



NAS + iSCSI Storage

ExtremeStor-*i*NAS

Administrator Guide

Contact Information

Globalstor Data Corp.

9960 Canoga Ave. Unit D9, Chatsworth, CA 91311

URL : <http://www.globalstor.com>

E-Mail : support@globalstor.com

TEL : 818-701-7771

FAX : 818-701-7756

Information in this document is subject to change without notice and does not represent a commitment on the part of Globalstor Data Corp. The software described in this document is furnished under a license agreement. The software may be used only in accordance with the terms of the license agreement. It is against the law to copy the software on any medium. No part of this manual may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording, for any purpose without the express written permission of Globalstor Data Corp. You may however make one print copy for your personal use.

Globalstor Data Corp. Reserves the right to revise this publication and make changes in the content hereof without the obligation of Globalstor to notify any person of such revision or change.

Copyright ? 2001-2006 Globalstor Data Corp. All rights reserved.

Table of Contents

1. INTRODUCTION TO EXTREMESTOR-INAS	7
1.1. SOFTWARE FEATURES.....	7
2. INSTALLATION OF EXTREMESTOR-INAS	9
2.1. NETWORK CONFIGURATION	9
2.1.1. <i>Configuring on Console</i>	9
3. USING WEB INTERFA CE	10
3.1. INTRODUCTION TO WEB INTERFACE	10
3.1.1. <i>Connecting to Web Interface</i>	10
3.1.2. <i>Main menus of ExtremeStor-iNAS Web Interface</i>	12
4. GENERAL INFORMATION	13
4.1. SYSTEM.....	13
4.1.1. <i>Summary</i>	14
4.1.2. <i>General</i>	15
4.1.3. <i>Time</i>	16
4.1.4. <i>Email</i>	17
4.1.5. <i>SNMP</i>	18
4.1.6. <i>ALERT</i>	19
4.1.7. <i>Power</i>	20
5. CONFIGURING STORAGE	21
5.1. CONFIGURING AND MANAGING DEVICES.....	21
5.1.1. <i>Using External Devices</i>	23
THE RELATIONSHIP OF DEVICES, RAID GROUP, VOLUME GROUP, AND VOLUME.....	24
5.2. CREATING AND MANAGING RAID GROUPS.....	25
5.2.1. <i>The levels of RAID Groups</i>	26
5.2.2. <i>Creating RAID Groups</i>	27

5.2.3. Deleting RAID Groups.....	30
5.2.4. Add Device	31
5.3. CONFIGURING VOLUME GROUPS.....	33
5.3.1. Creating a Volume Group.....	33
5.3.2. Expanding a Volume Group.....	34
5.3.3. Deleting a Volume Group.....	35
5.4. CONFIGURING VOLUMES	36
5.4.1. Creating a Volume	36
5.4.2. Deleting a Volume	38
5.4.3. Modifying Volume Properties.....	39
5.4.4. Expanding a Volume	41
5.4.5. Creating a Snapshot.....	42
5.4.6. Deleting a Snapshot.....	44
5.5. ASSIGNING VOLUME QUOTA.....	45
5.6 BACKUP/RESTORE.....	46
5.6.1 Backup.....	47
5.6.2 Restore.....	48
5.7. ISCSI.....	49
6. CAPACITY EXPANSION BY ISCSI.....	50
6.1. EXPORT/UNEXPORT/IMPORT/UNIMPORT IN DEVICES	51
6.1.1. Exporting devices.....	51
6.1.2. Unexporting devices.....	52
6.1.3. Importing devices.....	53
6.1.4 Unimporting devices.....	54
6.2. EXPORT/UNEXPORT/IMPORT/UNIMPORT IN RAID GROUP.....	55
6.2.1. Exporting RAID Group	55
6.2.2. Unexporting RAID Group.....	57
6.2.3. Importing RAID Group	58
6.2.4. Unimporting RAID Group.....	59

7. NETWORKING OPTIONS	60
7.1. INFORMATION - NETWORK INTERFACE.....	60
7.2. TCP/IP - MODIFYING NETWORK CONFIGURATION.....	61
7.2.1. <i>Network trunking</i>	61
7.2.2. <i>Force Full duplex mode</i>	61
7.3. DOMAIN NAME SEVER (DNS)	62
7.4. WINDOWS (CIFS) ACCESS.....	63
7.4.1. <i>Configuring Active Directory</i>	65
7.5. UNIX (NFS) ACCESS.....	68
7.6. MACINTOSH (AFP) ACCESS	71
8. MAINTENANCE	73
8.1. UPDATE OS	73
8.2. CONSOLE.....	74
8.3. SUPPORT	75
8.4. UPS SERVICE	76
8.5. SYSTEM DATA BACKUP/RESTORE.....	77
9. SECURITY (USER ACCOUNTS)	78
9.1. DEFINING A GROUP	78
9.1.1. <i>Group Import</i>	79
9.2. DEFINING A USER	81
9.2.1 <i>User import</i>	82
9.3. MODIFYING USER INFORMATION.....	84
9.4 CONNECTION.....	85
10. ACCESS CONTROL LISTS (ACLs)	86
10.1. INTRODUCTION TO ACCESS CONTROL LISTS (ACLs).....	86
10.2. CONFIGURING ACL	87
10.3. ADDING USER TO ACL	88
10.4. DELETING USER FROM ACL	92

10.5. BACKING UPACL	93
10.6. RESTORING ACL.....	95
11. MONITORING.....	96
11.1. STATUS.....	96
11.2 STATISTICS.....	97
11.3. REVIEWING THE EVENT LOG.....	98
11.4 LOG SETTINGS	99

1. Introduction to ExtremeStor-iNAS

1.1. Software Features

Optimum OS

Based on Linux, ExtremeStor-iNAS uses a minimized and optimized OS that is booted from 64MB of flash memory, both rapidly and safely.

System installation time is less than 15 minutes and safe booting with less than a 50 second boot time.

RAID Level 0,1,0+1,5, support

Allows configuring and using RAID in the Stand-alone NAS and between the two NAS units.

Supports RAID level 0, 1, 5 and guarantees safe and convenient use with compatible 'Hot Spare' of Hard Disk Drives.

System Data Backup

System configuration data resides in Flash Memory including network configuration, file system information (RAID, Volume) User/Group Quota, etc. are backed up in HDD. In case of Flash Memory failure, it provides quick restoration to current system environment.

Security

In the case of Web Interface control, ExtremeStor-iNAS provides high level of data security by employing encrypted 128bit Secure Socket Layer (SSL) transportation.

User Quota

Provides User Authorization to access certain volumes and management of capacity allocation.

Expansion on Demand

Minimized initial investment cost as expansion is possible at any time

Expanded units can be integrated with the current volume or it can be used separately.

Backup with NDMP

Backup of NAS data to Tape libraries through the network.

Easy management

Control of all disks and NAS units are available through the Web interface. It allows system's surveillance, management and remote area control of temperature, fan and power status.

Configuration of volumes, volume resizing, and replication are also available through web interface.

Storage Virtualization

Other NAS systems supposedly support capacity expansion with clustering of two to a maximum of four units, however, ExtremeStor-iNAS doesn't limit the number of units to be connected and allows unlimited unit and capacity expansion.

In addition, two or more units of ExtremeStor-iNAS can be connected on both LAN and WAN environments. Additionally ExtremeStor-iNAS allows configuration of disparate volume sizes of the units in the same area (LAN) and remote areas (WAN). Specifically you can expand the capacity from 0.96TB to hundreds of TBs without the limitation on physical distance as it uses industry standard Ethernet connectivity.

Dynamic Volume Expansion

ExtremeStor-iNAS allows resizing of the currently configured volumes. For example, using the User/Group Quota function, the assigned volume of 200GB, 500GB, and 100GB to A, B, and C departments respectively can be resized by simple user operation

Dynamic Volume Expansion is also available with the expanded NAS unit.

Clustering Automatic Fail-over

In a clustered configuration, two NAS units work in parallel to increase response time (load balancing), while the secondary system continuously makes exact backup copy of primary disks, all in real time. If one of the unit fails, then the other unit will take over the roles of the other one's providing consistent and stable service.

iSCSI technology

With the industry's leading technology, iSCSI, ExtremeStor-iNAS interoperates with other solutions effectively. iSCSI allows ExtremeStor-iNAS to provide both file I/O (to be used as NAS) and block I/O (to be used as disk array). It is a robust technology that supports configuration of various solutions and functions with ExtremeStor-iNAS.

IP Storage & IP SAN

DAS (Direct Attached Storage) or SAN storages that are connected by SCSI or FC(Fibre Channel) reveal some problems in security and has limitation on physical distance. IP-Storage and IP-SAN came along to complement these drawbacks.

IP-Storage and IP-SAN provides the following advantages using Ethernet connectivity:

- No limitation on physical distance
- Interoperable with the existing network environment
- Low or none existent maintenance costs
- Robust security

As 1Gb and 10Gb Ethernet enters the market, it rivals the speed of Fibre Channel. Considering the development pace and interoperability of Ethernet, IP-Storage and IP-SAN are expected to provide new solutions to storage issues .

2. Installation of ExtremeStor-iNAS

2.1. Network Configuration

If you have a DHCP server on your network, IP address will be assigned automatically and if you do not have a DHCP server, you must assign an IP address manually on Console.

2.1.1. Configuring on Console

IP setting is also available on Console mode by connecting Monitor and keyboard on the backplate of the system..

Default login IP & Password for Console are following.

ID : root

Password : ExtremeStor-iNAS

The following is the commands for IP setting on Console mode. Enter IP Address, Subnet mask and Gateway.

a) Configuring **NACLI**

```
# /nas/bin/nacli help↓
```

```
# nacli ip <eth?|bond?> <yes/no(for enable)> [static/dhcp] [ipaddr] [subnet_mask] [default_gateway]
```

<Eg.>

```
# nacli ip eth0 yes static 192.168.1.10 255.255.255.0 192.168.1.1
```

After completion of IP setting, you can use and manage NAS on Web interface environment.

b) ? Configuring **ifconfig**

eg)

```
# ifconfig eth0 192.168.100.10 netmask 255.255.255.0 up
```

** If you configured IP address in ifconfig, it is required to configure the IP address on the Web interface again.

3. Using Web Interface

All administration and management of ExtremeStor-iNAS is done on Web Interface. This chapter describes the following:

- How to connect to web interface
- The key menus available on Web Interface to administer ExtremeStor-iNAS.

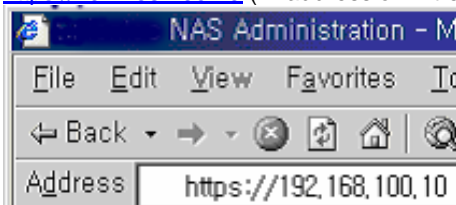
3.1. Introduction to Web Interface

3.1.1. Connecting to Web Interface

We will start from connecting to Web Interface to use ExtremeStor-iNAS in Web interface environment.

? Launch Web Browser from your Desktop or Notebook Computer. Refer to the following figure to insert IP address of the system in the address field of Web Browser.

<https://192.168.100.10> (IP address of ExtremeStor-iNAS)



[Note]

ExtremeStor-iNAS uses 128bit SSL encryption therefore it is required to use '**https**', not '**http**'.

? When Web browser is connected to the server, enter user ID and password. The defaults are '**admin**' for user ID and '**global**' for password.



[Note]

Change Administrator's password. When the password is changed, the password of Admin on the Web Interface and the Root password on the Console will change simultaneously. These two passwords are identical.

3.1.2. Main menus of ExtremeStor-iNAS Web Interface



This section describes the web administration menus of ExtremeStor-iNAS.

The NAS Web Interface consists of seven main menus and the definitions are defined below.



System menu allows you to check the status and management of the system including settings of mail & time. You can also initialize the system under Power menu.



You can see the list of available disks and create RAID Group, Volume, and Volume Group. Storage menu allows you to perform Import/Export with iSCSI technology. You can also set a Password for NDMP connection.



Network provides network status and allows you to setup Network Card. You can manage Shares for DNS, CIFS, NFS, and AFP.



You can manage share access for Groups and Users for shared volumes.



High Availability menu provides Disk Mirroring(clustering Failover) configuration.



Maintenance menu provides functions to administrate ExtremeStor-iNAS including Software Upgrade, Connecting to the server with Console, and sending email for technical supports.

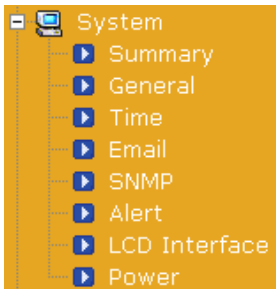


You can monitor the overall system with Monitoring Menu. It provides the list of the clients who are connected to the shared volume, Kernel and Booting information, and Service Program status.

4. General Information

This chapter explains the options that are available in **System** menu.

4.1. System







System menu provides Summary, General, Time, Email/Alert, SNMP, and Power status and configuration menus.

4.1.1. Summary

Summary shows the information of the system. System running time, Model name, OS version, Firmware version, CPU, Memory, and system serial number are shown under this menu.

Hints

-  Hostname not defined, currently using the serial number for the hostname.
-  Please change the administrator's password for security reasons.
-  Please set up the correct date & time.
-  Mail server not configured.

System

System has been up	21 Minutes 34 Seconds
Model Name	Splentec
OS Version	1.1H.748
Firmware Version	1.0
CPU	Dual Xeon(TM) CPU 2.40GHz
Memory	511 MB
Serial Number	splentec

Status

Network Status	 eth0: Not connected  eth1: Connected, 1000Mb/s, Full Duplex
RAID Status	Raid Group not defined

[Refresh](#)

Note

Check the OS version after Software update in order to make sure that the update has been completed successfully.


4.1.2. General

General menu provides following options :

Host Name	Name of the system.
Administrator's Password	Change Administrator's password. When the password is changed, the password of Admin on the Web Interface and the password of Root on the Console will change simultaneously. These two passwords are identical.
Code Page	Select appropriate language to display file/folder names correctly when sharing CIFS or NFS.


▶ Host Name

Host Name	<input type="text"/>
-----------	----------------------

 Save

▶ Administrator's Password

Current Password	<input type="password"/>
Enter New Password	<input type="password"/>
Re-enter New Password	<input type="password"/>

 Modify

▶ Codepage

Client Code Page	<div>English</div> <div> English Japanese Korean Simplified Chinese Traditional Chinese </div>
------------------	--

 Save

[Note]

Make sure to click '**Save**' button after modification.

The default value of Codepage is English. For Japanese and Chinese support, select the appropriate box on the Client Code Page.

4.1.3. Time

It allows setting of Time and Date for the system. Define the Time Zone that is applicable to your country.

▶ Date/Time

Date (MM/DD/YYYY)	07 / 06 / 2004
Time (HH:MM:SS)	15 : 57 : 56

[Save](#)

▶ Time Zone

Time Zone	Japan, Korea (GMT+9:00)
-----------	-------------------------

[Save](#)

▶ Network Time

Use NTP to Set Time Automatically	<input checked="" type="checkbox"/>
NTP Server	time.kriss.re.kr
Update Interval (Hours)	12

[Update Now](#)[Save](#)

Network Time: Provides setting for NTP Server. NTP server time will be automatically applied to the system according to update interval.
ex) NTP Server : tick.utoronto.ca

4.1.4. Email

You can assign a mail server to receive the mail that contains information of the events occurring in the system. Assign SMTP server for mail server.

? Go to **System->Email**.

? To set the E-mail Notification, you must first enable email, and then specify the SMTP server's IP address and designate the e-mail address you want the tool to send e-mail to. You may list multiple recipients (up to 3 email addresses) for the email notification. Place a semicolon between each e-mail address. The maximum number of letters is 126.

Example)

Admin Email Address:



admin@insightstor.com;demo@insightstor.com;test@insightstor.com

? Click **Save**.

? Click **Send a Test** to verify your settings.

Email

Event Notification	<input type="checkbox"/> Enable
Mail Server (SMTP)	<input type="text"/>
Admin Email Address	<input type="text"/>

 Send Test Mail  Save

Example)

Email

Event Notification	<input checked="" type="checkbox"/> Enable
Mail Server (SMTP)	<input type="text" value="mail.globalstor.com"/>
Admin Email Address	<input type="text" value="admin@globalstor.com"/>

 Send Test Mail  Save

4.1.5. SNMP

SNMP is a network protocol that provides management and administration of the system on the network. It is a useful function when managing more than one system. (Make sure to click '**Save**' button after modification)

ExtremeStor-iNAS

[ExtremeStor-iNAS supports SNMP Trap receiver]

 **SNMP**

Enable	<input type="checkbox"/>
Read Only Community	<input type="text" value="public"/>
Read-Write Community	<input type="text" value="private"/>
Trap Host Address	<input type="text"/>
Trap Community Name	<input type="text"/>
Contact Name	<input type="text" value="Unknown"/>
Location	<input type="text" value="Unknown"/>

 Save

Trap Host Address	IP address of the server that runs SNMP Trap receiver.
Trap Community Name	Name of COMMUNITY eg) Insight
Contact Name	Name of the System Manager who is in charge of ExtremeStor-iNAS administration.
Location	Name of the location ExtremeStor-iNAS is installed. Eg) Globalstor R&D Center

[TIP]

In order to have SNMP service, go to System -> Alert and check the trap events that you want to receive.

4.1.6. ALERT

ExtremeStor-iNAS shows the errors or events of the system to the administrator in real-time or inform by email. You can monitor the system status including disk error, RAID set, temperature, and power in real-time

Select the events that you want to receive by e-mail or SNMP. Click '**Save**' when done.

▶ Alerts

System start / shutdown	<input checked="" type="checkbox"/> Send Email Notification	<input type="checkbox"/> Send SNMP Trap
Device Failure	<input checked="" type="checkbox"/> Send Email Notification	<input type="checkbox"/> Send SNMP Trap
Power Failure	<input checked="" type="checkbox"/> Send Email Notification	<input type="checkbox"/> Send SNMP Trap
Fan Failure	<input checked="" type="checkbox"/> Send Email Notification	<input type="checkbox"/> Send SNMP Trap
System Overheat	<input checked="" type="checkbox"/> Send Email Notification	<input type="checkbox"/> Send SNMP Trap
RAID Event	<input checked="" type="checkbox"/> Send Email Notification	<input type="checkbox"/> Send SNMP Trap
Clustering / Failover Event	<input checked="" type="checkbox"/> Send Email Notification	<input type="checkbox"/> Send SNMP Trap

 Save

[TIP]


All the event boxes in the Send Email Notification are checked by default.

4.1.7. Power


You can control Power under this menu.

▶ Reboot / Shutdown

☒ Normal mode

 Starting the system in maintenance mode is intended for system engineers, any changes made in maintenance mode may make the system unusable.

☐ Start the system in maintenance mode

 Resetting the system to the factory defaults will not only delete any configuration changes, but also delete all existing data on the all disks, including external SCSI hard disks, if any.

☐ Reset to factory defaults

☐ Reset to factory defaults, except current network settings

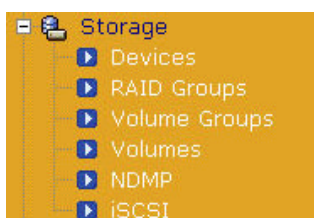
Reboot / Shutdown options – Options for rebooting or system shutdown.

Normal mode	The system reboot/shutdown normally.
Start the system in maintenance mode	The system starts with Maintenance mode.
Reset to factory defaults	The system will be initialized to factory defaults. User, Volume, and network configuration will be deleted. "The previous configurations cannot be recovered therefore, be caution for this option"
Reset to factory defaults except current network setting	All configurations will be initialized except Network. "The previous configurations cannot be recovered therefore, be caution for this option"

5. Configuring Storage

This chapter explains how to use the Storage menu to configure ExtremeStor-iNAS disks and volumes. It covers the following topics:

- Configuring and managing Devices
- Creating and managing Volume Groups
- Creating and managing Snapshots
- Configuring and managing NDMP
- Using iSCSI technology in ExtremeStor-iNAS



Use the **Storage** menu to view, add, and modify storage configuration options for devices, volumes, NDMP and use iSCSI benefits in ExtremeStor-iNAS.

5.1. Configuring and Managing Devices

Devices menu allows you to view the status of the disk drives installed on ExtremeStor-iNAS. ExtremeStor-iNAS offers to use up to twenty four local disks and external SCSI HDD and RAID are also viewed under this menu.

[Note]

Tape Drive and Library are used as target of NDMP but it cannot be used as Storage Device.

▶ Devices

Device	Model	Size	Status	Action
 h0b0t0l0	Seagate ST3160023AS	160.0GB	Available	 Export
 h0b1t1l0	Seagate ST3160023AS	160.0GB	Available	 Export
 h0b2t2l0	Seagate ST3160023AS	160.0GB	Available	 Export
 h0b3t3l0	Seagate ST3160023AS	160.0GB	Available	 Export

 Rescan
  Import

Status Headings	Definition
Device	The name of the drive
Model	The name and model name of the drive
Size	The total capacity of the drive
Status	The current condition of the drive:
	<div>Available</div> <p>Available devices on the system mean any device that is not part of RAID Group or have not been exported. For external SCSI storages, it means the external storage is available for use immediately.</p>
	<div>Fault</div> <p>If this status is shown, there is a problem with drive. In this case, the drive needs to be repaired.</p>
	<div>Used: RG0</div> <p>The drive is assigned to RAID Group.</p>
Action	<div>iSCSI Target</div> <p>The drive has been exported to another NAS system to be used as its local drive. In this case, primary NAS cannot use the drive as local disk.</p>
	In addition, exporting the drive to other NAS system is available in this menu. (Refer iSCSI for more information about Export)

5.1.1. Using External Devices

ExtremeStor-iNAS supports capacity expansion by using external SCSI devices. The maximum of fifteen SCSI devices can be attached with support from embedded SCSI Adaptor. You can use Disk Array When external device has been attached to the system, the following message will appear:

 h4b0t110	Device Vendor	1000.0GB	Available	 Export
--	---------------	----------	-----------	--

The above figure indicates SCSI drives are attached to the system and you can see that this device also supports Export function.

[TIP]

External devices can be used to add more capacity to existing RAID Groups or can configure RAID groups separately. Normally, external RAID can be configured with RAID of ExtremeStor-iNAS as RAID Level 1, Mirroring.

The relationship of Devices, RAID Group, Volume Group, and Volume

In IS8200, Device, RAID Group, Volume Group, and Volume have close relationship to each other. Read this section carefully and it will help you to have optimized Volume configuration in IS8200.

Device is a physical disk that provides physical Storage space. There are internal and external devices in ExtremeStor-iNAS. Internal device means HDD that is implemented in ExtremeStor-iNAS and external device means other storage systems that are connected to NAS by SCSI cable. The representative external device is Disk Array. In addition, one of the advantages that IS8200 gives is that support from iSCSI technology, IS8200 can use devices from remote IS8200 as internal devices.

When you have devices available, you could create **RAID Group**. Configure the RAID Group that is most appropriate for your usage. You could put priority in importance and purpose of the data.









After creating RAID Groups, you could group them as one **Volume Group**. Volume Group is a logical disk and you can create several Volume Groups. The size of the Volume group will be same as the size of the RAID Groups in the Volume Group. You can expand the size either by adding devices or creating new RAID Groups.




After Volume Group is created, you could create **Volume** within the Volume Group. Select one of the Volume Groups and create a volume within the available size in the Volume Group. You can expand the Volume size if there is available space in the Volume Group. If Volume Group size is full, you could create new RAID Group and expand the size.

5.2. Creating and Managing RAID Groups

RAID is a collection of disk drives that act as a single storage system. ExtremeStor-iNAS supports RAID level 0, 1, 0+1 and 5 and allows to configure spare disk. Refer to 5.2.1. for the definition of RAID Group prior to RAID Group creation.

RAID Groups

	Name	Level	Size	Status
	 RG0  h0b0t0i0 (160.0GB)  h0b1t1i0 (160.0GB)	RAID 0	298.1GB	ACTIVE
	 RG1  h0b2t2i0 (160.0GB)  h0b3t3i0 (160.0GB)	RAID 1	149.0GB	Resync (0.0%) finish=49.3min 52736K/sec

 Create  Add Device  Import  Export  Delete

5.2.1. The levels of RAID Groups

RAID 0 (Striped)

A RAID 0 stores equal portions of each file on each disk in the RAID Group. This technique, called data striping, is fast since it uses multiple physical devices to contain a single data set. However, RAID 0 offers no redundancy. If a disk drive fails, every file in the RAID is unavailable. It is not a recommended configuration for critical data.

RAID 1 (Mirrored)

A RAID 1 uses mirroring, which stores data on one disk copies it to a second disk, creating a redundant storage solution. RAID 1 is the most secure method for storing mission critical data because there is no catastrophic data loss when a disk fails. However, RAID 1 is the most expensive and least efficient storage method.

RAID 5 (Striping with Parity)

RAID 5 stores equal portions of each file on each disk and distributes parity information (error correction data) for each file across all disks in the group. This distributed parity allows the system recover from a single disk drive failure. RAID 5 gives the best combination of performance, usability, capacity, and data protection.

RAID5 + Hot Spare

Adding a spare device to RAID 5. In case of device failure in the RAID 5 group, the failed device will be automatically changed to the spare device.









* The following table summarized the benefits and drawbacks and requirements for each RAID:




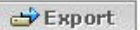

	RAID0	RAID1	RAID (0+1)	RAID5	RAID5 with Hot Spare
Data Loss Risk	High	Low	Very Low	Low	Very Low
Access Speeds	Fast	Slow	Slow	Fast	Fast
Cost/MB	Low	High	High	Low	Low
Min Disks required	2	2	4	3	4

5.2.2. Creating RAID Groups

? To create RAID Group, go to Storage -> RAID Groups on Web Interface and click **Create**.

▶ RAID Groups

	Name	Level	Size	Status
	 RG0  h0b0t0l0 (160.0GB)  h0b1t1l0 (160.0GB)	RAID 0	298.1GB	ACTIVE
	 RG1  h0b2t2l0 (160.0GB)  h0b3t3l0 (160.0GB)	RAID 1	149.0GB	Resync (0.0%) finish=49.3min 52736K/sec

The figure above is an example configuration of RAID Group with RAID 5 and hot spare.

? The screen shows the three types of supported RAID levels and describes the strengths and weaknesses of each. After selecting RAID level, select the devices you want added to the RAID. You can configure as many devices as you want in a RAID. If you create a RAID 5, you can configure one of the drives to be a hot spare. If you create more than one RAID 5 configuration and you want redundancy, you must specify one Hot Spare for each configuration.

▶ Select RAID Level

<input type="radio"/> RAID 0	Disk striping without data protection. The failure of just one drive will result in all data in an array being lost.
<input type="radio"/> RAID 1	Mirroring. All data is replicated on a number of separate disks. 100% redundancy of data. Highest disk overhead of all RAID types.
<input checked="" type="radio"/> RAID 5	Data blocks are distributed as with disk striping. Parity check data is distributed across all members of the array. Disk failure has a medium impact on throughput.

▶ Select Devices

Available Devices	RAID Devices	Spare Devices
<div>h0b0t0i0 (160.0GB)</div> <div>h0b1t1i0 (160.0GB)</div> <div>h0b2t2i0 (160.0GB)</div> <div>h0b3t3i0 (160.0GB)</div> <div> <input type="button" value="Add RAID"/> <input type="button" value="Add Spare"/> </div>	<div></div> <div> <input type="button" value="Remove"/> </div>	<div></div> <div> <input type="button" value="Remove"/> </div>

Select RAID Level	List of available RAID levels. Select one among 0, 1, and 5.
Select Devices	<p>? Available Devices : List of available devices.</p> <p>? RAID Devices : Devices to be added to RAID group. Select the devices and click Add RAID.</p> <p>? Spare Devices : Spare Disks to be used in RAID. Select a device and click Add Spare.</p>

? Click **Yes** for the following message to confirm RAID creation.

? Warning: Creating a new RAID Group will destroy existing data. Continue?



. The following figure shows when RAID Group has been created successfully. The RAID group is created with three devices and one spare device with RAID level 5. (It takes around 60 minutes to complete RAID configuration.)

▶ RAID Groups

	Name	Level	Size	Status
	RG0 h0b0t0I0 (160.0GB) h0b1t1I0 (160.0GB) h0b2t2I0 (160.0GB) h0b3t3I0 (160.0GB, Spare)	RAID 5	298.1GB	Resync (0.0%) finish=47.7min 54436K/sec

Create
 Add Device
 Import
 Export
 Delete

[Note]

You can use the RAID Group right after setting is done but it will cause slow I/O performance. We recommend to use the RAID Group when configuration is completed.

5.2.3. Deleting RAID Groups

? Select **radio button** on the left of RAID Group that you want deleted and click **Delete**.

RAID Groups

	Name	Level	Size	Status
<input checked="" type="radio"/>	<div>RG0</div> <div> <div>h0b0t0l0 (160.0GB)</div> <div>h0b1t1l0 (160.0GB)</div> <div>h0b2t2l0 (160.0GB)</div> <div>h0b3t3l0 (160.0GB, Spare)</div> </div>	RAID 5	298.1GB	Resync (0.0%) finish=47.7min 54436K/sec

. Review the information of the RAID Group to be deleted and click **Yes** when confirmed. Use with caution, as deleting RAID Group will delete all stored data.

? Confirm Deleting The Following RAID Group:

RAID Group Name	RG0
RAID Level	RAID 5
# Of Disks	3
# Of Spare disks	1
Size	298.1GB
Status	Resync (4.2%) finish=321.0min speed=7761K/sec

WARNING: This will delete the RAID group and its existing data permanently. This cannot be undone.
Continue?

[TIP]

If Volume has been configured under the RAID Group, deleting cannot be done. Deleting is done in below order:

Volume delete

↓
Volume Group delete




↓
RAID Group delete




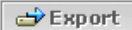
5.2.4. Add Device

If any device fails while system is in operation, you can replace the failed disk with a spare device. In this section, you can add a spare device to the RAID Group.

? Select the RAID Group that you want device to be added and click **Add Device**.




▶ RAID Groups

	Name	Level	Size	Status
	 RG0  h0b0t0i0 (160.0GB)  h0b1t1i0 (160.0GB)  h0b2t2i0 (160.0GB)	RAID 5	298.1GB	Resync (0.2%) finish=45.5min 56976K/sec


? Select the device to add and click Add.

▶ RAID Group

Name	Level	Size	Status
 RG0  h0b0t0i0 (160.0GB)  h0b1t1i0 (160.0GB)  h0b2t2i0 (160.0GB)	RAID 5	298.1GB	Resync (4.8%) finish=89.4min 27712K/sec

▶ Select Device

	Device	Model	Size
	 h0b3t3i0	Seagate ST3160023AS	160.0GB









? Confirm the information and click **Yes**.

. You could see that the device has been added as Spare.

RAID Groups

	Name	Level	Size	Status
	<div> RG0<div> h0b0t0i0 (160.0GB)  h0b1t1i0 (160.0GB)  h0b2t2i0 (160.0GB)  h0b3t3i0 (160.0GB, Spare)</div></div>	RAID 5	298.1GB	Resync (5.7%) finish=311.2min 7886K/sec

 Create  Add Device  Import  Export  Delete

[Warning]

After adding device, you must run 'Repair'.

5.3. Configuring Volume Groups

Volume Group is to create a logical storage area by grouping several RAID Groups as one large volume. If more capacity is needed for the Volume Group, it could easily expand the capacity by adding more RAID Groups to the Volume Group. This function is called Dynamic volume Expansion.

5.3.1. Creating a Volume Group


? Go to **Storage -> Volume Groups** and click **Create**.

▶ Volume Groups

	Name	Size	Free	Usage	Status
<div> Create Repair Extend Delete </div>					

? In the next window, enter a unique Volume Group name. Use up to 24 alphanumeric characters. Select RAID Group and click **Create**.

▶ Create Volume Groups

Volume Group Name	vg0
Select Devices	<input checked="" type="checkbox"/>  RG0 (RAID Level 5, Resync (9.8%), 298.1GB)

Create
Cancel

? Following figure shows a successfully created Volume Group.

▶ Volume Groups

	Name	Size	Free	Usage	Status
	 vg0  RG0	298.1GB	298.1GB	 100.0% Free	ACTIVE
<div> Create Repair Extend Delete </div>					

5.3.2. Expanding a Volume Group

You can expand the Volume Group capacity by adding more RAID Groups or external Storage Device (Disk Array) to existing Volume Group if there is not enough space on the enclosure.

? Select a Volume Group to expand and Click **Extend**.

Volume Groups

	Name	Size	Free	Usage	Status
	vg0 RG0	298.1GB	298.1GB	 100.0% Free	ACTIVE

Create Repair **Extend** Delete

? Select RAID Group to add and click **Extend**.

Extend Volume Group

Volume Group Name	vg0
Select RAID Group(s)	<input checked="" type="checkbox"/> RG1 (RAID Level 0, ACTIVE, 298.1GB)

Extend Cancel

Following figure shows a successfully expanded Volume Group.

Volume Groups

	Name	Size	Free	Usage	Status
	vg0 RG0 RG1	596.1GB	596.1GB	 100.0% Free	ACTIVE

Create Repair **Extend** Delete

5.3.3. Deleting a Volume Group

You can delete a Volume Group but if there is a Volume that was created under the Volume Group, the Volume Group will not be deleted. You must delete the Volume prior to deleting the Volume Group.


? Select a Volume Group to delete and Click **Delete**.

Volume Groups

	Name	Size	Free	Usage	Status
	 vg0  RG0  RG1	596.1GB	596.1GB	 100.0% Free	ACTIVE

? A confirmation window will appear. Click **Yes** if the information is correct.

? Confirm Deleting The Following Volume Group:

Volume Group Name	 vg0
Size	596.1GB (596.1GB Free)
Status	ACTIVE

WARNING: This will delete the volume permanently. This cannot be undone. Continue?

[TIP]

If Volume has been configured under the RAID Group, deleting cannot be done. Deleting is done in below order:


Volume delete

↓
Volume Group delete

↓
RAID Group delete

5.4. Configuring Volumes

▢ Volumes

	Name	Size	Free	Usage	Status
	 vg0  vol	10GB	10.0GB	<div><div></div></div> 100.0% Free	ACTIVE

 Create
  Repair
  Quota
  Snapshot
  Extend
  Modify
  Delete

Volume is a logical partition of a Volume Group that enables you to create storage areas within the Volume Group. Volume is a subordinate of Volume Group, therefore, Volume Group must be created prior to creating a Volume. Volume size can be expanded within the capacity available on Volume Group.

5.4.1. Creating a Volume

Volume can be created under previously created Volume Group. Select a Volume Group that was created in the previous step and start Volume creation.

? Go to **Storage -> Volumes** and click **create**.

▢ Volumes

	Name	Size	Free	Usage	Status
--	------	------	------	-------	--------

 Create
  Repair
  Quota
  Snapshot
  Extend
  Modify
  Delete

[TIP]

Once Volume is created, a volume can be expanded but not shrunk. Therefore, it is important that you assign appropriate size at initial configuration.

? In the next screen, select Volume Group and enter Volume Name, Volume Group and the size. Use up to 24 alphanumeric characters for Volume name. Select the permissions and click **Create** when configuration is done.

▶ **Create Volume**

Volume Group	<input checked="" type="radio"/> vg0 (586.1GB Free)
Volume Name	<input type="text" value="vol2"/>
Volume Size	<input type="text" value="10"/> <input type="radio"/> MB <input checked="" type="radio"/> GB
Owner Of The Volume	<input type="text" value="{nas}"/>
Group Of The Volume	<input type="text" value="{system}"/>
User Permission	<input checked="" type="checkbox"/> Read <input checked="" type="checkbox"/> Write <input checked="" type="checkbox"/> Execution
Group Permission	<input checked="" type="checkbox"/> Read <input checked="" type="checkbox"/> Write <input checked="" type="checkbox"/> Execution
Other Permission	<input checked="" type="checkbox"/> Read <input type="checkbox"/> Write <input checked="" type="checkbox"/> Execution
User/Group Quota	<input checked="" type="checkbox"/> Enable

Heading	Definition
Volume Name	Name of the Volume
Volume Group	A Volume Group that the Volume belongs
Size	Capacity of the Volume.
Owner Of The Volume	A User that owns the Volume. If user is not created, select 'nas'.
Group Of The Volume	A group that the Owner of the Volume is belongs. If a group is not created, select 'System'.
User Permission	Permissions for the Owner of the Volume
Group Permission	Permissions for the users that are in the same group with the Owner of the Volume.
Other Permission	Permissions for all other users.
User/Group Quota	Enable Quota configuration for Users and Groups.

? The following screen shows when a Volume is created successfully. When a volume is created, a folder will be created under /Shared directory.

Volumes

	Name	Size	Free	Usage	Status
	vg0 vol	10GB	10.0GB	 100.0% Free	ACTIVE
	vg0 vol2	10GB	10.0GB	 100.0% Free	ACTIVE

Create
 Repair
 Quota
 Snapshot
 Extend
 Modify
 Delete

5.4.2. Deleting a Volume

You can delete a volume. If the volume is shared with other servers, you need to 'Unmount' the volume first.

? Select a volume to delete and click **Delete**.

Volumes

	Name	Size	Free	Usage	Status
	vg0 vol	10GB	10.0GB	 100.0% Free	ACTIVE
	vg0 vol2	10GB	10.0GB	 100.0% Free	ACTIVE

Create
 Repair
 Quota
 Snapshot
 Extend
 Modify
 Delete

. Confirm the information and click **Yes** if the information is correct.

? Confirm Deleting The Following Volume:

Volume Name	vol2
Volume Group	vg0 (576.1GB Free)
Volume Size	10GB (10.0GB Free)
Status	ACTIVE

WARNING: This will delete the Volume, and all existing data permanently. This cannot be undone.
Continue?

☐ Yes
 ☐ No

5.4.3. Modifying Volume Properties

You can modify volume properties including User, User Group, and Quota under this menu.

? Select the volume you want modified and click **Modify**.

► Volumes

	Name	Size	Free	Usage	Status
	vg0 vol	10GB	10.0GB	 100.0% Free	ACTIVE

Create
 Repair
 Quota
 Snapshot
 Extend
 Modify
 Delete

? Modify the categories and click **Modify** when done.

► Modify Volume

Volume Name	vol
Volume Group	vg0
Status	ACTIVE
Volume Size	10GB (10.0GB Free)
Owner Of The Volume	{nas}
Group Of The Volume	{system}
User Permission	<input checked="" type="checkbox"/> Read <input checked="" type="checkbox"/> Write <input checked="" type="checkbox"/> Execution
Group Permission	<input checked="" type="checkbox"/> Read <input checked="" type="checkbox"/> Write <input checked="" type="checkbox"/> Execution
Other Permission	<input checked="" type="checkbox"/> Read <input type="checkbox"/> Write <input checked="" type="checkbox"/> Execution
Quota	<input checked="" type="checkbox"/> Enable

Modify
 Cancel



[TIP]

User and Group cannot be created if there is no Volume. Create a Volume prior to create User and Group because you need to have at least one Volume to create User and Group. When User and Group are created, return to this menu to assign 'Owner Of The Volume' and 'Group

Of The Volume'.

Example of Modifying Volume Properties

Modify Volume

Volume Name	 vol	
Volume Group	 vg0	
Status	ACTIVE	
Volume Size	10GB (10.0GB Free)	
Owner Of The Volume	{nas}	
Group Of The Volume	{nas} user1	
User Permission	<input checked="" type="checkbox"/> Read <input checked="" type="checkbox"/> Write <input checked="" type="checkbox"/> Execution	
Group Permission	<input checked="" type="checkbox"/> Read <input checked="" type="checkbox"/> Write <input checked="" type="checkbox"/> Execution	
Other Permission	<input checked="" type="checkbox"/> Read <input type="checkbox"/> Write <input checked="" type="checkbox"/> Execution	
Quota	<input checked="" type="checkbox"/> Enable	

 Modify  Cancel

“Owner Of The Volume” shows list of registered users. Select a user that will own the volume. Apply the same for “Group Of The Volume”

5.4.4. Expanding a Volume

You can expand the capacity of an existing volume.

? Select a volume you want extended and click **Extend**.



► Volumes



	Name	Size	Free	Usage	Status
	 vg0  vol	10GB	10.0GB	<div><div></div></div> 100.0% Free	ACTIVE

 Create
  Repair
  Quota
  Snapshot
  **Extend**
 Modify
  Delete

? Check the size of the Volume Group first and then enter the capacity to extend. Click **Extend** when done.

► Extend Volume

Volume Name	 vol	
Current Volume Size	10GB (10.0GB Free)	<div><div></div></div>
Status	ACTIVE	
Volume Group	 vg0 (586.1GB Free)	<div><div></div></div>
Enter Extend Size	<input type="text" value="10"/> <input type="radio"/> MB <input checked="" type="radio"/> GB	

 Extend
  Cancel

5.4.5. Creating a Snapshot

A Snapshot creates a consistent, stable, point-in-time view of a volume. The Snapshot records any changes made in the volume to which it is linked. Once a Snapshot is taken, it filters out the changes that have been made to the volume since the Snapshot was taken. When complete, the Snapshot may be copied, stored, or backed-up. You may take multiple Snapshots to provide images of the volume at different points in time.








[Note]

The primary purpose of a Snapshot is to assist in the backup of a volume and are not intended as a sole backup device and not used for I/O service.

? Select a Volume that you want to create a Snapshot and click **Snapshot**.

Volumes





	Name	Size	Free	Usage	Status
	 vg0 vol	20GB	20.0GB	 100.0% Free	ACTIVE

 Create  Repair  Quota  **Snapshot**  Extend  Modify  Delete

? Enter Snapshot name and the size. The size of the Snapshot is dependant on the data I/O occurrence but normally, snapshot size of 15-20% of the Volume capacity is enough.



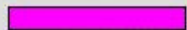

▶ Create Snapshot

- ! A Snapshot Volume is an alias for an existing Volume, but can only be accessed read-only and contains an image of the Volume "frozen in time", i.e. while applications continue to change the data on the Volume this logical device contains the unchanging image of the Volume of the time when the snapshot was created. This makes it possible to do a consistent backup without shutting anything down or using any special software, because this method is independent of any software.
- ! It can be as large (maximum of 1.1x the size of the original volume) or as small as you like but it must be large enough to hold all the changes that are likely to happen to the original volume during the lifetime of the snapshot.
- ! The snapshot does not need the same amount of storage the origin has. In a typical scenario, 15-20% might be enough. In case the snapshot runs out of storage, it can be extended.

Snapshot of	 vol		
Volume Group	 vg0 (576.1GB Free)		
Current Volume Size	20GB (20.0GB Free)		
Snapshot Name	<input type="text" value="2004-07-06-175511"/>		
Snapshot Size	<input type="text" value="2"/>	<input type="radio"/> MB	<input checked="" type="radio"/> GB

? The following figure shows a successfully create Snapshot

▶ Volumes





	Name	Size	Free	Usage	Status
	 vg0  vol	20GB	20.0GB	 100.0% Free	ACTIVE
	 2004-07-06-175511	2GB	2.00GB	 100.0% Free	Snapshot

5.4.6. Deleting a Snapshot

You can delete a snapshot if it does not have sufficient reserved space or when you need to create a new snapshot.

? Select a Snapshot you want to delete and click **Delete**.

Volumes

	Name	Size	Free	Usage	Status
	 vg0  vol	20GB	20.0GB	 100.0% Free	ACTIVE
	 2004-07-06-175511	2GB	2.00GB	 100.0% Free	Snapshot

? Confirm the information and click **Yes** if the information is correct.

Confirm Deleting The Following Volume:

Volume Name	 2004-07-06-175511
Volume Group	 vg0 (574.1GB Free) 
Volume Size	2GB (2.00GB Free) 
Status	Snapshot

WARNING: This will delete the Volume, and all existing data permanently. This cannot be undone.
Continue?

[Note]

Use with caution as deleting of Snapshot will result in all backup data loss in the Snapshot and it cannot be recovered.

5.5. Assigning Volume Quota

A Quota limits the amount of storage space on a volume that a user or group can consume. First enable quotas for a volume, and then assign the quotas to the individual users or groups. Between user and group, the priority goes to group first.

? Select a volume to assign user quota and click **Quota**.

► Volumes

	Name	Size	Free	Usage	Status
	vg0 vol	20GB	20.0GB	<div><div></div></div> 100.0% Free	ACTIVE

Create
 Repair
 Quota
 Snapshot
 Extend
 Modify
 Delete

? Assign quotas to each user or group and click **Save**. If it is set to '0 MB', it means the quota is unlimited. 'Select All Users' or 'Select All Groups' allow to assign identical amount of quota to all.

► Volume

Volume Name	vol
Volume Usage	20GB (20.0GB Free) <div><div></div></div> 100.0% Free

► Select users/groups

Name	Currently In Use	Limit
<input type="checkbox"/> user1 (staff1)	0.00 MB	Unlimited
<input type="checkbox"/> staff1	0.00 MB	Unlimited

Select All Users
 Select All Groups
 Unselect All
 Invert Selection

► Enter new quota limit




Limit (Enter 0 for unlimited)	<input type="text" value="0"/> MB
-------------------------------	-----------------------------------

Save
 Cancel

5.6 Backup/Restore



This menu provides backup/restore of data in ExtremeStor-iNAS to Singe SCSI tape device.

Backup

Select Tape Device	
Volume Directory	<input type="text"/> 
Type	<input checked="" type="radio"/> Full Backup <input type="radio"/> Incremental Backup Level 1 
Options	<input type="checkbox"/> Overwrite the tape <input type="checkbox"/> Send backup result alert mail

 History  Backup

Restore

Select Tape Device	
Target	<input checked="" type="radio"/> Restore to the following directory
Volume Directory	<input type="text"/> 
Options	<input checked="" type="checkbox"/> Restore quota settings <input type="checkbox"/> Don't overwrite existing files <input type="checkbox"/> Send restore result alert mail

 History  Restore

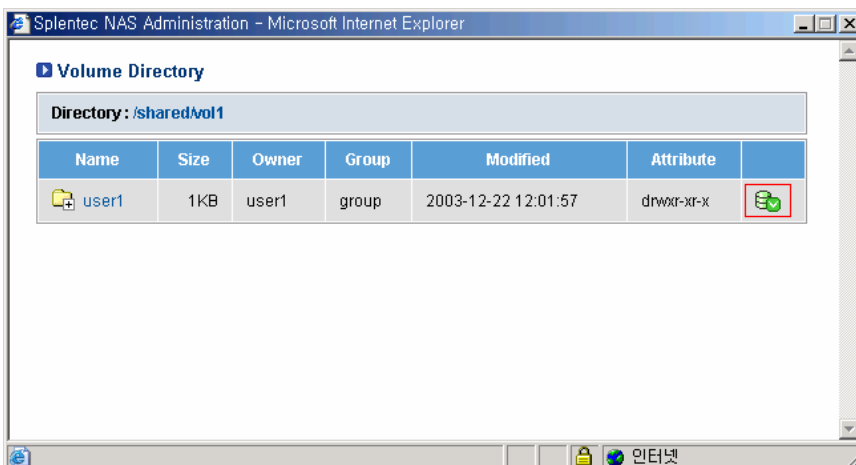
5.6.1 Backup

? Select Tape Device by clicking pull down menu.

Backup

Select Tape Device	
Volume Directory	<input type="text"/>
Type	<input checked="" type="radio"/> Full Backup <input type="radio"/> Incremental Backup <input type="text" value="Level 1"/>
Options	<input type="checkbox"/> Overwrite the tape <input type="checkbox"/> Send backup result alert mail



? Click on Folder icon in Volume Directory and it shows list of User Home Directories in all volumes. Select volumes or User Home Directories to backup. Then click on Green icon to designate the selected ones as backup source. After everything is done, click on Backup button to commence backup.



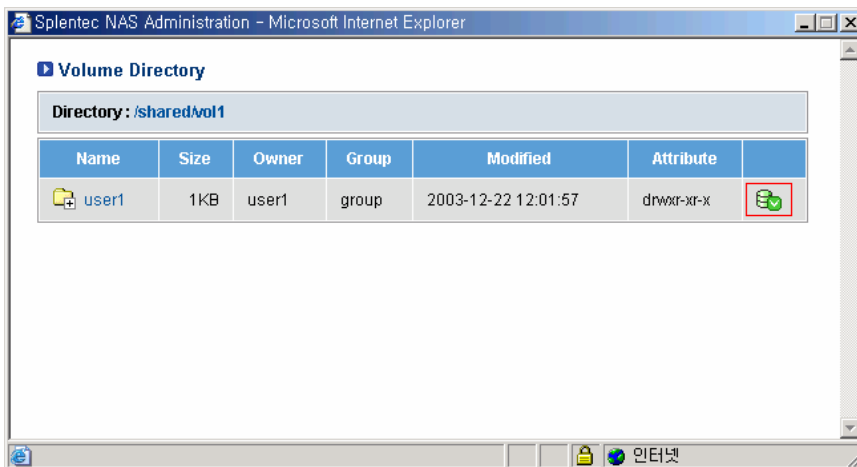
5.6.2 Restore

? Select Tape Device where backed up file resides.

▶ Restore

Select Tape Device	
Target	<input checked="" type="radio"/> Restore to the following directory
Volume Directory	<input type="text"/> 
Options	<input checked="" type="checkbox"/> Restore quota settings <input type="checkbox"/> Don't overwrite existing files <input type="checkbox"/> Send restore result alert mail

? Click on Folder icon in Volume Directory and it shows list of User Home Directories in all volumes. Restore is done as identical to Backup. Select volumes or User Home Directories to restore. Then click on Restore button to commence restore.




5.7. iSCSI

In this section, you can enter the values for iSCSI options. The default are the most optimized values, therefore we recommend you to keep the default values.

[Note]

Please connect your local Technical supports for iSCSI settings.

▣ iSCSI Settings

 These settings are only for advanced users, and now are ready to be used by iSCSI Target and Initiator. If you are not sure about these settings, they can be used as optimal settings, because these settings have already carefully optimized.

Session Type	Normal
Max Connections	1
Target Portal Group Tag	1
Initial R2T	0
Bidirectional Initial R2T	1
Immediate Data	1
Max Burst Size	524288
First Burst Size	262144
Default Time To Retain	20
Default Time To Wait	2
Max Outstanding R2T	1
Data PDU In Order	1
Data Sequence In Order	1
Error Recovery Level	0
Header Digest	None,CRC32C
Data Digest	None,CRC32C
OFMarker	0
IFMarker	0
OFMarker Interval	2048
IFMark Interval	2048
Authentication Method	None
Max Receive PDU Data Size	32768

6. Capacity Expansion by iSCSI

ExtremeStor-iNAS supports flexible capacity expansion by allowing remote devices and RAID Groups to be used as local disks and this method is called Export and Import.

Export : A job that supports sharing of local disks with other ExtremeStor-iNAS systems. Exported disks cannot be used as local disks by its own system. That means the unit that exports devices will become Storage Unit.

Import : A job that supports sharing of remote devices to be used as local disks. The unit that exports the devices will become Master(Controlling) unit. The maximum of 128 devices can be imported

6.1. EXPORT/UNEXPORT/IMPORT/UNIMPORT in Devices

ExtremeStor-iNAS allows to add devices for capacity expansion.

6.1.1. Exporting devices



? Select the device you want exported and click **Export**.

 h0b3t3i0	Seagate ST3160023AS	160.0GB	Available	 Export
--	---------------------	---------	-----------	--

? In the next window, Disk ID and Target Name will be automatically assigned from the system. The System also assigns Target Alias but you could change it to your preferred name. Click **Export**. (The Target Name will be used when importing the exported device.)







Export Devices



Disk ID	h0b3t3i0
Target Name	iqn.2000-10.com.splentec.splentec-h0b3t3i0
Target Alias	device h0b3t3i0 on splentec-splentec

 Export
  Cancel

? Confirm that device are exported as iSCSI Target in the following figure.

Devices

Device	Model	Size	Status	Action
 h0b0t0i0	Seagate ST3160023AS	160.0GB	Used: RG0	
 h0b1t1i0	Seagate ST3160023AS	160.0GB	Used: RG0	
 h0b2t2i0	Seagate ST3160023AS	160.0GB	Available	 Export
 h0b3t3i0	Seagate ST3160023AS	160.0GB	iSCSI Target	 iSCSI...

 Rescan
  Import

[TIP]

Copy the target name and paste it to the 'Remote Target Name' box when importing.

6.1.2. Unexporting devices

? Click **iSCSI..** to unexport the device.



? Click **Unexport** to unexport the device.

Exported Device Settings

Disk ID	h0b3t3i0
Target Name	iqn.2000-10.com.splentec.splentec-h0b3t3i0
Target Alias	device h0b3t3i0 on splentec-splentec



[TIP]







In order to unimport the device successfully, unimport the device first and then unexport the device.



6.1.3. Importing devices

After exporting, it is required to import the device to be used as local system.

? Click **Import** on bottom of the Screen. Rescan button is for refreshing the status of the devices.

▣ Devices



Device	Model	Size	Status	Action
 h0b0t0l0	Seagate ST3160023AS	160.0GB	Used: RG0	
 h0b1t1l0	Seagate ST3160023AS	160.0GB	Used: RG0	
 h0b2t2l0	Seagate ST3160023AS	160.0GB	Available	 Export
 h0b3t3l0	Seagate ST3160023AS	160.0GB	iSCSI Target	 iSCSI...

 Rescan
  Import

? In the next window, enter the values for Remote Target Name and Remote IP Address and click **Import**.

▣ Import Remote Device

Remote Target Name	<input type="text"/>
Remote IP Address	<input type="text"/>

 Import
  Cancel









Remote Target Name	The target name of another ExtremeStor-iNAS that the device will be imported to (that means the device that is exported in the previous section.)
Remote IP Address	The IP address of another ExtremeStor-iNAS that exported the device..



6.1.4 Unimporting devices

If you want to stop sharing of devices to other ExtremeStor-iNAS system, ExtremeStor-iNAS allows to unimport the device. Unimport means the device is no longer used by the NAS system that has imported the device and the device will be used in its original NAS system.

? Select **iSCSI** in under Action.

▶ Devices

Device	Model	Size	Status	Action
 h0b0t0l0	Seagate ST3160023AS	160.0GB	Used: RG0	
 h0b1t1l0	Seagate ST3160023AS	160.0GB	Used: RG0	
 h0b2t2l0	Seagate ST3160023AS	160.0GB	Available	 Export
 h0b3t3l0	Seagate ST3160023AS	160.0GB	iSCSI Target	 iSCSI...
 1.2.3.234:H0B0T9L0	iqn.2000-10.com.splentec.40cf18d3-h0b0t9l0	36.7GB	Available	 iSCSI...

 Rescan
  Import

? In the next window, click **unimport**.

▶ Imported Device Settings

Target Name	iqn.2000-10.com.splentec.40cf18d3-h0b0t9l0
Remote IP Address	1.2.3.234

 Reconnect
  Unimport
  OK

[TIP]

In order to unimport the device successfully, unimport the device first and then unexport the device.

6.2. EXPORT/UNEXPORT/IMPORT/UNIMPORT in RAID Group

6.2.1. Exporting RAID Group

? Select the RAID group you want exported and click Export

▶ RAID Groups

	Name	Level	Size	Status
⊙	<div>RG0</div> <div>h0b0t0i0 (160.0GB)</div> <div>h0b1t1i0 (160.0GB)</div>	RAID 0	298.1GB	ACTIVE

Create
Add Device
Import
Export
Delete

? In the next window, RAID Group and Target Name will be automatically assigned from the system. The System also assigns Target Alias but you could change it to your preferred name. Click **Export**. (The Target Name will be used when importing the exported device.)

▶ Export RAID Group

RAID Group	RG0
Target Name	iqn.2000-10.com.splentec.splentec-rg0
Target Alias	raid group rg0 on splentec-splentec

Export
Cancel

? Confirm that RAID Group is exported as iSCSI Target in the following figure.

▶ RAID Groups

	Name	Level	Size	Status
⊙	<div>RG0 - EXPORTED</div> <div>TN=iqn.2000-10.com.splentec.splentec-rg0</div> <div>Unexport</div> <div>h0b0t0i0 (160.0GB)</div> <div>h0b1t1i0 (160.0GB)</div>	RAID 0	298.1GB	ACTIVE

Create
Add Device
Import
Export
Delete

? When RAID Group is Exported, the system cannot operate S/W functions as it is working in iSCSI Storage mode.

! Results

The system is configured as a storage unit, the action is disabled on this system. Please connect to master unit for this action. You may reset the system to the factory default state for the further action

6.2.2. Unexporting RAID Group

? Click **Unexport** to unexport the device.

▶ RAID Groups

	Name	Level	Size	Status
	<div><div> RG0 - EXPORTED</div><div>TN=iqn.2000-10.com.splentec.splentec-rg0</div><div> Unexport</div><div> h0b0t0i0 (160.0GB)</div><div> h0b1t1i0 (160.0GB)</div></div>	RAID 0	298.1GB	ACTIVE
<div><div> Create</div><div> Add Device</div><div> Import</div><div> Export</div><div> Delete</div></div>				

6.2.3. Importing RAID Group

? Click **Import** on bottom of the Screen. Rescan button is for refreshing the status of the devices.

RAID Groups


	Name	Level	Size	Status
	 RG0  h0b0t0l0 (160.0GB)  h0b1t1l0 (160.0GB)	RAID 0	298.1GB	ACTIVE

 Create
  Add Device
  **Import**
 Export
  Delete

? In the next window, enter the values for Remote Target Name and Remote IP Address and click **Import**.

Import Remote RAID Group

Remote Target Name	<input type="text"/>
Remote IP Address	<input type="text"/>

 **Import**
 Cancel

Remote Target Name	The target name of another NAS that the device will be imported to (that means the device that is exported in the previous section.)
Remote IP Address	The IP address of another NAS that exported the device..

? Imported RAID Group will work as Local RAID Group.

Note


It is not recommended to use Import and Export under one NAS system.

6.2.4. Unimporting RAID Group

? Select **Unimport** in the imported RAID group..

RAID Groups

	Name	Level	Size	Status
	 RG0  h0b0t0i0 (160.0GB)  h0b1t1i0 (160.0GB)	RAID 0	298.1GB	ACTIVE
	 1.2.3.234:RG0 -  IMPORTED TN=iqn.2000-10.com.splentec.40cf18d3-rg0  Unimport	REMOTE	71.7GB	ACTIVE

 Create Add Device Import Export Delete

? When Unimport is performed successfully, RG0 of 192.168.100.11 will be removed from RAID Groups list.

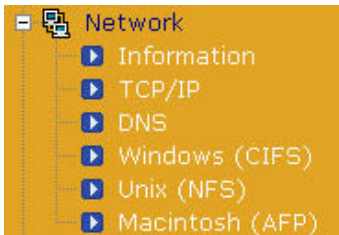
[TIP]

In order to unimport the RAID GROUP definitely, unimport the device first and then unexport the device.

7. Networking Options

This chapter provides an overview of the Network menu functions. It describes how to:

- Review network information.
- Configure network file protocols, including TCP/IP and DNS.
- Connect to the NAS from a client including, Windows, McIntosh OS, and Sun OS.



7.1. Information - Network Interface

Use this screen to check the network Status of NAS including IP Address, Subnet Mask, Gateway, and Network Card.

▶ Network Information

Port Name	eth0 (e1000)	eth1 (e1000)
Enabled	Yes	Yes
IP Address Obtained By	static	static
IP Address	192.168.1.1	1.2.3.232
Subnet Mask	255.255.255.0	255.255.255.0
Default Gateway	192.168.1.1	
Ethernet Address	00:30:48:71:E9:A9	00:30:48:71:E9:A8
Link Status	Not connected	Connected
Speed	Unknown(65535)	1000Mb/s
Duplex	Unknown(255)	Full Duplex

[Refresh](#)

TCP/IP is a configuration of the three network cards on NAS. IP Address has been assigned with DHCP, however, it is recommended use static IP Address.


7.2. TCP/IP - Modifying Network configuration

Select a network card that you want modified among the three and TCP/IP Settings window will appear. Enter the IP Address, Subnet Mask, and Default Gateway.

TCP/IP Settings

Select an Adapter	eth0 (tg3)
Adapter Information	Connected, MAC: 00:04:76:F6:A4:79
Enable	<input checked="" type="checkbox"/> Enable the selected adapter <input type="radio"/> Obtain TCP/IP settings automatically using DHCP
Settings	<input checked="" type="radio"/> Use the following settings: IP Address: <input type="text"/> Subnet Mask: <input type="text"/> Default Gateway: <input type="text"/>
	<input checked="" type="radio"/> Advanced settings
	<input checked="" type="radio"/> Set up trunking with eth0 interface
	<input type="checkbox"/> Force full duplex mode

WARNING: After changing the TCP/IP settings, existing sessions may be disconnected, including this WebAdmin session.

 Save

7.2.1. Network trunking

☒ Advanced settings
☒ Set up trunking with eth0 interface

Network Trunking is bonding two or more NIC to improve Network Performance. It will configure based on the first NIC of eth0.

? In 'Select an Adapter' menu, select eth1 and then select "Set up trunking with eth0 interface" to bond two NICs.

7.2.2. Force Full duplex mode

This command is to provide Full Duplex Mode in force in case HUB doesn't support Full Duplex Mode. .

7.3. Domain Name Sever (DNS)

Modification of Domain Server is available in DNS menu. Enter the Domain Server if there is one connected to the network.

DNS

Domain Name	<input type="text"/>
DNS1 IP Address	<input type="text" value="168.126.63.1"/>
DNS2 IP Address (* Optional)	<input type="text"/>
DNS3 IP Address (* Optional)	<input type="text"/>

 Save

7.4. Windows (CIFS) Access

You can configure CIFS Share to share a volume in ExtremeStor-iNAS to Windows clients. Windows clients can access the Volumes and use it as its local directory.

In order to share access for CIFS, the following are required:

- ✍ A created volume
- ✍ The volume requires to be registered to Share list.
- ✍ User ID is required to connect to the shared volume. (Using Active Directory)

? Go to **Network->Windows (CIFS)** and click **Add** under **CIFS Shares**.

** The service menu is for Active Directory. Enter the Domain Name that you have created under Primary Domain Controller (PDC) and select Domain in the Security field. When you click on Save button, the system will automatically add the users who are registered under PDC.

Service

Enable Service	<input checked="" type="checkbox"/>
Security	<input checked="" type="radio"/> Workgroup <input type="radio"/> Domain
Workgroup / Domain Name	WORKGROUP
Wins Server	
Domain Server	*
Domain User Options	<input type="checkbox"/> Create Home Directories For Domain Users
Domain User Home Volume	
Description	SPLNTEC NAS
Share User's Home Dir	<input type="radio"/> Yes <input checked="" type="radio"/> No
Allow public file sharing (No password)	<input type="radio"/> Yes <input checked="" type="radio"/> No

Save

CIFS Shares

	Name	Volume	Description	Permission
<p>Add Modify Delete</p>				

In case of CIFS Share, "Share User's Home Dir" shows User's Home Directory with the shared Volume.

? Enter Share name and select a volume to share and its permissions.

Share Name	Enter a unique share name.. When connecting to ExtremeStor-iNAS from Windows, this name will be shown as a Directory..
Select volume to Share	Select a volume to share under the 'Share Name'.
Permission	The two permissions, Read Only and Read/Write, are available for users. (The available permissions can be modified on ACL).
Description	Enter more explanation of the share.

? Enter a share name (for example 'nas_share' in the below figure) and click **Add**.

■ Add Share

Share Name	<input type="text" value="nas_share"/>
Select Volume To Share	<div>(Path, User, Group)</div> <div>/shared/vol, {nas}, {system}</div>
Permission	<input type="checkbox"/> Read Only <input type="checkbox"/> Public (No Password)
Description	<input type="text"/>

☞ The following screen shows 'nas_share' CIFS share has been created successfully.

■ CIFS Shares

	Name	Volume	Description	Permission
<input checked="" type="radio"/>	nas_share	/shared/vol		Read/Write

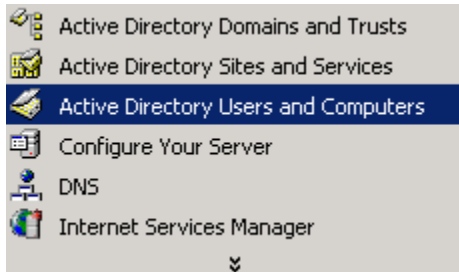
[TIP]

In Permission, Read only means shared volume can be only read.

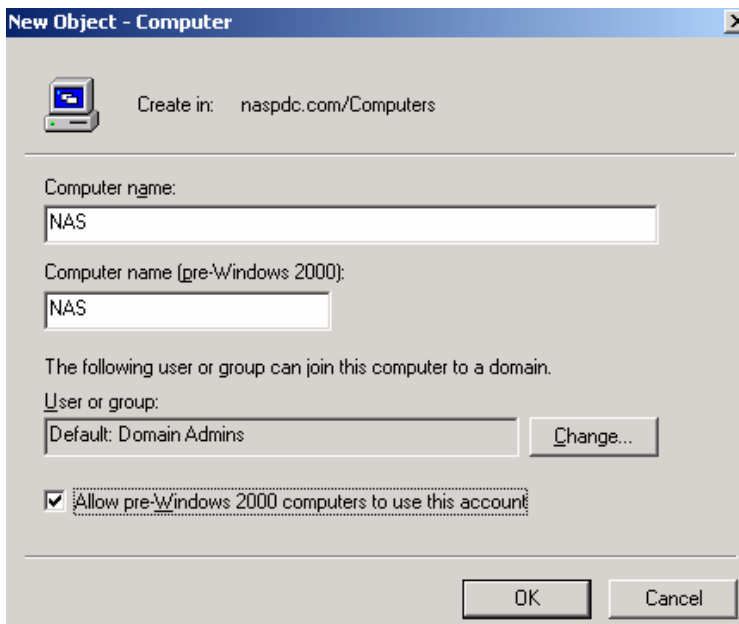
Public (No Password) means shared volume can be access without User ID and Password.

7.4.1. Configuring Active Directory

? In PDC, select **Computer** in New Object under Active Directory Users and Computers.
PDC? Active Directory Users and Computers ?? New Object? Computer ??? ?? .



? In order to use the default account in PDC, enable “**Allow pre-Windows 2000 computer to use this account**”.



[TIP]

Computer name: enter the Host Name of NAS. Host Name is configured at System -> General menu in ExtremeStor-iNAS Web Interface.

? Enable the service and enter the DNS Name of PDC at Workgroup/Domain Name field and click **Save**. In case the DNS Name is Naspdc.com, just enter “**naspdc**”.

Service

Enable Service	<input checked="" type="checkbox"/>
Security	<input type="radio"/> Workgroup <input checked="" type="radio"/> Domain
Workgroup / Domain Name	<input type="text" value="naspdc"/>
Domain Server	<input type="text" value="*"/>
Domain User Options	<input type="checkbox"/> Create Home Directories For Domain Users
Domain User Home Volume	<input type="text" value="/shared/vol1"/>
Description	<input type="text" value="NAS"/>
Share User's Home Dir	<input checked="" type="radio"/> Yes <input type="radio"/> No
Allow public file sharing (No password)	<input checked="" type="radio"/> Yes <input type="radio"/> No

 Save

CIFS Shares

	Name	Volume	Description	Permission
--	------	--------	-------------	------------

 Add  Modify  Delete

? When the configuration is completed successfully, the following message will be displayed.




Results

System successfully joined to the domain: naspdc

 OK

? In Modify Volume menu, you can check that the system has joined 'naspdc' domain successfully and displays default accounts of PDC in 'Owner Of The Volume' and 'Group Of The Volume' fields.

► Modify Volume

Volume Name	 vol1		
Volume Group	 nas_vol		
Status	ACTIVE		
Volume Size	186GB (185.98GB Free)		
Owner Of The Volume	<input type="text" value="user1"/>		
Group Of The Volume	<input type="text" value="group1"/>		
User Permission	group1		
Group Permission	NASPDC\Domain Admins		
Other Permission	NASPDC\Domain Users		
Quota	NASPDC\Domain Guests		
	NASPDC\Domain Computers		
	NASPDC\Domain Controllers		
	NASPDC\Cert Publishers		
	NASPDC\Schema Admins		
	NASPDC\Enterprise Admins		
	NASPDC\Group Policy Creator Owners		
	NASPDC\DnsUpdateProxy		

7.5. Unix (NFS) Access

UNIX servers can use the storage space in ExtremeStor-iNAS as if it is their local directory.






? Go to **Network->Unix(NFS)** and click **Add** under **NFS Share**. As same for CIFS, ExtremeStor-iNAS supports shares for volumes.

▶ Service

Enable Service	<input checked="" type="checkbox"/>
----------------	-------------------------------------

 Save


▶ NFS Shares

	Volume	Host	Permission	Option
<div>  Add  Delete  Add Host  Modify Host  Delete Host </div>				

? Select a Volume to share, Host, and the permission for users.

▶ Add NFS Share Directory

Select Volume To Share	(Path, User, Group) /shared/vol, {nas}, {system}
Description	
Host	*
Permission	<input type="radio"/> Read Only <input checked="" type="radio"/> Read / Write <input checked="" type="checkbox"/> Allow Root Access
Options	

 Add  Cancel

Select Volume to Share	Select a volume to share in NFS. For Unix, Share name will be entered in the Unix Server.
Description	Enter more explanation of the share.
Host	Enter a Host that can be shared with NFS. Host means Host name or IP Address of Unix or Linux server that is remotely performing NFS Mount after NFS share is configured. ("*" means NAS supports mount by all NFS protocols.)
Permission	The two permissions, Read Only and Read/Write, are available for users. Allow Root Access means allowing the Root to access the NFS share.

Options	You can set the options. Refer to man page 'share NFS' in NFS or 'Export' in Linux
---------	---


? The following screen shows NFS share has been created successfully. Now you can select a volume and host to use and configure permissions.

▶ Service

Enable Service	<input checked="" type="checkbox"/>
----------------	-------------------------------------

 Save

▶ NFS Shares

	Volume	Host	Permission	Option
	/shared/vol	*	Read / Write, Allow Root Access	

 Add
  Delete
  Add Host
  Modify Host
  Delete Host

? Configuring NFS Mount in the server:

1) Linux Server

```
[root@LinuxServer:/] mount -t nfs 192.168.100.10:/shared/vol1 /mnt
```

2) UNIX Server

```
[root@UnixServer:/] mount -F nfs 192.168.100.10:/shared/vol1 /mnt
```

? In case of adding NFS Host in 'Read Only' mode.

▶ Add NFS Share Host

Shared Volume	/shared/vol
Host	<input type="text" value="192.168.100.40"/>
Permission	<input checked="" type="radio"/> Read Only <input type="radio"/> Read / Write <input checked="" type="checkbox"/> Allow Root Access
Options	<input type="text" value="Read Only-Solaris8"/>

 Add
  Cancel

[TIP]

To allow only specific host to share NFS service, enter the Host Name or IP Address of the host in 'Add Host' field. To modify previous configuration, go to 'Modify Host'.


7.6. Macintosh (AFP) Access

AFP is a network shared protocol that is used in Macintosh. In order to use shared Volume, it is required to create Share list. Just clicking on Add button will create the list automatically.




? Go to **Network->Macintosh(AFP)** and click **Add** under **AFP Shares**.

Service

Enable Service	<input checked="" type="checkbox"/>
AppleTalk Over IP	<input checked="" type="radio"/> Yes <input type="radio"/> No
AppleTalk Address	<input type="text"/>
Share User's Home Dir	<input type="radio"/> Yes <input checked="" type="radio"/> No

 Save




AFP Shares

	Name	Description
<div>  Add  Modify  Delete </div>		

? Select a Volume to share and click **Add**. ExtremeStor-iNAS supports shares for volumes.

Add AFP Share

Volume Name	(Path, User, Group) /shared/vol, {nas}, {system}
	<input type="text"/>
Description	<input type="text"/>

 Add
  Reset
  Cancel

? Confirm that AFP Share has been created successfully.

▶ Service

Enable Service	<input checked="" type="checkbox"/>
AppleTalk Over IP	<input checked="" type="radio"/> Yes <input type="radio"/> No
AppleTalk Address	<input type="text"/>
Share User's Home Dir	<input type="radio"/> Yes <input checked="" type="radio"/> No

 Save

▶ AFP Shares

	Name	Description
<input checked="" type="radio"/>	/shared/vol	nas_share

 Add

 Modify

 Delete

? Using AFP share in Mac:

When Login window appears in Mac, enter the user ID and password that is created in ExtremeStor-iNAS. If it is not shown in Mac Chooser screen, indicate the server such as afp://ipaddress and you will be able to use it.

[TIP]

Appletalk address is consisted of a node number and a network number that are same as IP Address in TCP/IP. However, Appletalk address is automatically assigned by the system therefore it is unnecessary to change.


8. Maintenance

This Chapter explains how to maintain the system.

8.1. Update OS

Use **Update OS** to update OS to new version. Select the file to update by using Browse and click Update OS.

▶ Update OS

 **WARNING:** The system should be restarted after updating the OS. If you are ready to update OS and the system is ok to be restarted, select a patch file and click the [Update OS] button below. Please note that after pressing [Update OS] button, it may take more than one minute before you see the results screen.

Current OS Version	1.1H.748
Select New Patch File	<input type="text"/> <input type="button" value="찾아보기..."/>

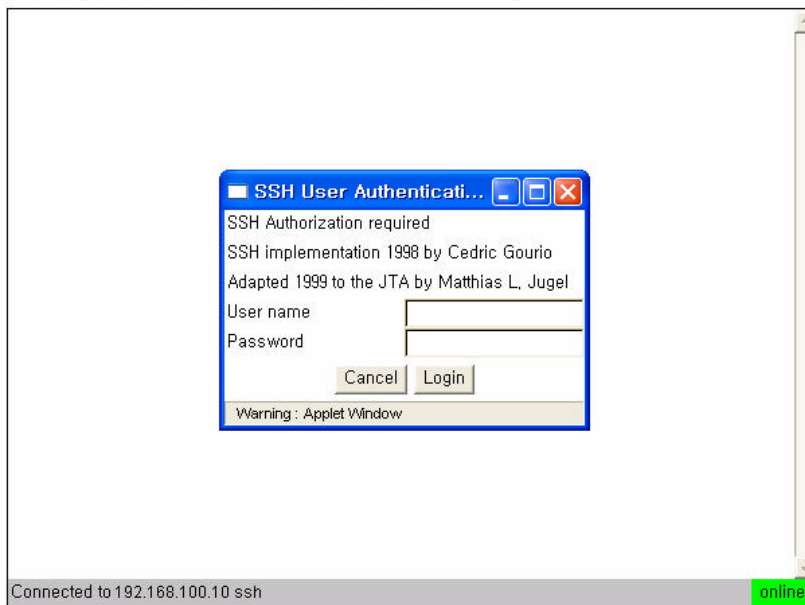
8.2. Console

Connect to ExtremeStor-iNAS on the Web interface with SSH Shell is available in Console menu. You can connect to ExtremeStor-iNAS from remote terminal and it provides high security.

[Note]

The default login are ID: root and password: ExtremeStor-iNAS.

▶ To begin, click inside of the black box after successful login...



8.3. Support

When a problem occurs to the system, clicking 'Submit' button will transfer configuration and log files to ExtremeStor-iNAS Support Center for analyzing the system. Mail server needs to be configured for sending mails.

■ Contacts

For technical support:
Send an [email to technical support](#)

■ Tech Support Report

The system information can be emailed to Splentec NAS Technical support to help us assist you with your problem. The email will include log files, system configuration files, and system status reports, but not including any form of confidential information. The information submitted will be used only for the technical support.

Enter Email Recipient	<input type="text" value="support@globalstor.com"/>
Send Full Logs	<input checked="" type="radio"/> Yes <input type="radio"/> No

Submit

[TIP]

You can configure maximum of three emails accounts for Tech Support Report. There should be no space between the accounts.

Eg) [white@globalstor.com:red@globalstor.com:blue@globalstor.com](#)

8.4. UPS Service

ExtremeStor-iNAS supports UPS service setting to attach UPS system.

? Select UPS type and UPS cable under drop down menu. Then select Serial Connection Port and click on Save button to commence the service.

** It is required to purchase Serial Cable that comes along with the UPS system. Standard Serial cable may not work.

UPS Service

Enable Service	<input type="checkbox"/>
UPS Type	smartups
UPS Cable	smart
Serial Connection Port	/dev/ttyS0


 Save

8.5. System Data Backup/Restore

This menu allows System configuration settings including network configuration, file system information (RAID, Volume) User/Group Quota, etc. that resides in Flash Memory to be backed up in HDD. It provides quick restoration to current system settings in case of system or flash memory failure


? Select Configuration backup file and click on Restore.

Backup Configuration Settings

 The current NAS configuration settings can be saved to your local system, and this configuration file can be used later to restore the old settings. Please note that this will include every configuration settings, but not any data on volumes.

 Backup

Restore Configuration Settings

 **WARNING:** The system should be restarted after restoring the old configuration settings. Please note that old configuration settings files also include your(admin) password setting, and network configuration settings.

Select configuration backup file

찾아보기...

 Restore

9. Security (User accounts)

ExtremeStor-iNAS uses 128bit encryption for security and connecting to the system is only available with SSH when using Web server and remote connection. ExtremeStor-iNAS follows Unix security system for user accounts, therefore in order to access the storage of ExtremeStor-iNAS, configuration of users and Groups are required.

User name and Password should be specified correctly to create user accounts and note that the system doesn't allow special characters.

You can also create Groups and Groups are created only by the System Administrator. Group ID starts from 500 by defaults.

It is required to create Group prior to creating User so that the user can be added to the group.

9.1. Defining a Group




Groups

	Name	Group ID	Members
<div>  </div>			

? Go to **Security -> Groups** and click **Add** button to define a group. In the next screen, enter a unique name for the group you want to create and the group ID. Click **Add** when done.

Add Group

Group Name	<input type="text" value="group1"/>
Group ID	<input type="text" value="500"/>

9.1.1. Group Import

This menu allows to import Group information that is saved in the existing server and use the same Groups in ExtremeStor-iNAS system. Using this option, you can avoid to create new groups in ExtremeStor-iNAS system.

? Click **Import** under Users.

Users

	Name	User ID	Group Name	Real Name	Home Directory
 Import  Add  Modify  Delete					



? Use 'Browse' button to find the file that contains Group information.

Import group file

Import a /etc/group file to create group accounts. Any group accounts, that have same groupnames, or GIDs will be skipped during the import.

Select An Existing Group File

Browse...

 **Import**
 **Cancel**

? The following figure shows successfully imported 'group' file.











File Import Results

-  group user1 (GID:500) imported successfully
-  group user2 (GID:501) imported successfully
-  group user3 (GID:502) imported successfully
-  group user4 (GID:503) imported successfully
-  group user5 (GID:504) imported successfully
-  group user6 (GID:505) imported successfully
-  group user7 (GID:506) imported successfully
-  group user8 (GID:507) imported successfully
-  group user9 (GID:508) imported successfully
-  group user0 (GID:509) imported successfully

 **OK**

. Check that the Groups are registered successfully.

Groups

	Name	Group ID	Members
	user1	500	
	user2	501	
	user3	502	
	user4	503	
	user5	504	
	user6	505	
	user7	506	
	user8	507	
	user9	508	
	user0	509	

[Import](#)[Add](#)[Modify](#)[Delete](#)

[TIP]

The passwords file exists in '/etc/passwd' directory in Unix systems. Download the file by FTP or other file transfer method and modify the file to contain only necessary information.




9.2. Defining a User

Users

	Name	User ID	Group Name	Real Name	Home Directory
<div>  Import  Add  Modify  Delete </div>					

? You need to have user ID to access the shared volume of ExtremeStor-iNAS. Go to **Security - > Users** and click **Add** button to define a user. In Add User screen, enter the user name, real name, password, user ID, Group name and click **Add** when done.

Add User

Username	user1
Real Name	test-user
Enter Password	*****
Confirm Password	*****
User ID	500
Group Name	Same As User Name
Base Home Directory	/shared/vol1
Home Directory	/shared/vol1/user1
<div>  Add  Reset  Cancel </div>	

User ID	Enter User ID.
Group Name	You can create a new group that the user will belong to or select from existing groups.
Base Directory	The Volume that the user will be used.
Home Directory	A Directory under the Volume that the user will be used.
Description	More explanation of the user.

9.2.1 User import

This menu allows to import 'passwd' file that is saved in the existing server and use the same users in ExtremeStor-iNAS system. Using this option, you can avoid to create new users in ExtremeStor-iNAS system.

? Click **Import** under Users.

Users

	Name	User ID	Group Name	Real Name	Home Directory
<div> <input type="button" value="Import"/> <input type="button" value="Add"/> <input type="button" value="Modify"/> <input type="button" value="Delete"/> </div>					

? Use 'Browse' button to find the file that contains User ID & Password.

Import passwd file

Import a /etc/passwd file to create user accounts. Any user accounts, that have same usernames, or UIDs will be skipped during the import. User accounts will be created with the same password, which is specified below. Please be advised that a group file must be imported before the passwd file. User's passwords can be changed by users on the WebAdmin login screen with their own username & password.

Base Home Directory	/shared/vol
Password For New User Accounts	globalstor
Select An Existing Passwd File	C:\Wpasswd <input type="button" value="Browse..."/>

"Password For New User Accounts" means default passwords that will be assigned to all newly created users. The above figure shows an example that all new users will have password of 'spntec' by default. Each user can change the password later.

? The following figure shows successfully imported 'passwd' file.

File Import Results

- user user1 (UID:500) imported successfully
- user user2 (UID:501) imported successfully
- user user3 (UID:502) imported successfully
- user user4 (UID:503) imported successfully
- user user5 (UID:504) imported successfully
- user user6 (UID:505) imported successfully
- user user7 (UID:506) imported successfully
- user user8 (UID:507) imported successfully
- user user9 (UID:508) imported successfully
- user user0 (UID:509) imported successfully

? Check that the users are registered successfully.

► Users

	Name	User ID	Group Name	Real Name	Home Directory
	user1	500	user1		/shared/vol/user1
	user2	501	user2		/shared/vol/user2
	user3	502	user3		/shared/vol/user3
	user4	503	user4		/shared/vol/user4
	user5	504	user5		/shared/vol/user5
	user6	505	user6		/shared/vol/user6
	user7	506	user7		/shared/vol/user7
	user8	507	user8		/shared/vol/user8
	user9	508	user9		/shared/vol/user9
	user0	509	user0		/shared/vol/user0

Import

Add

Modify

Delete

[TIP]

The passwords file exists in '/etc/passwd' directory in Unix systems.

Download the file by FTP or other file transfer method and modify the file to contain only necessary information.

9.3. Modifying User information.

After System Administrator has created User account, the actual user can change his password.

? In the login window of the Web Interface, enter the username and the password.

Administration Login



Username	<input type="text" value="user1"/>
Password	<input type="password" value="•••••"/>

Login

? In the next window, enter the new password and click **Save**.

Change Password


User Name	user1
Real Name	
User ID	500
Group Name	group1
Enter Current Password	<input type="password"/>
Enter New Password	<input type="password"/>
Confirm New Password	<input type="password"/>

 Save  Cancel

9.4 Connection

This is an option for 'rsh' and 'rlogin' support.

Connection

 **WARNING:** For security reasons, the services are disabled by default. The system not properly administrated are vulnerable to unauthorized access. Avoid using rsh, rlogin, telnet, ftp, instead use ssh, scp, sftp.

Enable	<input checked="" type="checkbox"/> Allow root rsh access <input checked="" type="checkbox"/> " " Allow root rlogin
Trusted host	<input type="text" value="192.168.100.30"/>

Save

Trusted host: normally use 'FQDN (Fully Qualified Domain Name) hostname' of rsh client.

ex) Linux> rsh 192.168.100.10 ps -ef

ex) Linux> rlogin 192.168.100.10 -l root

[Warning]

As it could cause security problem, **unclick** the enable checkbox when this menu is not in use.

10. Access Control Lists (ACLs)

10.1. Introduction to Access Control Lists (ACLs)



Access Control Lists (ACLs) comprise a list of access control entries(ACE). Each ACE is the metadata stored on the file system that determine the access parameters for a user or group.

The advantages are:

- ✍ You can set detailed permission on objects (files and folders) for all users on ExtremeStor-iNAS, including Active Directory or NT 4.0 server users
- ✍ You can set the default inheritance on a directory so that subordinate objects inherit permissions set on the directory.

You can assign the following access permissions to specific files and folders on ExtremeStor-iNAS system.

Read	User/Group can only read the contents of the files/folders
Write	User/Group can create, modify, delete files but not read files/folders
Execution	User/Group can execute any program.


Example of using ACL

You can assign access permissions to Individual user or folders (such as folders for departments in company) according to the usage.




Folders (Departments)	Permissions		
Sales	Read	write	Execute
Management	Read	X	Execute
Marketing	X	Write	X
Development	X	X	Execute

After configuration is done, like the above table, ExtremeStor-iNAS will refer to the configuration and control the access of users.

10.2. Configuring ACL

? Select a directory you want to perform ACL and click on  icon.

▶ ACL

Directory: /shared					
Name	Owner	Group	Modified	Attribute	
 vol  ACL Backup	{nas}	{system}	2004-07-06 19:06:56	drwxrwxr-x	

? Select Owner of the directory, Group to use the directory and permissions to the directory.


▶ Object

Directory Name	/shared/vol
Modified	2004- 7- 6 19:06:56
Owner	<input type="text" value="user1"/>
Group	<input type="text" value="staff1"/>
User Permission	<input checked="" type="checkbox"/> Read <input checked="" type="checkbox"/> Write <input checked="" type="checkbox"/> Execution
Group Permission	<input checked="" type="checkbox"/> Read <input type="checkbox"/> Write <input checked="" type="checkbox"/> Execution
ACL Mask	<input checked="" type="checkbox"/> Read <input checked="" type="checkbox"/> Write <input checked="" type="checkbox"/> Execution
Other Permission	<input type="checkbox"/> Read <input type="checkbox"/> Write <input type="checkbox"/> Execution


 Save

▶ ACL




Name	Permission	
------	------------	--

 Add  Save  Cancel

10.3. Adding user to ACL

? Select a directory you want to add user to and click on  icon.


▶ ACL

Directory: /shared					
Name	Owner	Group	Modified	Attribute	
 vol  ACL Backup	{nas}	{system}	2004-07-06 19:06:56	drwxrwxr-x	

? In the next window click **Add**.

▶ Object

Directory Name	/shared/vol
Modified	2004- 7- 6 19:06:56
Owner	{nas} ▼
Group	{system} ▼
User Permission	<input checked="" type="checkbox"/> Read <input checked="" type="checkbox"/> Write <input checked="" type="checkbox"/> Execution
Group Permission	<input checked="" type="checkbox"/> Read <input checked="" type="checkbox"/> Write <input checked="" type="checkbox"/> Execution
ACL Mask	<input checked="" type="checkbox"/> Read <input checked="" type="checkbox"/> Write <input checked="" type="checkbox"/> Execution
Other Permission	<input checked="" type="checkbox"/> Read <input type="checkbox"/> Write <input checked="" type="checkbox"/> Execution

 Save

▶ ACL

Name	Permission	
------	------------	--

 Add  Save  Cancel

? Select user and permissions to add and click **Save**.

▶ Add ACL Entry

Select ID	<div>user: user</div>
Permission	<div><input checked="" type="checkbox"/> Read <input checked="" type="checkbox"/> Write <input checked="" type="checkbox"/> Execution</div>

Add

No

- . Confirm that **User 1** has been added to ACL.

▶ **Object**

Directory Name	/shared/vol
Modified	2004- 7- 6 19:06:56
Owner	{nas} ▾
Group	{system} ▾
User Permission	<input checked="" type="checkbox"/> Read <input checked="" type="checkbox"/> Write <input checked="" type="checkbox"/> Execution
Group Permission	<input checked="" type="checkbox"/> Read <input checked="" type="checkbox"/> Write <input checked="" type="checkbox"/> Execution
ACL Mask	<input checked="" type="checkbox"/> Read <input checked="" type="checkbox"/> Write <input checked="" type="checkbox"/> Execution
Other Permission	<input checked="" type="checkbox"/> Read <input type="checkbox"/> Write <input checked="" type="checkbox"/> Execution

 Save












▶ **ACL**

Name	Permission	
 user1	<input checked="" type="checkbox"/> Read <input checked="" type="checkbox"/> Write <input checked="" type="checkbox"/> Execution	


 Add  Save  Cancel

- ? Check the configuration of ACL on File and Directory.

▶ **ACL**

Directory: /shared/vol/user1						
Name	Size	Owner	Group	Modified	Attribute	
 Component	1KB	user1	staff1	2004-07-06 19:48:08	drwxr-xr-x	
 FileGroups	1KB	user1	staff1	2004-07-06 19:48:08	drwxr-xr-x	
 Media	1KB	user1	staff1	2004-07-06 19:48:08	drwxr-xr-x	
 RegistryEntries	1KB	user1	staff1	2004-07-06 19:48:11	drwxr-xr-x	
 Script Files	1KB	user1	staff1	2004-07-06 19:48:12	drwxr-xr-x	
 Setup.map	40KB	user1	staff1	2004-06-28 13:46:32	-rwxr--r--	

? Notice that the icon has changed in the last column.

 Setup.map	40KB	user1	staff1	2004-06-28 13:46:32	-rwxr--r--	
---	------	-------	--------	---------------------	------------	---




[TIP]

You can configure separate permissions on file and directory by using ACL.

10.4. Deleting user from ACL

? Select a directory you want to delete user from and click on  icon.

▶ ACL

Directory : /shared					
Name	Owner	Group	Modified	Attribute	
 vol  ACL Backup	{nas}	{system}	2004-07-06 19:52:39	drwxrwxr-x	

? Click on an icon that looks like Trash Can.

▶ Object

Directory Name	/shared/vol
Modified	2004- 7- 6 19:52:39
Owner	{nas} ▼
Group	{system} ▼
User Permission	<input checked="" type="checkbox"/> Read <input checked="" type="checkbox"/> Write <input checked="" type="checkbox"/> Execution
Group Permission	<input checked="" type="checkbox"/> Read <input checked="" type="checkbox"/> Write <input checked="" type="checkbox"/> Execution
ACL Mask	<input checked="" type="checkbox"/> Read <input checked="" type="checkbox"/> Write <input checked="" type="checkbox"/> Execution
Other Permission	<input checked="" type="checkbox"/> Read <input type="checkbox"/> Write <input checked="" type="checkbox"/> Execution

 Save

▶ ACL

Name	Permission	
 user1	<input checked="" type="checkbox"/> Read <input checked="" type="checkbox"/> Write <input checked="" type="checkbox"/> Execution	

 Add  Save  Cancel

? Confirm the information and click **Yes**.

? Confirm Deleting The Following ACL entry:


Name	 vol
ACL ID	 user1

WARNING: This will delete the ACL entry permanently. This cannot be undone. Continue?




☐ Yes

☐ No

10.5. Backing up ACL


? Select a directory you want to backup and click on  icon.

▶ ACL

Directory: /shared					
Name	Owner	Group	Modified	Attribute	
 vol  ACL Backup	{nas}	{system}	2004-07-06 20:00:35	drwxrwxr-x	

? Enter backup name and click **Create**.

▶ Create ACL Backup

Volume Name	 vol
Backup Name	ACL-2004-07-06-200308
Options	<input checked="" type="checkbox"/> Include ACLs on subfolders and files

 Create



☐ Cancel

? Confirm the backed up ACL.

▶ Volume

Volume Name	 vol
-------------	---

▶ Saved ACLs

	Name	Size	Created
	 ACL-2004-07-06-200308	6KB	2004- 7- 6 20:05:30

 Create Restore Delete Cancel

10.6. Restoring ACL

? Select an ACL to restore and click **Restore**.

Volume

Volume Name	 vol
-------------	---



Saved ACLs

	Name	Size	Created
	 ACL-2004-07-06-200308	6KB	2004- 7- 6 20:05:30

 Create  Restore  Delete  Cancel

? Confirm the information and click **Yes**.

? Confirm Restoring The Following ACL Backup:

Volume Name	 vol
ACL File	 ACL-2004-07-06-200308

WARNING: This will restore all ACL entries from the ACL Backup file, Continue?

 Yes  No

11. Monitoring



This Chapter covers how to use the Monitoring. It includes the following information:

- Status
- Statistics
- Reviewing the event log
- Event log settings

11.1. Status

This menu shows the status of CIFS, AFP, and NFS connections.

▶ Current CIFS Connections

Service	User	Group	System	Connection Date	
IPC\$	user1	staff1	skyfire (1.2.3.26)	Tue Jul 6 19:47:20 2004	
nas_share	user1	staff1	skyfire (1.2.3.26)	Tue Jul 6 19:48:59 2004	

▶ Current AFP Connections

User	Group	System	Connection Date	
------	-------	--------	-----------------	--

▶ NFS Connection History

Mount Point	IP Address
-------------	------------

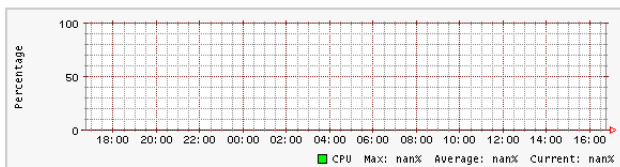
11.2 Statistics

This menu displays Disk I/O, Network I/O, CPU Load, and Temperature status in graph form.

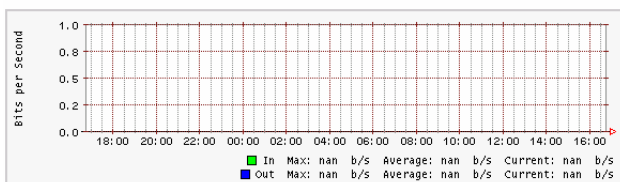
Updated: Thu Apr 24 16:43:17 2003

Daily (5 Minutes Average)

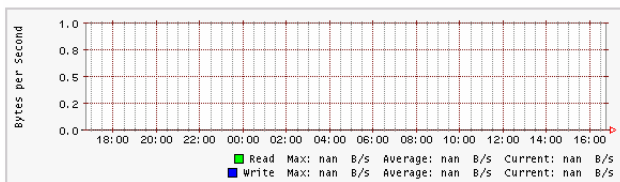
CPU Utilization



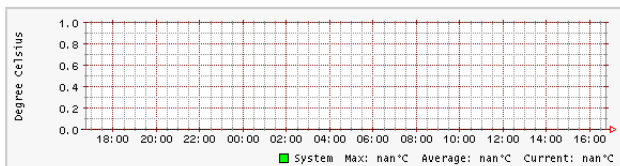
Network Traffic



Disk I/O



Temperature



11.3. Reviewing the Event Log





You can view the summary of all operations performed on the server including system operation kernel, and booting. When error occurs to the system you could promptly check the status of the system and recover from the error immediately.

View Events contains summary of the events that occurs in System Operation and program service.

View Kernel Logs contains summary of the events that occurs in Kernel level, mainly about devices.

View Boot Logs contains errors and other events that occur while booting the system.

[Following are the icons and the definitions]

 Debug	For program debug. Customer can ignore this message
 Information	Status of the system
 Panic	System down
 Warning	Error

11.4 Log Settings

In this menu, you could set the Log size, displaying, and whether to email the log files to the administrator when it is full.

Log Settings

Log Debug Messages	<input checked="" type="checkbox"/>
Maximum Log Size	<input type="text" value="5"/> MB (1~5)
Display Lines Per Page	<input type="text" value="100"/>
Email Log Files When Full	<input type="checkbox"/> Enable

[Save](#)