **Source Port** and input the **Target IP**, and then click **OK** button.
3. The connection is **added**.

To delete multi connections per session of the replication task path, please follow the procedures.

1. Select the task path in **QReplicas** tab, and then click ▼ -> **Delete** Connection.
2. Select the connection(s) which want to be deleted, and then click **OK** button.
3. The multi connection(s) are deleted.

6.12.5 Task Shaping

If the replication traffic affects the normal usage, we provide a method to limit it. There are eight shaping groups which can be set. In each shaping group, we also provide peak and off-peak time slot for different bandwidth. The following take an example of setting shaping group.

1. In QReplicas tab, click Shaping Setting Configuration button.

QReplica - Shaping Setting Configuration

Shaping Group: Shaping Group1 (Peak: 100MB; Off-peak: 200MB) ▼

Peak: 100 MB

☒ **Enable Off-Peak**

Off-Peak: 200 MB

	00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23
Sun.	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Mon.	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Tue.	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Wed.	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Thu.	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Fri.	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Sat.	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

OK Cancel

2. Select a Shaping Group to setup.
3. Input the bandwidth (MB) at the Peak time.
4. If needed, check **Enable Off-Peak**, and then input the bandwidth (MB) at **Off-Peak** time. And define the off-peak hour.
5. Click **OK** button.
6. In QReplicas tab, select the task, and then click ▼ -> **Set Task Shaping**.

QReplica - Set Task Shaping

Shaping: N/A

- Shaping Group1 (100MB)
- Shaping Group2 (100MB)
- Shaping Group3 (100MB)
- Shaping Group4 (100MB)
- Shaping Group5 (100MB)
- Shaping Group6 (100MB)
- Shaping Group7 (100MB)
- Shaping Group8 (100MB)

OK Cancel

7. Select a Shaping Group from the drop down list. And then click **OK** button.
8. The shaping group is applied to the replication task.

6.12.6 Schedule QReplica Task

The replication task can be set by schedule such as hourly or daily. Please follow the procedures.

1. In QReplicas tab, select the task, and then click ▼ -> **Schedule**.
2. Check the schedules which you want. They can be set by monthly, weekly, daily, or hourly. Click **OK** to apply.

QReplica - Set a QReplica Schedule

Set a QReplica Schedule: SourceVD

Months in the Year: ☐ All
☐ 01 ☐ 02 ☐ 03 ☐ 04
☐ 05 ☐ 06 ☐ 07 ☐ 08
☐ 09 ☐ 10 ☐ 11 ☐ 12

Weeks in the Month: ☐ All
☐ 1 ☐ 2 ☐ 3 ☐ 4
☐ 5

Days of the Week: ☐ All
☐ Sun ☐ Mon ☐ Tue ☐ Wed
☐ Thu ☐ Fri ☐ Sat

Hours in the Day: ☐ All
☐ 00 ☐ 01 ☐ 02 ☐ 03
☐ 04 ☐ 05 ☐ 06 ☐ 07
☐ 08 ☐ 09 ☐ 10 ☐ 11
☐ 12 ☐ 13 ☐ 14 ☐ 15
☐ 16 ☐ 17 ☐ 18 ☐ 19
☐ 20 ☐ 21 ☐ 22 ☐ 23

Minutes in the Hour: ☐ All
☐ 00 ☐ 15 ☐ 30 ☐ 45

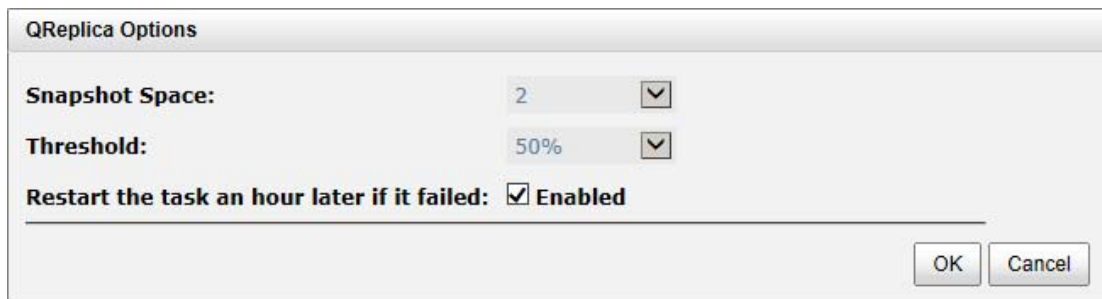
OK Cancel



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

6.12.7 QReplica Options

There are three QReplica options, described on the following.



QReplica Options

Snapshot Space: 2 ▼

Threshold: 50% ▼

Restart the task an hour later if it failed: ☒ Enabled

OK Cancel

- **Snapshot Space:** This setting is the ratio of the source virtual disk and snapshot space. If the ratio sets to 2, it means when the replication process is starting, the system will book the free RAID group space to set as the snapshot space which capacity is double the source virtual disk automatically. The options are 0.5 ~ 3.
- **Threshold:** The setting will be effective after enabling schedule replication. The threshold will monitor the usage amount of the snapshot space. When the used snapshot space achieves the threshold, system will take a snapshot and start replication process automatically. The purpose of threshold could prevent the incremental copy failure immediately when running out of the 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 start replication job automatically. And then continue monitoring the snapshot space. When the rest snapshot space has been used 50%, in other words, the total snapshot space has been used 75%, the system will start replication task again.
- **Restart the task an hour later if it failed:** The setting will be effective after enabling schedule replication. When running out of the snapshot space, the virtual disk replication process will be stopped because there is no more available snapshot space. If this option is checked, the system will clear the snapshots of replication in order to release snapshot space automatically, and the replication task will be restarted after an hour. This task will start a full copy.



CAUTION:

The default snapshot space allocated by the system is two times the size of source virtual disk. That is the best value of our suggestion. If user sets snapshot space by manually and lower than the default value, user should take the risk if the snapshot space is not enough and the replication task will fail.

6.12.8 Delete QReplica Task

To delete the replication task, please follow the procedures.

1. Select the task in **QReplicas** tab, and then click ▼ -> **Delete**.
2. Click **OK** button to delete the replication task.

6.12.9 Clone Transfers to QReplica

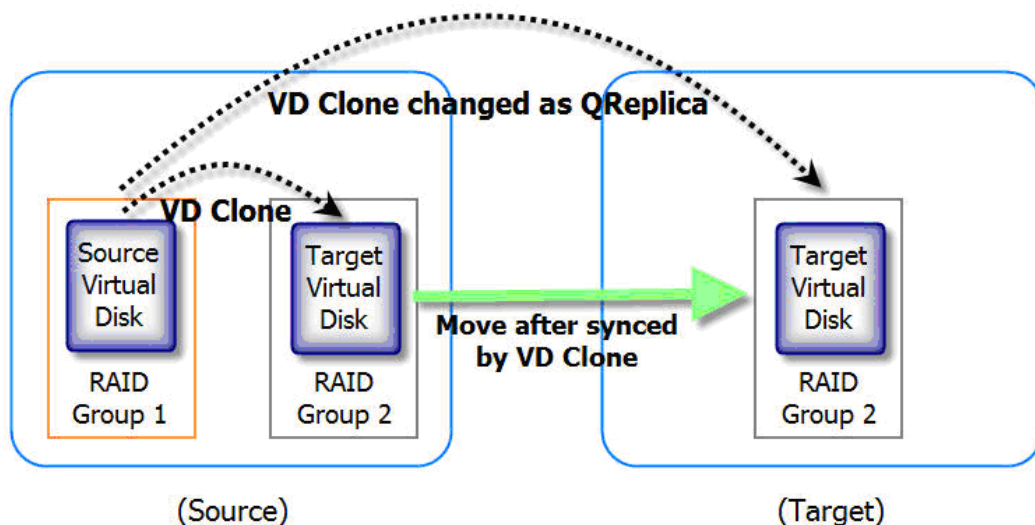
It is always being a problem that to do full copy over LAN or WAN when the replication task is executed at the first time. It may take days or weeks to replicate data from source to target within limited network bandwidth. We provide two methods to help user shorten the time of executing full copy.

1. One is to skip full copy on a new, clean virtual disk. The term "clean" means that the virtual disk has never been written data since created. For a new created virtual disk which has not been accessed, the system will recognized it and skip full copy automatically when the replication job is created on this virtual disk at the first time.



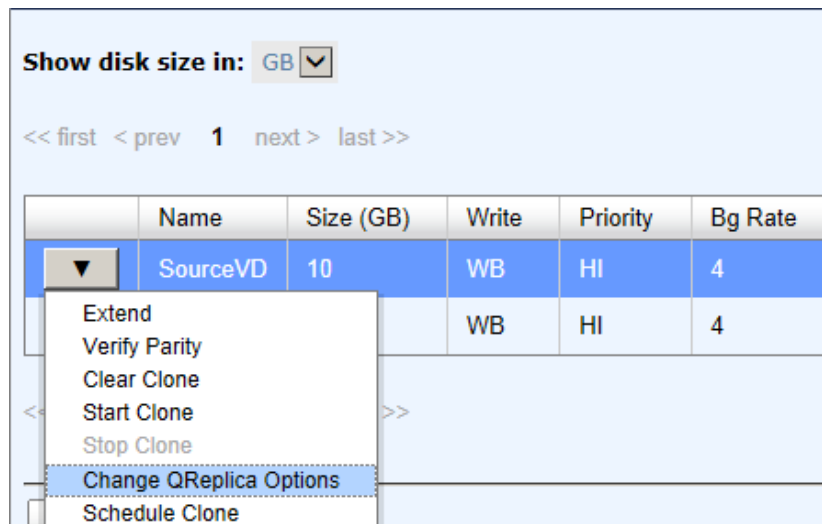
NOTE: Any IO access to the new created virtual disk will make it as "not clean", even though executing "Erase" function when a virtual disk is created. The full copy will take place in such a case.

2. The other way is to use virtual disk clone function, which is a local data copy function between virtual disks to execute full copy at the first time. Then move all the physical drives of the target virtual disk to the target system and then turn the cloning job into replication task with differential copy afterward.



To do that virtual disk clone transfers to QReplica, please follow the procedures.

1. Create a cloning job on an existing virtual disk with data stored already.
2. It is better that there is no host connected to the source virtual disk. Then run **Set Clone**, Start Clone to synchronize the data between source and target virtual disks.
3. After the data is synchronized, change the cloning job to a QReplica task. Select the source virtual disk, and then click ▼ -> **Change QReplica Options**.



4. The **Clone** status of the source virtual disk will be changed from the name of the target virtual disk into **QRep**.



CAUTION:

Changing a cloning job to a replication task is only available when the cloning job has been finished. This change is irreversible.

5. Deactivate the RAID group which the target virtual disk resides in and move all physical disks of the RAID group to the target system. Then activate the RAID group in the target system. Remember to set snapshot space for the target virtual disk. And then attach the target virtual disk to a LUN ID.
6. In Volume Configuration -> QReplicas tab at the source side, click Rebuild button to rebuild the replication task which is changed from a cloning job formerly.
7. Rebuild the clone relationship, select a source virtual disk.

Rebuild the Clone Relationship - Select a Source Virtual Disk

<< first < prev 1 next > last >>

	Name	Size (GB)	Status	RAID	LUN #	Snapshot #	RAID Group
<input checked="" type="radio"/>	SourceVD	10	Online	RAID 5	1	1	R5

<< first < prev 1 next > last >>

Next >> Cancel

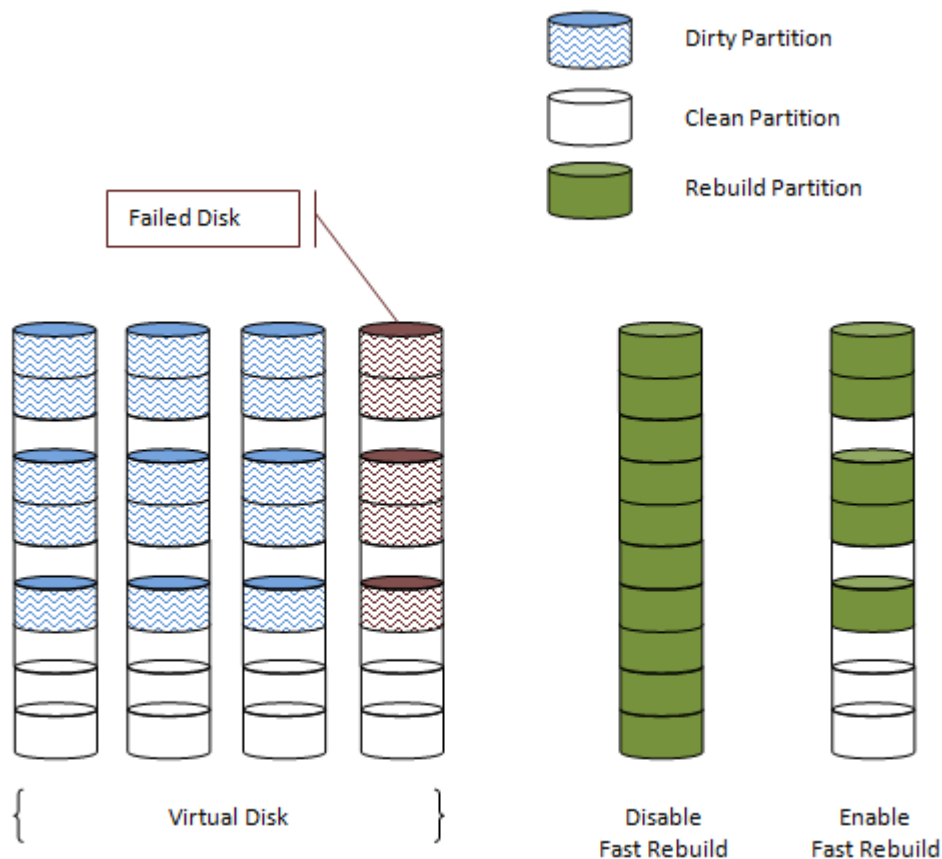
8. Next steps are the same as the procedure of creating a new replication task.
9. If a wrong target virtual disk is selected when rebuilding the replication task, there will be an alert and the system stops the creation.

6.13 Fast Rebuild

When executing rebuild, the Fast Rebuild feature skips any partition of the virtual disk where no write changes have occurred, it will focus only on the parts that have changed. This mechanism may reduce the amount of time needed for the rebuild task. It also reduces the risk of RAID failure caused by reducing the time required for the RAID status from degraded mode to healthy. At the same time, it frees up CPU resources more quickly to be available for other I/O and demands.

6.13.1 Solution

Without Fast Rebuild feature, rebuild will start from the beginning partition to the end. It may spend lots of time to complete the task. When enabling Fast Rebuild feature, it will rebuild the partition with the changed only.



NOTE:

With less changed partition, the Fast Rebuild feature may go faster. If the virtual disk is full of changed partition. The rebuild may take the same time without Fast Rebuild feature.

6.13.2 Configuration

When creating a virtual disk, enable the Fast Rebuild. The default is disabled.

The screenshot shows the 'Create a Virtual Disk' configuration window. The 'Fast Rebuild' option is currently set to 'Disabled', but the dropdown menu is open, showing 'Enabled' as the selected option. Other configuration options include: Virtual Disk Name (VD-01), Data Storage (R5), Size (30 GB), Stripe Size (KB) (64), Block Size (Bytes) (512), Cache Mode (Write-back Cache), Priority (High Priority), Bg Rate (4), Read-Ahead (Enabled), AV-Media Mode (Disabled), Erase (Do Not Erase), and Disk Type (RAID). The 'OK' and 'Cancel' buttons are at the bottom right.

6.13.3 Constraint

Here are some constraints about Fast Rebuild.

- Only thick/fat RAID group supports this feature. Thin provision RAID group already has this feature implement.
- When rebuild happened in a fast rebuild virtual disk, clean partitions are not rebuilt since there are no data saved there. Though clean partitions are never rebuilt, their health status is good.
- If all partitions of the fast rebuild virtual disk are clean, then no rebuild would happen and no event would be sent.
- The RAID stacks could not use optimize algorithm to compute parities of a partition which is not rebuilt. Thus, the performance of random write in a clean partition would be worse.



CAUTION:

The fast rebuild should not be enabled for a virtual disk whose access pattern is random write.

6.14 SSD Caching

The traditional storage technology is stored in the HDDs (Hard Disk Drives) and SSDs (Solid-State Drives) are mainly used in mission critical applications where the speed of the storage system needed to be as high as possible. In recent years, the capacity of HDDs has increased; but their random input/output (I/O) has not increased at the same rate. For some applications such as enterprise web with database, cloud and virtualization which require both high capacity and performance, HDDs have the superiority in capacity but lower speed. It means the pure HDD storage is not enough for those applications.

Using the superiority of SSDs, offer exceptionally high speed, SSD caching technology provides the best way to fulfill cost-effectively the performance and capacity requirements of their enterprise applications. Integrated HDDs and SSDs into the storage combine the benefits of both. SSD cache feature enables the system to use SSDs as extended cache, thus increasing the performance of random I/O applications such as databases, file servers, and web servers, etc.

Generally, the SSD caching is useful for the following features:

1. Due to the HDD IOPS, read performance cause the bottleneck.
2. In working space, read I/O is much more than write.
3. The best performance is in the case, the working data size is repeatedly accessed and smaller than the size of SSD cache capacity.

6.14.1 Solution

SSD caching is the secondary cache used to enable better performance. One and more SSDs could be assigned to a single virtual disk to be its SSD caching space. Be attention that the cache volume is not available for regular data storage. Currently, the maximum SSD cache size allowed in a system is 2.4TB.

6.14.2 Methodology

When the read or write I/O performs, this feature copies the data from HDD into SSD. At the next time, any subsequent I/O read of the same logical block addresses can be read directly from SSD. It increases the overall performance with a much lower response time. If the SSDs fail unfortunately, you won't worry the data loss because the data caching in the SSD is a copy of the original which is residing on HDD.

SSD caching is divided into group of sectors of equal sizes. Each group is called a cache block; each block is divided into sub-blocks. The I/O type configured for a virtual disk would affects size of the cache block and size of sub-blocks.

6.14.3 Populating the Cache

The actions that read data from the HDD and write to the SSD are called populating the cache. It is a background operation that typically immediately follows a host read or write operation. The constraint is that two parameters are used to determine when to start a cache-populate operation:

1. Populate-on-read threshold: The value is great than zero. If it is zero, no action is performed for read cache.
2. Populate-on-write threshold: It's the same action as read.

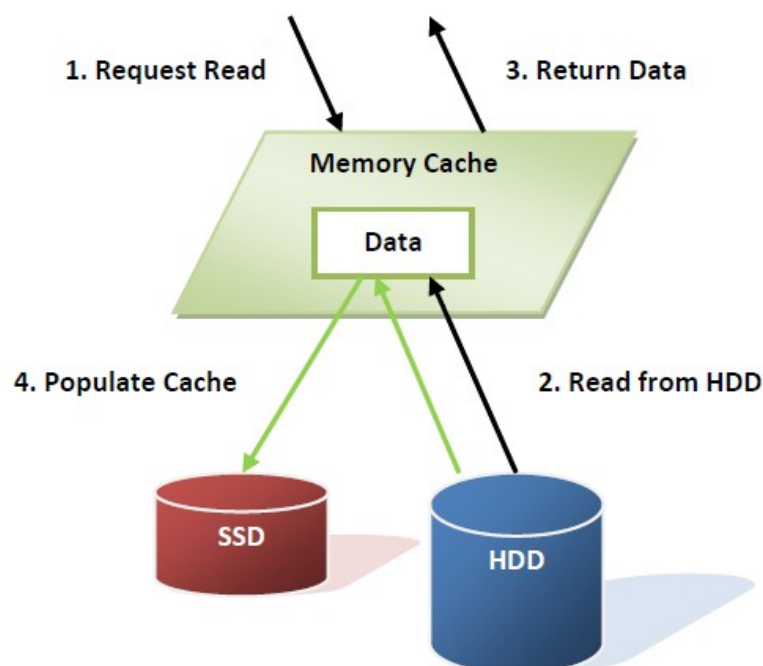
According to these values, each cache block has associated to its read and write counts. When a host requests the read data located on the cache block, its read count is increment. If a cache hit does not occur, and the read count is greater than or equal to the populate-on-read threshold, then a cache-populate operation is performed with the host read concurrently. If a cache hit occurs, a populate operation is not performed. If the read count is smaller than the threshold, the count continues and a populate operation is not performed neither.

For write cases, it's the same scenario as read. We provide the figures to describe more details on the following.

6.14.4 Read/Write Cache Cases

- Read Data with Cache Miss

The following figure shows the steps of the controller which handles a host read request when some of the data is not in the SSD cache.

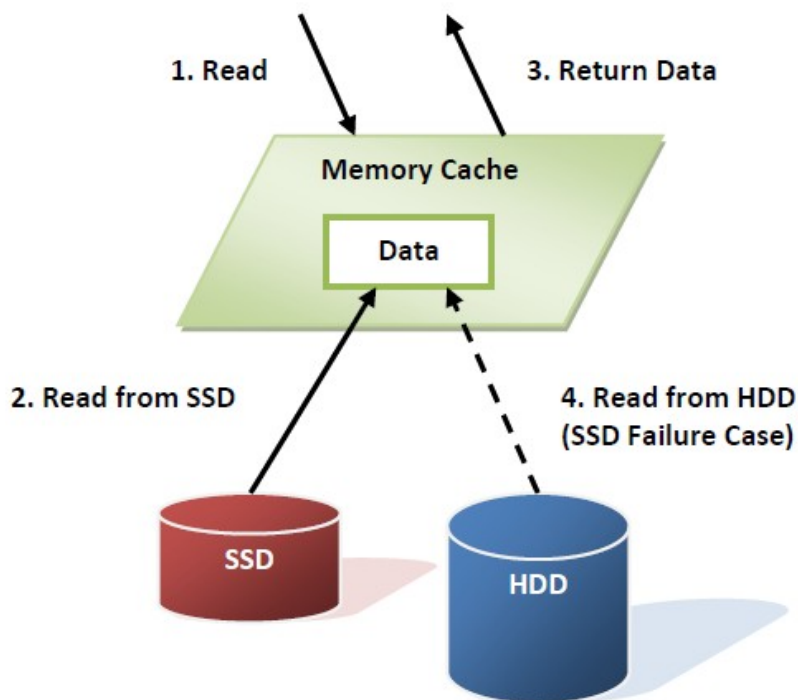


The following steps describe details about a host read with a cache miss:

1. A host requests a read data.
2. Read data from the HDD.
3. Return requested data to the host.
4. Populate the cache to SSD.

- **Read Data with Cache Hit**

The following figure shows the steps of the controller which handles a host read request when the data is in the SSD cache.

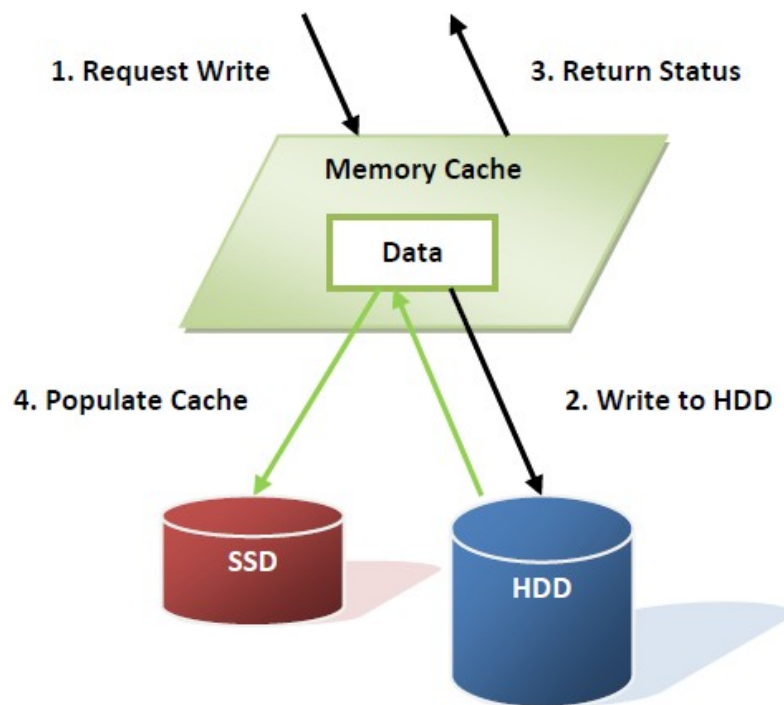


The following steps describe details about a host read with a cache hit:

1. A host requests a read data.
2. Read data from the SSD.
3. Return requested data to the host.
4. If SSD has error, read data from the HDD.

- Write Data

The following figure shows the steps of the controller which handles a host write request.



The following steps describe details about a host write:

1. A host requests a write data.
2. Write data to the HDD.
3. Return the status to the host.
4. Populate the cache to SSD.

6.14.5 I/O Type

The type of I/O access is a user-selectable SSD cache configuration. The user-selectable I/O type controls the SSD cache internal settings for cache block size, sub-block size, populate-on-read threshold, and populate-on-write threshold. Three pre-defined I/O types are supported; they are database, file system, and web service. The user can select an I/O type to set the SSD cache of a virtual disk. When enabled SSD caching, the user can also change it online. But the cached data would be purged if the I/O type is changed. You may select the suitable I/O types depends on the application to get the best performance. If the above three applications are not suitable, the last item is customization which you may set the configurations by yourself.

I/O Type	Block Size (Sectors)	Sub-block Size (Sectors)	Populate-on-Read Threshold	Populate-on-Wrote Threshold
Database	1MB (2,048)	8KB (16)	2	0
File System	2MB (4,096)	16KB (32)	2	2
Web Service	4MB (8,192)	64KB (128)	2	0
Web Service	1MB/2MB/4MB	8KB/16KB/64KB	≥ 0	≥ 0

The block size affects the cache use and the warm up time. The cache use shows how much of the allocated cache actually holds the user data. And the warm up time is the process of how long to fill the cache. You can image that the highest cache use is obtained when all of the frequently reread data is located very close to other data that is frequently reread. Using a larger cache block size of I/O type is more useful to performance than a smaller one. Conversely, when frequently reread data is located far from other data that is frequently reread, the lowest cache use is obtained. In this case, the lowest cache block size of I/O type allows the most user data to be cached.

The sub-block size affects the cache warm up time, too. A larger sub-block size causes cache to fill more quickly than a smaller one, but it can also affect the response time of host I/O. Also occupy the system resource, such as CPU utilization, memory bandwidth, or channel utilization. A very high locality of reference can be more useful from a larger sub-block size than from a smaller one, especially if those blocks that are reread frequently reside in the same sub-block. This occurs when one I/O causes the sub-block to be populated and another I/O in the same sub-block gets a cache hit.

These are tradeoff depend on the applications. Users may set them by experience to get the best performance. Here we provide a formula which can calculate the estimate warm up time.

We define that

- T: Warm up time; seconds required.
- I: Best random IOPS of HDD.
- S: I/O Size.
- D: Number of HDDs.
- C: Total SSD caching capacity.
- P: Populate-on-read or Populate-on-write threshold

We assume that random read/write from HDD to achieve the capacity of SSD should be

$$C * P = I * S * D * T$$

So we can estimate the warm up time, at least.

$$T = (C * P) / (I * S * D)$$

The real case may be longer than the estimate time. Here we take an example on the following.

- I: 250 IOPS (Random IOPS per HDD)
- S: 64KB (Web service)
- D: 16 HDDs
- C: 480GB (1 SSD)
- P: 2 (Populate-on-read threshold)

Warm up time $T = (480\text{GB} * 2) / (250 * 64\text{KB} * 16) = 3932.16$ seconds = 65.536 minutes

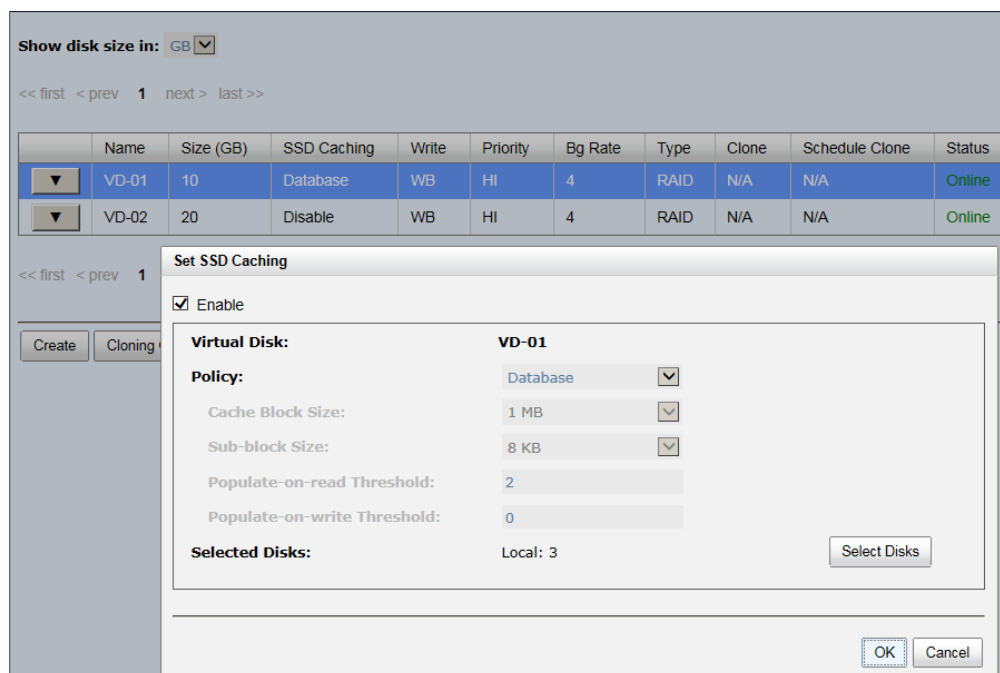
6.14.6 Configuration

Activate the license key

User needs to obtain a license key and download it to the system to activate the SSD caching function in **System Maintenance -> Upgrade -> SSD Caching License**. Each license key is unique and dedicated to a specific system. To obtain the license key, please contact sales for assistance.

Take an example of enabling SSD caching.

1. After creating a virtual disk, click ▼ -> **Set SSD Caching** of the selected virtual disk.
2. Check **Enable** box.
3. Select the policy by drop down menu.
4. Click **Select Disks** button, and then check the SSDs which are provided for SSD caching.
5. Click **OK** button to enable SSD caching.



6.14.7 Constraint

Here are some constraints about SSD caching.

- Only SSD could be used SSD caching space of a virtual disk.
- A SSD could be assigned to one and only one virtual disk as its caching space.
- Up to 8 SSDs could be used as SSD cache of a virtual disk.
- Support up to 2.4TB of SSD caching space in one system.

Chapter 7 Troubleshooting

7.1 System Buzzer

The system buzzer features are listed below:

- The system buzzer alarms 1 second when system boots up successfully.
- The system buzzer alarms continuously when there is error occurred. The alarm will be stopped after error resolved or be muted.
- 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

Physical Disk 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.
INFO	PD RPS started L2L	Assign PD <slot> to replace PD <slot>.
INFO	PD RPS finished L2L	PD <slot> is replaced by PD <slot>.
ERROR	PD RPS failed L2L	Failed to replace PD <slot> with PD <slot>.

Hardware 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 space
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 port reply error	SAS frontend reply terminated abnormally
INFO	FC port reply error	FC HBA port <number> reply terminated abnormally
INFO	FC unknown port reply error	FC frontend reply terminated abnormally
INFO	Port linkup	The Port <number> link status is changed to Up.
INFO	Port linkdown	The Port<number> link status is changed to Down.

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 reset	Watchdog timeout reset occurred

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 started	VD <name> starts migration.
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	VD attach LUN	LUN <number> is attached to VD <name>.
INFO	VD detach LUN	LUN <number> is detached from VD <name>.
INFO	RG activated	RG <name> has been manually activated.
INFO	RG deactivated	RG <name> has been manually deactivated.
DEBUG	VD rewrite started	Rewrite at LBA <address> of VD <name> starts.
DEBUG	VD rewrite finished	Rewrite at LBA <address> of VD <name> completes.
DEBUG	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>.
DEBUG	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>.
DEBUG	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 create global	Failed to create the global cache.
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.
WARNING	RG disk missing	RG <name> can not be activated because of missing disks.
ERROR	PD VD read write fault	Read error at LBA <address>-<address> of PD <slot> and rewrite failed at LBA <address>-<address> of VD <name>.
ERROR	PD IO retry fault	Over I/O retry limit in last 10 minutes on PD <slot>, replacing the disk is highly recommended.
ERROR	PD substitute L2L	Over I/O retry limit in last 10 minutes on PD <slot>, the disk is disabled for automatic rebuilding with PD <slot>.

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 failed	JBOD <name> PD [<string>] upgrade 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	JBOD SMART T.E.C	JBOD <name> disk <slot>: S.M.A.R.T. Threshold Exceed Condition occurred for attribute <string>
WARNING	JBOD SMART fail	JBOD <name> disk <slot>: Failure to get S.M.A.R.T information
INFO	JBOD CTR inserted	Controller(<number>) of JBOD <name> is inserted into system
WARNING	JBOD CTR iremoved	Controller(<number>) of JBOD <name> is removed from system
WARNING	JBOD degraded	JBOD <name> is in degraded mode.
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>.
DEBUG	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 OT	Temperature of <string> read as <string> in 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
INFO	JBOD HDD path NG	Path redundancy to JBOD <name> PD <number> is lost
INFO	PD RPS started L2F	Assign JBOD <name> PD <slot> to replace PD <slot>.
INFO	PD RPS started F2L	Assign PD <slot> to replace JBOD <name> PD <slot>.
INFO	PD RPS started F2F	Assign JBOD <name> PD <slot> to replace JBOD <name> PD <slot>.
INFO	PD RPS finished L2F	PD <slot> is replaced by JBOD <name> PD <slot>.
INFO	PD RPS finished F2L	JBOD <name> PD <slot> is replaced by PD <slot>.
INFO	PD RPS finished F2F	JBOD <name> PD <slot> is replaced by JBOD <name> PD <slot>.
ERROR	PD RPS failed L2F	Failed to replace PD <slot> with JBOD %4d PD <slot>.
ERROR	PD RPS failed F2L	Failed to replace JBOD <name> PD <slot> with PD <slot>.
ERROR	PD RPS failed F2F	Failed to replace JBOD <name> PD <slot> with JBOD <name> PD <slot>.
ERROR	PD VD read write fault	Read error at LBA <address>-<address> of JBOD <name> PD <slot> and rewrite failed at LBA <address>-<address> of VD <name>.
ERROR	PD IO retry fault	Over I/O retry limit in last 10 minutes on JBOD <name> PD <slot>, replacing the disk is highly recommended.
ERROR	PD substitute L2F	Over I/O retry limit in last 10 minutes on PD <slot>, the disk is disabled for automatic rebuilding with JBOD <name> PD <slot>.
ERROR	PD substitute F2L	Over I/O retry limit in last 10 minutes on JBOD <name> PD <slot>, the disk is disabled for automatic rebuilding with PD <slot>.

ERROR	PD substitute F2F	Over I/O retry limit in last 10 minutes on JBOD <name> PD <slot>, the disk is disabled for automatic rebuilding with JBOD <name> PD <slot>.
-------	-------------------	---

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 complete	All volumes in controller <number> completed 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	Replication portal is enabled
INFO	Qrep portal disabled	Replication portal is disabled
INFO	VD replicate started	VD <name> starts replication process.
INFO	VD replicate finished	VD <name> finished replication process.
WARNING	VD replicate failed	The replication in VD <name> 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>.

QThin Events

Level	Type	Description
WARNING	RG threshold hit	The used capacity of RG <name> exceeds <number> percent.
INFO	RAID set created	RAID set <number> has been added into RG <name>.
INFO	RAID set deleted	RAID set <number> was deleted from RG <name>.
INFO	VD reclaim started	VD <name> starts space reclamation process.
INFO	VD reclaim completed	VD <name> finished space reclamation process.
WARNING	VD reclaim aborted	The space reclamation in VD <name> was aborted.

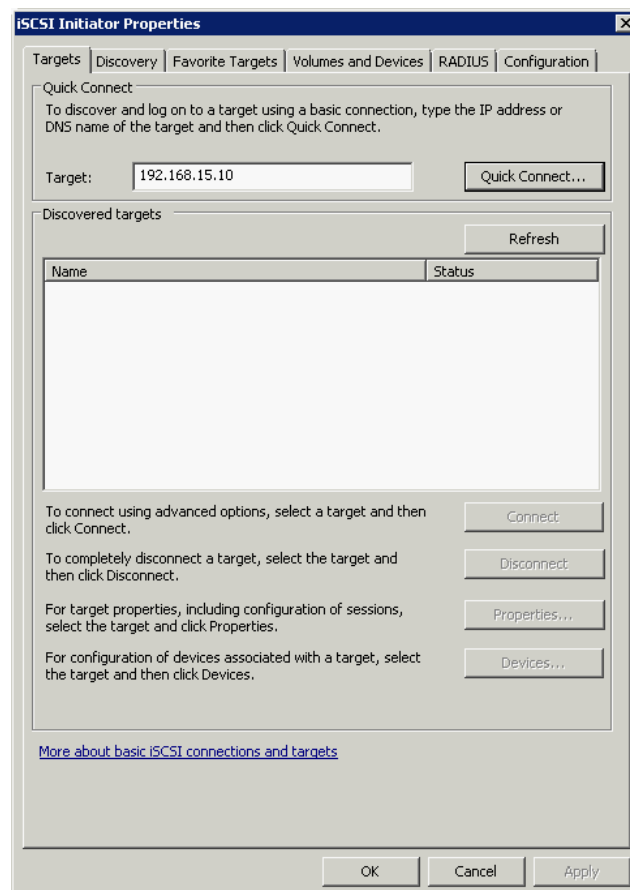
- DEBUG level events are displayed in download event log file only.

Appendix

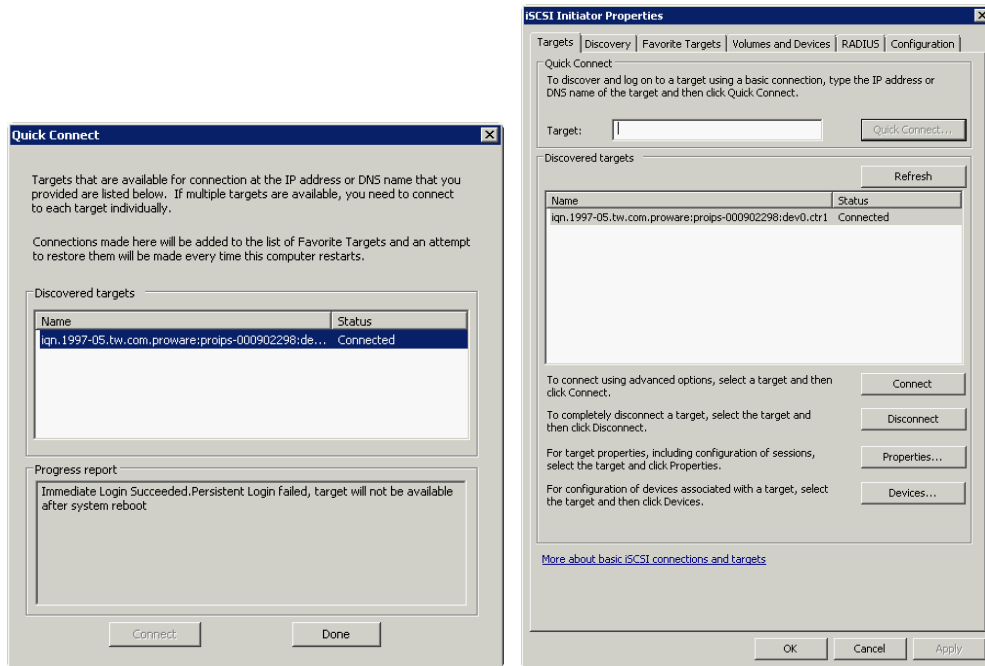
A. Microsoft iSCSI initiator

Here is the step by step to setup Microsoft iSCSI Initiator. Please visit Microsoft website for latest iSCSI initiator. This example is based on Microsoft Windows Server 2008 R2.

- Connect
 1. Run Microsoft iSCSI Initiator.
 2. Input IP address or DNS name of the target. And then click **Quick Connect**.



3. Click **Done**.



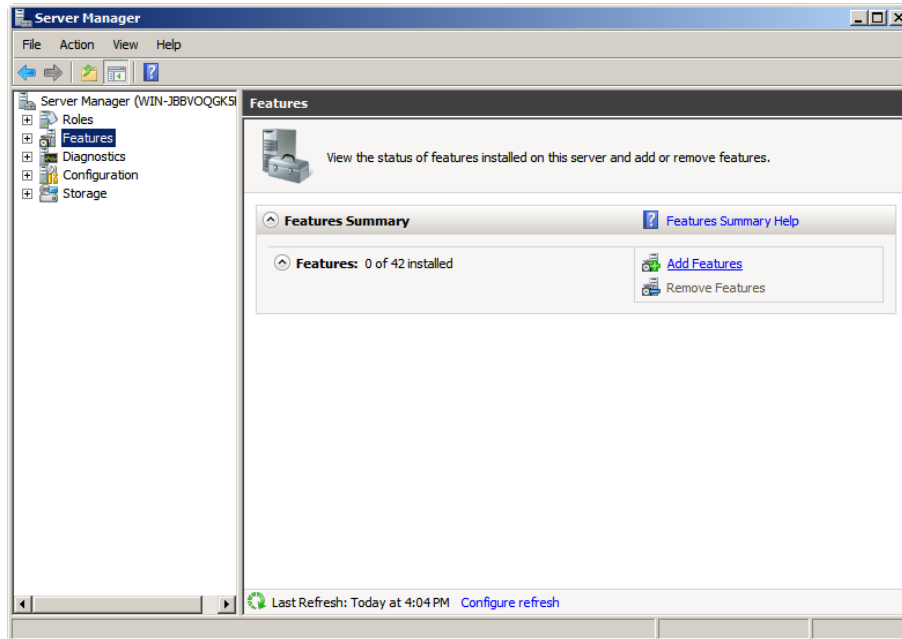
4. It can connect to an iSCSI disk now.

- **MPIO Service**

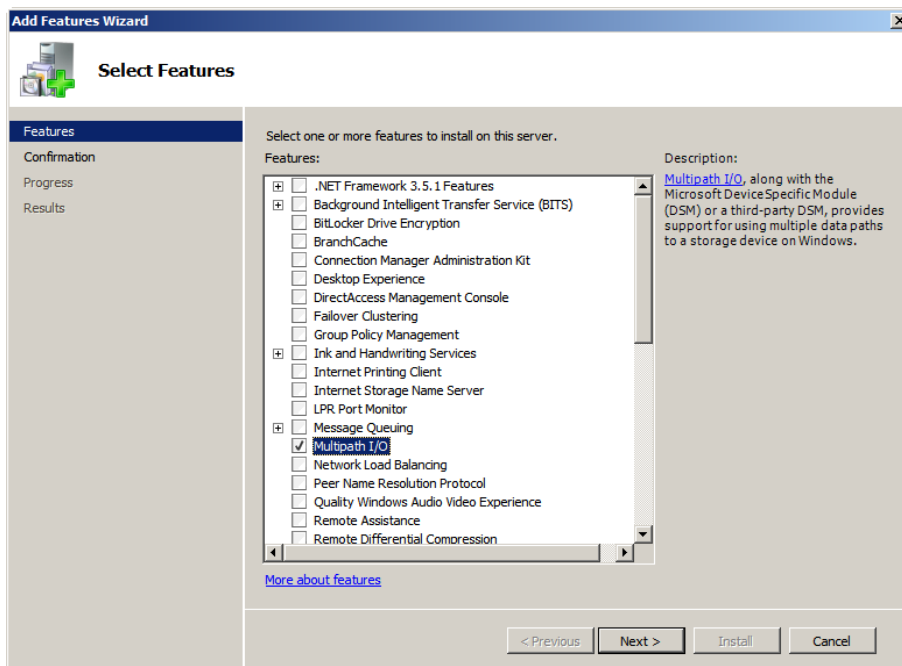
5. Please run Server Manager with below path:

Control Panel\System and Security\Administrative Tools

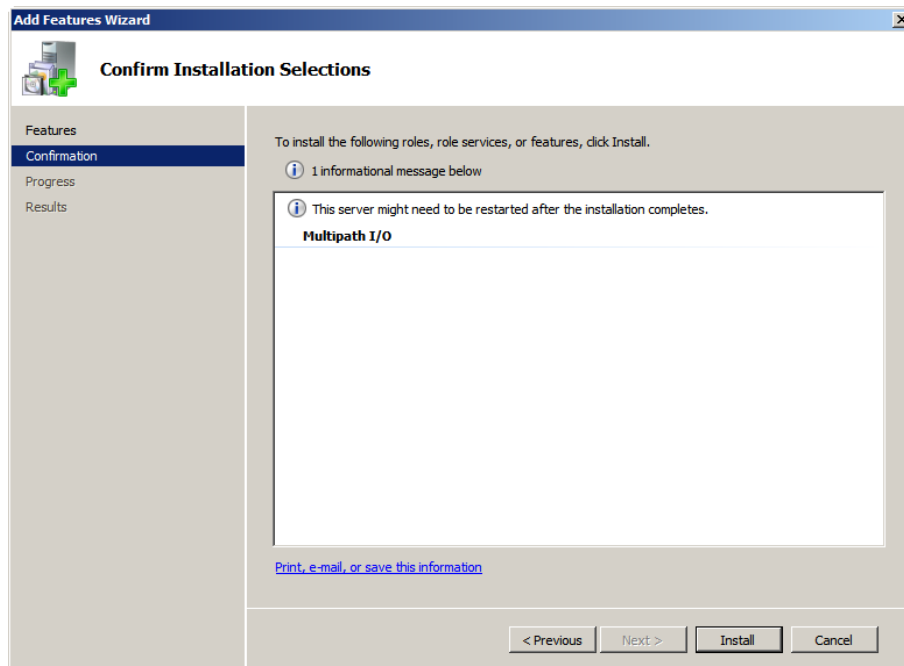
6. Click **Feature** and select **Add Features**.



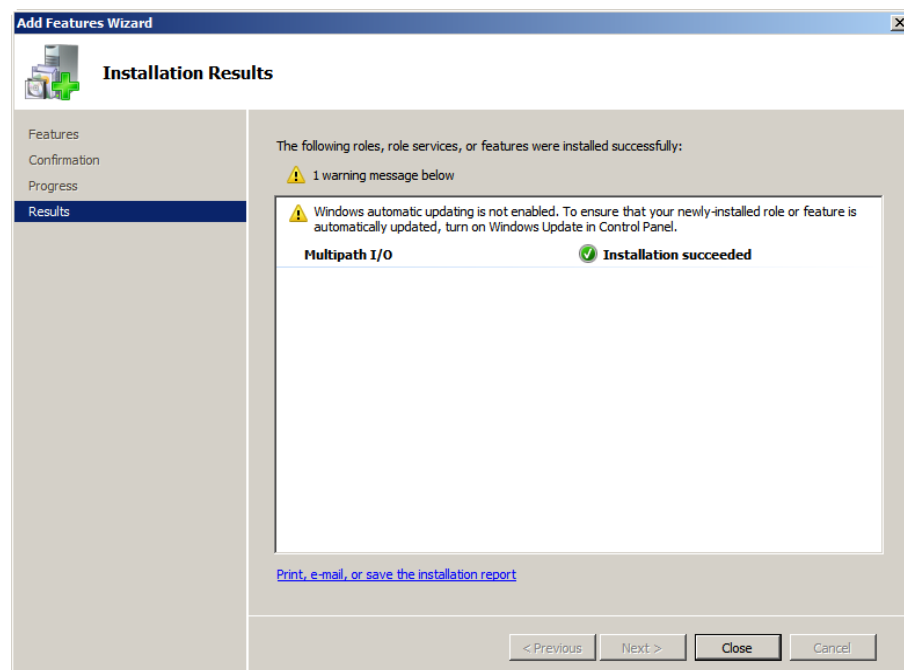
7. Please choose the checkbox of Multipath I/O



8. Install:



9. Installation succeeded.

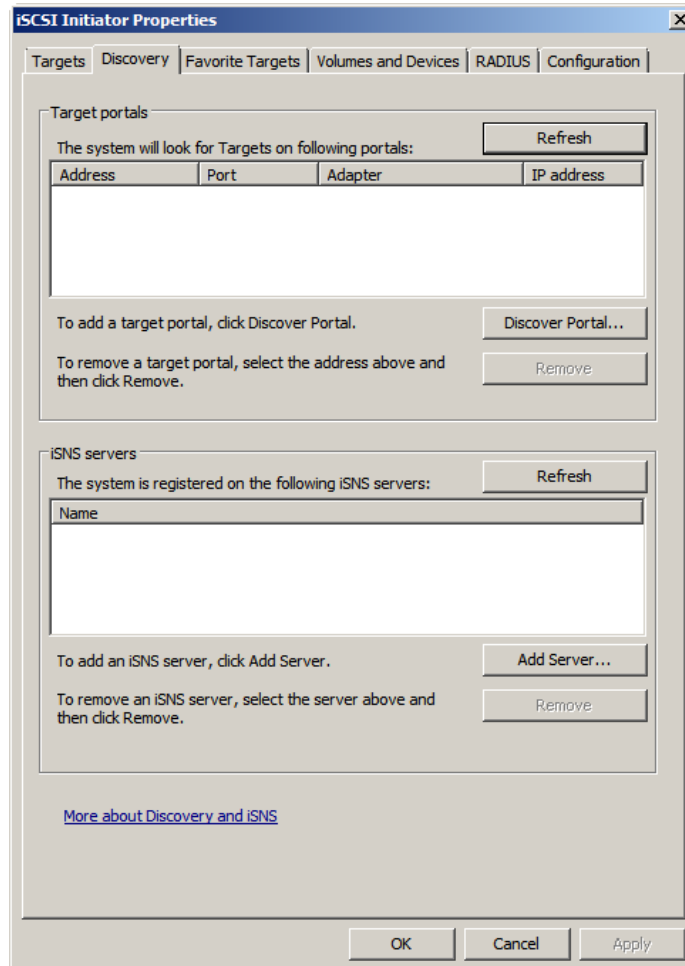


- **Starting iSCSI Initiator**

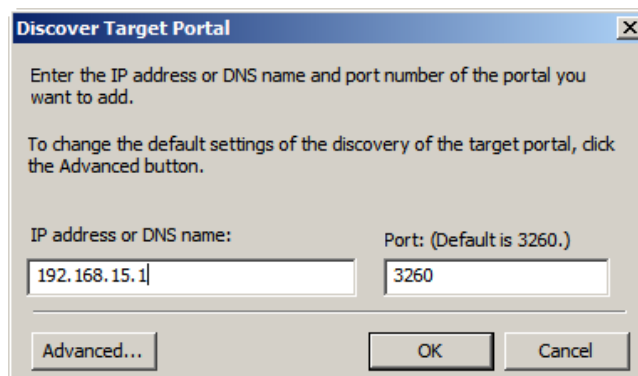
10. Please run iSCSI initiator with below path:

Control Panel\System and Security\Administrative Tools

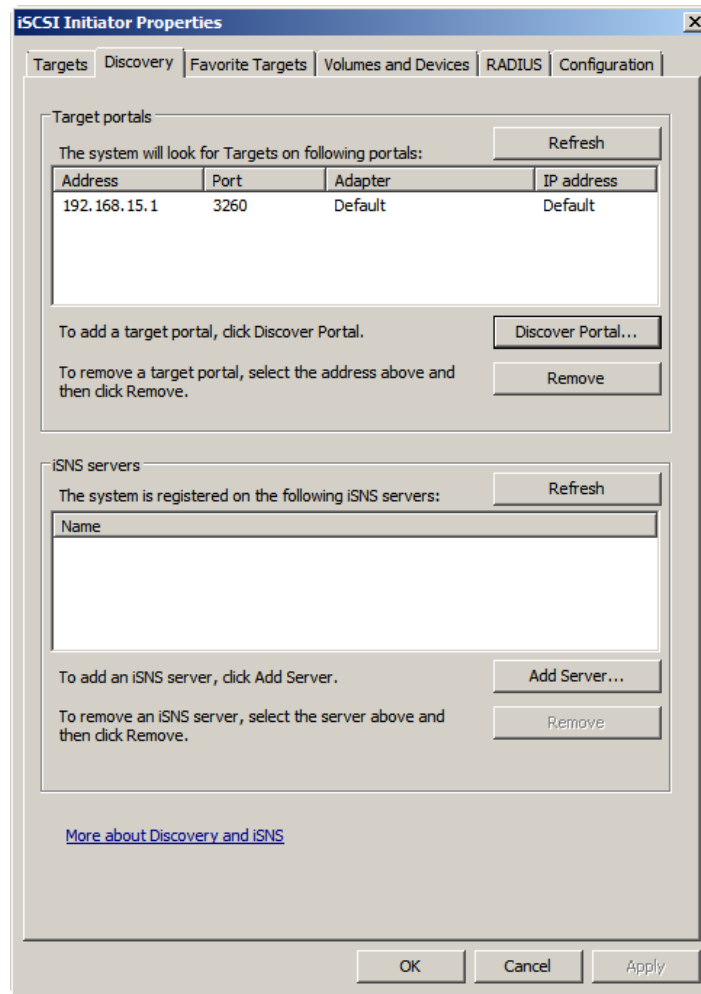
11. Click **Discovery** tab **Discover Portal**



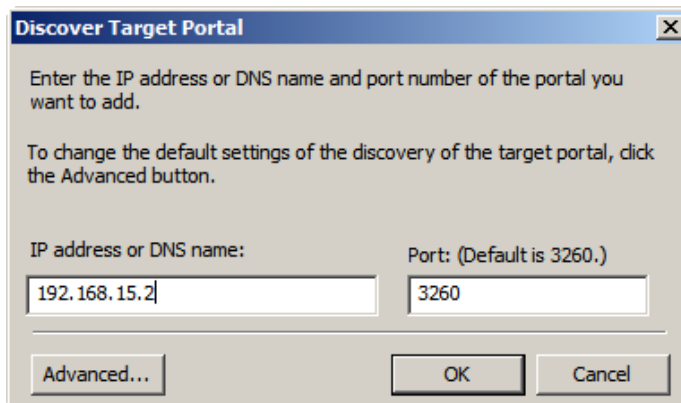
12. Input the IP address of controller1



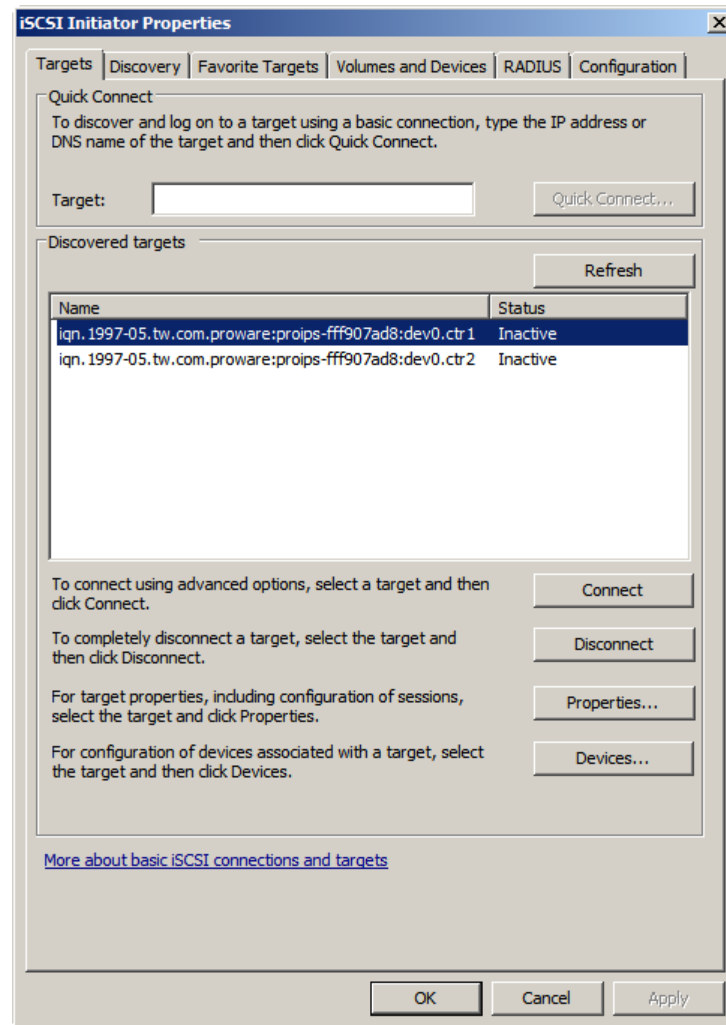
13. Click **Discover Portal**



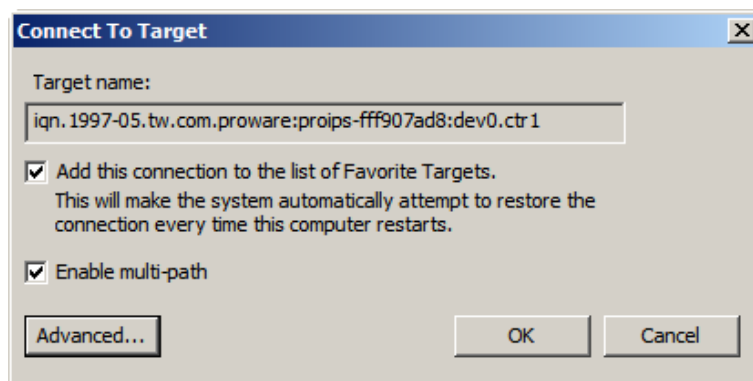
14. Input IP address of controller2



15. Please connect ctrl1



16. Choose checkbox of Enable multipath-path



17. Please select the IP address for Initiator & Target of controller1

The 'Advanced Settings' dialog box has two tabs: 'General' and 'IPsec'. The 'General' tab is active. It contains the following fields and options:

- Connect using:** A dropdown menu showing 'Microsoft iSCSI Initiator'.
- Local adapter:** A dropdown menu showing 'Microsoft iSCSI Initiator'.
- Initiator IP:** A text field containing '192.168.15.101'.
- Target portal IP:** A dropdown menu showing '192.168.15.1 / 3260'.
- CRC / Checksum:** Two checkboxes, 'Data digest' and 'Header digest', both of which are unchecked.
- Enable CHAP log on:** An unchecked checkbox.
- CHAP Log on information:** A section with explanatory text and two input fields:
 - Name:** A text field containing 'iqn.1991-05.com.microsoft:win-jbbvoqgk5e1'.
 - Target secret:** An empty text field.
- Perform mutual authentication:** An unchecked checkbox.
- Use RADIUS to generate user authentication credentials:** An unchecked checkbox.
- Use RADIUS to authenticate target credentials:** An unchecked checkbox.

At the bottom of the dialog are three buttons: 'OK', 'Cancel', and 'Apply'.

18. Please connect ctrl2.

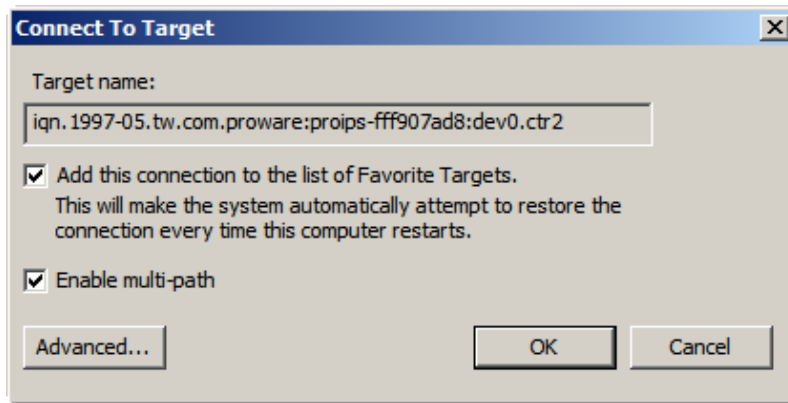
The 'iSCSI Initiator Properties' dialog box has several tabs: 'Targets', 'Discovery', 'Favorite Targets', 'Volumes and Devices', 'RADIUS', and 'Configuration'. The 'Targets' tab is active. It contains the following elements:

- Quick Connect:** A section with instructions and a 'Quick Connect...' button.
- Discovered targets:** A table listing discovered targets. A 'Refresh' button is located to the right of the table header.

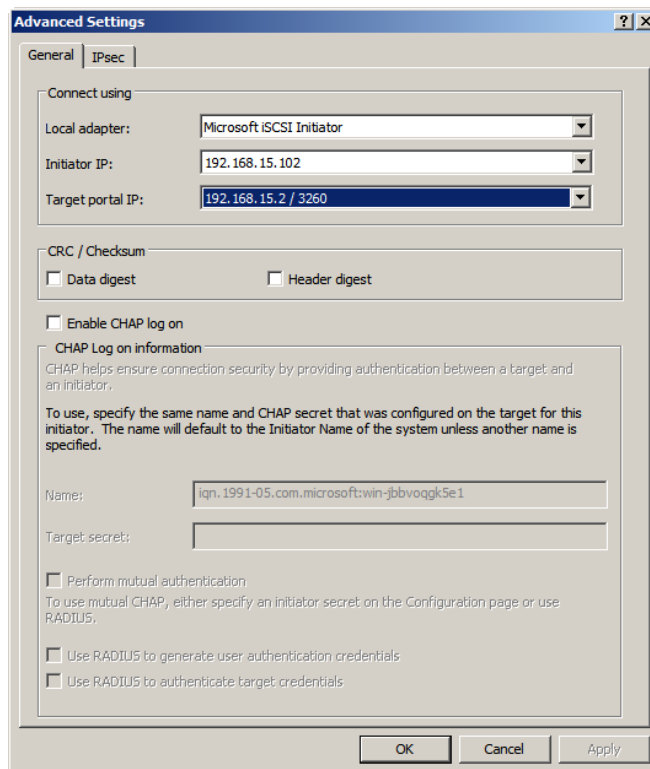
Name	Status
iqn.1997-05.tw.com.proware:proips-fff907ad8:dev0.ctr1	Connected
iqn.1997-05.tw.com.proware:proips-fff907ad8:dev0.ctr2	Inactive
- Connect/Disconnect/Properties/Devices buttons:** Four buttons are located at the bottom right of the dialog: 'Connect', 'Disconnect', 'Properties...', and 'Devices...'.

At the bottom of the dialog are three buttons: 'OK', 'Cancel', and 'Apply'.

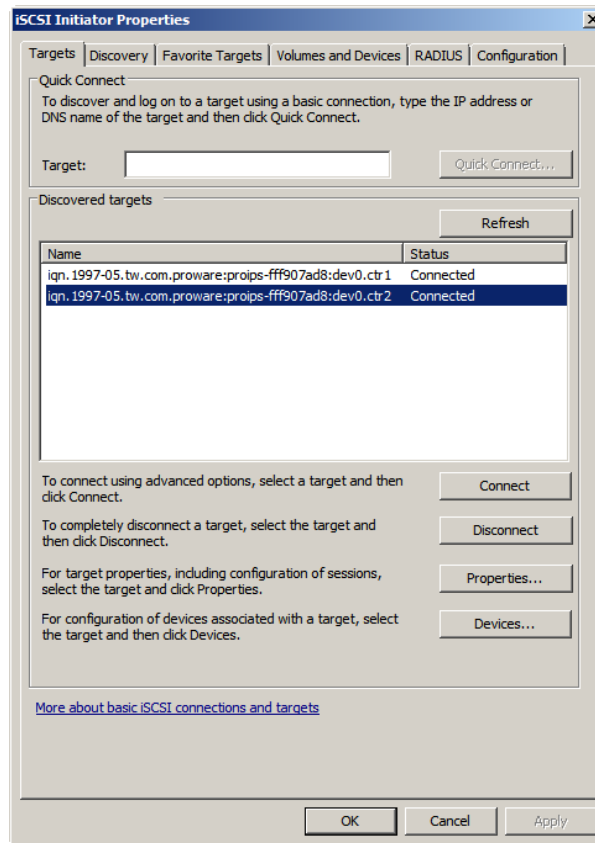
19. Choose checkbox of Enable multipath-path.



20. Please select the IP address for Initiator & Target of controller2.



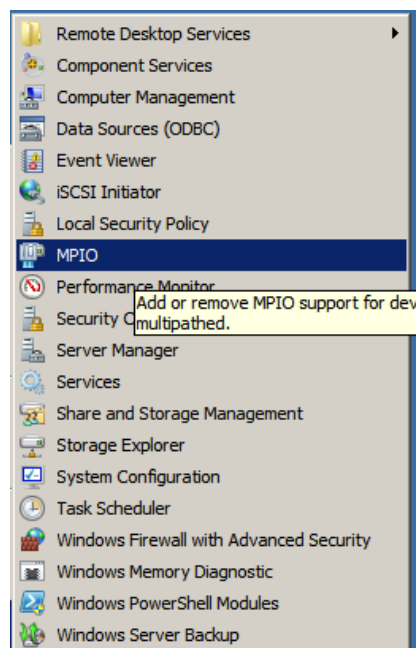
21. iSCSI initiator install finish.



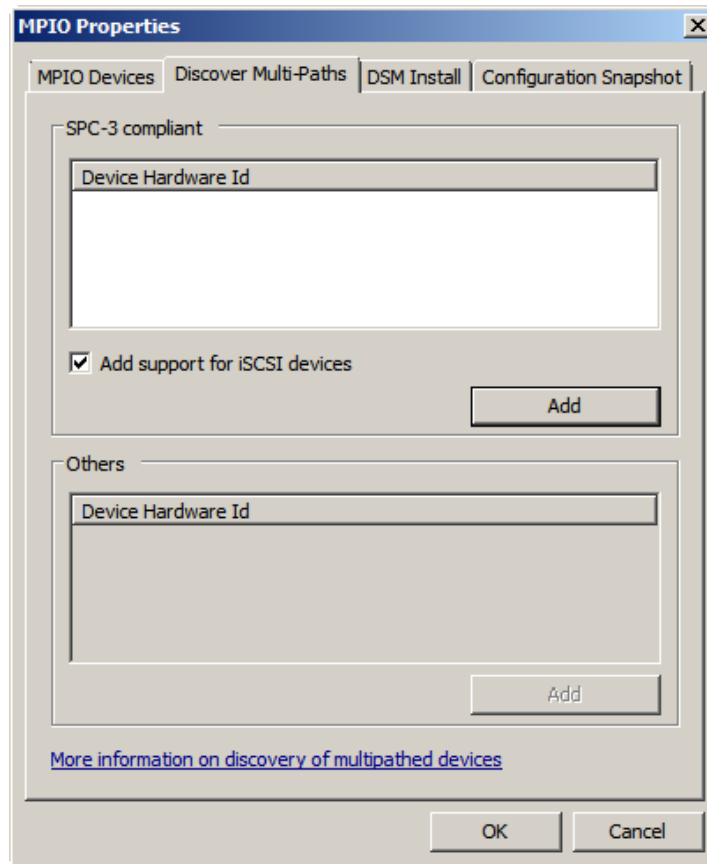
● Setup MPIO

22. Please run MPIO with below path:

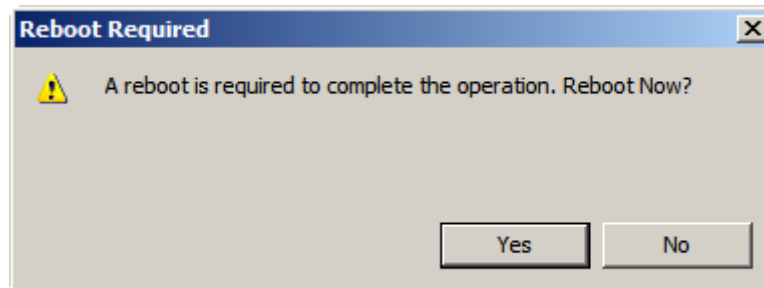
Control Panel\System and Security\Administrative Tools



23. Click tab of **Discover Multi-Paths**
24. Choose checkbox of **Add support for iSCSI devices**

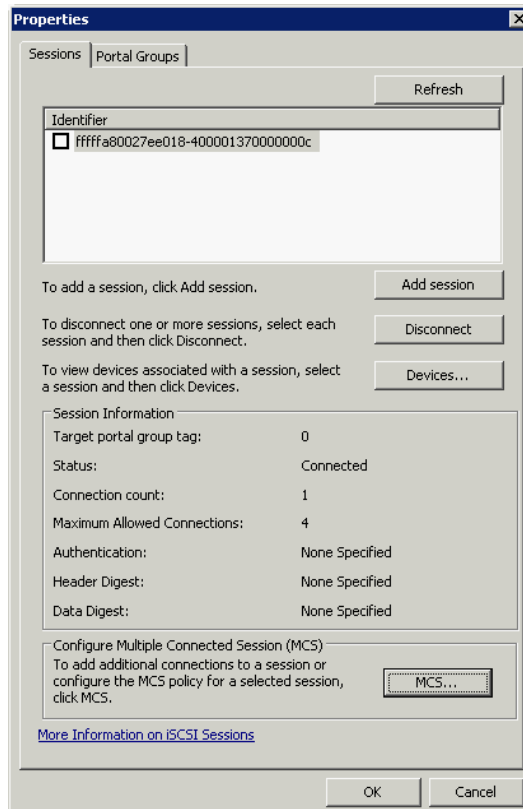
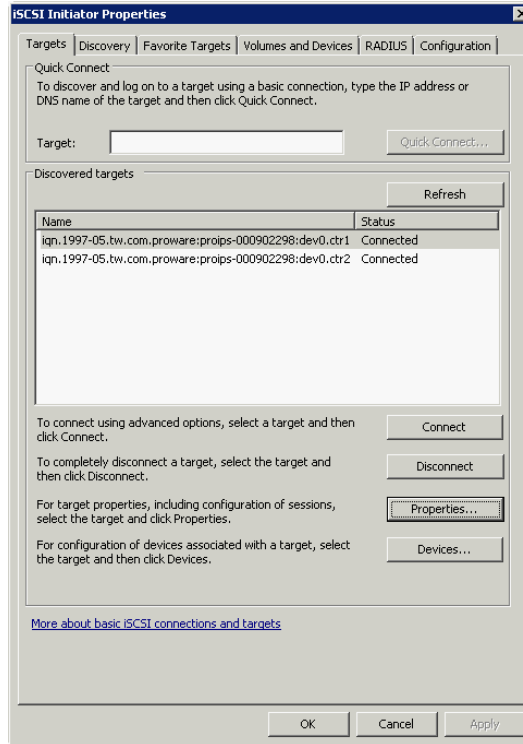


25. Reboot

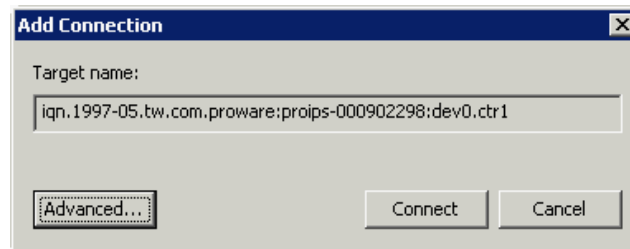
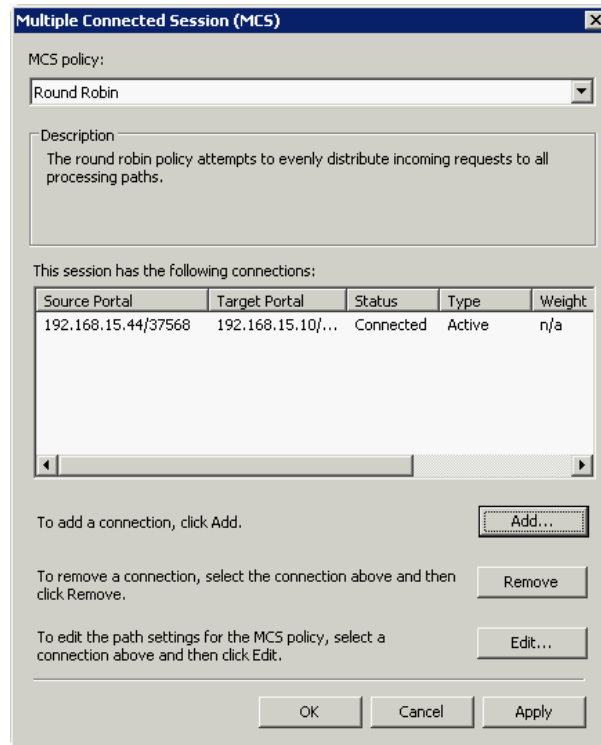


- **MC/S**

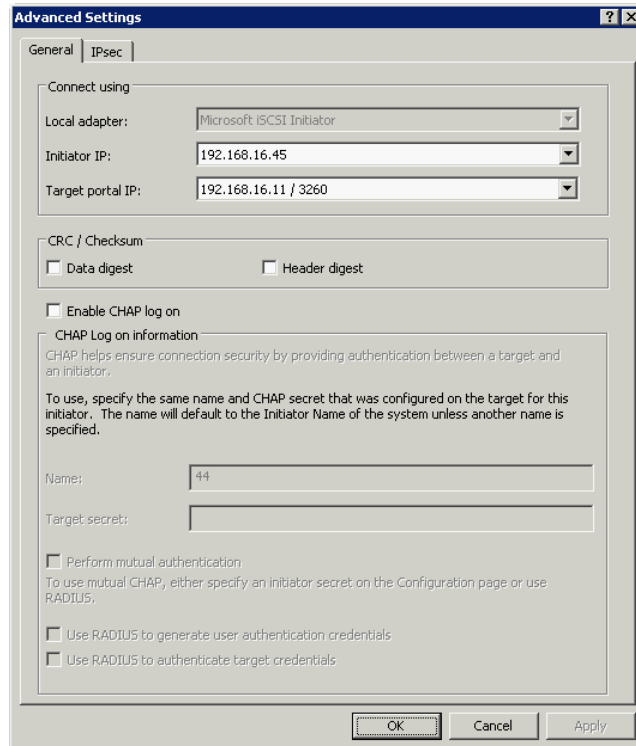
26. If running MC/S, please continue.
27. Select one target name, click **Properties...**
28. Click **MCS...** to add additional connections.



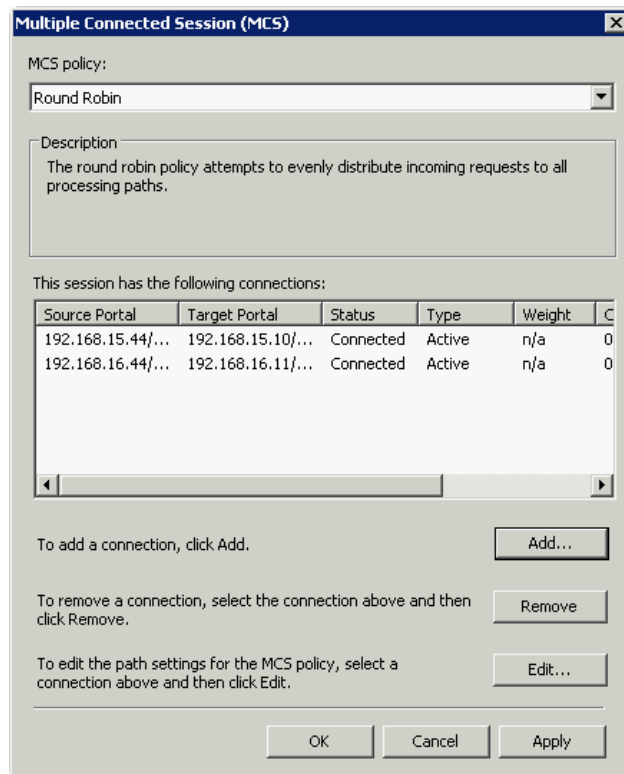
29. Click **Add....**
30. Click **Advanced....**



31. Select Initiator IP and Target portal IP, and then click **OK**.
32. Click **Connect**.
33. Click **OK**.



The 'Advanced Settings' dialog box has two tabs: 'General' and 'IPsec'. The 'IPsec' tab is active. It contains several sections: 'Connect using' with dropdowns for 'Local adapter' (Microsoft iSCSI Initiator), 'Initiator IP' (192.168.16.45), and 'Target portal IP' (192.168.16.11 / 3260); 'CRC / Checksum' with checkboxes for 'Data digest' and 'Header digest'; 'Enable CHAP log on' with a checkbox; 'CHAP Log on information' with a text area explaining CHAP and fields for 'Name' (44) and 'Target secret'; and three checkboxes for 'Perform mutual authentication', 'Use RADIUS to generate user authentication credentials', and 'Use RADIUS to authenticate target credentials'. At the bottom are 'OK', 'Cancel', and 'Apply' buttons.



The 'Multiple Connected Session (MCS)' dialog box shows the 'MCS policy' set to 'Round Robin'. A 'Description' box explains that the round robin policy attempts to evenly distribute incoming requests. Below, a table lists the connections for this session:

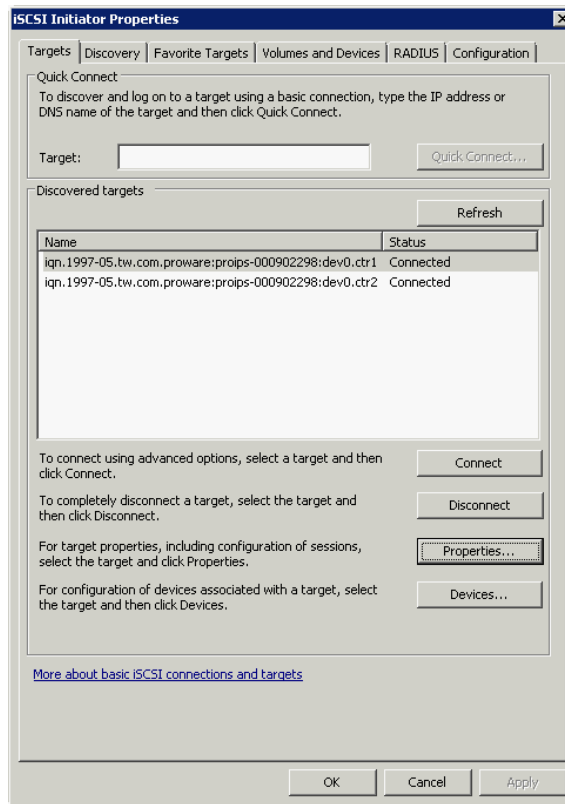
Source Portal	Target Portal	Status	Type	Weight	C
192.168.15.44/...	192.168.15.10/...	Connected	Active	n/a	0
192.168.16.44/...	192.168.16.11/...	Connected	Active	n/a	0

Below the table are instructions and buttons: 'To add a connection, click Add.' with an 'Add...' button; 'To remove a connection, select the connection above and then click Remove.' with a 'Remove' button; and 'To edit the path settings for the MCS policy, select a connection above and then click Edit.' with an 'Edit...' button. At the bottom are 'OK', 'Cancel', and 'Apply' buttons.

34. Done.

- **Disconnect**

35. Select the target name, click **Disconnect**, and then click **Yes**.



36. Done, the iSCSI device disconnect successfully.

LIMITED WARRANTY

This Limited Warranty is provided by Rocstorage, Inc. (hereinafter: Rocstor) for all lines of products.

General Terms

EXCEPT AS EXPRESSLY SET FORTH IN THIS LIMITED WARRANTY, ROCSTOR MAKES NO OTHER WARRANTIES OR CONDITIONS, EXPRESS OR IMPLIED, INCLUDING ANY IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. ROCSTOR EXPRESSLY DISCLAIMS ALL WARRANTIES AND CONDITIONS NOT STATED IN THIS LIMITED WARRANTY. ANY IMPLIED WARRANTIES THAT MAY BE IMPOSED BY LAW ARE LIMITED IN DURATION TO THE LIMITED WARRANTY PERIOD. SOME STATES OR COUNTRIES DO NOT ALLOW A LIMITATION ON HOW LONG AN IMPLIED WARRANTY LASTS OR THE EXCLUSION OR LIMITATION OF INCIDENTAL OR CONSEQUENTIAL DAMAGES FOR CONSUMER PRODUCTS. IN SUCH STATES OR COUNTRIES, SOME EXCLUSIONS OR LIMITATIONS OF THIS LIMITED WARRANTY MAY NOT APPLY TO YOU.

This Limited Warranty applies to the Rocstor branded hardware products sold by or leased from Rocstorage, Inc., its worldwide subsidiaries, affiliates, authorized resellers, or country distributors (collectively referred to in this Limited Warranty as “Rocstor”) with this Limited Warranty. This Limited Warranty is applicable in all countries and may be enforced in any country where Rocstor or its authorized service providers offer warranty service subject to the terms and conditions set forth in this Limited Warranty. However, warranty service availability and response times may vary from country to country and may also be subject to registration requirements in the country of purchase.

Rocstor warrants that the Rocstor hardware product and all the internal components of the product that you have purchased or leased from Rocstor are free from defects in materials or workmanship under normal use during the Limited Warranty Period. The Limited Warranty Period starts on the date of purchase or lease from Rocstor. Your dated sales or delivery receipt, showing the date of purchase or lease of the product, is your proof of the purchase or lease date. You may be required to provide proof of purchase or lease as a condition of receiving warranty service. You are entitled to warranty service according to the terms and conditions of this document if a repair to your Rocstor branded hardware is required within the Limited Warranty Period. This Limited Warranty extends only to the original purchaser or lessee of this Rocstor branded product and is not transferable to anyone who obtains ownership of the Rocstor branded product from the original purchaser or lessee.

Rocstor products are manufactured using new materials or new and used materials equivalent to new in performance and reliability. Spare parts may be new or equivalent to new. Spare parts are warranted to be free from defects in material or workmanship for thirty (30) days or for the remainder of the Limited Warranty Period of the Rocstor hardware product in which they are installed, whichever is longer.

Rocstor's Obligation under the Limited Warranty

During the Limited Warranty Period, Rocstor will repair or replace the defective component parts or the hardware product. All component parts or hardware products removed under this Limited Warranty become the property of Rocstor. The replacement part or product takes on either the Limited Warranty status of the removed part or product or the thirty (30) day limited warranty of the spare part. In the unlikely event that your Rocstor product has a recurring failure, Rocstor, at its discretion, may elect to provide you with a replacement unit of Rocstor's choosing that is at least equivalent to your Rocstor branded product in hardware performance. Rocstor reserves the right to elect, at its sole discretion, to give you a refund of your purchase price or lease payments (less interest) instead of a replacement. This is your exclusive remedy for defective products. The original Limited Warranty is not extended when the product, or a part of the product, is repaired or replaced during the Limited Warranty period. Rocstor shall not be responsible or liable for backing up any data that is on a drive being returned for service

YOU SHOULD MAKE PERIODIC BACKUP COPIES OF THE DATA STORED ON YOUR HARD DRIVE OR OTHER STORAGE DEVICES AS A PRECAUTION AGAINST POSSIBLE FAILURES, ALTERATION, OR LOSS OF THE DATA. BEFORE RETURNING ANY UNIT FOR SERVICE, BE SURE TO BACK UP DATA AND REMOVE ANY CONFIDENTIAL, PROPRIETARY, OR PERSONAL INFORMATION. ROCSTOR IS NOT RESPONSIBLE FOR DAMAGE TO OR LOSS OF ANY PROGRAMS, DATA, OR REMOVABLE STORAGE MEDIA. ROCSTOR IS NOT RESPONSIBLE FOR THE RESTORATION OR REINSTALLATION OF ANY PROGRAMS OR DATA OTHER THAN SOFTWARE INSTALLED BY ROCSTOR WHEN THE PRODUCT WAS MANUFACTURED.

Rocstor does not warrant that the operation of this product will be uninterrupted or error-free. Rocstor is not responsible for damage that occurs as a result of your failure to follow the instructions that came with the Rocstor branded product.

This Limited Warranty does not apply to expendable parts. This Limited Warranty does not extend to any product from which the serial number has been removed or that has been damaged or rendered defective (a) as a result of accident, misuse, abuse, or other external causes; (b) by operation outside the usage parameters stated in the user documentation that shipped with the product and/or posted on the Rocstor website; (c) by the use of parts not manufactured or sold by Rocstor; (d) as a result of normal wear; or (e) by modification or service by anyone other than (i) Rocstor, (ii) a Rocstor authorized service provider, or (iii) your own installation of end-user replaceable Rocstor or Rocstor approved parts if available for your product in the servicing country.

These terms and conditions constitute the complete and exclusive limited warranty agreement between Rocstor and you regarding the Rocstor branded product you have purchased or leased. These terms and conditions supersede any prior agreements or representations including representations made in Rocstor sales literature or advice given to you by Rocstor or an agent or employee of Rocstor-that may have been made in connection with your purchase or lease of the Rocstor branded product. No change to the conditions of this Limited Warranty is valid unless it is made in writing and signed by an authorized representative of Rocstor.

Buyer's Obligation under the Warranty

The person requesting coverage under this warranty shall prove that he or she is the original purchaser and declares that the product has not been sold, leased, bartered or otherwise changed possession. **The purchaser shall frequently backup the Amphibious hard drive and backup the data immediately prior to returning the drive for warranty service.**

The buyer must notify Rocstor and show proof of notification, through any reasonable means of communication. See Full Street address email address and toll free phone numbers below or updated contact information are available on Rocstor.com website. The notification shall identify any defect, malfunction, or nonconformity promptly upon discovery. Rocstor will acknowledge receipt of the communication and issue a Return Merchandise Authorization (RMA) code. The buyer is obligated to securely and safely package(s) the product, preferably in the original packing materials, WITH THE RMA number, and deliver it together with a copy of the original purchase receipt and a description of the problem to the Rocstor home office. Buyer is responsible for the product until it is received by Rocstor. It is recommended that the product be insured during transportation by the sender. You must prepay any shipping charges, taxes, or duties associated with transportation of the product. In addition, you are responsible for insuring any product shipped or returned for service. You assume risk of loss during shipping.

Limitation of damages (Liability)

IF YOUR ROCSTOR BRANDED HARDWARE PRODUCT FAILS TO WORK AS WARRANTED ABOVE, THE ORIGINAL PURCHASER'S SOLE AND EXCLUSIVE REMEDY SHALL BE REPAIR OR REPLACEMENT. ROCSTOR'S MAXIMUM LIABILITY UNDER THIS LIMITED WARRANTY IS EXPRESSLY LIMITED TO THE LESSER OF THE PRICE YOU HAVE PAID FOR THE PRODUCT OR THE COST OF REPAIR OR REPLACEMENT OF ANY ROCSTOR HARDWARE COMPONENTS THAT

MALFUNCTION IN CONDITIONS OF NORMAL USE. ROCSTOR IS NOT LIABLE FOR ANY DAMAGE TO ANY OTHER PRODUCT CONNECTED TO A ROCSTOR PRODUCT.

Limitation on Consequential Damages

ROCSTOR IS NOT LIABLE FOR ANY DAMAGES CAUSED BY THE PRODUCT OR THE FAILURE OF THE PRODUCT TO PERFORM, INCLUDING ANY LOST PROFITS OR SAVINGS OR SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES. ROCSTOR IS NOT LIABLE FOR ANY CLAIM MADE BY A THIRD PARTY OR MADE BY YOU FOR A THIRD PARTY. THIS LIMITATION OF LIABILITY ALSO APPLIES WHETHER DAMAGES ARE SOUGHT OR A CLAIM IS MADE UNDER THIS LIMITED WARRANTY OR AS A TORT CLAIM (INCLUDING NEGLIGENCE AND STRICT PRODUCT LIABILITY), A CONTRACT CLAIM OR ANY OTHER CLAIM. THIS LIMITATION OF LIABILITY CANNOT BE WAIVED OR AMENDED BY ANY PERSON. THIS LIMITATION OF LIABILITY WILL BE EFFECTIVE EVEN IF YOU HAVE ADVISED ROCSTOR OR AN AUTHORIZED REPRESENTATIVE OF ROCSTOR OF THE POSSIBILITY OF ANY SUCH DAMAGES.

THIS LIMITED WARRANTY GIVES YOU SPECIFIC LEGAL RIGHTS. YOU MAY ALSO HAVE OTHER RIGHTS THAT MAY VARY FROM STATE TO STATE OR FROM COUNTRY TO COUNTRY. YOU ARE ADVISED TO CONSULT APPLICABLE STATE OR COUNTRY LAWS FOR A FULL DETERMINATION OF YOUR RIGHTS.

Disclaimer

We accept no liability for any loss of data, damages and the inability of Rocstor products to work with any third party equipment. Nor can Rocstor accept any liability or responsibility for software or third party hardware products.

Limited Warranty Period

The limited warranty period for Amphibious X7 is one (1) Year Parts and Labor. This Limited Warranty extends only to the original purchaser or lessee of this Rocstor branded product and is not transferable to anyone who obtains ownership of the Rocstor branded product from the original purchaser or lessee.

Types of Limited Warranty Service

Your Rocstor Limited Warranty consists of repair or replacement of defective parts, including hard drives identified by Rocstor Support Organization as "pre-failure."

Carry-in Limited Warranty Service Available Monday - Friday

Under the terms of carry-in service, you may be required to deliver your Rocstor product to the Rocstor Service Center or an authorized service location for warranty repair. You must prepay any shipping charges, taxes or duties associated with transportation of the product. In addition, you are responsible for insuring any product shipped or returned for service. You assume risk of loss during shipping.

YOU SHOULD MAKE PERIODIC BACKUP COPIES OF THE DATA STORED ON YOUR HARD DRIVE OR OTHER STORAGE DEVICES AS A PRECAUTION AGAINST POSSIBLE FAILURES, ALTERATION OR LOSS OF THE DATA. BEFORE RETURNING ANY UNIT FOR SERVICE, BE SURE TO BACK UP DATA AND REMOVE ANY CONFIDENTIAL, PROPRIETARY OR PERSONAL INFORMATION. ROCSTORAGE IS NOT RESPONSIBLE FOR DAMAGE TO OR LOSS OF ANY PROGRAMS, DATA OR REMOVABLE STORAGE MEDIA. ROCSTORAGE IS NOT RESPONSIBLE FOR THE RESTORATION OR REINSTALLATION OF ANY PROGRAMS OR DATA OTHER THAN SOFTWARE INSTALLED BY ROCSTORAGE WHEN THE PRODUCT WAS MANUFACTURED.

Rocstorage shall not be responsible or liable for backing up any data that is on a drive being returned for service. Expect that all data on the drive will be destroyed and not retrievable when returned for warranty service.

Rocstor Replaceable Parts Program

Where available, the Rocstor Replaceable Parts program ships approved replacement parts directly to you to fulfill your warranty. This will save considerable repair time. After you call the Rocstor Technical Support Center at **818.727.7000** a replaceable part can be sent directly to you. Once the part arrives, call the Rocstor Technical Support Center. A technician will assist you over the phone to ensure that the installation is quick and easy.

Service Upgrades

Rocstor offers extra coverage for your product. For information on service upgrades, visit www.rocstor.com. Service upgrades purchased in one country are not transferable to another country.

Capacity Disclaimer

Actual accessible hard drive capacity will indicate up to 10% lower than stated under different Operating Systems and formatting.

The storage volume is measured in total bytes before formatting. References to round numbers of gigabytes or terabytes are an approximation only. For example, a disk drive labeled as having 500GB (Gigabytes) has space for approximately 500,000,000 bytes before formatting. After formatting, the drive capacity is reduced by about 5% to 10% depending on the operating system and formatting used or "1GB = 1,000,000,000 bytes.

Options and Software

The Limited Warranty terms and conditions for Rocstor options are as indicated in the Limited Warranty applicable to Rocstor options. **ROCSTOR DOES NOT WARRANTY SOFTWARE PRODUCTS, INCLUDING ANY SOFTWARE PRODUCTS OR THE OPERATING SYSTEM PREINSTALLED BY ROCSTOR.** Rocstor's only obligations with respect to software distributed by Rocstor under the Rocstor brand name are set forth in the applicable end-user license or program license agreement. Non-Rocstor hardware and software products are provided "AS IS" and without any Warranty. However, non-Rocstor manufacturers, suppliers or publishers may provide their own warranties directly to you.

The data stored in Rocstor and Rocsecure storage product lines are not guaranteed by Rocstor (or the hard disk manufacturer.) We are not responsible for any loss of data. Always back up data regularly

TECHNICAL SUPPORT

Software Technical Support

Software technical support is defined as assistance with questions and issues about the software that was either preinstalled by Rocstor on the Rocstor branded product or that was included with the Rocstor branded product at the time of your purchase or lease of the product. Technical support for software is available for the first ninety (90) days from date of product purchase or lease. Your dated sales or delivery receipt, showing the date of purchase or lease of the product, is your proof of the purchase or lease date. You may be required to provide proof of purchase or lease as a condition of receiving software technical support. After the first ninety (90) days, technical support for software that was either preinstalled by Rocstor on the Rocstor branded product or included with the Rocstor branded product at the time of your purchase or lease of the product is available for a fee.

WARNING: The individual user should take care to determine prior to use whether this device is suitable, adequate or safe for the use intended. Since individual applications are subject to great variation, the manufacturer

“Rocstor” makes no representation or warranty as to the suitability or fitness of these devices for any specific application.

Technical Support

All Rocstor hard drives are backed by free telephone technical support for two (2) years from the date of purchase. Please register your product with Rocstor. To register, fill in the Limited Warranty Registration form in the Support tab at www.rocstor.com.

Free telephone technical support is available weekdays from 9 AM until 6 PM Pacific Standard Time. Customers in the United States and Canada can call toll-free: **(818) 727-7000**; all others must call **(818) 727-7000**.

When calling for support, please have the product’s serial number (printed on the label on the bottom of the drive) and system hardware information available.

Trademarks Acknowledgements

© 2017, Rocstorage, Inc; acknowledges the following trademarks for company names or products mentioned within the Rocstor site, portal pages and articles/text/manuals:

Rocstor, Rocsecure and Rocpower are registered trademarks of Rocstorage, Inc. Amphibious, Rocport, Rocbit, Rocsafe ... are the trademarks of Rocstorage, Inc. "store your future", "secure your future" and "power your future" are the slogan marks of Rocstorage, Inc.

Apple, the Apple logo, Mac, Power Macintosh, FireWire, and Mac Pro, Leopard, Snow Leopard ... are trademarks of Apple Computer, Inc. in the United States and other countries.

Microsoft, MS-DOS, Windows CE, Windows NT, Windows 98, Soft Windows, Vista, Windows 7 ... are registered trademarks of Microsoft Corporation in the United States and other countries.

Intel, Itanium, Pentium XXX, Celeron, and Xeon MMX ... are registered U.S. trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

This product is (may also be) integrated with SATA hard drives from the following manufactures:

Seagate, Samsung, Western Digital, Hitachi, Toshiba, Fujitsu ...

All other names are trademarks of their respective companies.

Rocstor wishes to acknowledge the use of tables, charts, graphs and texts from the Wikipedia website.

© 2000 - 2013

Copyrights

© 2016 Rocstorage, Inc. This Manual is protected by United States copyright law and may **not** be reproduced, distributed, transmitted, displayed, published or broadcast without the prior written permission of Rocstorage, Inc. You may not alter or remove any trademark, copyright or other notice from copies of this Manual.



Designed, integrated and assembled by Rocstor in the U.S.A.
using domestic and/or foreign components.

Rocstor is a California Company; U.S.A.

Contact Information

Corporate Headquarters

92445 De Soto Ave
Chatsworth, California 91311
U.S.A. Office: +1 (818) 727-7000
Email: info@Rocstor.com

Technical Support / RMA

Tel: (818) 727-7000 (USA and Canada)
Tel: +1 (818) 727-7000 (Domestic and

Hours: 9:00 am - 5:00 pm PST
Mon - Fri (excluding holidays)
Email: support@Rocstor.com

Sales Info

Hours: 8:00 am - 5:00 pm PST
Mon - Fri (excluding holidays)
Email: sales@Rocstor.com

Corporate, Government and Academic Customers

Our Corporate Sales Team's goal is to help our U.S.A. and Canadian customers find a storage solution that best serves their needs. We will help you determine your best purchasing options. For more information please contact the appropriate department below or call us at +1 (888) 877-7716

General sales information: sales@Rocstor.com
Corporate sales information: corporate_sales@Rocstor.com
Educational sales information: academic_sales@Rocstor.com
Federal, State & Local government sales information: government_sales@Rocstor.com

