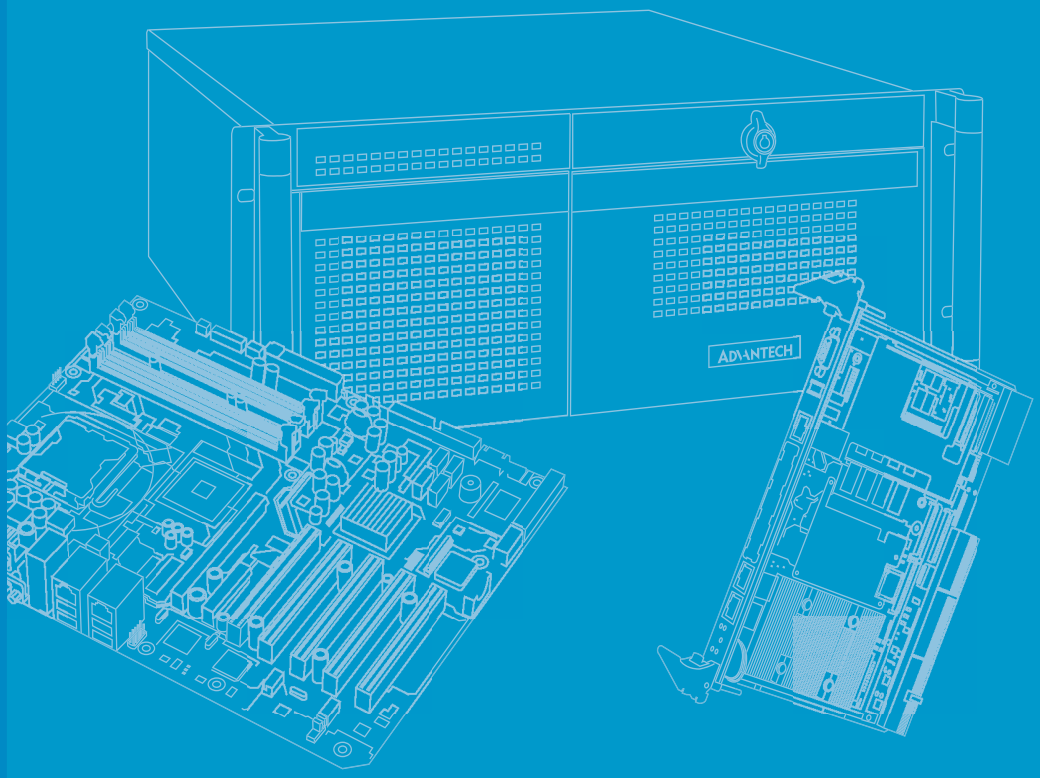
User Manual



ASR-5300I Series

SANWatch Web-Based Interface

ADVANTECH

Enabling an Intelligent Planet

Copyright

Acknowledgements

Part No. 2001R53040 Edition 1

Printed in Taiwan April 2016

Contents

Chapter 1 Overview 1

1.1 Introduction 2
1.2 Connecting SANWatch to Storage Subsystems 3
1.2.1 Elements of a Storage Subsystem Network 3
1.2.2 Computer Requirements 3

Chapter 2 Installation 5

2.1 Installing Java 6
2.2 Initiating SANWatch Installation 7
2.3 Installing SANWatch 10
2.4 Installing the EonPath (Multipathing) Driver 13
2.5 Installing the VSS Module (for Windows) 13
2.6 Uninstalling/Upgrading SANWatch 14

Chapter 3 SANWatch Interface 15

3.1 Introduction 16
3.2 Navigating the User Interface 16
3.2.1 Logging onto the User Interface 16
3.2.2 Changing Login Passwords 17
3.2.3 Getting to Know the User Interface 18
3.2.4 Navigating the Interface 19
3.3 Working with the Devices View 20
3.3.1 Viewing the Hardware List and Status 20
3.3.2 Adding a New Device (RAID Subsystem or JBOD Expansion Enclosure) 21
3.3.3 Removing a Device (RAID Subsystem or JBOD Expansion Enclosure) 23
3.3.4 Editing Groups and Group Assignments 23
3.3.5 Exporting System Settings 25
3.3.6 Resetting/Shutting Down the System 25
3.4 Data Replication 26
3.4.1 Opening the Replication Manager 26
3.4.2 Diagnosing the Network Status for Replication 28
3.4.3 Creating a Volume Copy 29
3.4.4 Creating a Volume Mirror 33
3.4.5 Editing/Deleting a Replication Pair 36
3.4.6 Mapping the Source or the Target to Host LUN 36
3.4.7 Switching the Roles of a Replication Pair 43
3.4.8 Syncing a Replication Pair 44
3.4.9 Using the Incremental Recovery Option in Asynchronous Mirroring 44
3.4.10 Configuring Automatic Failover for Remote Replication 45
3.5 Notifying Users of System Events 48
3.5.1 Activating Notification Settings 48
3.5.2 Notification via Email 49
3.5.3 Notification via Fax 50
3.5.4 Notification via SMS 52
3.5.5 Notification via SNMP 53
3.5.6 Notification via Broadcasting 54
3.5.7 Sending the System Log to Users 55

Chapter 4 Working with Devices 57

4.1 Introduction 58
4.2 Viewing the Overall Status 58
4.2.1 Monitoring System Performance 60
4.2.2 Viewing the Hardware Status LED 61
4.2.3 Viewing System Information 64
4.3 Configuring System Settings 66
4.3.1 Summary of System Configurations 67
4.3.2 Updating the Firmware 70
4.3.3 Configuring Voltage/Temperature Thresholds 73
4.3.4 Configuring the IP Address 74
4.3.5 Configuring Power Saving Settings 76
4.3.6 Configuring Time Settings 77
4.3.7 Trunking Host Interfaces to Increase Bandwidth 78
4.3.8 Muting the Beeper 79
4.3.9 Exporting System Settings 79
4.3.10 Exporting/Importing NVRAM 79
4.4 Working with System Events 80
4.4.1 Types of Events 80
4.4.2 Viewing the Event Log 81
4.4.3 Exporting the Event Log 82
4.4.4 Activating Triggers (Thresholds) 82

Chapter 5 Working with Drives 85

5.1 Introduction 86
5.2 Viewing Drive Status 86
5.3 Scanning Drives 87
5.4 Cloning a Drive 89
5.5 Replacing a Drive 90
5.6 Identifying a Drive 91
5.7 Configuring Reserved Drive Space 92
5.8 Assigning Spare Drives 93
5.9 Monitoring Disk Drive Usage (Performance Monitor) 94

Chapter 6 Working with Channels 99

6.1 Introduction 100
6.2 Viewing Channel Configurations 100
6.3 Configuring the Host Channel Settings 101
6.4 Checking System Health 103

Chapter 7 Working with Hosts 105

7.1 Introduction 106
7.2 Adding a Host 106
7.3 Removing (Disconnecting) a Host 107
7.4 Editing Multipath Devices through EonPath 108
7.5 Monitoring Multipath Devices in EonPath 109
7.6 Flushing the Database Host Cache 110
7.7 Configuring In-Band Flushing Using a DB Flush Agent 112
7.8 Viewing DB Flush Events (Windows) 114
7.9 Using DB Flush Agent in Oracle 10g 115
7.10 Using DB Flush Agent in MS SQL 117
7.11 Enabling SA Login in MS SQL 120
7.12 Configuring Out-of-Band Flushing 123

Chapter 8 Working with Logical Volumes 125

8.1 Introduction 126
8.2 Viewing the Logical Volume Status 126
8.3 Configuring Logical Volume Properties 128
8.4 Adding a Logical Drive to an Existing Logical Volume 129

Chapter 9 Working with Logical Drives 131

9.1 Introduction 132
9.2 From Physical Drive to Logical Drive to Logical Volume 132
9.3 Viewing the Logical Drive Status 133
9.4 Adding Disk Drives to a Logical Drive 134
9.5 Expanding the Size of a Logical Drive 135
9.6 Configuring Logical Drives 136
9.7 Scanning Logical Drives 139
9.8 Migrating a Logical Drive Between RAID 5 and RAID 6 139
9.9 Rebuilding a Logical Drive 140

Chapter 10 Working with the Partitions View ...141

10.1 Introduction 142
10.2 General Rules 142
10.3 Viewing the List of Partitions 143
10.4 Creating a Partition 144
10.5 About Thin Provisioning 146
10.6 Provisioning and Reserved Space 147
10.7 Mapping/Unmapping Partitions to a Host 149
10.8 Deleting Partitions 155

Chapter 11 Working with Partitions 157

11.1 Introduction 158
11.2 Viewing Partition Status 158
11.3 Expanding Partitions 160
11.4 Reclaiming Unused Partition Space 161
11.5 Configuring Host LUN Maps 162
11.6 Managing LUN Mapping on the Host Side 162
11.7 Configuring Out-of-Band Flushing Using a DB Flush Agent 174

Chapter 12 Working with Snapshots.....179

12.1 General Snapshot Rules 180
12.2 Taking Snapshots 182
12.3 Recovering a Source Partition from a Snapshot (Rollback) 184
12.4 Mapping a Snapshot Image to the Host 185
12.5 Recovering a Database Volume from Grouped Snapshots 187
12.6 Creating a Volume Copy from a Snapshot Image 188
12.7 Making Backups of Snapshot Images 189

Chapter 13 Working with Schedules 191

13.1 Introduction 192
13.2 Viewing Schedules 192
13.3 Creating Schedules: General Rules 193

13.4 Taking Snapshots by Schedule 194
13.5 Creating a Volume Mirror by Schedule 196
13.6 Creating Tiered Data Migration by Schedule 199
13.7 Scanning Disk Drives by Schedule 201
13.8 Editing/Deleting Schedules 202
13.9 Backing Up or Restoring Schedule Settings 204

Appendix A TCP/IP and UDP Port Assignments..... 205

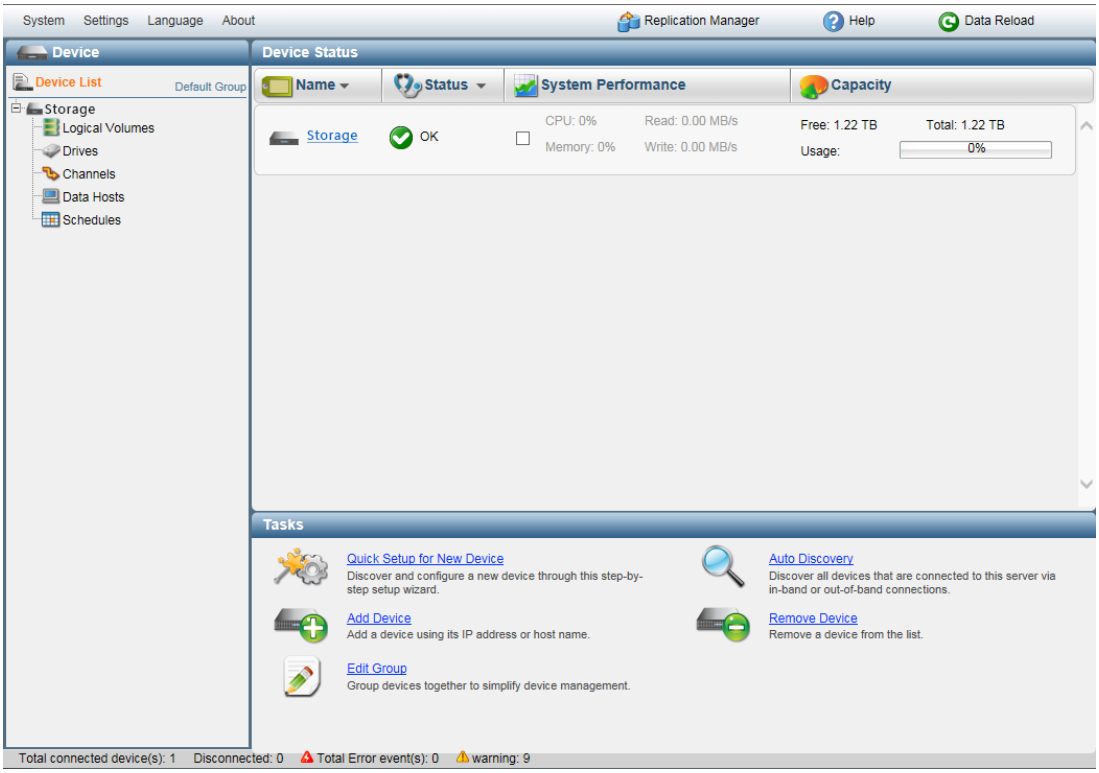
A.1 TCP/IP and UDP Port Assignments..... 206

Chapter 1

Overview

1.1 Introduction

The SANWatch browser interface is the proprietary software suite for Advantech's storage systems. SANWatch can be accessed via a web browser providing both the computer and subsystems are online. Users are no longer required to install complex desktop applications to the local computer because everything is available over the network.



1.2 Connecting SANWatch to Storage Subsystems

SANWatch, storage subsystems, and host computers can be connected in either an in-band (via host links) or out-of-band (via a LAN management port) connection. Because SANWatch is web-based, the GUI can be accessed from anywhere on the network. The flexible connection schemes allow users to manage SANWatch according to their specific needs and system configurations, particularly regarding the following two factors:

- Local management vs. remote management
- Full configuration vs. monitoring and notification

1.2.1 Elements of a Storage Subsystem Network

Storage Subsystems	A storage subsystem refers to a hard drive array (RAID subsystems + JBODs).
Host Computer	The host computer refers to the computer to which the storage subsystem's host links are connected.
Remote Computer	The remote computer refers to a computer on the network to which the host computer is connected via LAN.
In-Band Connection	In-band connection refers to the host computer and the storage subsystems connected through host links: Fibre, SAS, or iSCSI host connectors on the storage subsystem controller module.
Out-of-Band Connection	Out-of-band connection refers to the host computer and the storage subsystems connected through Ethernet: Management LAN connector on the storage subsystem controller module.

1.2.2 Computer Requirements

Computer Requirements	Hardware ■ Broadband access OS ■ Microsoft Windows 7, 8 (32/64 bit), Windows Server 2003 R2, 2008/2012 (32/64 bit) ■ Apple Mac OS X 10.5/10.6 or later ■ Redhat Linux Browser ■ Internet Explorer 7 or later ■ Firefox 3.5 or later ■ Google Chrome v15.0.874 or later
Firewall	If the browser-based interface cannot be accessed in a Windows environment (such as Windows Server 2003), the default network firewall setting of the OS is most likely set to "High," forbidding users from entering the user interface as an administrator. Please change the network settings in the OS.

Chapter 2

Installation

This section lists the installation procedures for SANWatch and other software modules included in the CD-ROM.

2.1 Installing Java

SANWatch installation requires Java version 6 or later. When installing SANWatch on a computer (details provided in the subsequent section), the installation wizard or scripts provided with the SANWatch installation CD will assist with Java 6 installation. However, users can also download an installation package from http://java.com/download to manually install a newer version.

Users wanting to install Java 6 via the SANWatch installation CD can skip to the next section.

For Windows	The Java installation package can be downloaded from http://java.com/download.
For Mac OS X	Before installing Java on a Mac, ensure the root user is enabled. For instructions on how to enable the root user, visit Apple Support. Manual installation of Java varies depending on the OS version. For OS X Snow Leopard 10.6 or earlier, users can install Java using Software Update (at the Apple icon > Software Update). For OS X 10.7 Lion or later, users can install Java by downloading an Java installation package from http://java.com/download.

For Linux	Below are brief instructions on how to download and install Java for Linux, and then enable Java in Firefox. For more options and details, visit http://java.com/download.
	Download the Java self-extracting binary file for Linux.
	Change the file permission to be executable.
	`chmod a+x jre-<version>-linux-i586.bin`
	Select the installation directory.
	`cd <directory path name>`
	Run the self-extracting file.
	`./jre-<version>-linux-i586.bin`
	Verify the jre <version> sub-directory under the current directory.
	Go to the plugins subdirectory in Firefox.
	`cd <Firefox installation directory>/plugins`
	Create a symbolic link.
	`ln -s <Java installation directory>/plugin/i386/ns7/libjavaplugin_oji.so`
	Start Firefox, and run this applet to verify Java installation.

For Solaris	Below are brief instructions on how to download and install the Java 6 self-extracting binary file for 32-bit Solaris, and then enable Java in Firefox. For more options and details, see Installation Package Overview > JRE Installation Procedures > JRE Plugin Installation Procedures for Firefox.
	Download the Java self-extracting binary file for Solaris.
	Change the file permission to be executable.
	`<SPARC processors> chmod +x jre-<version> <update> -solaris-sparc.sh`
	`<x86/x64/EM64T processors> chmod +x jre-<version> <update> -solaris-i586.sh`
	Select the installation directory, and run the self-extracting file.
	`<SPARC processors> ./jre-6 <update> -solaris-sparc.sh`
	`<x86/x64/EM64T processors> ./jre-6 <update> -solaris-i586.sh`
	Verify the jre1.6.0_<version> sub-directory under the current directory.
	Remove the symbolic links to libjavaplugin-oji.so and libnpjp2.so from the Firefox plugins directory.
	Create a symbolic link to the Java Plugin in the Firefox plugins directory.
	`ln -s <JRE>/lib/sparc/libnpjp2.so`
	Start the Firefox browser.
	Type `about:plugins` in the browser's location bar to verify Java Plugin installation.

2.2 Initiating SANWatch Installation

The methods and tools for SANWatch installation vary depending on the OS, but they are designed to assist with installing Java 6 (optional) and launching the SANWatch Installation Wizard.

For users who choose NOT to install the Java provided on the installation CD, ensure Java 6 or later is already installed on the computer.

For Windows	From the installation CD, locate the “SANWatch” folder and open “Setup.exe.” Proceed to the next section.
For Mac	From the installation CD, locate the “SANWatch” folder and open “install.app.” Proceed to the next section.

For Linux and Solaris

Note: Users wanting to install the data host only instead of the GUI-based SANWatch can skip to the next section.

Locate and copy the “SANWatch” folder on the installation CD to your computer.

Open the command line utility of your OS (such as Terminal for Linux), and log into the command line shell as root.

For Linux users, locate the “SANWatch” folder copied to your computer, and browse the contents to ensure the “linux.sh” script is in the folder. For users using Solaris, ensure “unix.sh” is in the folder.

```
 [root@localhost ~]# cd <computer_path>/fscommand/
 [root@localhost <computer_path>/fscommand]# ls -l
...
-rw-r--r--. 1 root root        4279 Jun 23 19:55 linux.sh
...
-rw-r--r--. 1 root root        2037 Jun 23 19:55 unix.sh
```

If using Linux, make “linux.sh” executable, and then execute it.

```
[root@localhost <computer_path>/fscommand]# chmod +x linux.sh
[root@localhost  <computer_path>/fscommand]#  ./linux.sh
```

If using Solaris, make “unix.sh” executable, and then execute it.

```
[root@localhost <computer_path>/fscommand]# chmod +x unix.sh
[root@localhost  <computer_path>/fscommand]#  ./unix.sh
```

The first two sections of the script will guide users through Java installation. If Java 6 or later is already installed on your computer, you can skip Java installation by typing “no” and pressing Enter. Otherwise, keep typing “yes” (shown below) and pressing Enter until Java is installed on your computer.

```
************************************************************
   Java-based GUI RAID Manager Installation Proce-
dure
  ************************************************************
SECTION I: JRE <version> Installation
...
Would you like to install JRE <version> now?
Please type yes or no.
yes
...
Done.
...
Install JRE v1.6.0_25 finished!
------------------------------------------------------------
SECTION II: Java Plug-in v1.2.2 Installation
...
Would you like to install Java Plug-in v1.2.2 now?
Please type yes or no.
yes
...
                Java(TM) Plug-in 1.2.2 Pre-Release
                  Binary Code Evaluation License
...
Do you agree to the above license terms?
If you do not agree to the terms, installation
cannot proceed
    Please type yes or no.
yes
```

The final section of the script asks whether users want to install SANWatch. Simply type “yes” and press Enter to proceed to the next section.

```
------------------------------------------------------------
SECTION III: Java-based GUI RAID Manager Instal-
lation
*NOTE: To install and configure Java-based GUI
RAID Manager successfully,
       We highly recommend you refer to INSTALLA-
TION GUIDE first.
Would you like to install Java-based GUI RAID Man-
ager now?
Please type yes or no.
yes
```

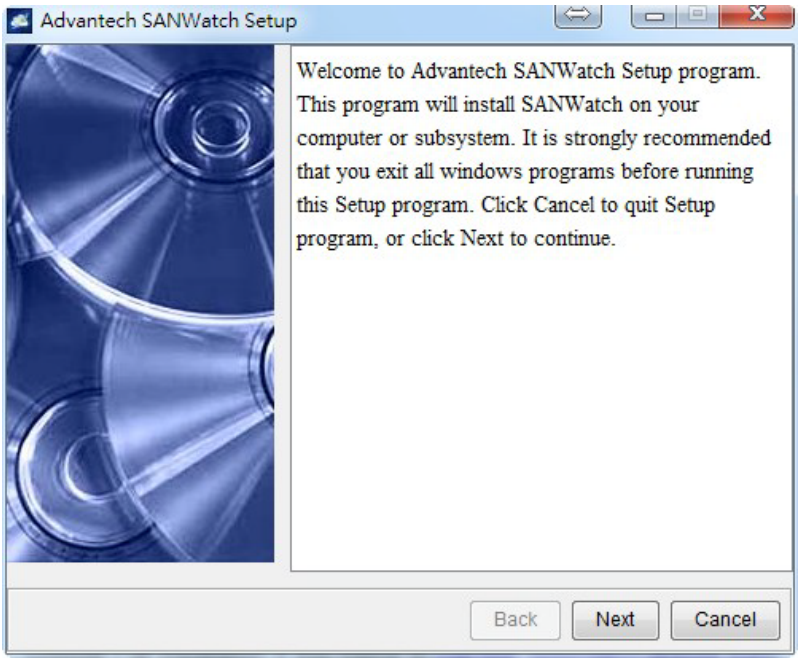
2.3 Installing SANWatch

This section explains how to install the entire web-based SANWatch GUI on various OS platforms.

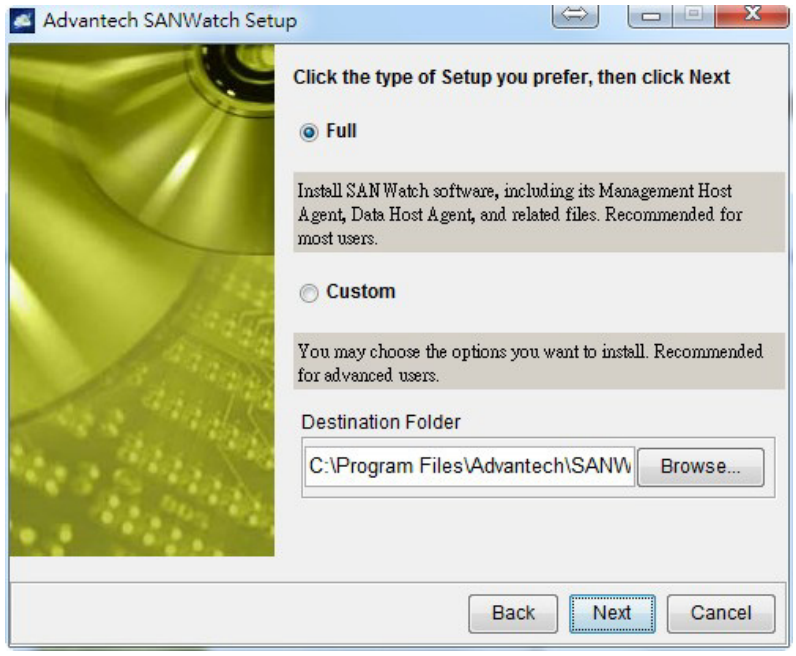
For the Linux platform, only the data host agent can be installed to reserve system resources.

Installing SANWatch

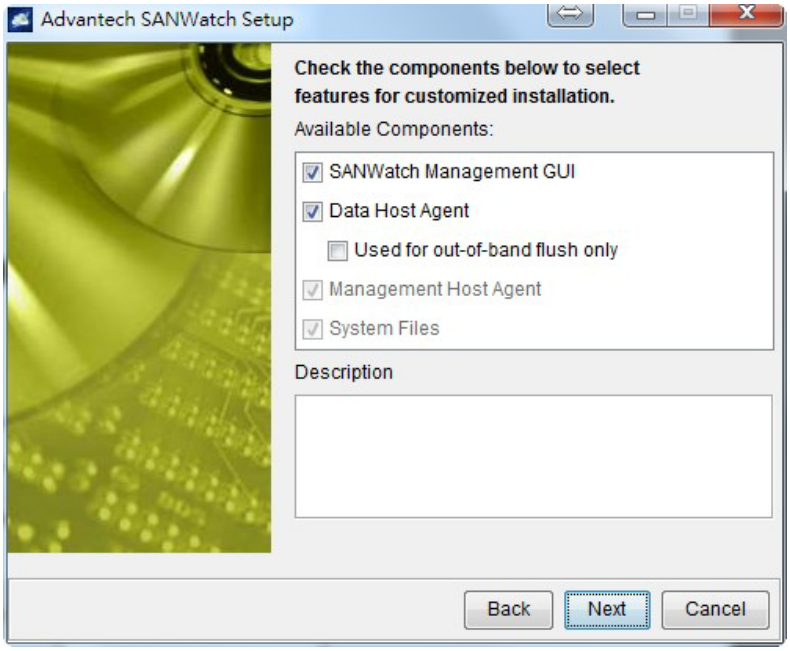
1. After initiating installation, users are guided to the SANWatch Setup wizard. Click Next to continue.



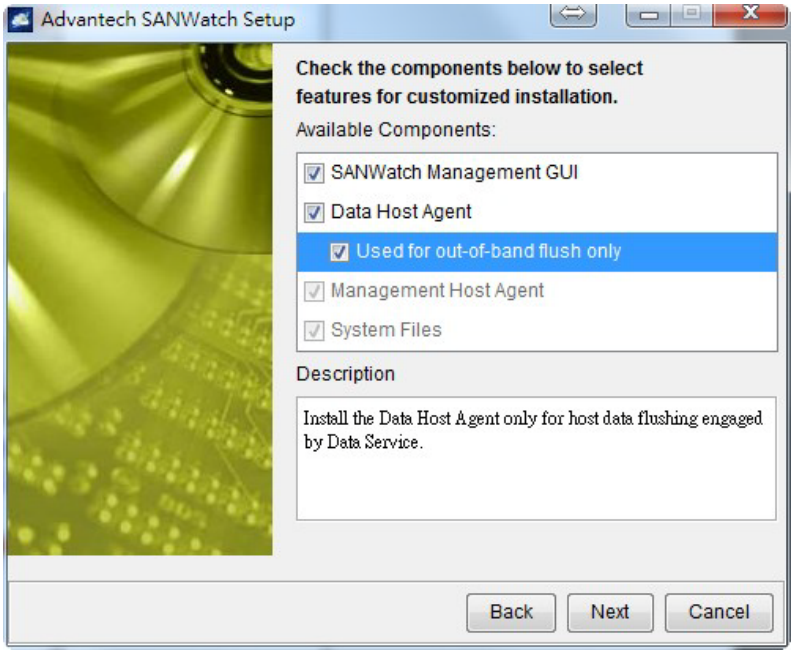
2. The installation program queries whether Full or Custom installation is preferred. Users can specify the installation folder here.
   Choose Full installation if you intend to manage SANWatch directly from the host computer. Then skip to Step 4.



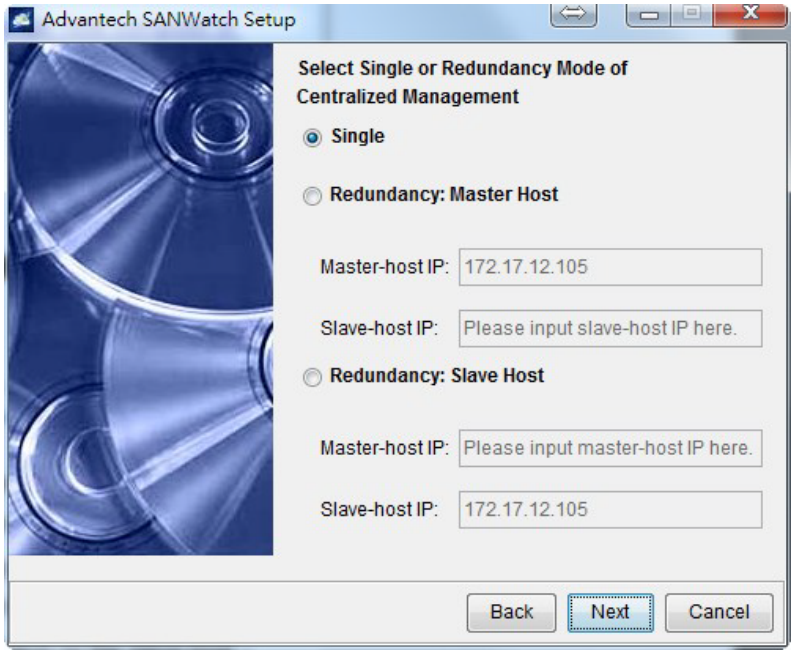
3. Otherwise, choose Custom installation, and in the Component List section, select the module(s) required according to the computer on which SANWatch is being installed.



If using DB Flush Agent to take snapshots with database applications, select Data Host Agent and/or Out-of-Band Flush Only. Click Next to continue.



4. Select whether SANWatch is to be installed on a single host computer or redundant host computers. For redundancy mode, specify the IP addresses of the master and slave host computers. If managing the RAID subsystem network using dual computers, we strongly recommend first installing and logging into SANWatch on the master host, and ensuring the system is online before installing SANWatch on the slave host.



When installation is complete, restart the computer.

Installing data host agent only (Linux command line)

1. Extract the SANWatch installation package using the following command:
   `unzip SANWatch_[x.0.x.xx].zip`
2. Navigate to the SANWatch directory:
   `cd SANWatch-[x.0.x.xx]`
3. Change the access permission of the executable file:
   `chmod 755 linuxCmd.sh`
4. Run linuxCmd.sh:
   `./linuxCmd.sh`
5. Type “yes” when prompted with the question “Would you like to install Java-based RAID Manager now?”
6. When asked whether to install all agents or selected agents only, use the “-s /usr/local dataHost” command to install the data host agent.

The data host agent should now be successfully installed and will be activated automatically during system startup, eliminating the need to manually start the service.

2.4 Installing the EonPath (Multipathing) Driver

Installation Procedures (Windows)

Activate SANWatch and enter the EonPath directory in the CD-ROM.

Select the suitable installation file and execute it.

File	OS Version	Bit
Eonpath-v1.23.2.50_2K8_2K12_x64	Windows Server 2008/2012	64-bit
Eonpath-v1.23.2.50_2K8_2K12_x86	Windows Server 2008/2012	32-bit
Eonpath-v1.23.2.50_2K8_2K12_x64_R2	Windows Server 2008/2012 R2	64-bit
Eonpath-v1.23.2.50_W7_x64	Windows 7	64-bit

The setup wizard will appear. Follow the instructions and complete the installation.

Restart the computer when installation is complete.

Open the Server Manager from Start > Administrative Tools > Server Manager.

In Server Manager, select Action > Add Features.

In the Features list that appears, select Multipath I/O and install it (if not already installed).

Configuration Steps (Mac OS)

Enter the “MPIO” folder and follow the instructions.

Here is the version information. For more details, refer to the product-to-version matrix from the vendor.

EonPath v2.01: MAC OS X 10.7

EonPath v1.01: MAC OS X 10.6

Configuration Steps (Linux OS)

The multipathing driver is supported in Linux OS natively.

2.5 Installing the VSS Module (for Windows)

VSS (Microsoft VisualSourceSafe) is a package for creating virtual libraries of computer files, including those in databases, in a Windows environment. VSS is required for taking snapshots while using database applications (Oracle, SQL, MS Exchange).

Installation Procedures

Activate SANWatch and enter the “VSS” directory in the CD-ROM.

Select the suitable installation file and execute it.

File	OS	Bit
VSS-v1.0.1.23_x86	Windows Server	32-bit
VSS-v1.0.1.23_x64	Windows Server	64-bit

The setup wizard will appear. Follow the instructions to complete the installation.

Reboot the computer when installation is complete.

Uninstalling/upgrading SANWatch

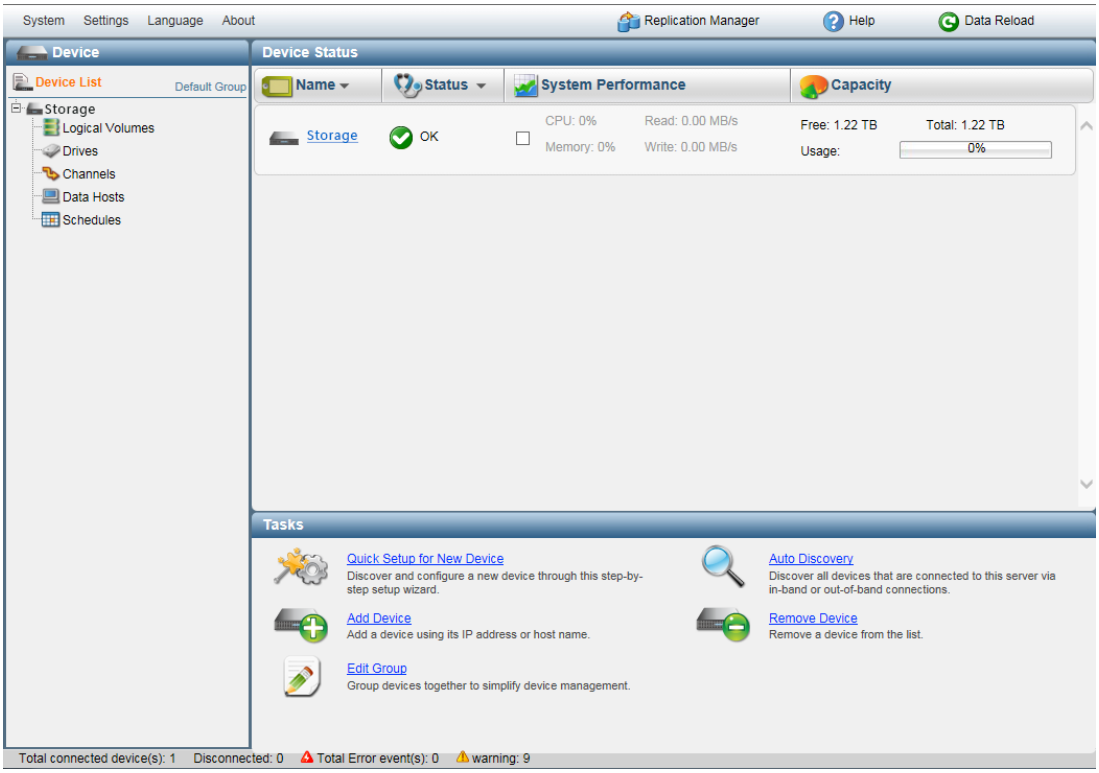
2.6 Uninstalling/Upgrading SANWatch

Uninstalling SANWatch	The procedure for uninstalling SANWatch is the same as that for any other application. In Windows, go to Start > All Programs > Advantech Inc > Uninstall SANWatch.
Upgrading SANWatch	To upgrade SANWatch to a newer version, uninstall the current version before installing the latest version. Visit the support site for the latest version of SANWatch.

Chapter 3

SANWatch Interface

3.1 Introduction



This chapter describes how to navigate the SANWatch Home interface and use the functions available from there. Users can learn the basic GUI elements and how to find online help tools, add and configure hardware devices (RAID subsystems or JBODs), as well as configure data replication (volume mirror and volume copy) and automatic event notifications.

3.2 Navigating the User Interface

3.2.1 Logging onto the User Interface

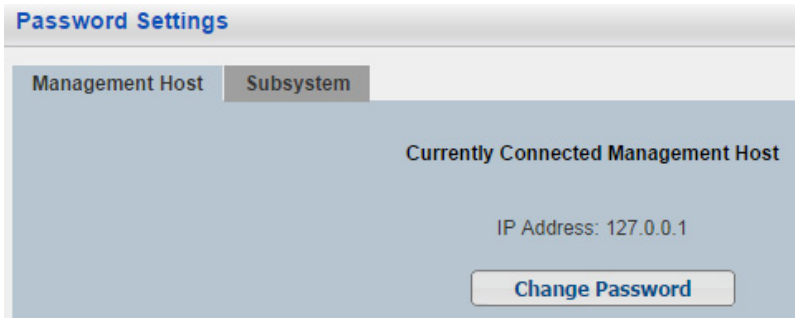
Logging onto the SANWatch Management Host Interface is easy and straightforward. Simply double click on the SANWatch icon.

Log On	The Log On screen will appear. Enter the password (the default password is **root**) and click Login. (Check Remember Password to automatically log onto the interface in the future.) The user interface will appear.
Log Off	Select the System > Log Off menu. The user interface will return to the Log On screen.

3.2.2 Changing Login Passwords

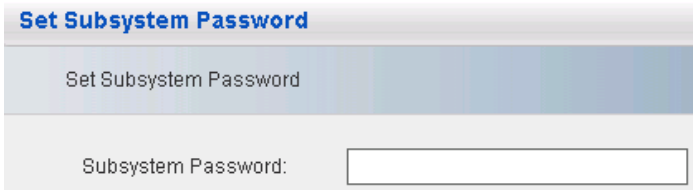
You can modify the default SANWatch login password, or set a new password for storage subsystems.

Go To	SANWatch Home > Top menu bar > Settings > Password Settings
Changing SANWatch Login Password	Select the Management Host tab, click Change Password, and enter the existing password and new password (twice for confirmation). The default login password is **root**.



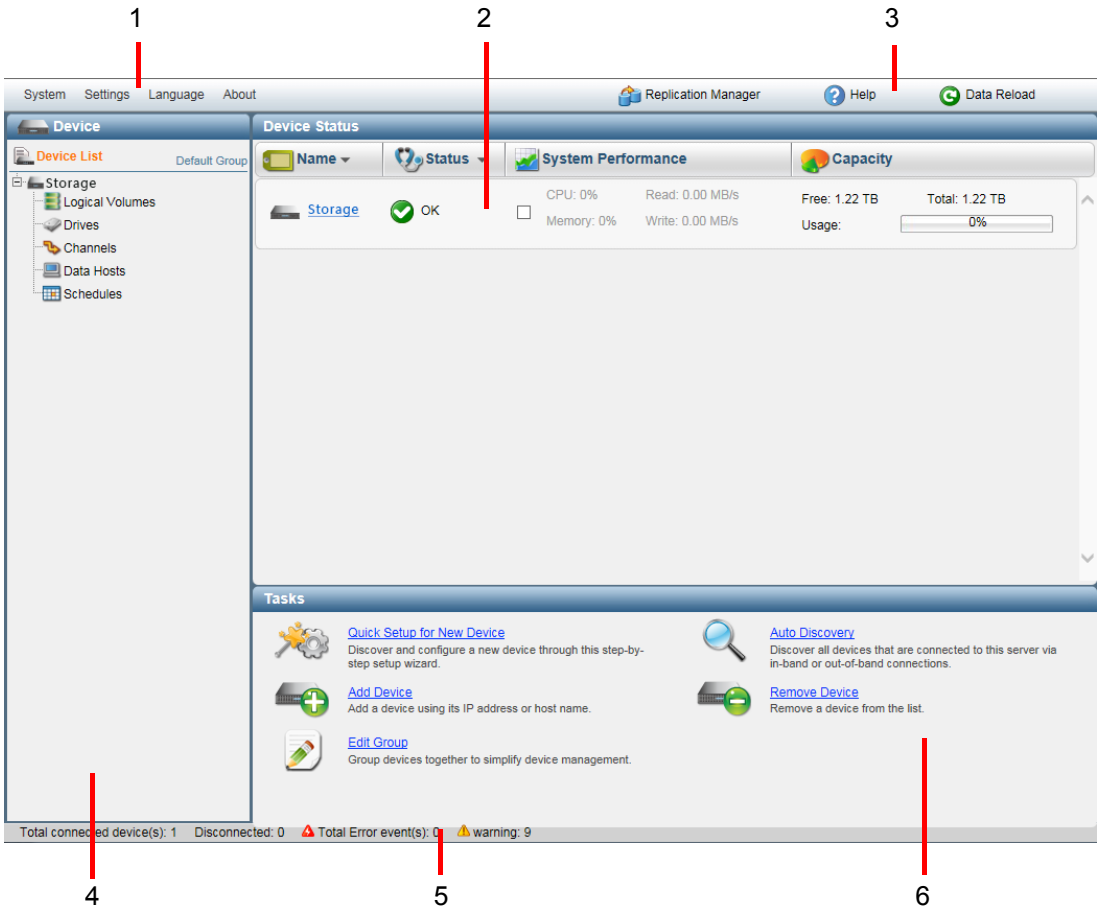
Assigning a Password to a Subsystem	After setting up a password for the subsystem, users will need to input this password whenever they wish to access or configure the hardware settings for that subsystem. Select the Subsystem tab to view the list of subsystems and their passwords. Highlight the storage subsystem from the list and click the Edit Password button.

Enter a new password.



After specifying a password, users will be asked to enter the password when accessing the hardware device page.

3.2.3 Getting to Know the User Interface



Display Element	Description
1: Top menu bar (Left)	The menu items located at the top left allow users to export the system settings, log off/shutdown the subsystem (NOT supported by EonServ), configure notifications and passwords, change the display language, and view the SANWatch version information.
2: Main window	The current status and configurations of the item chosen in the left sidebar will appear in this area.
3: Top menu bar (Right)	Users can access the Replication Manager to configure and run data replications, Online Help (this help document), and refresh the screen contents.
4: Side column	Users can view the system configurations (device sidebar) or storage configurations (pool sidebar) in a tree structure for an overview of the entire system. Details of the chosen (highlighted) item will appear to the right in the main window area.
5: Status bar	Summary of current device configurations and system events are updated in the bottom status bar.
6: Shortcuts in the tasks section	Convenient shortcuts to major functions are available for the item highlighted in the sidebar/main window area.

3.2.4 Navigating the Interface

Although SANWatch is a browser-based software, most operations are designed as intuitive, desktop-like features.

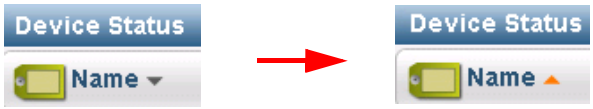
Selecting an Item

If the mouse cursor shape transforms into a pointing hand when hovered over an item, users may select this item. The text color may also change, as shown in the following example.
(Example: Pool List > Pool 1)

Depending on the item selected, a drop down list may appear when the mouse cursor is hovered over the menu.
(Example: Language menu)

Changing the Sequence

Clicking on the small triangle icon next to a column header reverses the order of a list.



Closing a Pop-Up Window

Click the Close/Cancel button at the bottom

or click the  icon at the top right to close a pop-up window.

Refreshing the Screen

Click the Data Reload menu at the top right bar. The user interface contents will be updated to the latest status.

Event Notices

A sign may appear on the device icon (x or △)when there are events that require the user's attention.

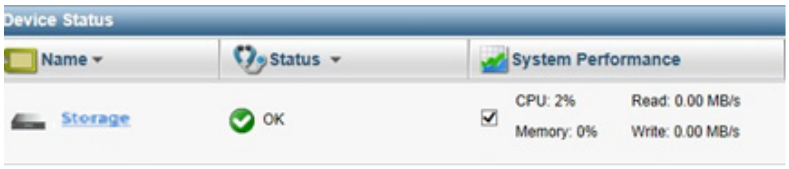
3.3 Working with the Devices View

This chapter describes how to monitor and configure the hardware; for example, RAID subsystems, JBOD expansion enclosures, and hard drives.

3.3.1 Viewing the Hardware List and Status

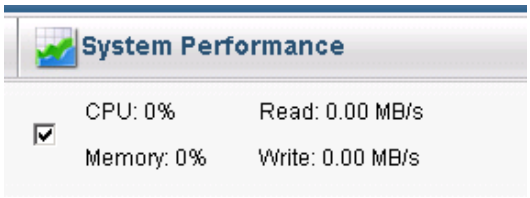
All hardware information can be accessed via the device sidebar of the user interface.

Go To	SANWatch Home > Device sidebar > Device List
Steps	Click the Device tab in the left sidebar and a list of hardware recognized by the system will appear. The hardware status summary will appear to the right, in the main screen.



System Performance

To enable monitoring of the system performance, check the System Performance checkbox.

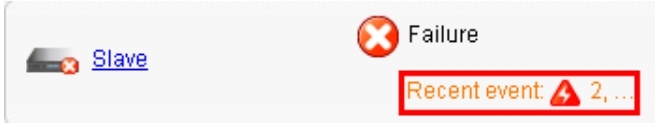


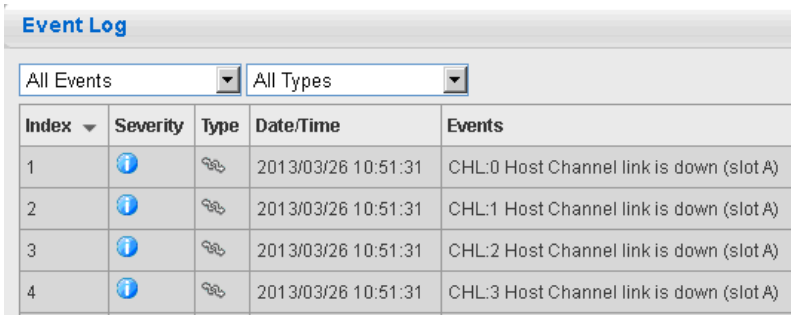
Because the monitoring function affects system performance, this function is disabled by default.

System Status

The system status column shows the status of each hardware device.

If system events have been reported, users can click the Recent Event link to view all events related to that hardware device.





To refresh the status (to ensure the hardware status has been updated), click Data Reload on the top menu bar.

3.3.2 Adding a New Device (RAID Subsystem or JBOD Expansion Enclosure)

To configure a RAID subsystem or JBOD expansion enclosure via the SANWatch browser interface, simply connect the device to the network and use the one-touch device discovery functions introduced in this section.

Prerequisites	Before adding a subsystem/JBOD to the user interface, ensure that the subsystem is connected to the network and has been assigned a valid IP address. If using Internet Explorer, go to Tools > Internet Options > Security, and then execute the following procedures before adding a new device: ■ Click Sites and add 127.0.0.1 to the list of trusted websites. ■ Click Custom Level and enable Active Scripting under Scripting.
Go To	SANWatch Home > Device sidebar > Device List > Tasks section

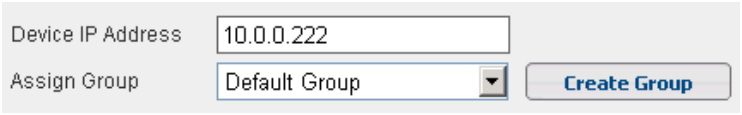
Steps

Users can add (discover) a device using two methods, that is, specify a known IP address or search a range of IP addresses.

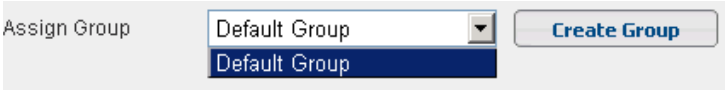
Specifying an IP Address

Click Add Device in the Tasks section.

Enter the IP address of the device.



By default, the device will be added to a device group called Default Group. Users can assign the device to a different group or even create a new group. (To learn more about device groups, refer to the next section of this manual.)



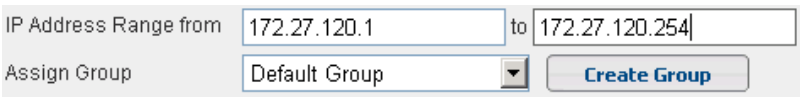
The device will be added to the host computer. Click Cancel to stop the process.

The new device will appear in the sidebar when done.

Searching for a range of IP addresses

The Auto Discovery function can be used to search for a device if the specific IP address is unknown but the subnet range is known. (This function can also be used to search multiple devices within a range of IP addresses.)

Enter the range of IP addresses.



By default, the device, if found, will be added to a device group called Default Group. Users can assign the device to a different group or even create a new group. (To learn more about device groups, refer to the next section of this manual.)

Click Start. The new device will appear in the sidebar when done.

3.3.3 Removing a Device (RAID Subsystem or JBOD Expansion Enclosure)

Devices can be easily removed/deregistered from the system. User data and device configurations are not affected; the device is simply deregistered from the system.

Go To	SANWatch Home > Sidebar > Device List > Tasks section
Steps	Click “Remove Device”.  Select the device for removal.  Click “Remove” at the bottom to remove the device.

3.3.4 Editing Groups and Group Assignments

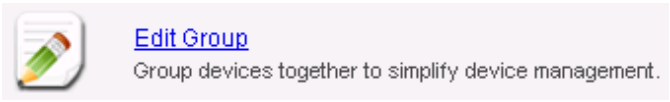
Users can organize devices into groups for convenient management of complex networks that comprise clusters of devices, especially if they feature multiple identical models.

Notes	■ All devices must be assigned to a group. (By default, all devices are assigned to a group called Default Group.) ■ Devices cannot be assigned to multiple groups. ■ All groups are listed in the sidebar. 

Creating a Group

Go to SANWatch Home > Sidebar > Device List > Tasks section

Click “Edit Group”.



Check the box next to the device to be added to the new group and click “Create Group” at the bottom. Input a group name and click “OK”.

Renaming a Group

Go to SANWatch Home > Sidebar > Device List > Tasks section

Click “Edit Group”.

Click to highlight the group to rename and click “Rename Group”.

Only the Default Group cannot be renamed.

Enter the new name and click “OK”.

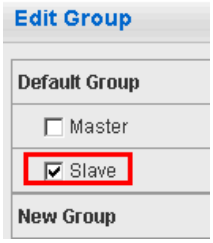
The new group name will appear in the list.

Reassigning a Device to Another Group

Go to SANWatch Home > Sidebar > Device List > Tasks section

Click “Edit Group”.

Check the device to be reassigned to a different group.



Click “Move Device” and select a group from the drop-down list.

Click “OK” and the device will be assigned to a different group.

Remove a Group

Go to SANWatch Home > Sidebar > Device List > Tasks section

Click “Edit Group”.

Click the name of the group to remove, click “Delete Group”, and click “Yes” in the confirmation message that appears.

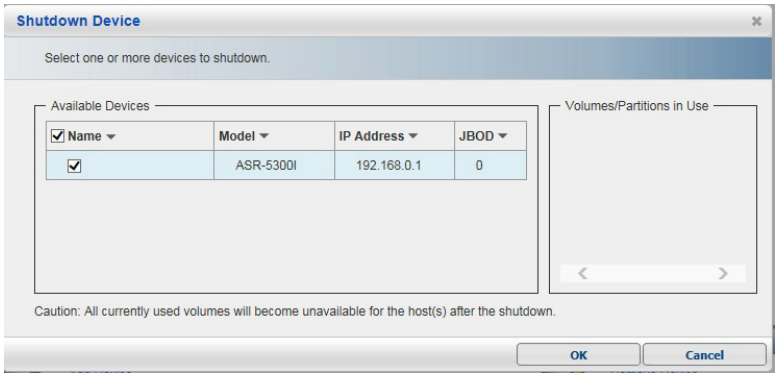
All devices assigned to the group will be moved to the Default Group.

3.3.5 Exporting System Settings

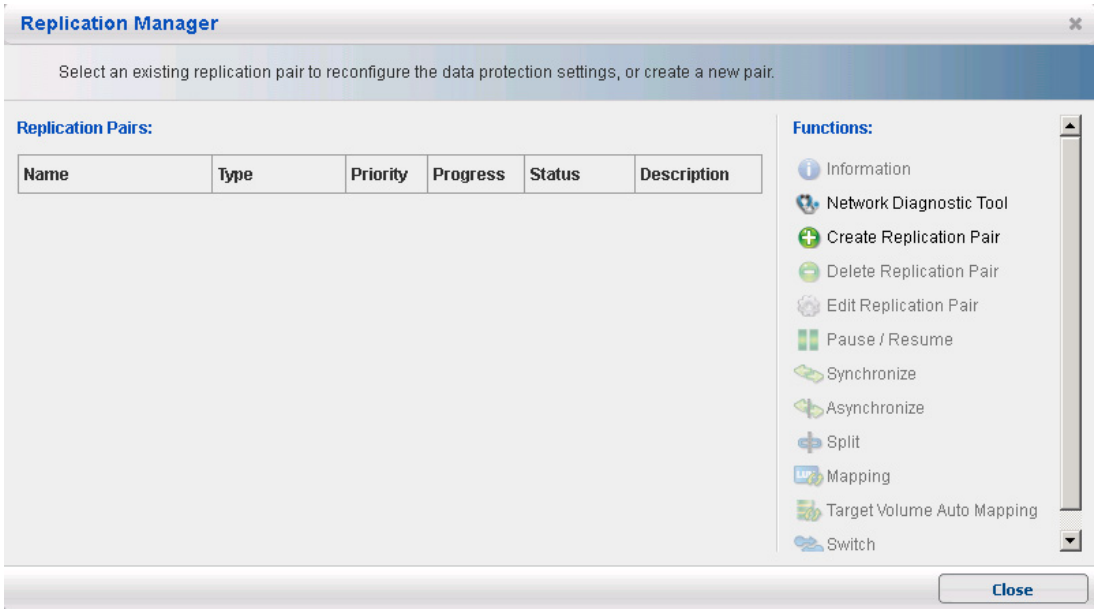
Go to	SANWatch Home > Top menu bar > System > Export System Information 
Steps	The list of connected devices (RAID subsystem or JBOD) will appear. Check the device(s) for exporting system information and click “OK”. The system information will be archived in a zip file (text format) and downloaded to a folder on the computer.

3.3.6 Resetting/Shutting Down the System

Before resetting or upgrading the subsystem, ensure all current tasks are completed and the system information is exported if necessary.

Go to	SANWatch Home > Top menu bar > System, and select Shutdown Device from the menu.
Steps	The list of connected devices (RAID or JBOD) will appear. Check the device to be shut down and click “OK”.  Currently used storage volumes will become unavailable for hosts and users after shutting down the device. (The user data on the device will remain intact.)

3.4 Data Replication



Volume copying and mirroring can be conducted within a single subsystem or across physically distant locations. For RAID systems, no difference exists between local replication and remote replication in terms of usage but the license is separated. Users should ensure they have the correct license (local replication or remote replication).

Note	For users trying to perform volume copying or mirroring between two volumes that belong to subsystems on different networks, the system's firewall settings may prevent management software from communicating with RAID systems and block data transmissions. In such cases, users (or the system administrator) may need to open certain TCP/IP ports to allow SANWatch and subsystems to communicate with each other through the firewall. Check the TCP/IP and UDP port list in the Appendix chapter.
Firmware Version on Remote Replication	Remote replication should only be executed if the same firmware version is shared among the subsystems involved (source and target devices).

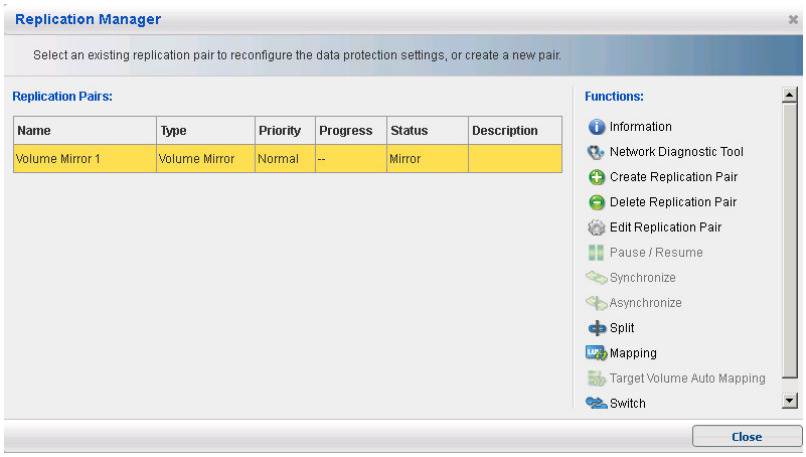
3.4.1 Opening the Replication Manager

All replication-related operations can be accessed and executed from the Replication Manager window. Users can create new replication pairs, view the progress, and reconfigure settings.

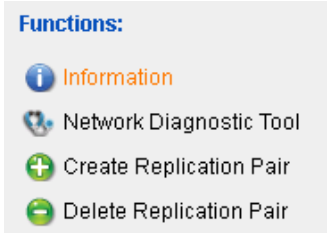
Go to	SANWatch Home > Top menu bar > Replication Manager 

Steps

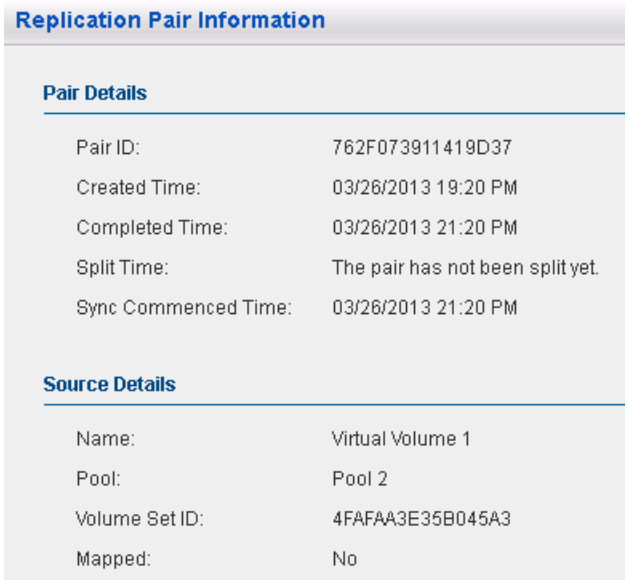
When the Replication Manager window is opened, a list of currently available replication pairs and their status will appear to the left.



Available functions are listed in the sidebar to the right. To view the configurations of replication pairs, click “Information”.



Detailed information about the replication pair will appear.



3.4.2 Diagnosing the Network Status for Replication

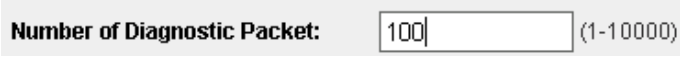
Users can check the devices available on the network to determine whether remote replication pairs can be safely created between devices.

Go To	SANWatch Home > Top menu bar > Replication Manager
Steps	Click Network Diagnostic Tool.

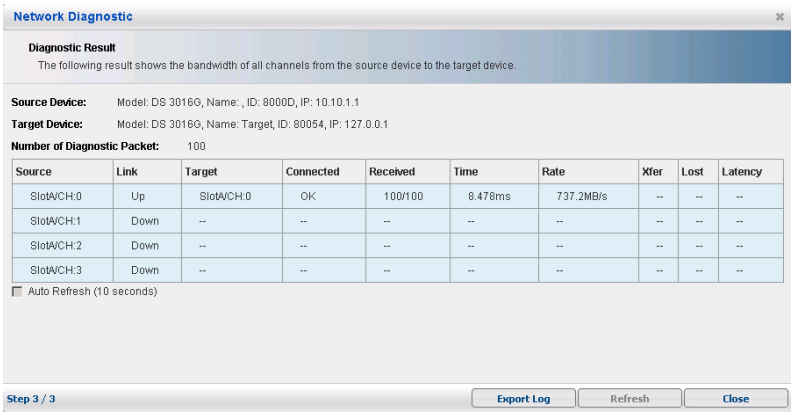
Highlight the source device to be diagnosed and click “Next”.

Highlight the system to be diagnosed and click “Next”.

Specify the diagnostic data packet value (64 K each). Valid values range between 1 and 10000.



Click “Diagnose” to view the diagnosis results.



The Link column shows whether the source and device systems are connected or not (and whether they can form a remote replication pair).

Source	Link	Target
SlotA/CH:0	Up	SlotA/CH:0
SlotA/CH:1	Down	--
SlotA/CH:2	Down	--
SlotA/CH:3	Down	--

To automatically refresh the status, check the Auto Refresh box.

To export the results to a local folder, click “Export”.

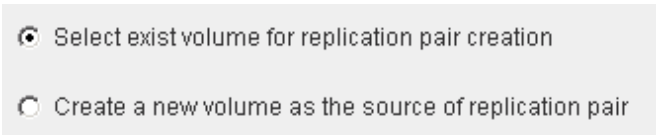
3.4.3 Creating a Volume Copy

If the target partition contains snapshot image(s), a volume copy cannot be created.

For more information about snapshots, go to the following location and click the Help icon at the top-right corner:

SANWatch Home > Device sidebar > Device List > device name > Logical Volumes > LV name > Partitions.

Go to	SANWatch Home > Top menu bar > Replication Manager
Steps	Click “Create Replication Pair” in the Functions area. **a. Method 1: Select the source device from an existing partition and click “Next”**.

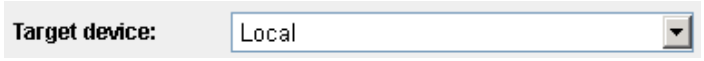


Select the source device and click “Next”.

The list of available partitions will appear. Highlight (yellow) the source and click “Next”.

Partition Name	Logical Volume	Status	Total Capacity
Partition 1	Logical Volume 1	The volume has been mounted.	10 GB
Partition 2	Logical Volume 1	The volume has been mounted.	10 GB
Partition 3	Logical Volume 1	The volume has been mounted.	10 GB

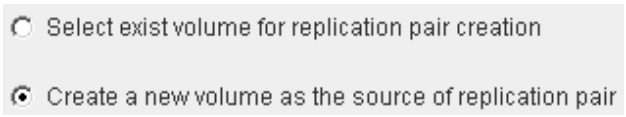
Select the target device (hardware) from the drop-down list. If the Local option is selected, the source and target partitions will be located on the same subsystem.



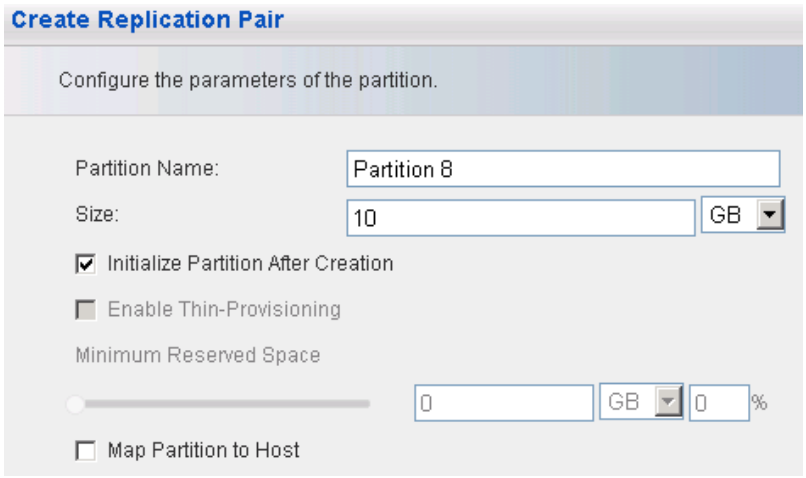
The list of available logical volumes or pools will appear. Highlight (yellow) the target logical volume or pool and click “Next”.

Logical Volume	Logical Drive Amount	Status	Total Capacity
Logical Volume 1	2 logical drive(s)	On-Line	409.44 GB

b. Method 2: Create a new partition as the source.

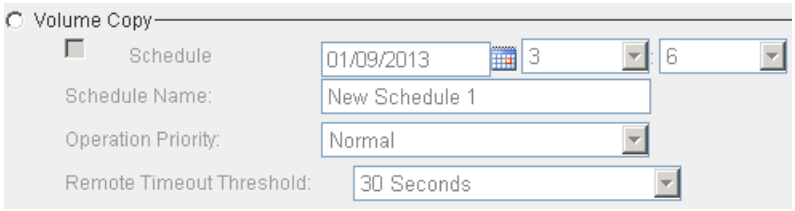


Click “Next” to create a new partition.

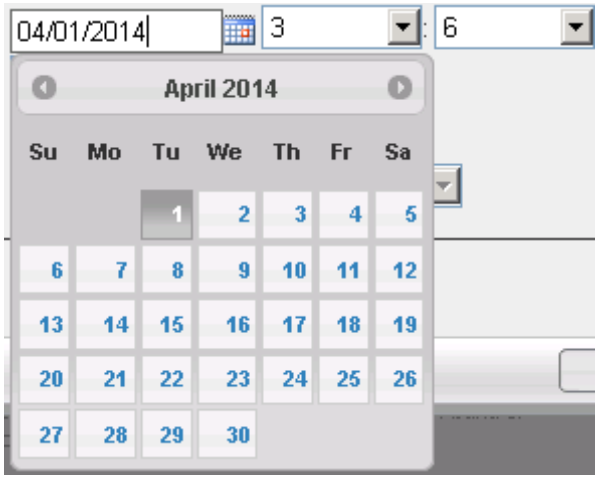


Enter the name of the volume copy.

Set up the volume copy schedule.



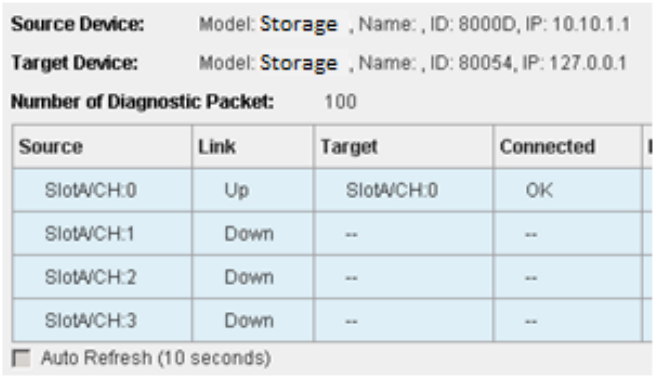
To schedule the volume copy process, check Schedule.
Click in the schedule box and set the date, time (24-hr format), and priority by clicking the date in the calendar and choosing time and priority from the drop-down boxes, then click “Next”.



If the source and target partitions are on located on different sub-systems, users may click “Diagnose Network” to check the network connection status.

Set the number of diagnostic packets.

Click “Diagnose” to view the connection status.

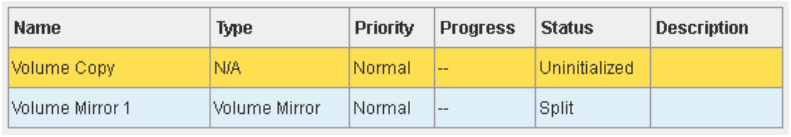


A summary will appear.

Confirm all settings and click “OK” to create a replication pair.

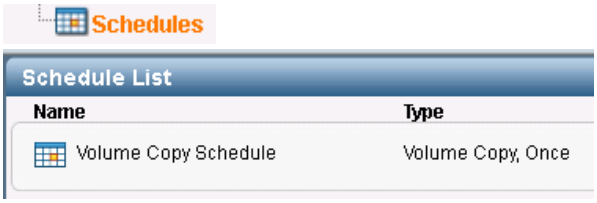
A progress window will show the creation progress.

The newly created replication pair will appear.



Name	Type	Priority	Progress	Status	Description
Volume Copy	N/A	Normal	--	Uninitialized	
Volume Mirror 1	Volume Mirror	Normal	--	Split	

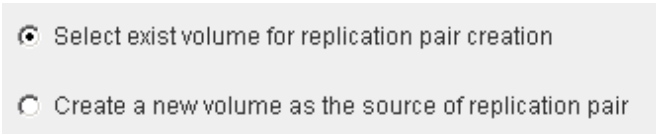
If the volume copy has been scheduled, it will appear in the Schedule view. Click the Schedules menu in the sidebar.



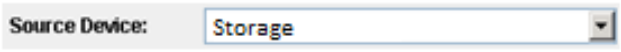
Parameters	**Remote Timeout Threshold**	The remote timeout threshold option allows users to avoid breaking a remote replication pair when the network connection between the source and the target is unstable or too slow. Users can choose how long the controller will wait (timeout). The replication pair will receive superior protection with a lengthier timeout period, but fewer interruptions can impact the host performance. The reverse is also true: shorter timeout --> less impact --> more risk of breaking the pair apart. **Enabled:** Depending on the situation, the controller either splits or halts the volume mirroring when no network activity occurs for the length of the timeout period. **Disabled:** Host I/O may be seriously impacted when the network connection is unstable.
	This option is for remote replication pairs only. For local replication pairs, this option is disabled.	
How Remote Timeout Threshold Works	**Stage 1: Syncing has been interrupted.** Background syncing will be paused for the wait (timeout) period (default: 30 seconds) before being resumed. **Stage 2: Fails to sync to the remote target.** If the target volume cannot be found, the unsynced data blocks will be marked. The system will continue syncing the next data blocks. An event will be posted. **Stage 3: Still fails to sync to the remote target.** The system attempts to sync the marked data blocks several times. If the target volume is not found, syncing will be aborted and unsynced data will be marked. An event will be posted. If the system reboots before the sync retry count reaches the threshold, the sync operation will be restarted after the reboot and the retry count will be reset. **Stage 4: Replication pair is marked as abnormal.** The status of the split replication pair will be updated as abnormal to warn users against creating a host LUN map with the abnormal target volume.	
Viewing the Progress	The newly created replication pair will be initialized upon creation or according to the schedule. Users can pause (and resume) the process.	
	The length of each process depends on the capacity of the replication pair. In some cases, the process finishes within a matter of seconds.	
	When initialization has been completed, the status of the replication pair will change to Completed.	
	If network connection is lost during the process, the status of the replication pair will change to Non-Complete.	

3.4.4 Creating a Volume Mirror

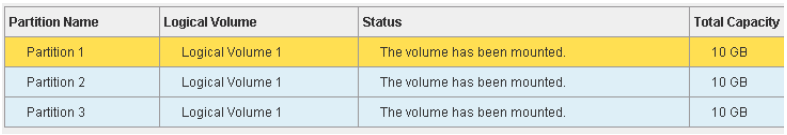
Notes	■ If the target volume contains a snapshot image(s), a volume mirror cannot be created. ■ Synchronous mirroring is NOT recommended over WAN connections as high I/O latency can cause the process to fail.
Go to	SANWatch Home > Top menu bar > Replication Manager Users can also schedule the creation of volume mirrors. For more information, visit the following location and click the Help icon at the top-right corner: SANWatch Home > Device sidebar > Device List > device name > Schedules
Steps	Click “Create Replication Pair” in the Sidebar. Select the source from an existing volume or create a new source volume and click “Next”.



Select the source device and click “Next”.

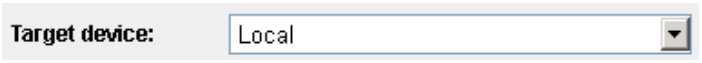


The list of available partitions will appear. Highlight (yellow) the source and click “Next”.



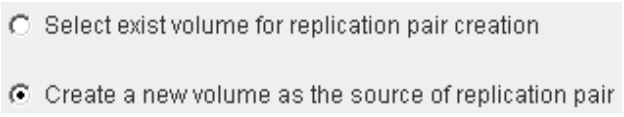
Partition Name	Logical Volume	Status	Total Capacity
Partition 1	Logical Volume 1	The volume has been mounted.	10 GB
Partition 2	Logical Volume 1	The volume has been mounted.	10 GB
Partition 3	Logical Volume 1	The volume has been mounted.	10 GB

Select the target device (hardware) from the drop-down list. If the Local option is selected, the source and target partitions will be located on the same subsystem.



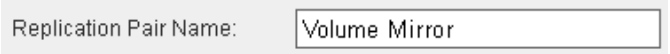
The list of available logical volumes or pools will appear. Highlight (yellow) the target logical volume or pool and click “Next”.

Create a new partition as the source.

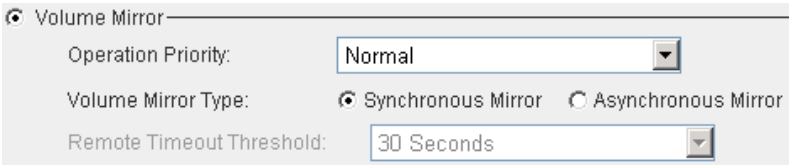


Click “Next” to create a new partition.

Enter the name of the volume mirror.



Set the volume mirror priority and type.



The options “Support Incremental Recovery” and “Compress Data Before Transmission” are only available when the source and the target reside in different locations (remote replication).

By default, “Support Incremental Recovery” is always enabled for synchronous mirroring, and disabled for asynchronous mirroring.

Set the remote timeout threshold. This option defines the duration of time that the system will continually attempt to establish a remote replication connection with the target device. If the specified timeout period is longer, the stability of the remote replication connection will increase because of fewer disruptions, but the system performance will be affected.

This option is only available when the source and the target reside in different locations (remote replication).

Users can click “Diagnose Network” to check the network connection status.

Set the Number of Diagnostic Packets

Click “Diagnose” to check the connection status.

Click “Next” to view a summary.

Click “OK” and the new replication pair will appear in the list.

Name	Type	Priority	Progress	Status	Description
Volume Mirror 1	Volume Mirror	Normal	--	Split	
Volume Sync Mirror 2	Volume Mirror	Normal	--	Mirror	

Parameters	**Synchronous/ Asynchronous**	When synchronous mode is enabled, the host writes data to both the source and the target simultaneously. In asynchronous mode, the host I/O is allocated to the source volume only for higher bandwidth and optimized performance. New data is written to the target later in batches, avoiding heavy I/O traffic.
	Incremental Recovery	Allows users to return to the source volume if recovered. New data accumulated in the target volume during downtime is then gradually copied to the source volume.
	Compress Data	If the bandwidth is insufficient for asynchronous mirroring, data compression reduces the required I/O.
	This option impacts the subsystem performance by requiring extra computing power.	
	Remote Timeout Threshold	The remote timeout threshold option allows users to avoid breaking a remote replication pair when the network connection between the source and the target is unstable or too slow. Users can specify the duration of time that the controller will wait (timeout). The replication pair will be better protected if the timeout period is lengthy, but fewer interruptions impact the host performance. The reverse is also true: shorter timeout --> less impact --> more risk of breaking the pair apart. **Enabled:** Depending on the situation, the controller either splits or halts volume mirroring if no network activity occurs for the duration of the timeout period. **Disabled:** Host I/O can be seriously impacted when the network connection becomes unstable.
	This option is for remote replication pairs only. If you create a local replication pair, this option will be disabled.	
How Remote Timeout Threshold Works	**Stage 1: Syncing has been interrupted.** Background syncing will be paused for the wait (timeout) period (default: 30 seconds) before being resumed. **Stage 2: Fails to sync to the remote target.** If the target volume cannot be found, the unsynced data blocks will be marked. The system will continue syncing the next data blocks. An event will be posted. **Stage 3: Still fails to sync to the remote target.** The system attempts to sync the marked data blocks several times. If the target volume is still not found, syncing will be aborted and unsynced data will be marked. An event will be posted. If the system reboots before the sync retry count reaches the threshold, sync operation will restart after the reboot and the retry count will be reset. **Stage 4: Replication pair is marked as abnormal** The status of the split replication pair will be updated as abnormal to warn users against creating a host LUN map with the abnormal target volume.	

Viewing the Progress	The newly created replication pair will be initialized upon creation or according to the schedule. The length of each process depends on the capacity of the replication pair. In some cases, the process finishes within a matter of seconds. When initialization has been completed, the status of the replication pair will change to Completed. If network connection is lost during the process, the status of the replication pair will change to Non-Complete.

3.4.5 Editing/Deleting a Replication Pair

Go To	SANWatch Home > Top menu bar > Replication Manager
Editing a Pair	Highlight a replication pair (yellow) in the list. Click “Edit Replication Pair” in the sidebar. Users can change the name and priority of the replication pair and add a short description.
Deleting a Pair	Highlight a pair (yellow) in the list. Click “Delete Replication Pair” in the sidebar. Deleting a volume copy pair removes the relationship between the source and target volume; however, the logical volumes or pools themselves stay intact. We recommend deleting volume copy pairs once the volume copy task has been completed as the pair only serves as a reference log. However, DO NOT remove a volume copy pair if the volume copy has not been completed. If removed prematurely, the target volume data will become corrupted and thus unusable. The ongoing task will also be interrupted.

3.4.6 Mapping the Source or the Target to Host LUN

Go To	SANWatch Home > Top menu bar > Replication Manager

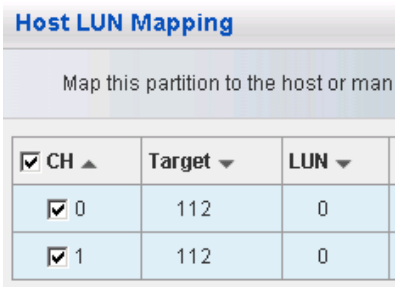
Steps

Highlight the replication pair (yellow).

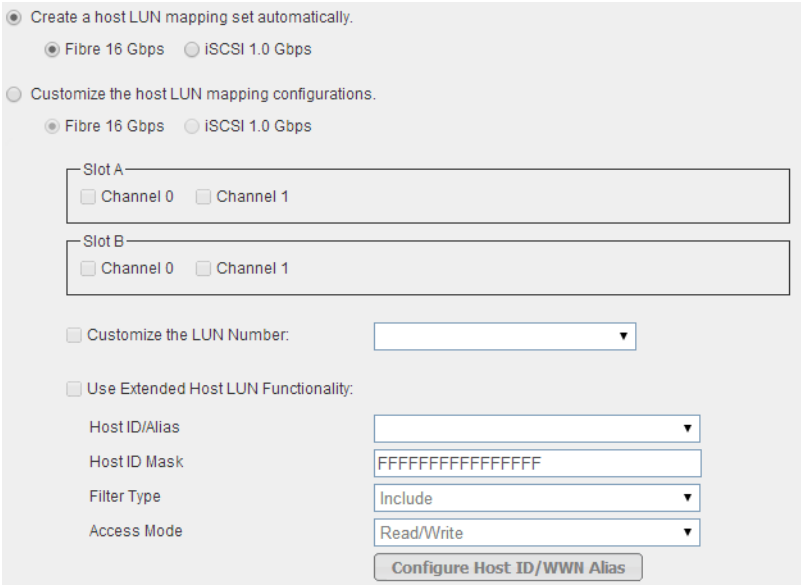
Click “Mapping” in the sidebar.

Select whether to map the source or the target (mapping to the target is not always available depending on the replication pair’s conditions)

Click “OK” to select the channel and click “Create”.

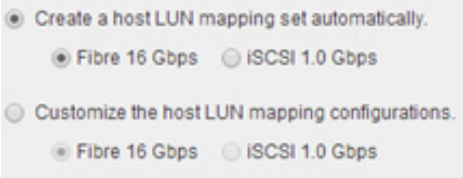


The mapping configuration window will appear.



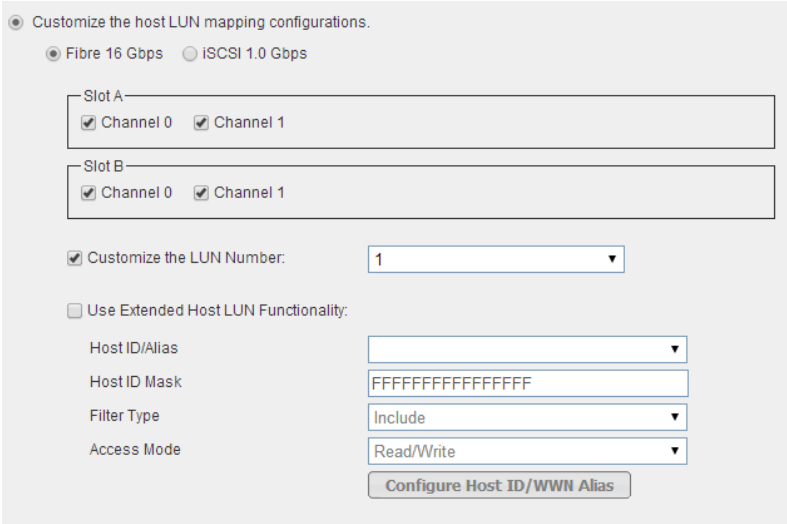
Automatic Configuration

To allow the system to conduct LUN mapping automatically, check the Automatic Configuration option. For hybrid models, select the host type.



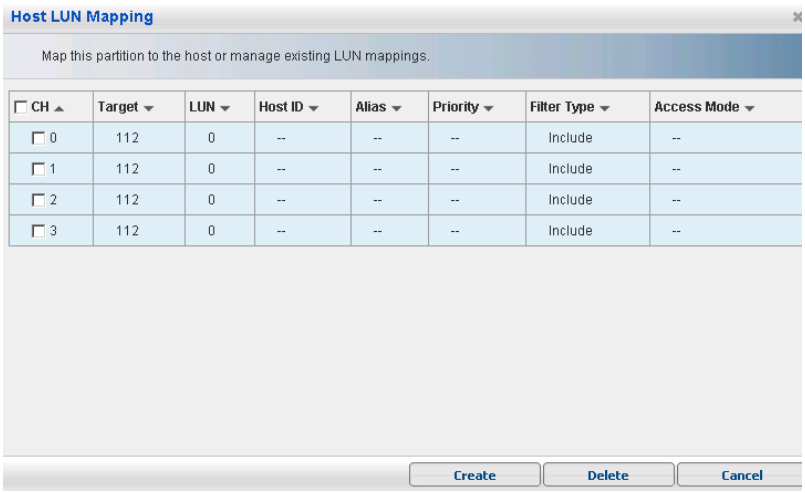
Manual Configuration

To manually configure LUN maps, check the Customize option and select the channels.



Select the LUN number from the drop-down list.

Click “OK”. A list of host LUN mapping configurations will appear in the window.

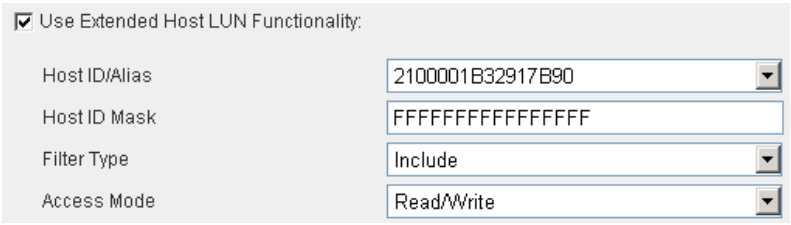


(To delete LUN maps, check the channels to be deleted and click “Delete”.)

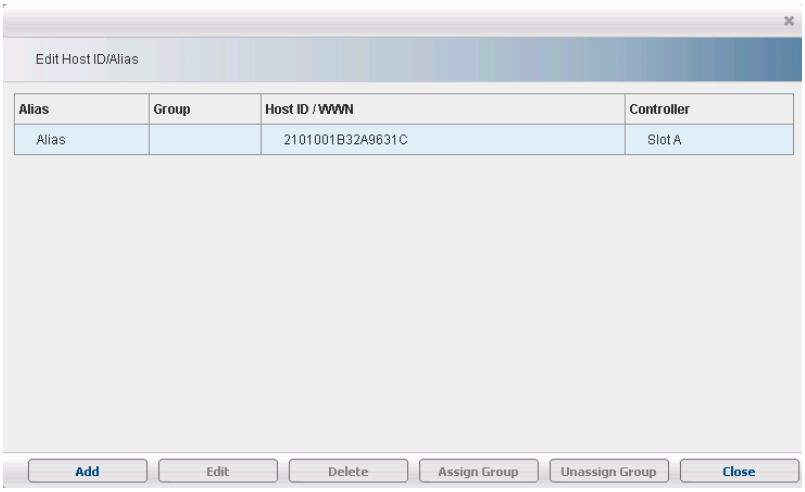
Using Extended LUN Mapping (Fibre Channel)

Extended LUN Mapping is available only for manual configuration.

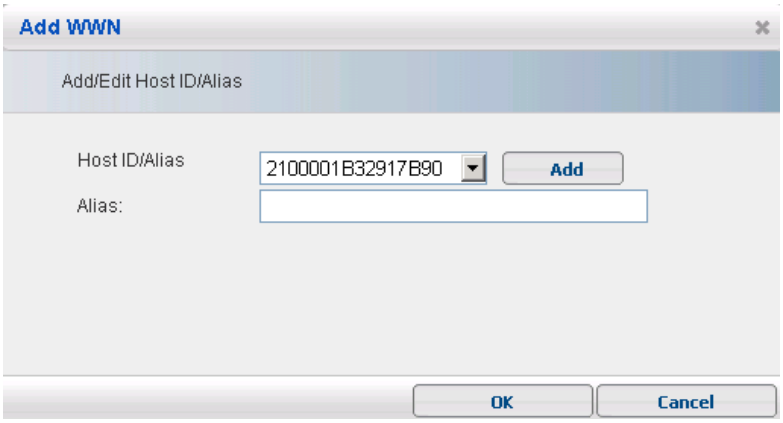
Click “Use Extended LUN Functionality” and enter or select the parameters.



- Host ID/Alias: Specifies the host ID, refers to the WWPN port name.
- Host ID Mask: Functions as a prefix mask in hexadecimal.
- Filter Type: Specifies whether to allow (include) or forbid (exclude) WWNs from access after filtering.
- Access Mode: Specifies the host’s access right to LUN maps, with read-only and read-write options.
- Configure Host-ID/WWN List (enabled only when Extended Host LUN Functionality has been enabled.)



In the Edit Host-ID/WWN list window, click “Add” to create an entry and enter the node name (WWN Name) for identifying HBA ports in SAN. An HBA card may have one node name and multiple port names. The node name can be a nickname, such as “SQLserver_port”, instead of the real name.



Click “OK”. Repeat the above process to create additional LUN maps, especially if multiple HBA ports are accessing the same virtual volume (e.g., in high-availability applications).

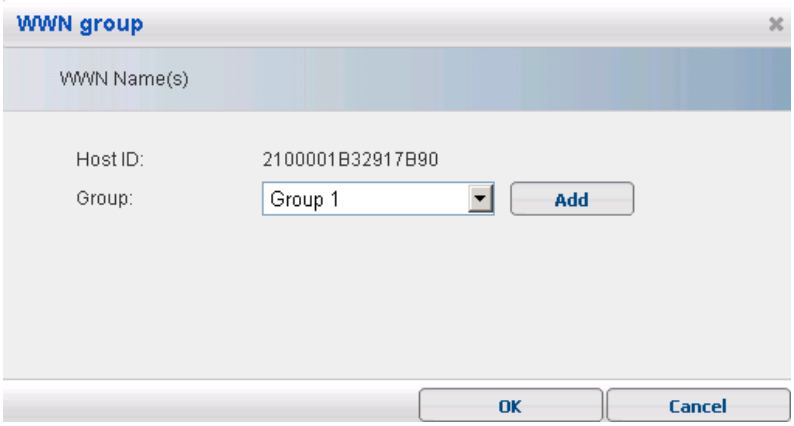
Assigning a WWN to a Group

A WWN group allows multiple host LUNs to be accessed in a single mask. This is useful in a clustered storage server environment.

To create a group and assign it a WWN, highlight a WWN (yellow).

Alias	Group	Host ID / WWN	Controller
Alias		2100001B32917B90	Slot A

Click “Assign Group” and select the group from the drop-down menu.



To add a new group, click “Add” and enter the group name.

The group name will appear in the list.

Alias	Group	Host ID / WWN	Controller
Alias	Group 1	2100001B32917B90	Slot A

To unassign a WWN from a group, click “Unassign Group”.

Deleting a WWN Name From the List

Highlight a WWN in the list and click “Delete”.

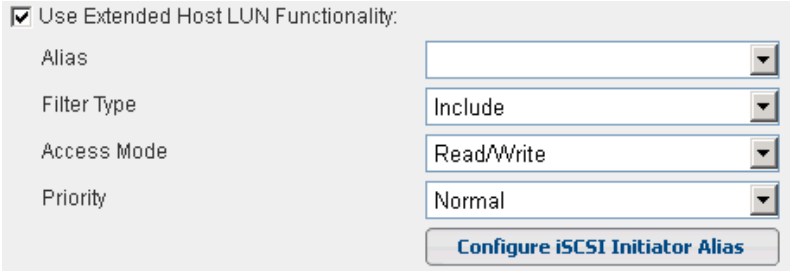
Changing the Alias Name

To edit the alias name of the WWN, click “Edit” and enter a new name.

Using Extended LUN Mapping (iSCSI Channel)

Extended LUN Mapping is available only for manual configuration.

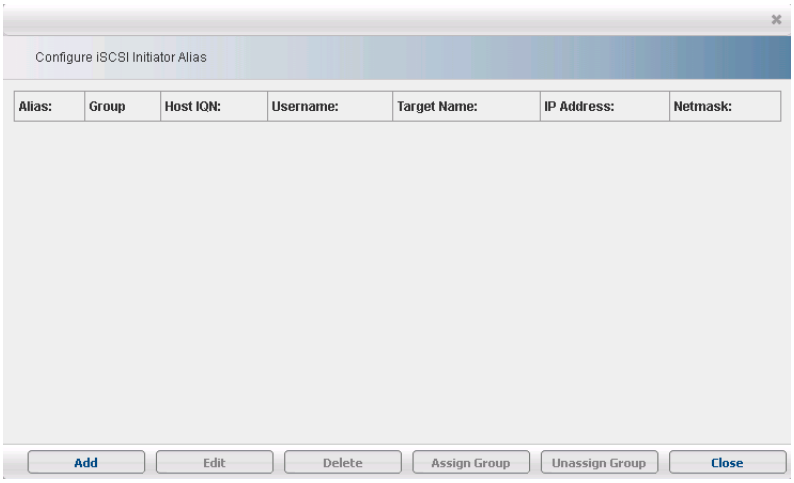
Click “Use Extended LUN Functionality” and enter the parameters.



- Alias: Specifies a pre-configured iSCSI initiator instance. To create a new initiator alias, click “Configure iSCSI Initiator Alias”.
- Filter Type: Specifies whether to allow (include) or forbid (exclude) initiators from access after filtering.
- Access Mode: Specifies the host’s access right to LUN maps, with read-only and read-write options.
- Priority: Specifies access priority. For example, high priority can be assigned to volumes that serve applications, and low priority to volumes that store archives or user data.

Configuring iSCSI Initiator Alias

Click “Configure iSCSI Initiator Alias”.



Click “Add” to create an entry and enter the parameters.

- Host IQN: Advantech’s storage IQN is composed of the system serial number and 3 more digits in the following format: iqn.2002-10.com.advantech:raid.snXXXXXX.XXX
  6 digits of the serial number follow “sn.”
  The next 3 digits denote the channel number, host ID, and LD ownership.
  The LD ownership digit is either “1” or “2”, where “1” indicates Controller A and “2” indicates Controller B. The IQN depends on the method of mapping the logical drive to the host ID/LUN. For example, if you map a logical drive to host channel 0 and AID1, the last 3 digits will be 011.
- Alias: Assign an easily remembered name to the iSCSI initiator.
- User Name/Password: Specifies the user name and password for CHAP authentication. This information is the same as the CHAP target node name and CHAP secret in the OS setting. The user password (one-way, from initiator) must be at least 12 bytes.
- Target Name/Password: Specifies the target name and password for CHAP authentication. This information is the same as the CHAP initiator node name and CHAP secret in the OS setting. The target password (two-way, outbound from storage) must be at least 14 bytes.
- IP Address/Netmask: Specifies the IP address and subnet mask, if necessary. Occasionally, multiple initiator ports on an application server can share the same IQN.

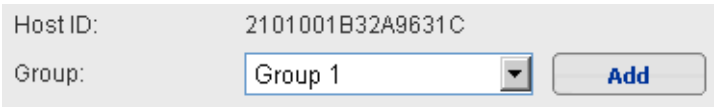
Click “OK”. Repeat the above process to create additional LUN maps, especially if multiple HBA ports have access to the same virtual volume (e.g., in high-availability applications).

Assigning an Initiator to a Group

A group allows multiple host LUNs to be accessed in a single mask. This is useful in a clustered storage server environment.

To create a group and assign an initiator to it, highlight an initiator (yellow).

Click “Assign Group” and select the group from the drop-down menu.



To add a new group, click “Add” and enter the group name.

The group name will appear in the list.

To unassign an initiator from a group, click “Unassign Group”.

Deleting an Initiator Name from the List

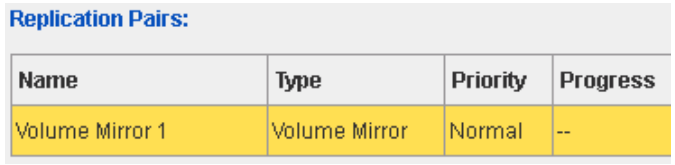
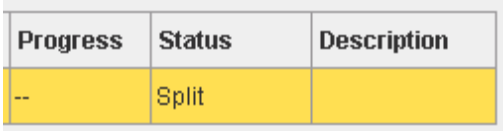
Highlight an initiator in the list and click “Delete”.

Editing the Initiator

To edit the configuration of an initiator, click “Edit”.

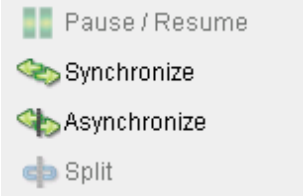
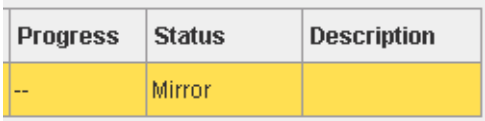
3.4.7 Switching the Roles of a Replication Pair

The roles (source and target) of a replication pair can be switched.

Notes	■ To switch roles, the replication pair must be split. Ensure no important data transaction is underway. ■ In a replication pair, the capacity of the target must equal or exceed that of the source. Therefore, to switch roles, ideally the source and target pair should have the same capacity.
Go To	SANWatch Home > Top menu bar > Replication Manager
Step 1: Splitting the Replication Pair	Highlight a replication pair.  Click “Split” in the sidebar.  The replication pair status will change to Split. 
Step 2: Switching the Roles	When the highlighted pair has been split, click “Switch” in the side-bar. The source and the target will swap roles. After completion, click “Information” to confirm the new parameters.

3.4.8 Syncing a Replication Pair

The replication pair can be synchronized (manually) to perform an incremental data recovery. When repairing damaged content of a source pair, the target data is copied (synced) to the source.

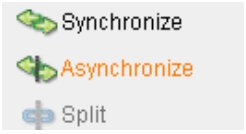
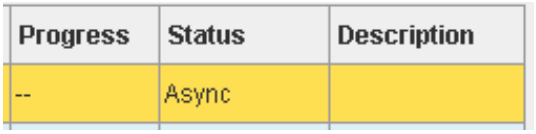
Notes	■ Sync/Async denotes a replication pair that has been split. Ensure no important data transactions are underway. ■ Synchronous mirroring is NOT recommended over WAN connections because high I/O latency can cause failure.
Go To	SANWatch Home > Top menu bar > Replication Manager
Syncing the Pair	Highlight a replication pair. Confirm that the status has been split. Click “Synchronize” in the sidebar.  The source and target will be synced and the status will return to normal. 

3.4.9 Using the Incremental Recovery Option in Asynchronous Mirroring

The Incremental Recovery option allows users to return to the source volume if recovered. New data accumulated in the target volume during downtime is then gradually copied to the source volume.

This option affects the I/O performance and requires additional space in the target volume because of the meta data necessary to keep track of the difference.

Conditions	When creating a volume mirror, select the volume mirror type as “Asynchronous Mirror” and enable “Support Incremental Recovery.” Users should also be mindful of the source volume condition. ■ If the source volume is still missing, users can map the target volume to the host and keep the data difference between the source volume (normal asynchronous mirroring). ■ If the source volume recovers, users must switch the source and target roles before starting asynchronous mirroring. See below for detailed steps. ■ The target volume must be unmapped.
Go To	SANWatch Home > Top menu bar > Replication Manager
Step 1: Splitting the Replication Pair	Highlight a replication pair. Click “Split” in the sidebar. The replication pair status will change to split.

Step 2: Switching the Roles	When the highlighted pair has been split, click “Switch” in the side-bar. The source and the target will swap roles. After completion, click “Information” to confirm the new parameters.
Step 3: Recovering the Pair	The source volume has become the target, and the target volume has become the source. Click “Asynchronize” in the Sidebar.  Wait until the status becomes Async.  Start the asynchronous volume mirroring process. The original source volume then receives the incremental difference from the original target volume and both keep each other synced. Select the Role Switch function again. The original source volume will again become the source of the volume pair, completing the recovery process. The incremental recovery process can be applied only once per pair.

3.4.10 Configuring Automatic Failover for Remote Replication

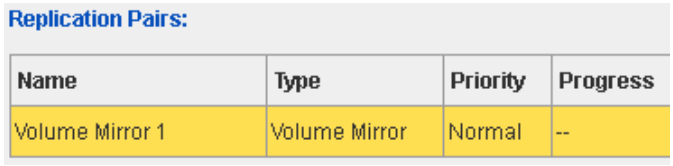
The automatic failover function ensures continuous data transmissions in the event of a break in the replication pair. If the host (recovery) agent fails to locate the source volume of a replication pair due to a disaster, such as a power outage, the host agent will map the target volume to the host for failover. Because the target volume is a copy of the source, users can continue operations using the data on the target side.

Because the failover task is initiated by the agent and involves mapping operations, the host will experience seconds or even minutes of downtime depending on the environment.

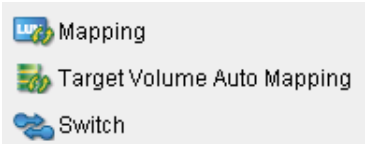
Notes	This feature is available when all of the following conditions have been met: ■ Remote replication pairs, not local replication pairs ■ Volume mirror pairs, not volume copy pairs ■ Volume mirrors pairs with source volumes already mapped
Go To	SANWatch Home > Top menu bar > Replication Manager

Steps

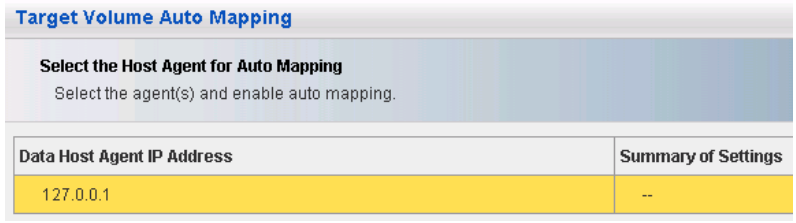
Highlight a replication pair.



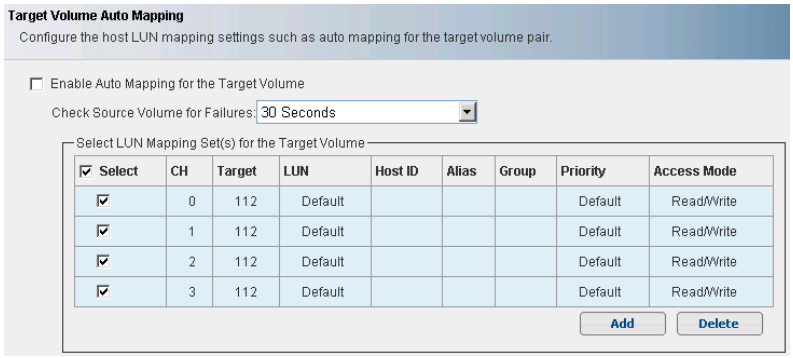
Click “Target Volume Auto Mapping” in the sidebar.



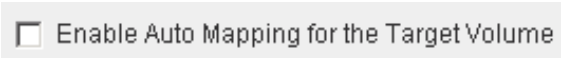
Select the host agent for configuring automatic failover and click “Next”.



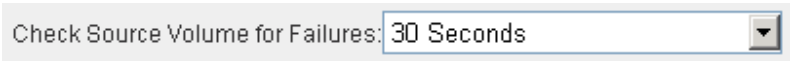
The Auto Failover configuration window will appear.



- Enable: Check this box to enable or disable auto failover (mapping).



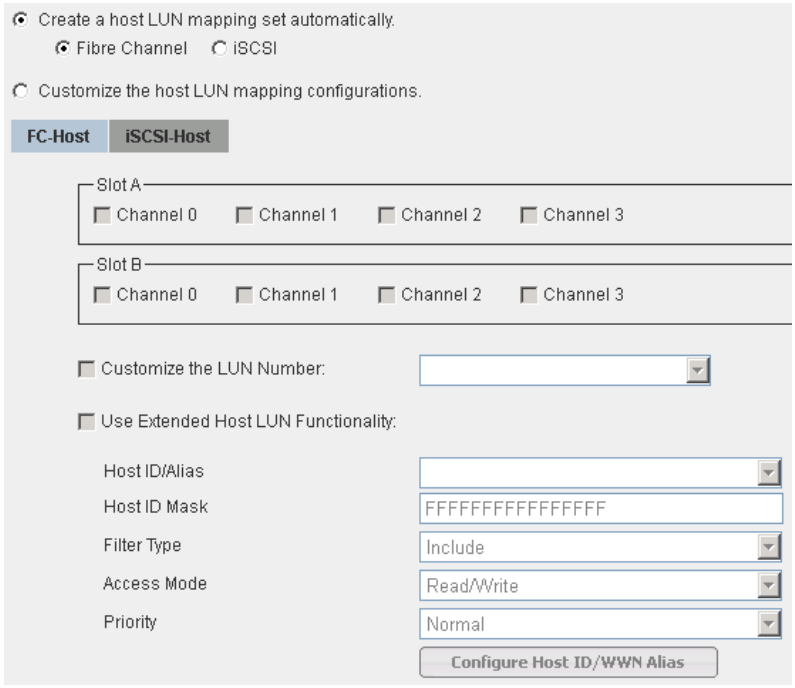
- Check Period: Specify the length of the timeout period for pausing and retrying the sync operation in the event of a failure.



- LUN Map List: Select the LUN map for the target volume. A new LUN map can be created (see the next step) by clicking “Add”.
- Trigger a File (optional): Check this box to run a script or program, such as a scanning script, after mapping the target volume to the host.

To add a new LUN map, click “Add”.

The LUN mapping window will appear. For details of LUN map creation, refer to the Mapping section.



Click “OK”. The Auto Map column shows the current auto failover (mapping) status of the replication pair. (An empty column means no settings have been configured.)

Replication Pairs:

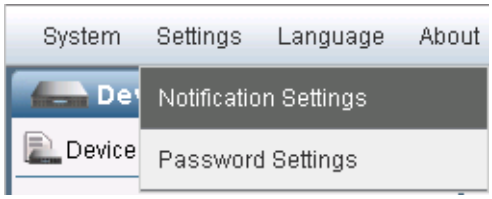
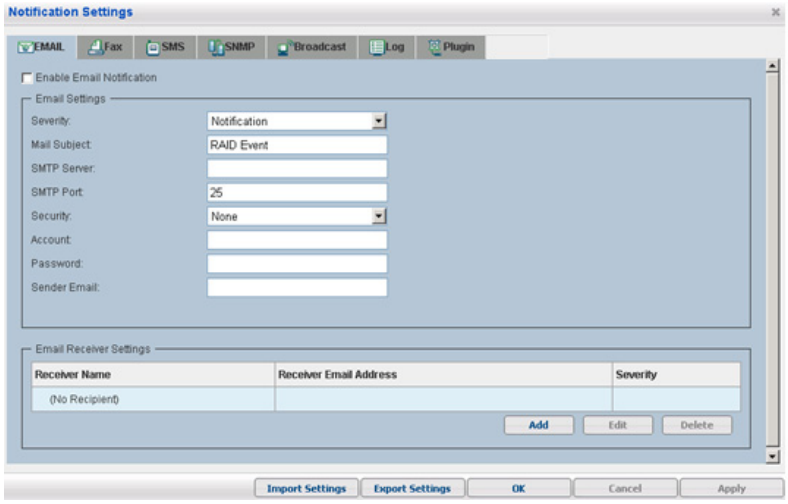
Name	Type	Priority	Auto Map
RemoteMirror 1	Volume Mirror	Normal	Enabled
RemoteMirror 2	Volume Mirror	Normal	--

3.5 Notifying Users of System Events

The following notification services are available:

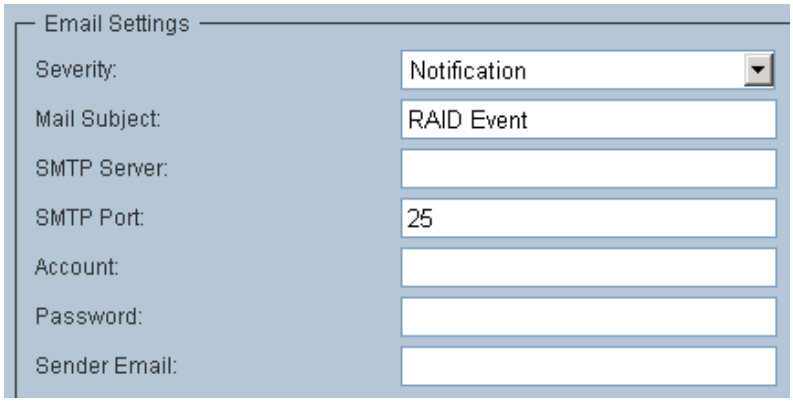
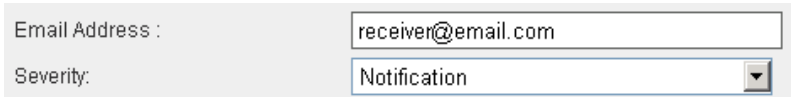
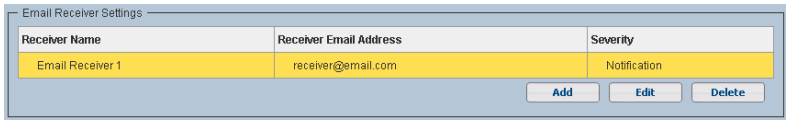
- Email: Notifies users via an email message.
- Fax: Notifies users via a fax message.
- SMS: Notifies users via an SMS message.
- SNMP: Notifies users via SNMP protocol.
- Broadcast: Sends notifications via LAN networks.
- Log: Notifies users by sending system logs via email.
- Plugin: Activates user-specified applications when a system event occurs.

3.5.1 Activating Notification Settings

Go To	SANWatch Home > Top menu bar > Settings > Notification Settings 
Steps	The notification settings appear in the main window and show email notification settings by default. 

3.5.2 Notification via Email

This option allows users to set the system to automatically send an email message notification when a system event occurs.

Go To	SANWatch Home > Top menu bar > Settings > Notification Settings > Email tab
Adding a Email Receiver Account	**Enabling Notifications** Check “Enable Email Notification”.  **Configuring Email Sender Settings** Enter the sender parameters in the Email Settings window.  **Configuring Email Receiver Settings** To add an email receiver account, click “Add” in the Email Receiver Settings options.  Enter the parameters and click “Add” to confirm.  The new email receiver account will appear in the Email Receiver Setting options.  **Completing Configuration** ■ Click “OK” to confirm and close the Notification Settings. ■ Click “Cancel” to reset the entered parameters. ■ Click “Apply” to confirm the entered parameters and continue configuring other notifications.

Parameters	**Email Address**	Specifies the email address of the receiver.
	Severity > Notification	Notifies users whenever a system event occurs.
	Severity > Warning	Notifies users of all warnings and critical messages.
	Severity > Critical	Notifies users only when critical issues occur.
	SMTP Server	Specifies the SMTP mail server name. Example: advantech@smtp.com
	SMTP Port	Specifies the SMTP mail server port number.
	Account	If sending an email requires logging into an account, specifies the account name.
	Password	If sending an email requires logging into an account, specifies the password.
	Sender Email	Specifies the sender email address.

3.5.3 Notification via Fax

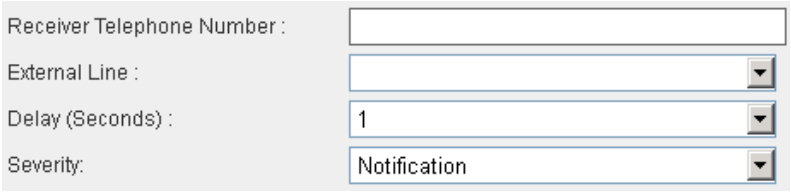
The computer must be equipped with the following modules to use this feature.

- Windows Messaging (MAPI) in Windows environment (software module)
- One modem port compatible with FAX Command Class 2.0 (hardware module)

Go To	SANWatch Home > Top menu bar > Settings > Notification Settings > FAX tab
Adding a FAX Receiver Account	**Enabling Notifications** Check “Enable Broadcast Notification”.  **Configuring Fax Settings** Specify the severity and fax queue size in the Fax Settings tab. Click “Add” in the Fax Receiver Setting options.

Enter the parameters and click “Add”.

The new fax recipient will appear in the SNMP Receiver Settings options.



Completing the Configuration

- Click “OK” to confirm and close the Notification Settings.
- Click “Cancel” to reset the entered parameters.
- Click “Apply” to confirm the entered parameters and continue configuring other notifications.

Parameters	**Receiver Telephone Number**	Specifies the Fax number, including the country code. Example: 14085555555
	Queue Size	Specifies the fax queue size.
	External Line	Sends out an outside line dial tone before the fax number. Range: 0 to 9.
	Delay (Seconds)	Specifies the interval between the outside line dial tone and the fax number in seconds. Range: 1 to 9.
	Severity > Notification	Notifies users of all events.
	Severity > Warning	Notifies users of all warnings and critical events.
	Severity > Critical	Notifies users only when critical issues occur.

3.5.4 Notification via SMS

The computer must be equipped with a GSM modem to enable this feature.
The following modems are tested and found to comply with SANWatch:

- Siemens TC35
- Wavecom Fast Rack M1206

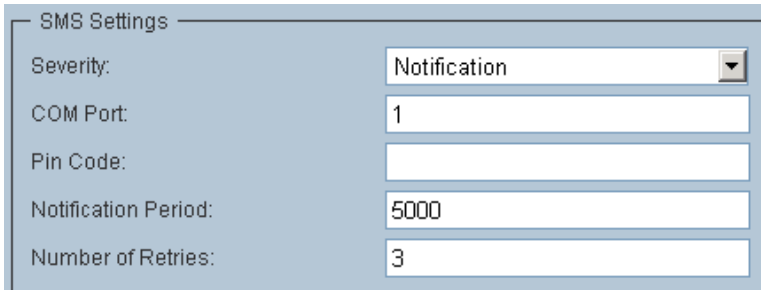
Go To	SANWatch Home > Top menu bar > Settings > Notification Settings > SMS tab

Enabling Notifications

Check “Enable SMS Notification”.

Configuring SMS Sender Settings

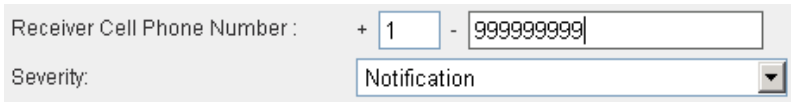
Enter the sender information and specify the severity.



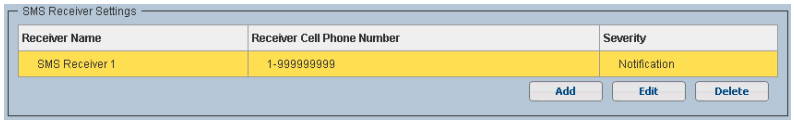
Configuring SMS Receiver Settings

Click “Add” in the SMS Receiver Setting tab.

Enter the parameters and click “Add”.



A new MSN recipient will appear.



Completing the Configuration

- Click “OK” to confirm and close the Notification Settings.
- Click “Cancel” to reset the entered parameters.
- Click “Apply” to confirm the entered parameters and continue configuring other notifications.

Parameters	**Receiver Cell Phone Number**	Specifies the phone number, including the country code, to which the SMS message will be sent. Example: +1-4085555555
	Severity > Notification	Notifies users of all events.
	Severity > Warning	Notifies users of all warnings and critical events.
	Severity > Critical	Notifies users only when critical issues occur.
	COM Port	Specifies the port number to which the message will be sent.
	Pin Code	Specifies the PIN code of the phone.
	Notification Period	Specifies the notification period of the SMS.
	Number of Retries	Specifies the number of times the SMS will be resent in the event it fails to send.

3.5.5 Notification via SNMP

SNMP (Simple Network Management Protocol) is a network protocol used to monitor network-attached devices.

Go To

SANWatch Home > Top menu bar > Settings > Notification Settings > SNMP tab

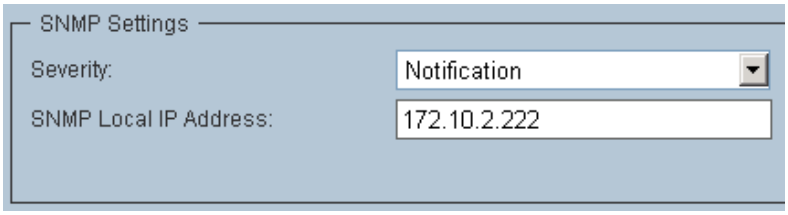
Adding an SNMP Receiver

Enabling Notifications

Check “Enable SNMP Notification”.

Configuring the Local Side

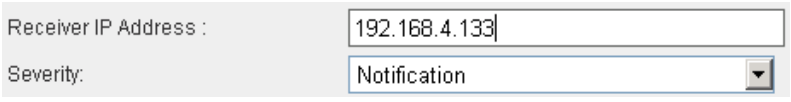
Select the severity and enter the IP address of the local side.



Configuring the Remote Side

Click “Add” to add an SNMP receiver.

Enter the parameters and click “Add”.



The new SNMP recipient will appear.

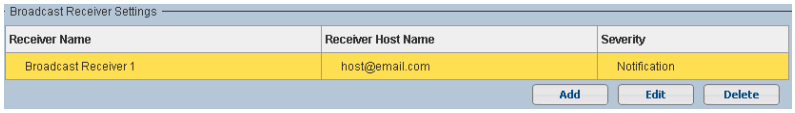
Completing the Configuration

- Click “OK” to confirm and close the Notification Settings.
- Click “Cancel” to reset the entered parameters.
- Click “Apply” to confirm the entered parameters and continue configuring other notifications.

Parameters	**Receiver IP**	Specifies the IP address of the SNMP receiver. Example: 192.168.4.133
	Severity > Notification	Notifies users of all events.
	Severity > Warning	Notifies users of all warnings and critical events.
	Severity > Critical	Notifies users only when critical issues occur.
	SNMP Local IP	Specifies the IP address of the SNMP sender. Example: 192.168.4.133

3.5.6 Notification via Broadcasting

This option involves sending notifications via LAN networks.

Go To	SANWatch Home > Top menu bar > Settings > Notification Settings > Broadcasting tab
Adding a new Broadcasting receiver	**Enabling Notifications** Check “Enable Broadcast Notification”.  **Configuring Settings** Click “Add” in the Broadcast Receiver Setting options. Enter the parameters and click “Add”. The host name must be entered as an email address.  The new Broadcast recipient will appear.  **Completing Configuration** ■ Click “OK” to confirm and close the Notification Settings. ■ Click “Cancel” to reset the entered parameters. ■ Click “Apply” to confirm the entered parameters and continue configuring other notifications.

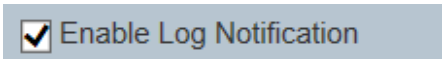
Parameters	**Receiver Host Name**	Specifies the email address of the receiver.
	Severity > Notification	Notifies users of all events.
	Severity > Warning	Notifies users of all warnings and critical events.
	Severity > Critical	Notifies users only when critical issues occur.

3.5.7 Sending the System Log to Users

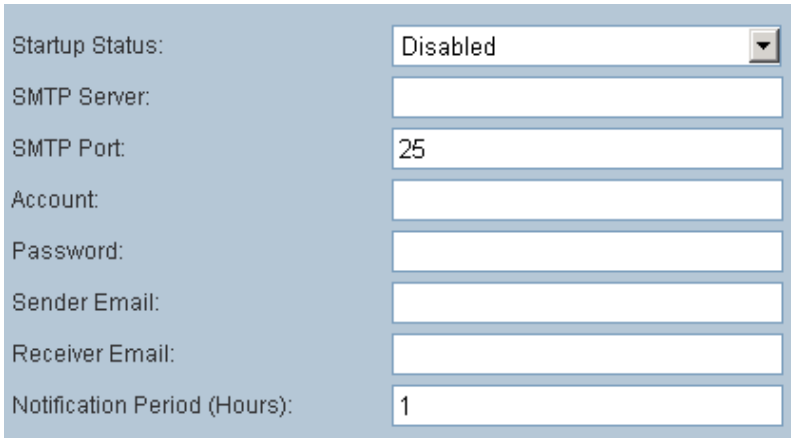
Users may periodically receive system log information by email.

Steps

Click the Log tab in the Notification Settings menu. (The log notification setting appears by default when notifications are enabled.) Check “Enable Log Notification”.



Enter the notification parameters.



Completing Configuration

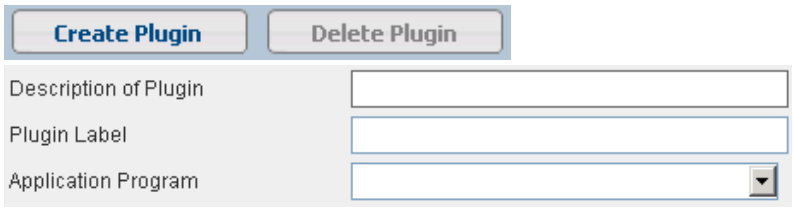
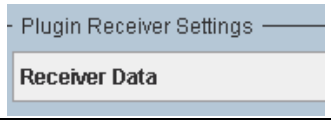
- Click “OK” to confirm and close the Notification Settings.
- Click “Cancel” to reset the entered parameters.
- Click “Apply” to confirm the entered parameters and continue configuring other notifications.

Parameters

Startup Status	Enables or disables log notifications.
SMTP Server	Specifies the SMTP mail server name. Example: Advantech@smtp.com
SMTP Port	Specifies the SMTP mail server port number.
Account	If sending an email requires logging into an account, specifies the account name.
Password	If sending an email requires logging into an account, specifies the password.
Sender Email	Specifies the email address of the sender.
Receiver Email	Specifies the email address of the receiver.
Notification Period	Specifies how frequently the log will be sent to the receiver.

3.5.7.1 Activating Applications Upon Events

Users can set the system to activate specific applications when a system event occurs.

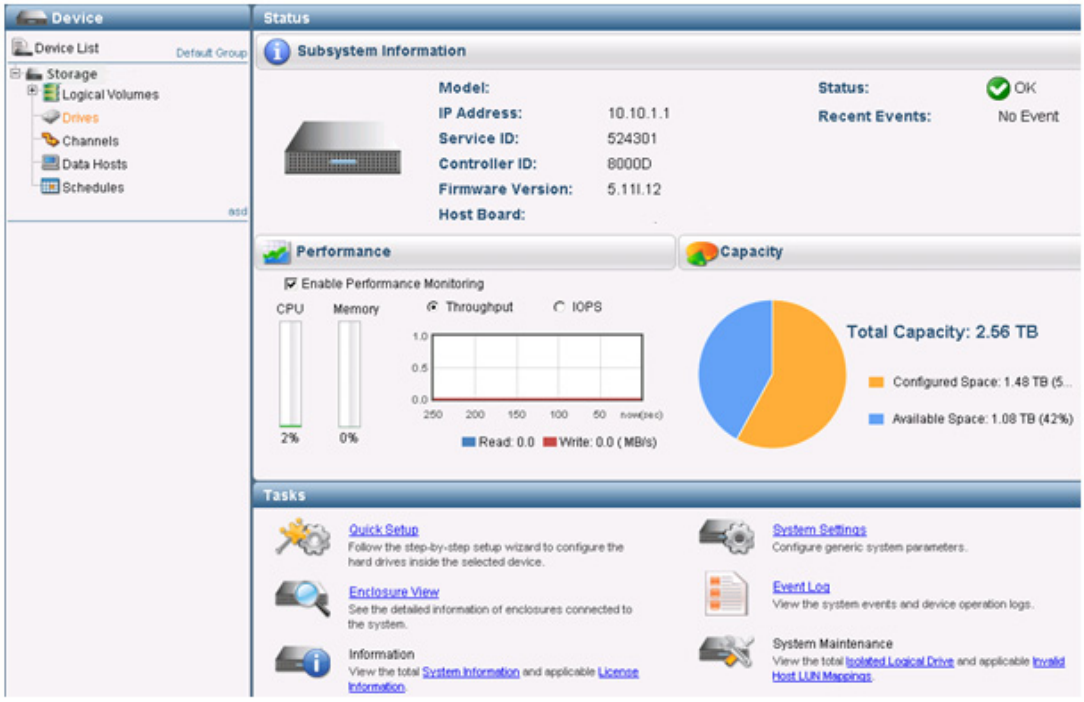
Steps	Copy the plugin executable file into the folder. Example: Application.exe (for Windows)	
Activate the Notification Settings	Click the Plugin tab in the Notification Settings menu. The Plugin setting will appear. **Creating the Plugin** Click “Create Plugin” in the Plugin options and enter the details of the plugin program.  **Creating the Receiver** Click “Add” to show an input field dialog box. Enter the configuration string to be read when the application program starts. An example configuration argument is provided below. "\plugin\userprogram.exe uid=xx model=xxx-xxx ip=xxx.xxx.xxx.xxx ctrlrName=N/A severity=1 evtStr="Evt String" recv="customized string" 	
Parameters	**Plugin Description**	User-defined description of the plugin program.
	Plugin Label	User-defined title of the plugin program.
	Application Program	The list of application programs stored in the plugin subfolder.

Chapter 4

Working with Devices

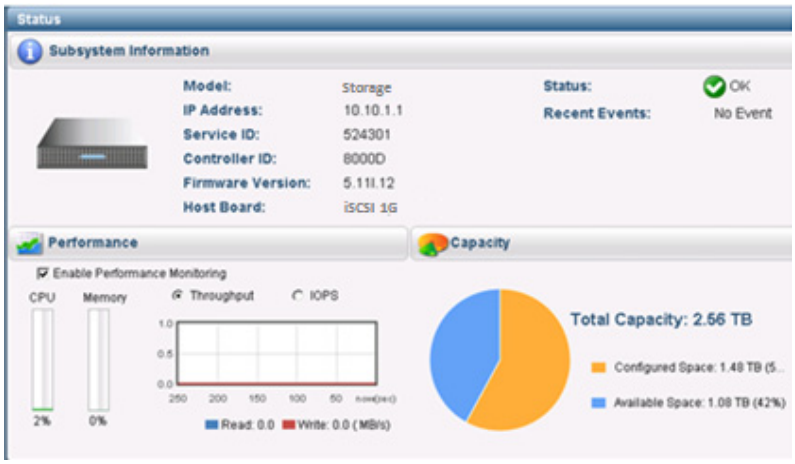
4.1 Introduction

This chapter explains how to view and configure the hardware parameters of a device, including the system performance, event log, hard disk drive, invalid/isolated logical drive, and host LUN settings.



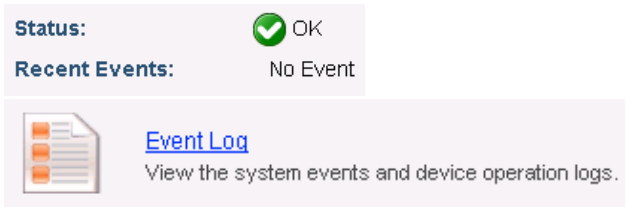
4.2 Viewing the Overall Status

The status of each device (RAID system or JBOD expansion enclosure) is summarized in the Subsystem Information page. This page enables users to understand the hardware configuration, performance, and storage capacity at a glance.

Go To	SANWatch Home > Device sidebar > device name
Viewing the Subsystem Information	The device status will be summarized in the Status window. 

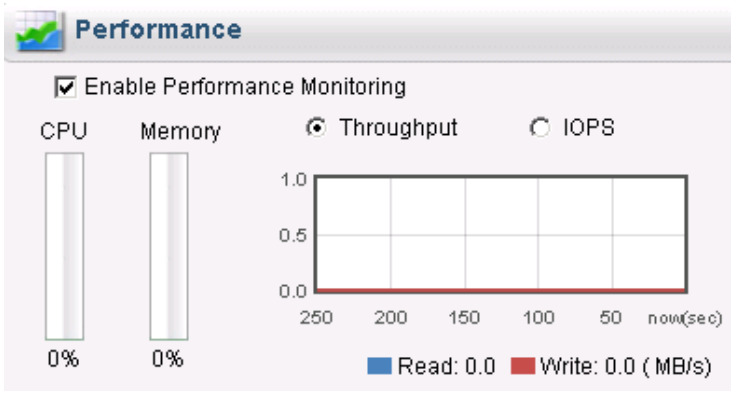
Hardware Configurations
The basic system configurations and overall system status are listed in the Subsystem Information window. The model name, IP address, controller ID (may be required for technical support requests), and firmware version are also provided.

Events
All recent system events will be listed in the Recent Events area. To view all past events, click “Event Log” in the Tasks section.

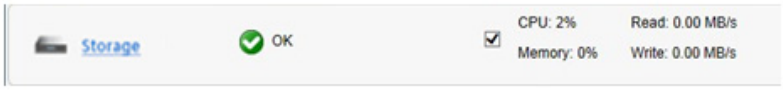


Performance Monitor
Check the Enable Performance Monitoring option to view the CPU/ memory usage and read/write throughput.

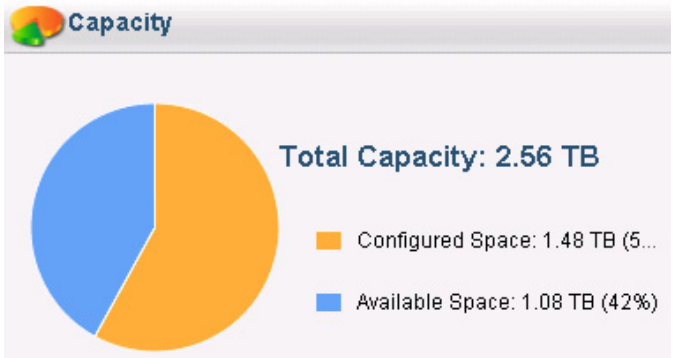
The performance monitor is disabled by default to save system resources.



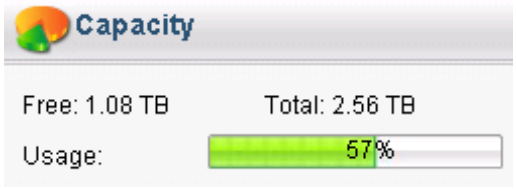
Users can also click “Device List” in the top-left corner to view a summary of the system performance according to device.



Storage Capacity
This enables users to view the ratio of used (configured) and remaining (available) capacity.



A quick summary is also provided in the Device Status list view.



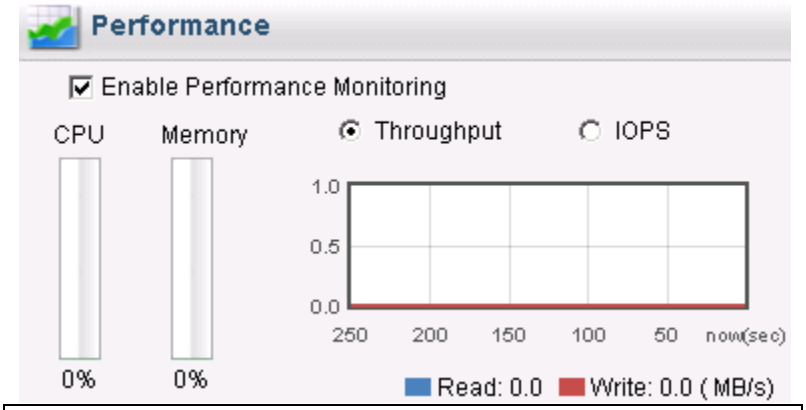
4.2.1 Monitoring System Performance

Users can quickly review the current system performance via the device home page. The System Information screen provides more detailed information, including controller throughput and cache usage data.

Because status monitor affects system performance, the monitoring functions are disabled by default.

Overall System Performance

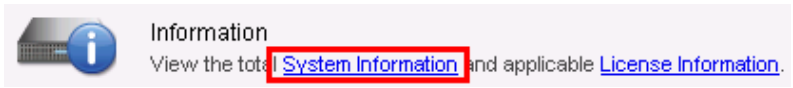
Go to SANWatch Home > Device sidebar > device name
Check the Enable Performance Monitoring option to view the CPU/ memory usage and read/write throughput.



The performance monitor is disabled by default to save system resources.

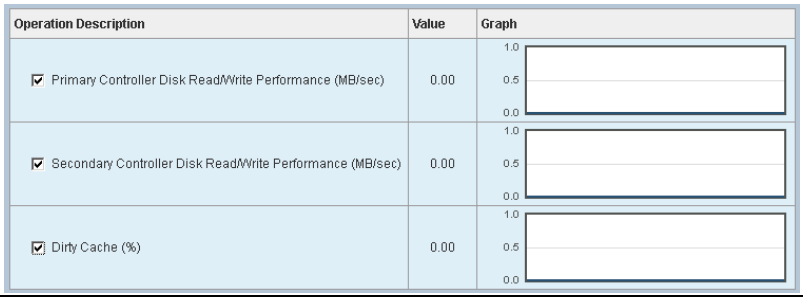
Controller Performance and Cache Usage

Click “System Information” in the Tasks section.



Select the Statistics tab in the System Information screen that appears.

Check the item to monitor: Controller read/write performance and cache usage (dirty cache).

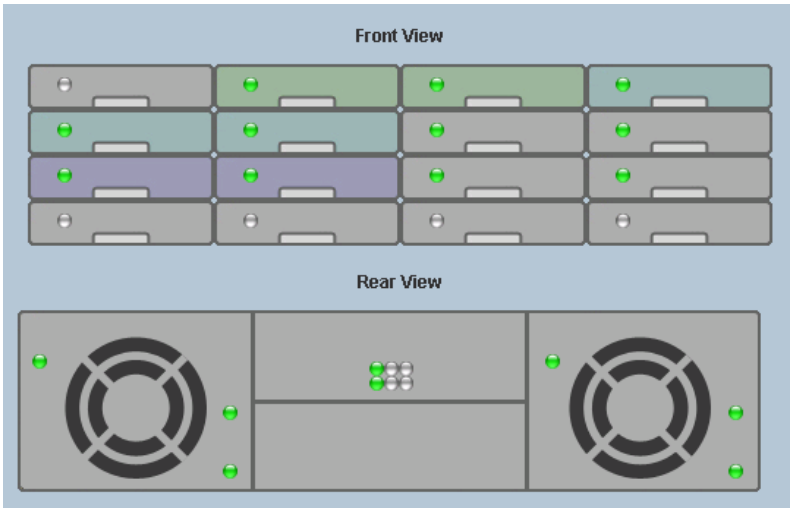


4.2.2 Viewing the Hardware Status LED

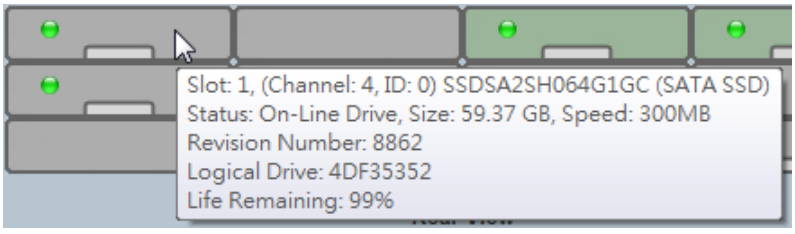
Enclosure View provides users with a brief overview of the hardware modules (hard drives, power supplies, and controllers) installed on the device, as well as the hardware status LEDs.

For precise definitions of the hardware indicator LEDs and their status, refer to the hardware manual.

Go To	SANWatch Home > Device sidebar > Device List > device name > Tasks section
Enclosure View	Click “Enclosure View” in the Tasks section. The front/rear view of the device will appear. Each circle (green/red) denotes an LED indicator.



To view the specifications of hardware module, hover the mouse cursor over the module. The information will be displayed in a tooltip.



“Life Remaining” is only available for SSD drives.

Hard Drives (Front View)

*  Currently installed

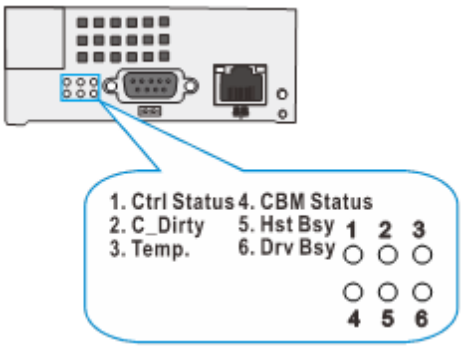
*  Currently uninstalled or in an error state

Power Supplies (Rear View)

The LED on the left side indicates the power supply status. The two LEDs on the right side indicate the cooling fan status.

Controllers (Rear View)

The six LEDs indicate the controller status.



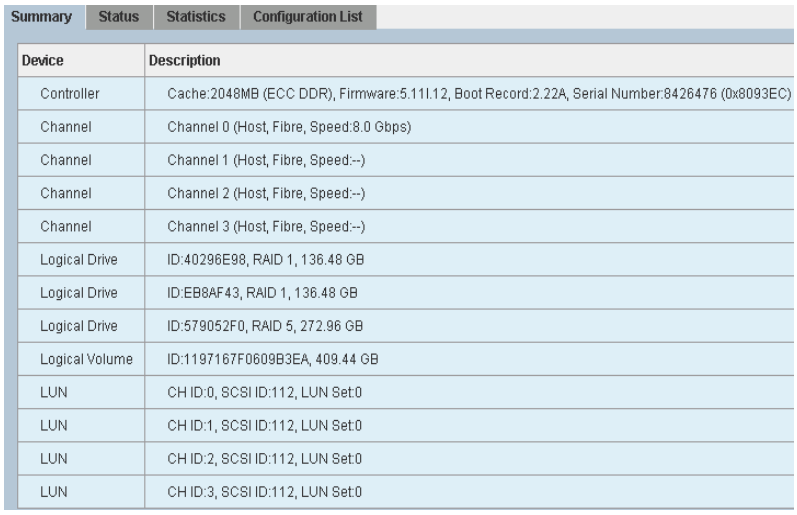
Name	Color	Status
1. Ctrl Status	Green/ Amber	**Green** indicates that a RAID controller is operating healthily. **Amber** indicates that a component failure has occurred, or inappropriate RAID configurations have caused system faults. The LED also emits amber light during the system initialization process.

2. C_Dirty	Amber	**Amber** indicates the following: ■ Cache memory is dirty. ■ Data in the flash backup module is being flushed to the cache. ■ Errors have occurred in the cache memory (ECC errors). ■ Data is being flushed from the flash backup module to the drive (when power is restored). ■ Battery voltage is lower than 2.5V. ■ Battery temperature reading is abnormal (outside the 0 ~ 45 °C range). ■ Battery is not present. **OFF** indicates the cache is clean and that the battery backup unit is capable of sustaining memory in case of a power loss. **Blinking Amber** indicates cached data is being transferred to the flash module after the occurrence of a power outage. Once the transfer is done, all LEDs will turn off. This signal is local to each controller.
3. Temp.	Amber	**Amber** indicates that the detected CPU/board/chassis temperature has exceeded the higher temperature threshold. **OFF** indicates that the detected temperature reading is within the safe range.
4. CBM Status	Green/ Amber	**Green steady on** indicates the CBM module is ready. Both a BBU and a flash module are present. **Amber** steady on indicates CBM failure, meaning either the BBU or flash module has failed. Amber light can also indicate that either BBU or flash is missing in a redundant-controller system. **Blinking** means a BBU is being charged. OFF means BBU is not installed in a single-controller “G” model.
5. Hst Bsy	Green	**Blinking Green** indicates traffic on the host bus.
6. Drv Bsy	Green	**Blinking Green** indicates traffic on the drive channels.

4.2.3 Viewing System Information

The System Information screen shows the current device status and configurations.

Go To	SANWatch Home > Device sidebar > Device List > device name> Tasks section
Steps	Click “System Information” in the Tasks section. The system information screen will appear.



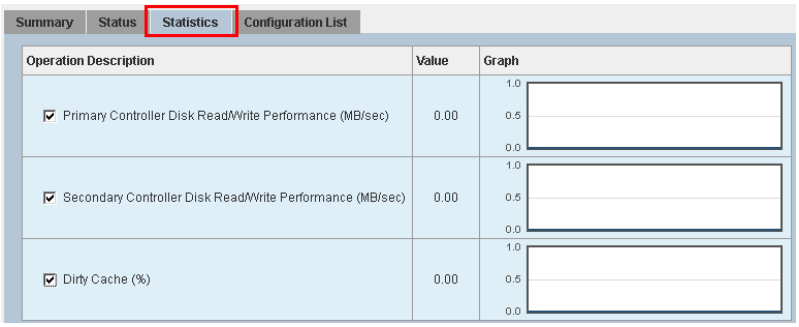
Entire System Configuration

To view all system information (settings) at once, select the Configuration List tab.

Controller/Cache Status

To monitor the controller throughput and cache usage (dirty cache), select the Statistics tab and check the items to monitor.

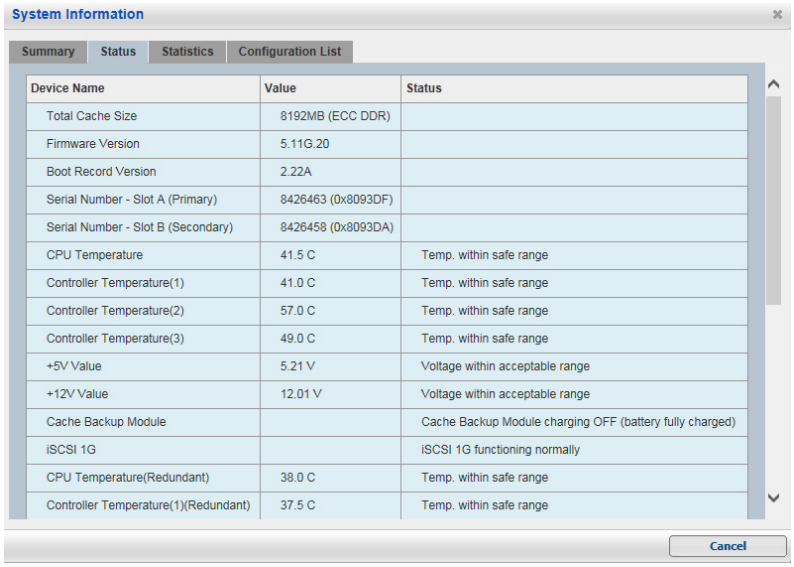
Users can view the overall system throughput and storage capacity usage from the Device home page screen in the Performance section.



Temperature/Voltage

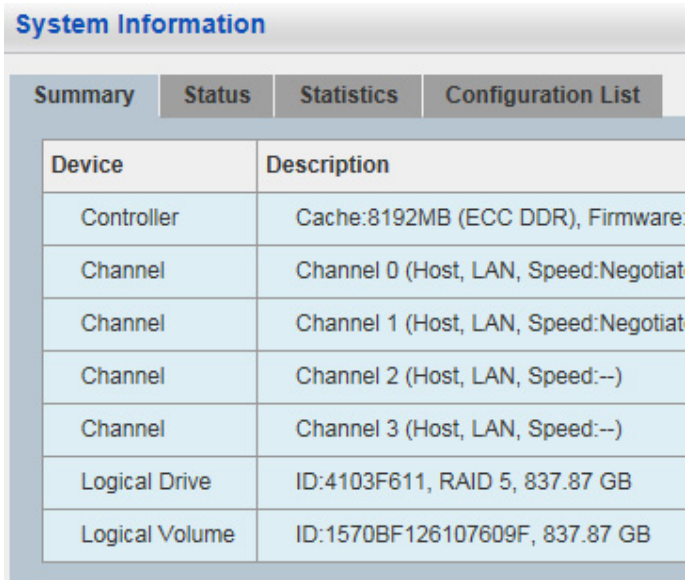
To monitor the voltage and temperature of the device, select the Status tab.

When the voltage/temperature reaches preconfigured thresholds, an event notification message will be sent to warn the user of the potential hazard. Users can change the threshold settings via the System Settings link in the Tasks section.



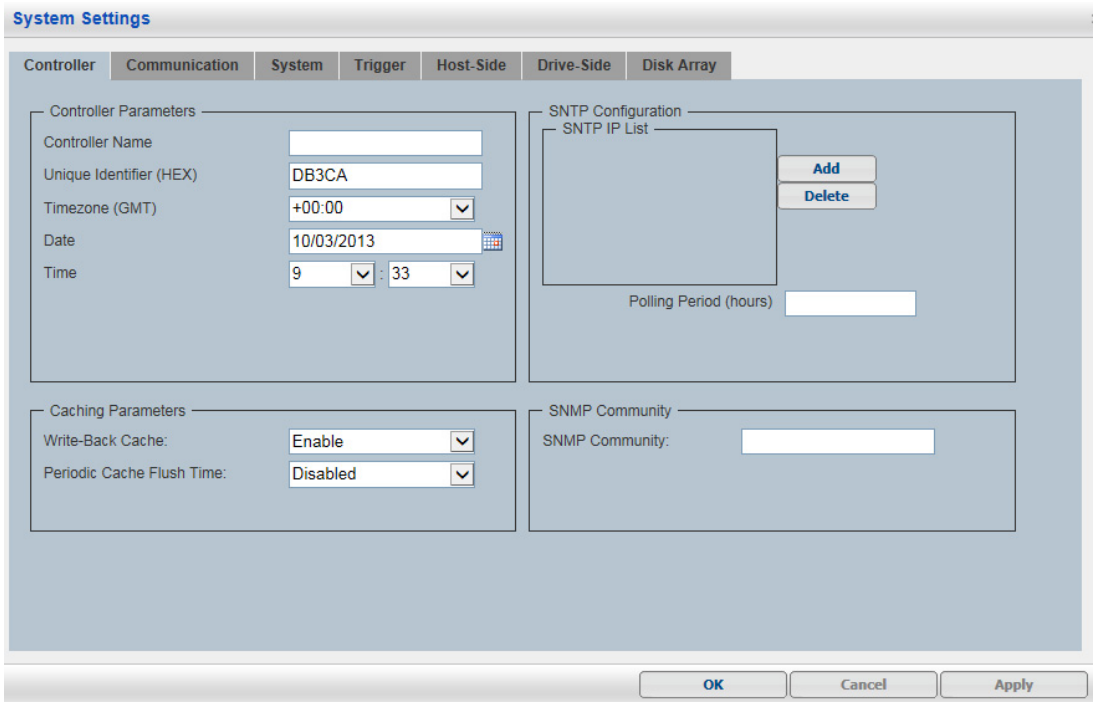
Controller and Channel Settings

To view the current controller and channel configurations, select the Summary tab.



To configure channel settings, click on the Channels link in the sidebar.

4.3 Configuring System Settings



4.3.1 Summary of System Configurations

<table>
<tr><td>Go To</td><td colspan="3">SANWatch Home > Device sidebar > Device List > device name > Tasks section</td></tr>
<tr><td>Steps</td><td colspan="3">Click “System Settings”.
 

The System Settings screen will appear.

To change the settings, pick an item, select a different option, and click “Apply” or “OK”. A list of configurable items is provided below. Default values are marked in bold.</td></tr>
<tr><td>Controller Tab</td><td colspan="3">For configuring the controller parameters.</td></tr>
<tr><td></td><td>Item</td><td>Options</td><td>Configuration List</td></tr>
<tr><td></td><td>Controller Name: (user-defined, empty)
Unique Identifier: (device-defined)
Time Zone: -12:45 to 00:00 to +13:45 Date/ Time: (computer-defined)</td><td>Controller Setting(s)</td><td>Controller Parameters</td></tr>
<tr><td></td><td>Caching Parameters</td><td>Write-Back Cache: Enabled / Disabled
Periodic Cache Flush Time (sec): Disabled</td><td></td></tr>
<tr><td></td><td>SNTP Configuration</td><td>SNTP IP List: (user-defined, empty)
Polling Period (hr): (user-defined, empty)</td><td></td></tr>
<tr><td></td><td>SNMP Community</td><td>(user-defined)</td><td></td></tr>
<tr><td>Communication Tab</td><td colspan="3">For configuring the network and serial communication settings.</td></tr>
<tr><td></td><td>Item</td><td>Options</td><td>Configuration List</td></tr>
<tr><td></td><td>Management Port</td><td>IPV4/IPV6</td><td></td></tr>
<tr><td></td><td>RS232</td><td>Terminal Emulation: Enabled
Baud Rate: 2400 ~ 38400</td><td>Communication > COM 1</td></tr>
<tr><td></td><td>Network Protocol Support</td><td>Enable network protocol support</td><td></td></tr>
<tr><td></td><td>ISNS (for iSCSI-host models only)</td><td>Add/Delete Server IP</td><td></td></tr>
<tr><td></td><td>Trunk Groups (iSCSI-host models only)</td><td>All channels except CH0</td><td></td></tr>
</table>

System Tab

For conducting system maintenance (reset, memory export/import, etc.).

Item	Options	Configuration List
System	Mute Beep Sound Reset Controller Shutdown Controller Force Fail Slot A Controller (R-models only) Force Fail Slot B Controller (R-models only) Restore Factory Defaults	
Download/Upload	Update FW Update FW and Boot Disk Import NVRAM from Host Disk Export NVRAM to Host Disk Import NVRAM from Disk Export NVRAM to Disk	
Password	Change admin password	
Redundant	Cache Synchronization on Write-Through Adaptive Write Policy	

Trigger Tab

For configuring the upper/lower temperature and voltage thresholds for the device, as well as the notification trigger events.
Highlight a threshold parameter and click “Configure” to set the upper/lower thresholds or check a trigger event.

Item	Options	Configuration List
Threshold	CPU temperature Controller temperature +5 Value +12 Value	Upper/Lower Threshold
Trigger	Controller Failure CBM Low or Failure Power Supply Failure Cooling Fan Failure Temperature Exceeding Threshold	NA

Host-Side Tab

For configuring the host computer and host interface settings.

Item	Options	Configuration List
Maximum Number of Queued I/O	1024	Host-Side Parameters
LUN per Host SCSI ID	N/A	Host-Side Parameters
Login Authentication with CHAP	Disable/Enable	Host-Side Parameters
Jumbo Frames	Disable/Enable	Host-Side Parameters
Max Concurrent Host-LUN Connections	4	Host-Side Parameters
Tags Reserved per Host-LUN Connection	4	Host-Side Parameters
Peripheral Device Type	(Various)	Host-Side Parameters
Peripheral Device Qualifier	Connected/Supported but not Connected	Host-Side Parameters
Device Supports Removable Media	Disable/Enable	Host-Side Parameters
LUN Applicability	First Undefined LUN /Only Undefined LUN 0's	Host-Side Parameters
Cylinder/Header/Sector	Various/Variable	Host-Side Parameters
Fibre Connection Option	Loop Only/Point to Point Only	Host-Side Parameters

Drive-Side Tab

For configuring the hard drive interface settings.

Item	Options	Configuration List
Auto-Assign Global Spare Drive	Disabled/Enabled	Drive-Side Parameters
Auto Rebuild on Drive Swap (sec)	Disabled/5 to 15 to 60	Drive-Side Parameters
SAF-TE/SES Device Check Period (sec)	Disabled/0.05 to 60.0	Drive-Side Parameters
Disk Access Delay Time (sec)	No Delay/5 to 60 to 75	Drive-Side Parameters
Disk I/O Timeout (sec)	0.5 to 30.0	Drive-Side Parameters
SMART	Disabled/Detect Only/Clone Only/ Copy & Replace/ Fail Drive	Drive-Side Parameters
Maximum Number of Tags	Disabled/1 to 4 to 128	Drive-Side Parameters
Drive Motor Spin Up	Disabled/Enabled	Drive-Side Parameters
Power Saving (Level 1 and Level 2)	Disabled/1 min to 1 hour	Drive-Side Parameters
SED Authentication Key	Create/Modify	Drive-Side Parameters

Disk Array

For configuring hard drive array settings.

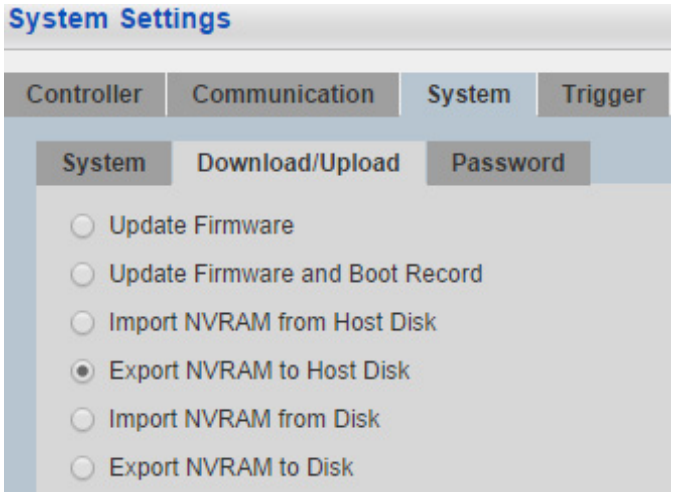
Item	Options	Configuration List
Rebuild Priority	Normal/Improved/ High	Disk Array Parameters
Verify Write on LD Initialization	Disable/Enable	Disk Array Parameters
Verify Write on LD Rebuild	Disable/Enable	Disk Array Parameters
Verify Write on Normal Access	Disable/Enable	Disk Array Parameters
Maximum Drive Response Timeout	Disable/160(ms) / 320(ms)/960(ms)	Disk Array Parameters
AV Optimization Mode	Disable/Fewer Streaming seconds	Disk Array Parameters
Read-Ahead Option for Media Editing	Disable/SD Stream (50Mb/s) seconds/ HD Stream (100Mb/s) seconds/2K_4K Stream (100Mb/s+) seconds	Disk Array Parameters

4.3.2 Updating the Firmware

Download the latest firmware from Advantech, and update the system OS (this web interface) of the subsystem controller(s).

Prerequisite I: Checking Current Firmware Version

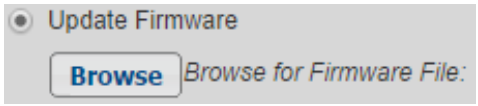
To check the firmware version, go to SANWatch Home > Device sidebar > Device List > device name > Status section. The firmware version information can be found in the Subsystem Information section.

Prerequisite II: Exporting System Configuration	Go to SANWatch Home > Device sidebar > device name > Tasks sidebar > System Settings > System tab > Download/Upload tab  Select Export NVRAM to Host Disk and click “OK”. For more information, click the Help icon at the top-right corner and look for the Exporting /Importing NVRAM section.
Prerequisite III: Obtaining the Firmware Package	Please contact the technical support department or your vendor to obtain the latest firmware package. Go to http://support.Advantech.com, and then get more information.

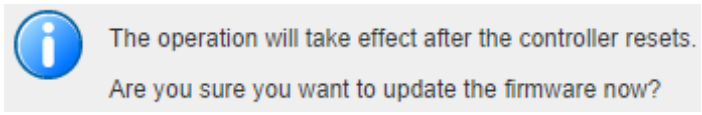
Updating the Firmware

Go to SANWatch Home > Device sidebar > Device List > device name > Tasks section
Click “System Settings”.
The System Settings screen will appear. Go to System > Download/Upload

Click “Browse” under Update Firmware, locate and open the BIN file downloaded from Advantech.



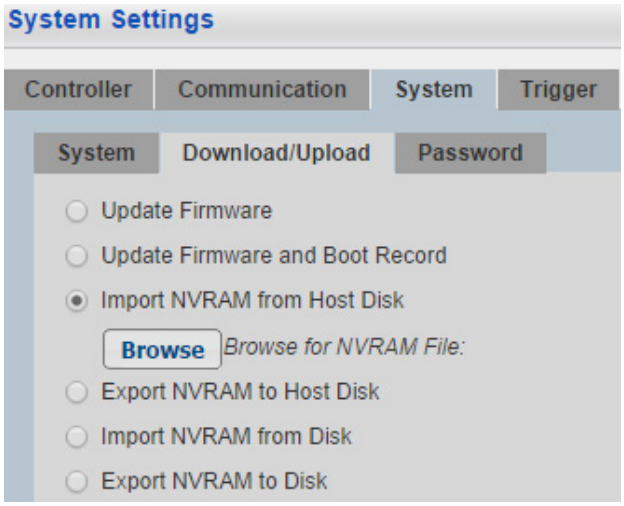
In the confirmation dialog that appears, click “Yes” to start the updating process.



Once updating is completed, the controller(s) must be reset for the update to take effect.
For R-models, click “Rolling Upgrade” to reset each controller individually and reduce system downtime. Alternatively, click “Reset” to reset all the controllers simultaneously.
For other models, click “Reset” to reset the controller.

Importing System Configurations

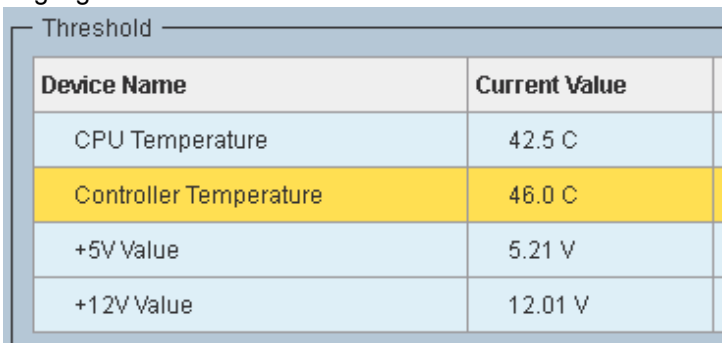
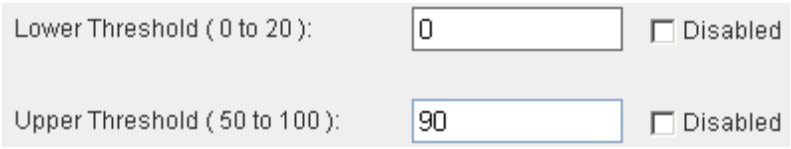
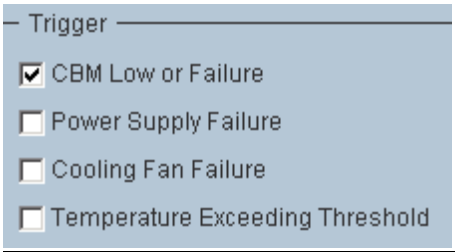
Go to SANWatch Home > Device sidebar > device name > Tasks sidebar > System Settings > System tab > Download/Upload tab



Select Import NVRAM from Host Disk and click “Browse” to locate the system configuration file exported prior to updating the firmware. For more information, click the Help icon at the top-right corner and look for the Exporting /Importing NVRAM section.

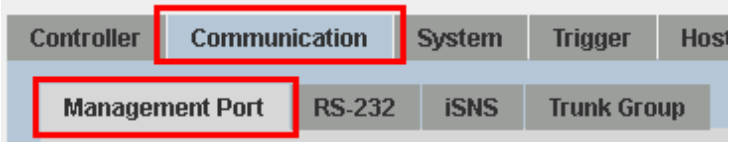
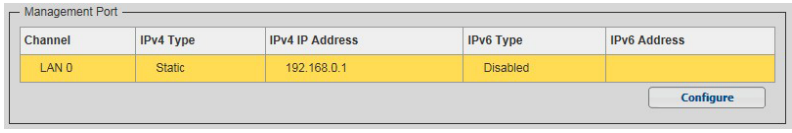
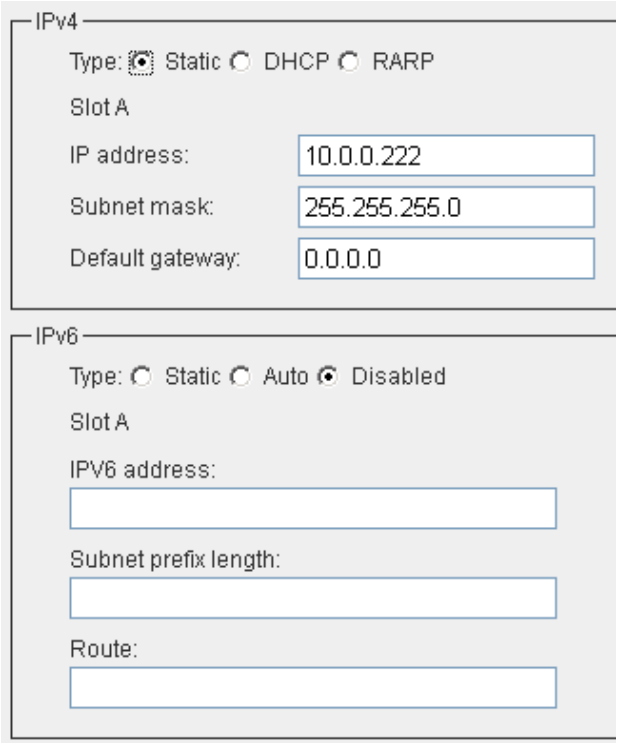
4.3.3 Configuring Voltage/Temperature Thresholds

A RAID subsystem or a JBOD enclosure is equipped with internal voltage and temperature sensors. When the current voltage/temperature reaches a preconfigured threshold, an event notification will be sent to warn the user of the potential hazard.

Go To	SANWatch Home > Device sidebar > Device List > device name > Tasks section
Configuring the Temperature/Voltage Thresholds	Click “System Settings”. The System Settings screen will appear. Select the Trigger tab. The threshold settings will appear. **Trigger** **Configuring the Voltage/Temperature Threshold** Highlight an item in the list.  Click “Configure”. The configuration screen will appear. Enter a threshold value, or click “Disable” to disable the threshold function (and notification).  . **Setting Event Triggers** Users can select the events that trigger the subsystem to send an event notification.  To receive notifications when the temperature reaches the threshold, ensure that the Temperature Exceeding Threshold checkbox is ticked.

4.3.4 Configuring the IP Address

The device IP address can be changed; however, the user interface at the old address will be disconnected. Users should be sure to note the new IP address and reconnect with the user interface using the new address.

Notes	Users cannot assign the following system reserved IP addresses to a subsystem: ■ 127.x.x.x ■ 128.0.x.x ■ 191.255.x.x ■ 192.0.x.x ■ 223.255.255.x
Go To	SANWatch Home > Device sidebar > Device List > device name > Tasks section
Steps	Click “System Settings”. The System Settings screen will appear. Select the Communication > Management Port tab.  Highlight the management (LAN) port to be configured and click “Configure”.  Users can configure the IP address (IPV4 or IPV6).  The following system reserved IP addresses should not be used for the subsystem: 169.254.1.1~169.254.254.254.

Parameters	**IPV4 Type**	■ Static: Specifies a fixed address. ■ DHCP: Allows the network router to assign an available address to the device. ■ RARP: Reverse Address Resolution Protocol is an old networking protocol used by a host computer to request its Internet Protocol (IPV4) address from an administrative host.
	IP Address/Subnet Mask/Default Gateway	Specifies (or lets the router pick) the IP address set for the device.
	IPV6 Type	■ Static: Specifies a fixed address. ■ Auto: Corresponds to the DHCP setting in the IPV4 address. The router automatically assigns an address to the device. ■ Disabled: Disables IPV6 (and enables IPV4).
	IPV6 Address	Specifies (or lets the router pick) the IP address set for the device.
	Subnet Prefix Length	Corresponds to the Subnet setting in IPV4.
	Route	A route is required to reach externally with IPV6 using an IPV6 router on the network.

4.3.5 Configuring Power Saving Settings

The power-saving option can enhance the disk spin-down function for all disks on the subsystem. When no host I/O exists, disk drives can enter two power-saving modes: Level 1 for idle mode and Level 2 for spin-down mode.

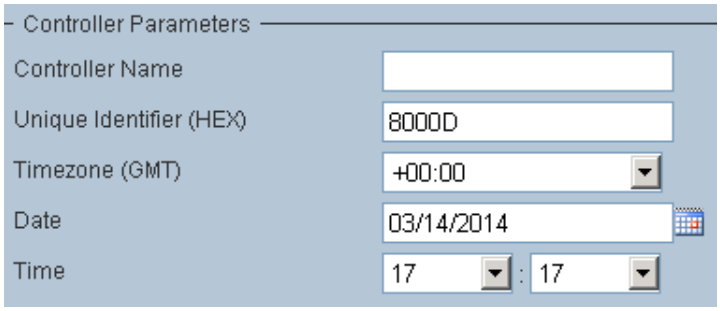
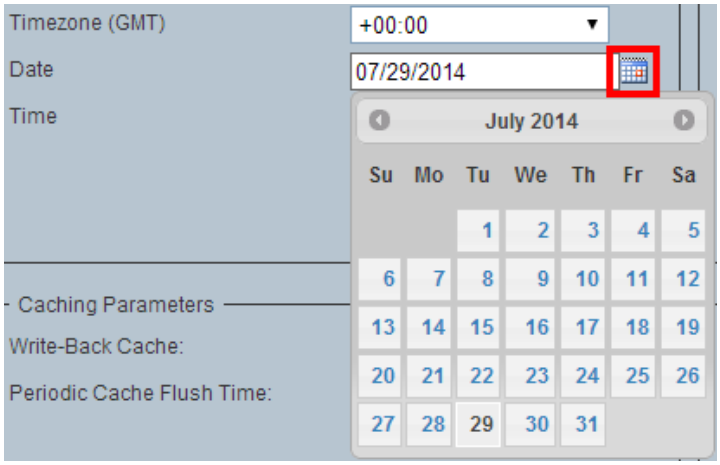
- Level 1: Hard disks enter the standby mode by reducing spinning speed (RPM)
- Level 2: Hard disk read/write heads become idle by moving away from disk surfaces

Users can further tailor the power saving settings by applying different settings to a logical drive, including its local spares. To do this, go to SANWatch Home > Device > Logical Volumes > Logical Volume Name > Logical Drives > Logical Drive Name ==> Tasks, and then click “Power Saving”.

Go To	SANWatch Home > Device sidebar > Device List > device name > Tasks section
Steps	Click “System Settings”. The System Settings screen will appear. Select the Drive-Side tab.  The power saving settings are located near the bottom.  **Power Saving Level** Select the Drive-Side tab and configure the power saving mode. The three options available are **Disabled, Level 1 only**, and **Level 1 then Level 2**. **Waiting Period** Users can also configure the duration of time allocated (waiting period) before the device switches over to power saving mode. ■ Level 1: 1 to 60 minutes without I/O requests ■ Level 2: 1 to 60 minutes of Level 1 state To configure power saving levels for individual logical drives, select the logical drive in the Device sidebar, and click “Power Saving” in the Tasks section.

Levels	Power Saving Ratio	Recovery Time	ATA Command	SCSI Command
Level 1	15 to 20%	1 second	Idle	Idle
Level 2	80%	30-45 seconds	Standby	Stop

4.3.6 Configuring Time Settings

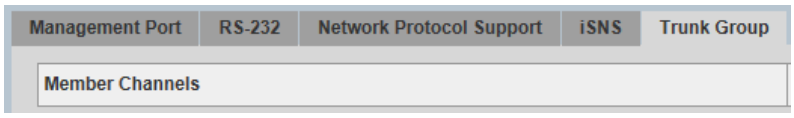
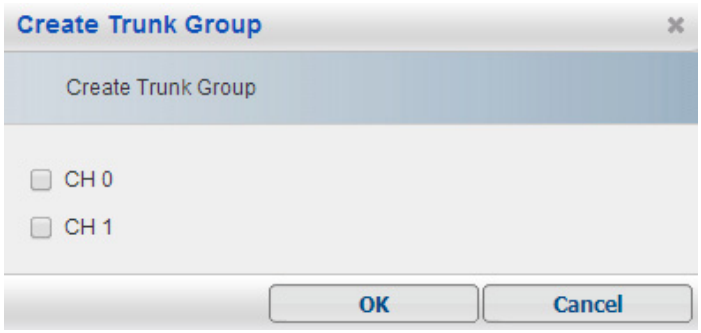
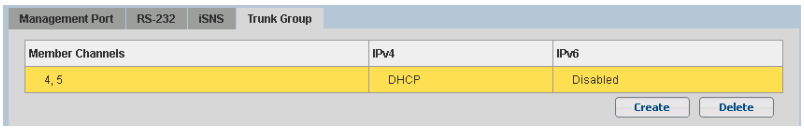
Go To	SANWatch Home > Device sidebar > Device List > device name > Tasks section
Steps	Click “System Settings”. The System Settings screen will appear. Select the Controller tab. **Controller** Configure the controller name, unique identifier, time zone, date, and time.  To configure the date, click the calendar icon to the right and select the correct date. 

4.3.7 Trunking Host Interfaces to Increase Bandwidth

Users can increase the network bandwidth by combining (trunking) multiple LAN interfaces and creating a link aggregation configuration.

Trunking offers the following benefits:

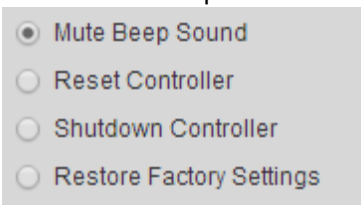
- Increased bandwidth: The bandwidths of multiple interfaces will be added.
- Improved security: Should a LAN interface fail, the other interfaces can ensure the network connection remains intact.

Notes	Multiple LAN ports on the hardware must be connected to the network. The network switch must be compatible with trunking. The trunking option is only available for iSCSI-host models.
Go To	SANWatch Home > Device sidebar > Device List > device name > Tasks section
Steps	Click “System Settings”. The System Settings screen will appear. Select the Communication tab and then the Trunk Group tab.  Click “Create”. In the popup window, select the LAN interfaces to be combined (trunked) and click “OK”.  The new trunk configuration will appear.  To delete a trunk group, click “Delete”.

4.3.8 Muting the Beeper

Each RAID system or JBOD expansion enclosure contains hardware that emits an audible beeping sound to notify users of system errors and hardware failures. Users can mute the sound directly via the hardware (please refer to the hardware manual for details) or remotely via the user interface.

The user interface only enables users to mute the beeper. The beeper function cannot be disabled from the user interface.

Go To	SANWatch Home > Device sidebar > Device List > device name > Tasks section
Steps	Click “System Settings”. The System Settings screen will appear. Select the System > System tab. Select Mute Beep Sound and click “OK”. 

4.3.9 Exporting System Settings

Go To	SANWatch Home > top menu bar > System > Export System Information
Steps	The list of connected devices (RAID subsystem or JBOD) will appear. Select the device and click “OK”. All system information can be saved to a local folder in a zip file.

4.3.10 Exporting/Importing NVRAM

NVRAM contains system configuration information that can be exported to preserve the system settings or imported to restore the system configurations.

When to Export NVRAM	■ After a firmware upgrade ■ Before replacing both controllers ■ After mapping logical drives to host LUN or changing system configurations
When to Import NVRAM	■ The system function is unstable ■ Both controllers have been replaced The firmware version of the NVRAM to be imported must match the firmware version of the current system.
Location	Two options are available for storing the NVRAM information. ■ Disk: Uses the internal storage of the subsystem. At least one logical drive must exist in the subsystem. ■ Host Disk: Uses the storage of the host computer.
Go To	SANWatch Home > Device sidebar > Device List > device name > Tasks section
Steps	Click “System Settings”. The System Settings screen will appear. Select the System > Download/Upload tab. Select a NVRAM option, click “Browse” to locate the file, and click “OK”.

4.4 Working with System Events

Events are signals from the storage subsystem that users and administrators should familiarize themselves with in order to manage the system.

In SANWatch, the Notification module collects the event status and communicates this information to the user through various channels. The following notification settings are available:

- Notifying users of the occurrence of a system event
- Periodically sending the system log
- Activating user-specified applications when a system event occurs

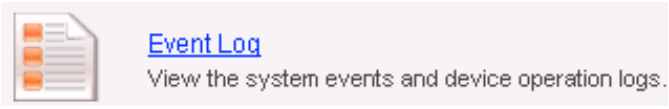
4.4.1 Types of Events

Events can be categorized according to (1) scope and (2) severity. For a detailed list of events and their descriptions, see the Troubleshooting Guide.

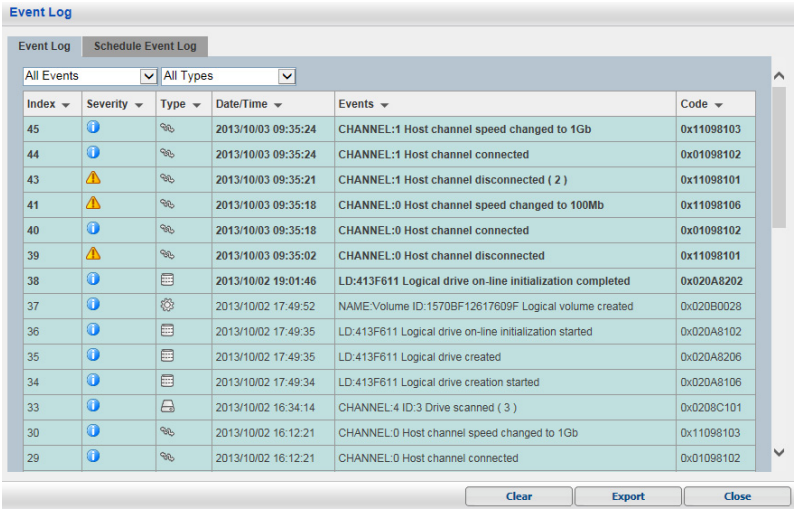
Scope of Events	**Event Type**	**Scope**
	Controller Event	Describes events related to the storage system controllers.
	Drive Event	Describes events related to the physical disk drives.
	Host Event	Describes events related to the host computer and host ports.
	Logical Drive Event	Describes events related to logical drives and logical volumes.
	System Event	Describes events related to the overall storage subsystem.
Severity of Events	This is a combination of the warning, error, and information levels.	
	Severity	**Description**
	critical error	Describes events that users should pay immediate attention to and perform required actions.
	error	Describes events that users should pay attention to and perform required actions.
	warning	Describes events that users should pay attention to.
	information	Describes events that notify users of non-critical changes in system status.

4.4.2 Viewing the Event Log

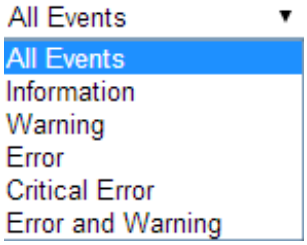
Go To	SANWatch Home > Device sidebar > Device List > device name > Tasks section
Procedures	Click “Event Log” in the Tasks section.

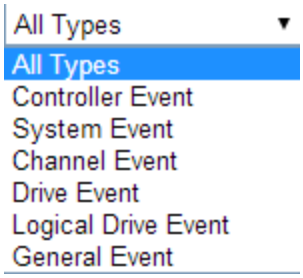


A list of events will appear.



Specify severity and type to filter the listed events.





Click the triangle next to a header to reverse the ascending or descending order.

Parameters	**Event Type**	Selects events according to type (scope).
	Severity	Selects events according to severity.

4.4.3 Exporting the Event Log

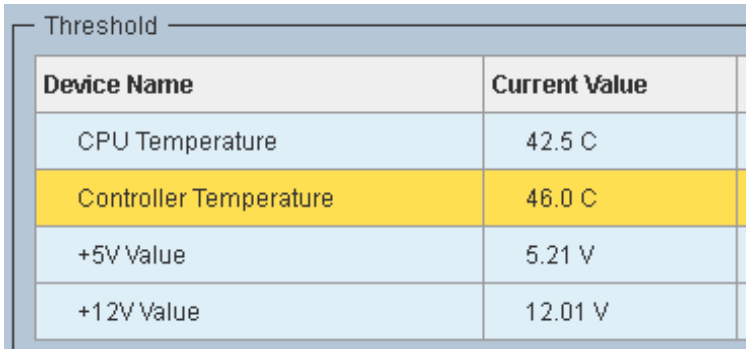
Go To	SANWatch Home > Device sidebar > Device List > device name > Tasks section
Steps	Click “Event Log” in the Tasks section. A list of events will appear. Click “Export”. The event log can be saved into a local file in text format.

4.4.4 Activating Triggers (Thresholds)

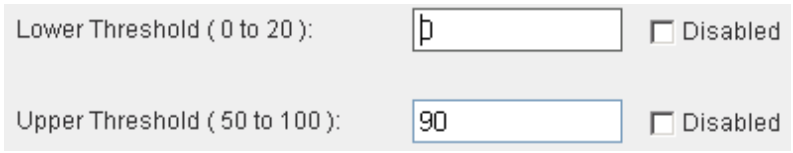
To receive event notifications (for when the system detects an abnormality, such as high temperatures or a power supply failure), ensure that the triggering function is enabled.

Go To	SANWatch Home > Device sidebar > Device List > device name > Tasks section
Steps	Click “System Settings” in the Tasks section. The System Settings screen will appear. Select the Trigger tab.

Configuring the Voltage/Temperature Threshold
Highlight an item in the list.

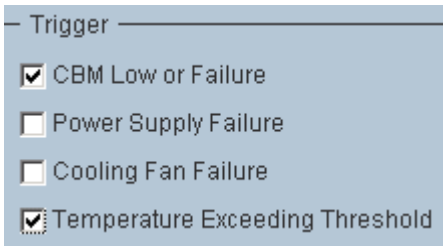


Click “Configure”. The configuration screen will appear. Enter a threshold value or click “Disable” to disable the threshold function (and notification).



Selecting Notification Triggers
Users can select which events will trigger a notification.

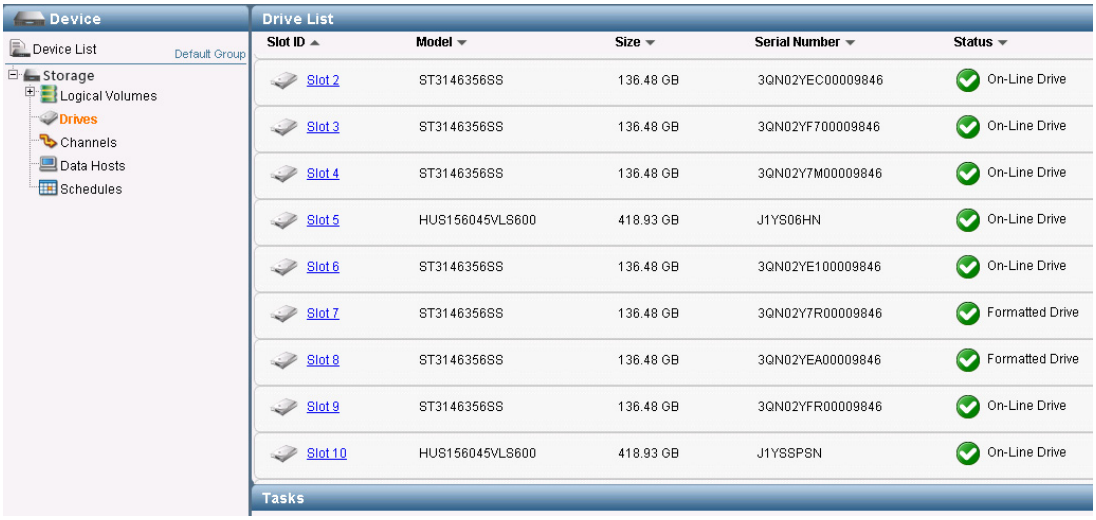
To receive notifications when the temperature reaches the pre-defined threshold, ensure that the Temperature Exceeding Threshold checkbox has been selected.



Chapter 5

Working with Drives

5.1 Introduction



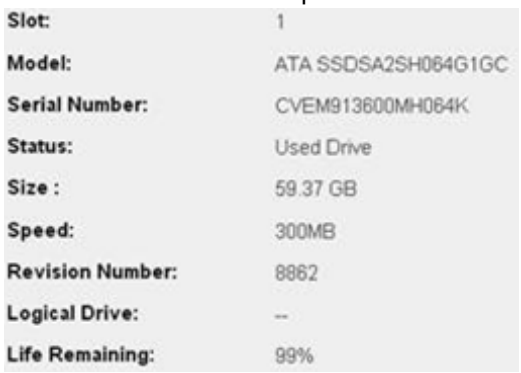
The Drives menu allows users to view the internal hard disk drive configurations (RAID subsystem or JBOD), monitor performance, identify drives with system errors (red system LED), clone (copy) drive contents, and delete internally reserved drive space to increase the storage capacity.

5.2 Viewing Drive Status

Viewing Drive Parameters

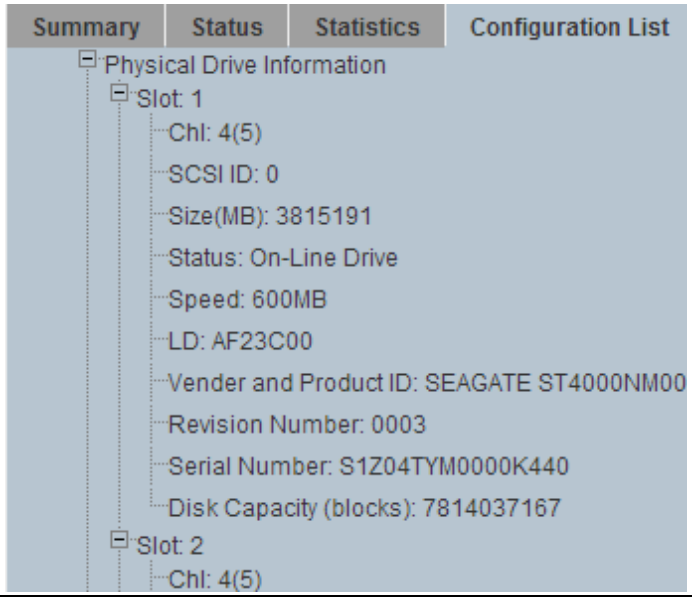
Go to SANWatch Home > Device sidebar > Device List > device name > Drives
The list of installed hard drives will appear.

Click the link to view the parameters of the hard drive.



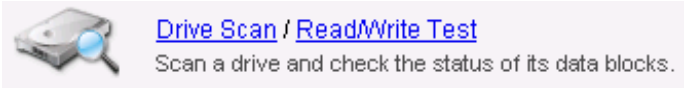
The “Life Remaining” parameter is only available for SSDs.

Click “Refresh” to update the parameters to the latest status.

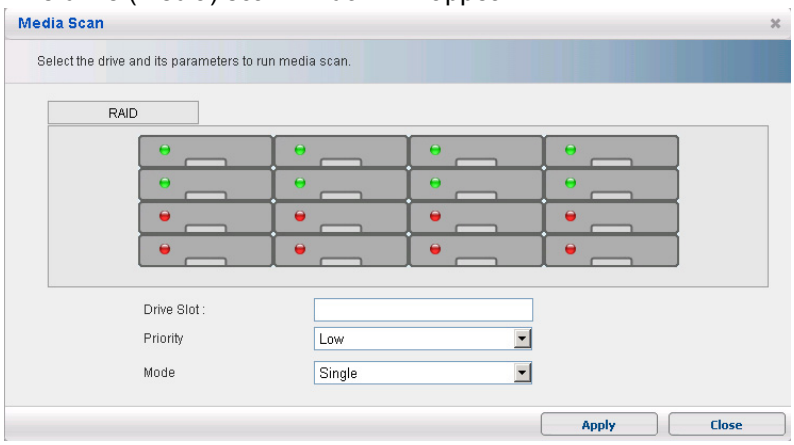
Viewing System Hardware Parameters (including drive parameters)	Go to SANWatch Home > Device sidebar > Device List > device name > Tasks section Click the System Information link in the Tasks section.  Click the Configuration List tab. All system parameters will be listed. 

5.3 Scanning Drives

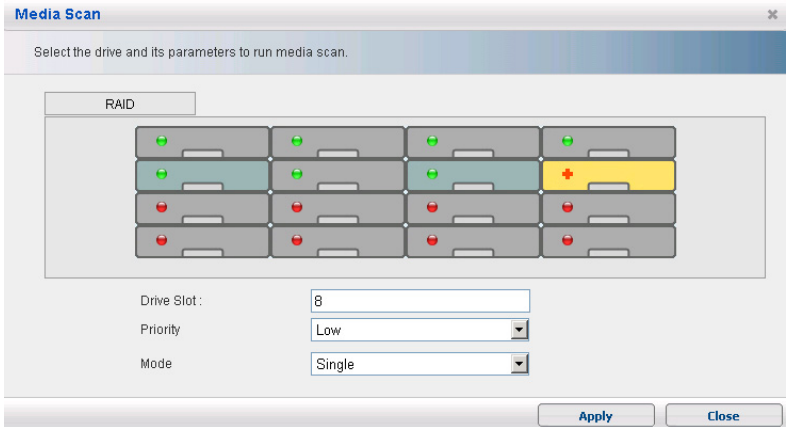
Only a disk enclosure spare drive or global spare drive can be scanned.

Go To	SANWatch Home > Device sidebar > Device List > device name > Drives > Tasks section
Scheduling Drive Scanning	Click “Drive Scan” in the Tasks section. 

The drive (media) scan window will appear.



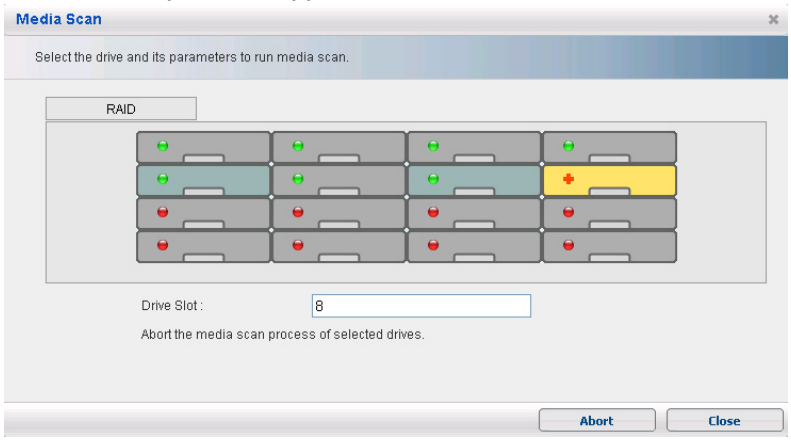
Select the drive to scan (Slot 8 in this case).



Select the priority and mode, and then click “Apply”.
The scan will start.

Aborting the Scan

To stop the scan from running, click the drive that is being scanned. The “Abort” option will appear, click this to terminate the scan.

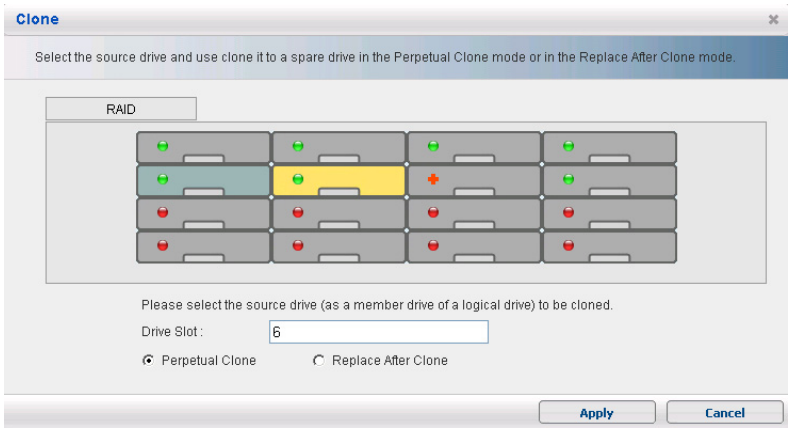


	Priority	Specifies the system resources allocated to scan operations. The higher the priority, the faster the scanning. However, system performance will be affected.
	Mode	Specifies whether scan operations are performed once (Execution Once) or continuously.

5.4 Cloning a Drive

Cloning refers to taking a backup copy of a drive at risk of failure in the near future. Users may receive notifications of events, such as bad sectors, that indicate drive failure. Should a drive fail, the clone drive automatically takes the place of the failed drive to prevent system downtime.

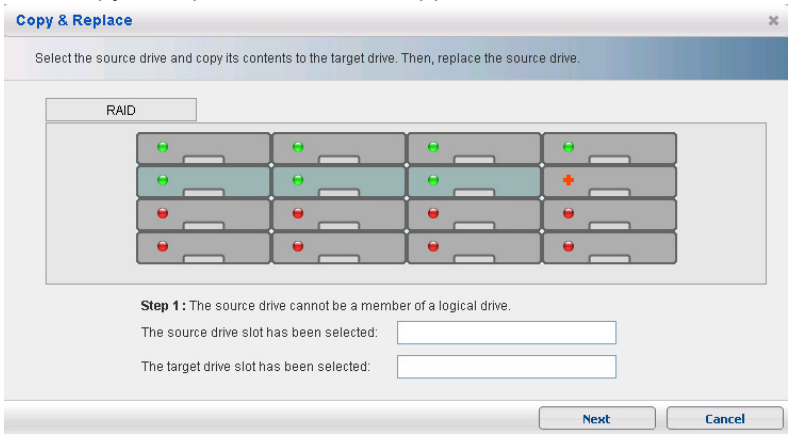
The source drive can be a member of a logical drive. The destination (target) drive must be a spare drive.

Go to	SANWatch Home > Device sidebar > Device List > device name > Drives > Tasks section
Steps	Click on the Clone menu in the Tasks section.  The front view of the drive slots will appear. Click to select the source drive. The source drive must be part of a logical drive.  Select clone type. ■ **Perpetual Clone:** The source drive continues operation after cloning. The target drive will be labeled as a “clone drive” and will not be used until the source drive fails. When the source drive actually fails, the target drive takes its place. ■ **Replace After Clone:** After cloning, the target drive takes the place of (replaces) the source drive. The source drive will not be used any more until replaced by a new drive. Click “Apply”. The target drive (a spare drive) will be chosen automatically and the source drive will be cloned.

5.5 Replacing a Drive

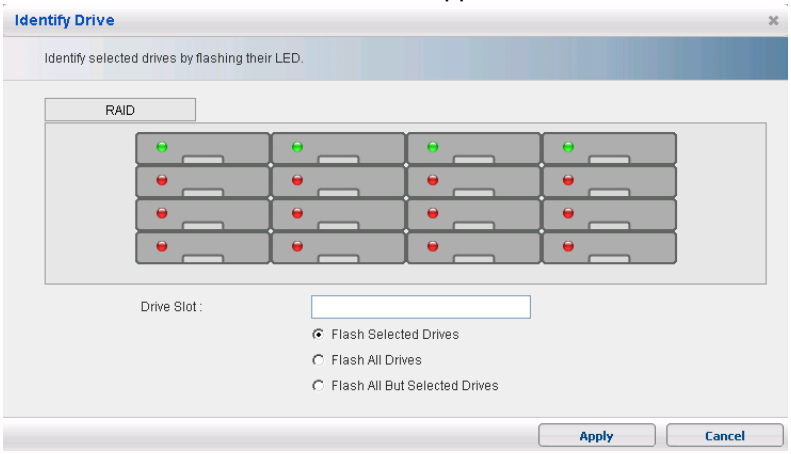
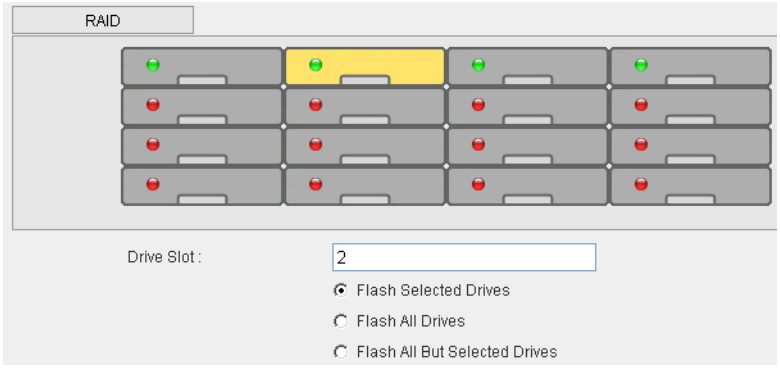
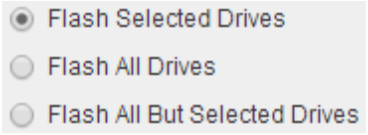
Instead of waiting for a drive to fail (and be automatically replaced), users can also manually replace a drive that is likely to fail in the near future.

The source drive must be a member of a logical drive. The destination (target) drive must not be a member of a logical drive nor a spare drive.

Go To	SANWatch Home > Device sidebar > Device List > device name > Drives > Tasks section
Steps	Click on “Copy & Replace” in the Tasks section. The Copy & Replace window will appear.  Select the source drive, and click “Next”. The source drive must be part of a logical drive. Select the target drive, and click “Apply”. The target drive cannot be a member of a logical drive. The content of the source drive will be copied to the target drive. Then the target drive will take the place of the source drive.

5.6 Identifying a Drive

Users can flash the drive tray LEDs to identify the drive hardware of a storage subsystem enclosure.

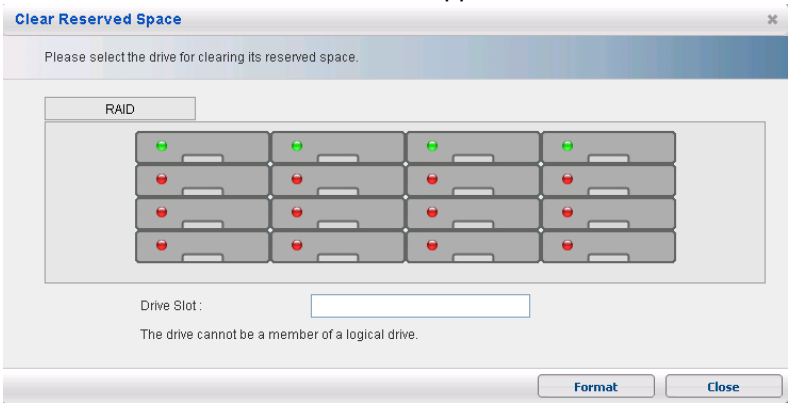
Go To	SANWatch Home > Device sidebar > Device List > device name > Drives > Tasks section	
Steps	Click “Drive Identification”. The front view of the drive slots will appear.  Select the drive for identification. The drive will be highlighted and its ID number will appear in the Drive Slot field.  Select how the hard drive LED(s) will be flashed and click “Apply”.  The LED of the selected (or unselected) drives will turn blue for 5 to 10 seconds.	
Parameters	**Flash Selected Drive**	Flashes only the LED of the selected drive.
	Flash All Drives	Flashes the LED of all drives in the subsystem enclosure.
	Flash All but Selected Drives	Flashes the LED of all drives in the storage subsystem enclosure but the selected drive.

5.7 Configuring Reserved Drive Space

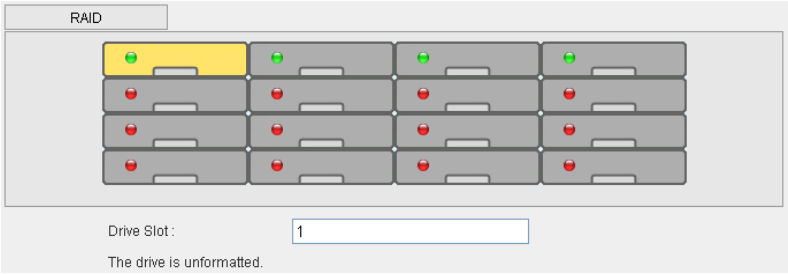
A formatted drive includes a reserved section for event logs and storage virtualization to ensure these contents are not erased upon system reset. Users can remove the reserved section (unformatting a drive) to change the drive status to “new.” This is necessary for debugging purposes, especially before conducting a read/write test on a drive. Otherwise, removing the reserved section is not recommended.

Go To	SANWatch Home > Device sidebar > Device List > device name > Drives > Tasks section
Steps	Click on the Reserved Space link in the Tasks section.

The front view of the drive slots will appear.



Click the drive to format or reformat. The selected drive will be highlighted and its ID number will appear in the Drive Slot field.



The system determines if the drive has been formatted or not.

- If the drive has been formatted, click the Reformat button at the bottom to proceed.
- If the drive has been unformatted, click the Format button at the bottom to proceed

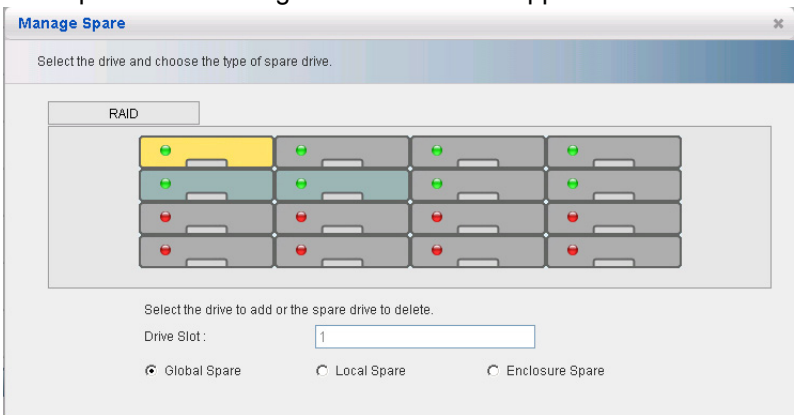
5.8 Assigning Spare Drives

Only a hard drive that is not yet part of a logical drive can be assigned as a spare drive.

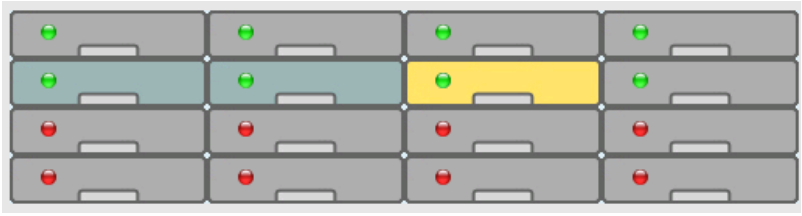
Warning! *We strongly recommend assigning a spare drive. The risk of data loss is increased without a spare drive!*

Go To	SANWatch Home > Device sidebar > Device List > device name > Drives > Tasks section
Steps	Click on the Spare Drive Maintenance link in the Tasks section.

The Spare Drive Management window will appear.



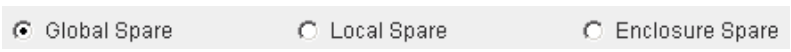
Highlight an available drive.



The drive slot number will also appear.

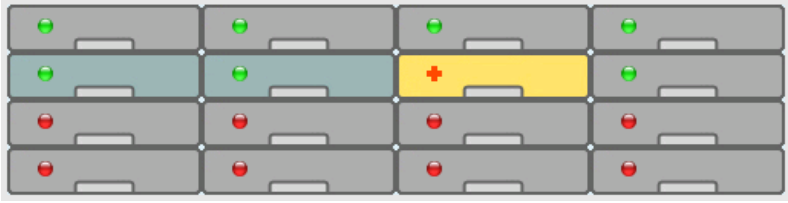
The drive must not be a part of an existing logical drive.

Select the type of the spare drive.



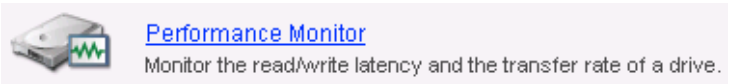
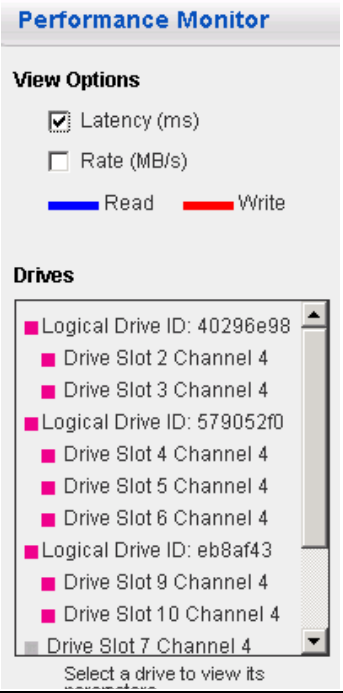
- Global spare: Spare drive for logical volumes
- Local spare: Spare drive for logical drives
- Enclosure spare: Spare drive for that particular subsystem enclosure

Click “Add”. The drive will be set as a spare drive.

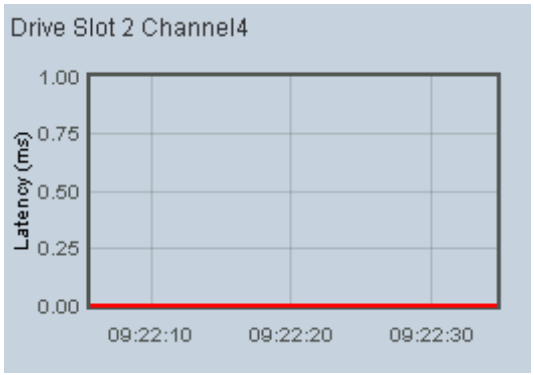
Deleting Spare Drives	This option is available when one or more spare drives exist. Click on Spare Drive Maintenance in the Tasks section. The Spare Drive Management window will appear. Highlight an existing spare drive (marked by the plus sign to the left).  The drive slot ID will also appear.  Click “Delete” to delete the spare drive. The drive will revert back to being a standard (unused) drive.

5.9 Monitoring Disk Drive Usage (Performance Monitor)

The Performance Monitor allows real-time monitoring of disk drive performance and usage to enable the identification of performance bottlenecks.

Go To	SANWatch Home > Device sidebar > Device List > device name > Drives > Tasks section
Opening the Performance Monitor	Click the Performance Monitor link in the Tasks section.  The Disk Performance Monitor will open and update the disk drive usage in real time. 

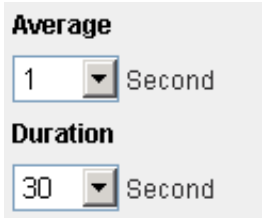
Monitor Graph



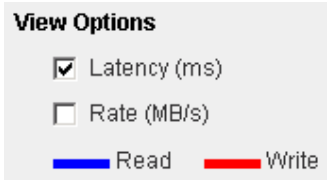
- Title: Specifies the slot location and host channel ID of every drive.
- Vertical axis: Shows the latency. 1.00 millisecond = 100%.
- Horizontal axis: Shows the current time

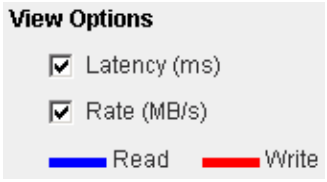
Configuring the Axis

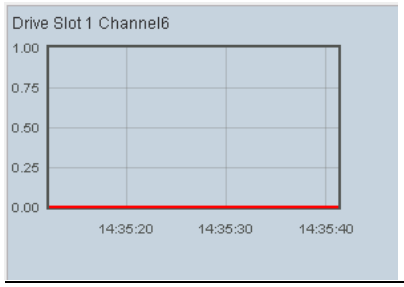
To set the average time and duration (x-axis), use the drop-down menu in the sidebar.

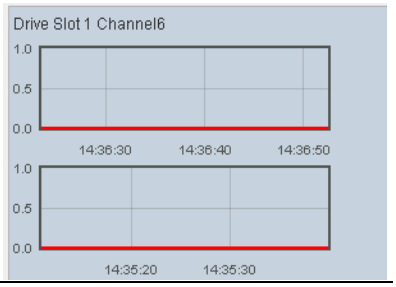


The y-axis item can be selected from the sidebar. By default, the y-axis is set to show both latency and data rate. This can be set to show just data rate or latency.





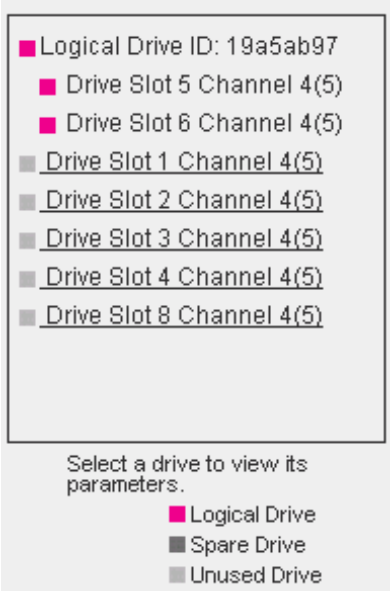




Average	Specifies the data averaging period: 1, 2, 4, and 8 seconds.
Duration	Specifies the time range of the monitor screen: 30, 60, 90, 120, and 160 seconds.

Drive Categories and List

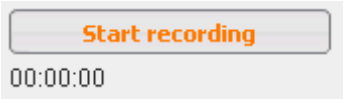
All physical and logical drives are categorized and listed in the sidebar.



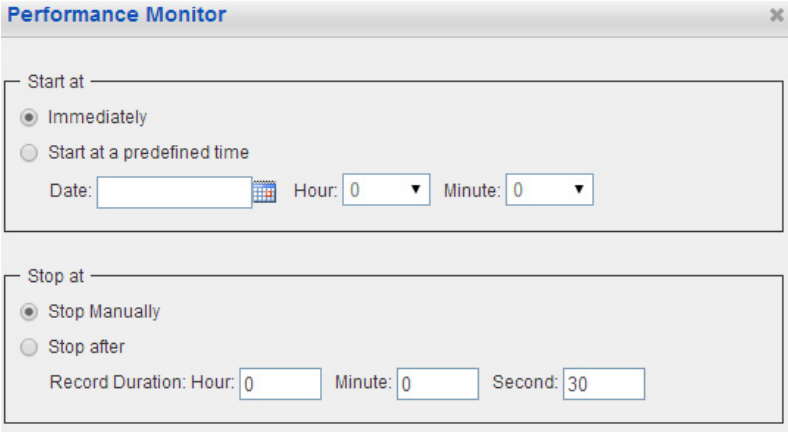
Logical Drive	The hard disk is part of a logical drive.
Spare Drive	The hard disk is part of a local or global spare drive.
Unused Drive	The hard disk does not exist, or is not part of a logical drive.

Recording the Status

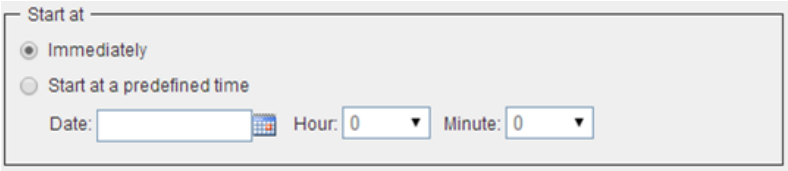
Disk performance data can be recorded into a log file. Simply click the Start Recording button.



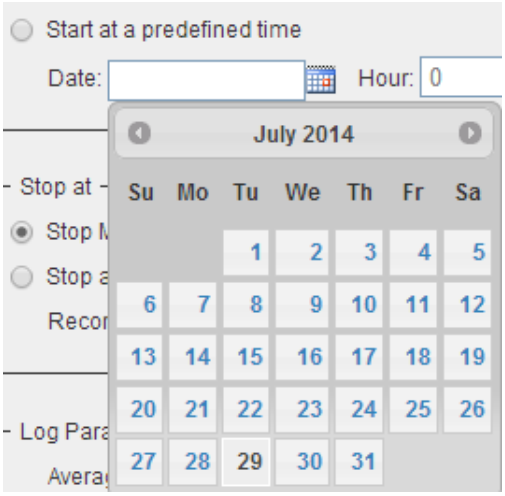
The recording window will appear.



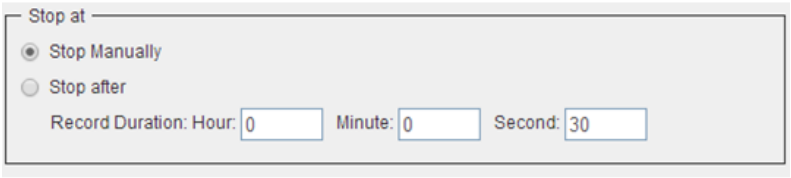
Select the starting time: right now or later.



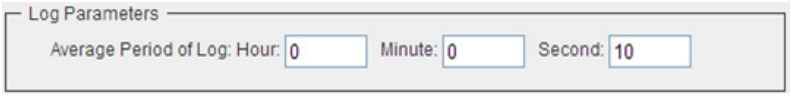
To select the start date, click on the calendar icon.



Set the end time either manually or after a fixed period.



Select how frequently the data will be sampled.

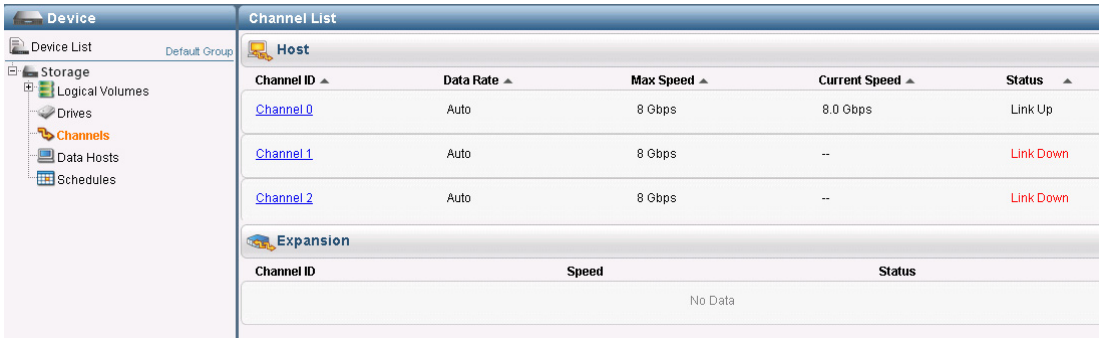


Click “OK”. Once recording, the button will show “Stop Recording and Download Log”. Click this button to manually stop the recording and/or download the result to a local file.

Chapter 6

Working with Channels

6.1 Introduction

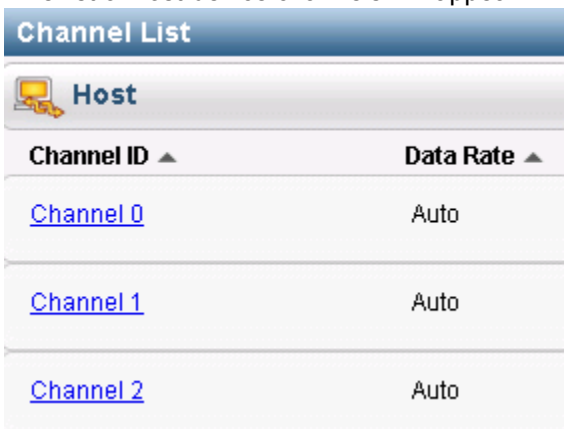


This chapter describes how to view and adjust the host channel configurations, assign an alias to a channel, group channels, and check whether channels are fully connected.

6.2 Viewing Channel Configurations

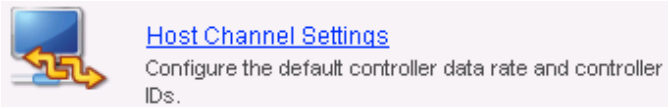
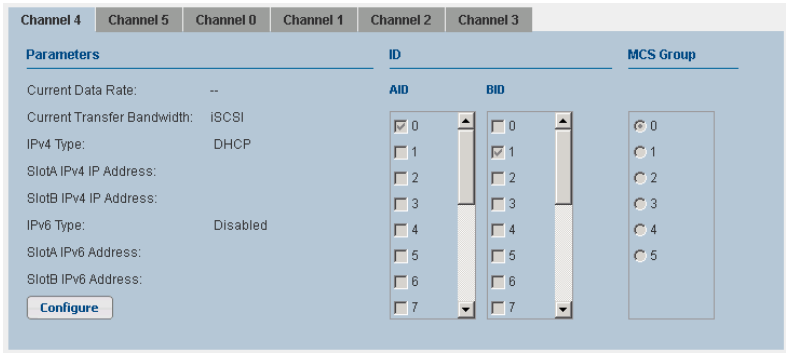
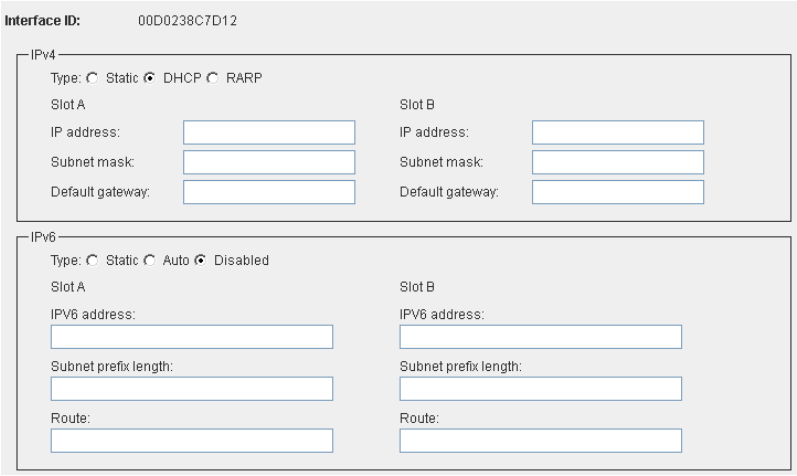
Viewing Channel Parameters

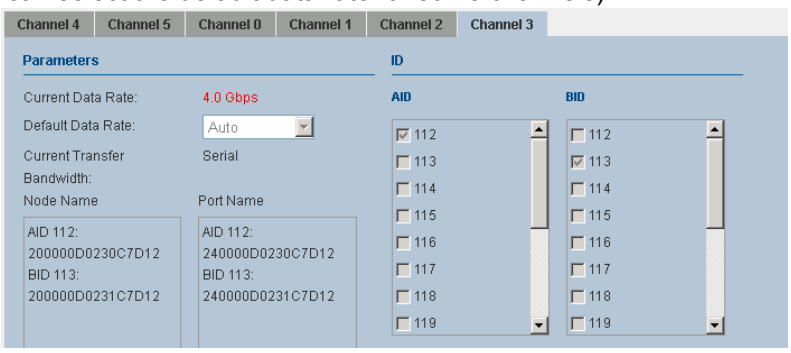
Go to SANWatch Home > Device sidebar > Device List > device name > Channels
The list of host-device channels will appear.



Click on the link to see the parameters of each channel.
Click “Refresh” to update the parameters to the latest status.

6.3 Configuring the Host Channel Settings

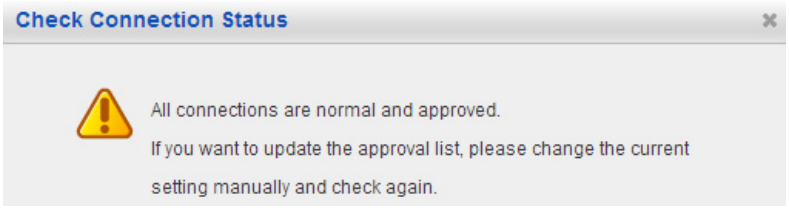
Go To	SANWatch Home > Device sidebar > Device List > device name > Channels > Tasks section
Steps	Click on the Host Channel Settings link in the Tasks section.  The list of channels and their configurations will appear.
iSCSI Channel Configurations	 Click “Configure” to modify the IP address, subnet, and gateway (route). Note that each slot has a unique IP configuration. 

iSCSI Parameters	**Channel ID**	Specifies the LUN mapping ID number.
	MCS Group	MC/S (Multiple Connections Per Session) protocol allows combining several channels to improve performance and failover rates.
	Type	(Configurable) ■ Static: Specifies a fixed IP address. ■ DHCP (Auto): Allows the router/switch to pick an available IP address for the subsystem. ■ RARP: The Reverse Address Resolution Protocol (RARP) requests the IP (IPv4) address from an administrative host. ■ Disable: Disables the IPV6 address protocol (used when IPV4 is used instead of IPV6).
	IP Address	(Configurable) Specifies the IP address in IPV4 or IPV6 format.
	Subnet Mask, Default Gateway, or Route	(Configurable) Allows users to specify the surrounding subnet and gateway, enabling the subsystem to specify the network subdivision.
Fibre Channel Configurations	Fibre Channel ports have a few configurable parameters (users can select the default data rate for some channels). 	
Fibre Channel Parameters	**Channel ID**	Specifies the LUN mapping ID number.
	Data Rate	Specifies the data rate of the Fibre Channel.

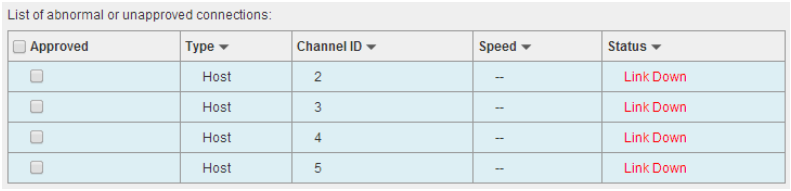
6.4 Checking System Health

Go To	SANWatch Home > Device sidebar > Device List > device name > Channels > Tasks section
Steps	Click the System Health Status Settings link in the Tasks section.

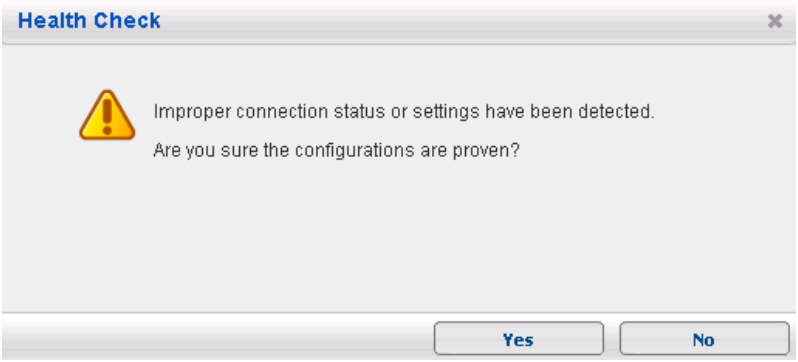
The system will check all channel connections, and display the following message if all connections are standard and approved.



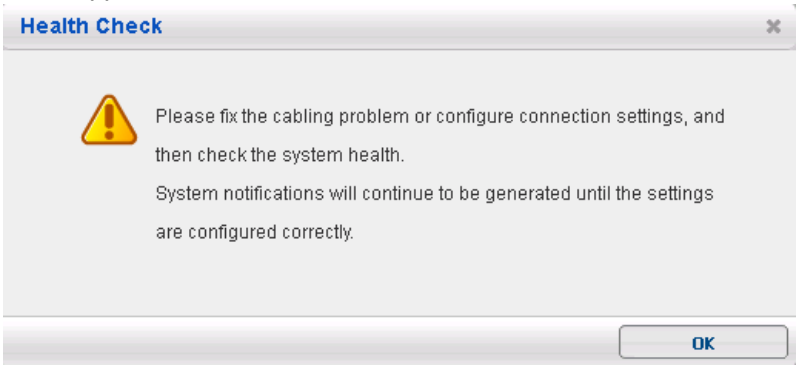
If any abnormal or unapproved connections are found, the system will display the status of these connections in a list.



Select the connection(s) to approve. If the connection is found to be unhealthy (i.e., contains network irregularities), the following warning message will appear.



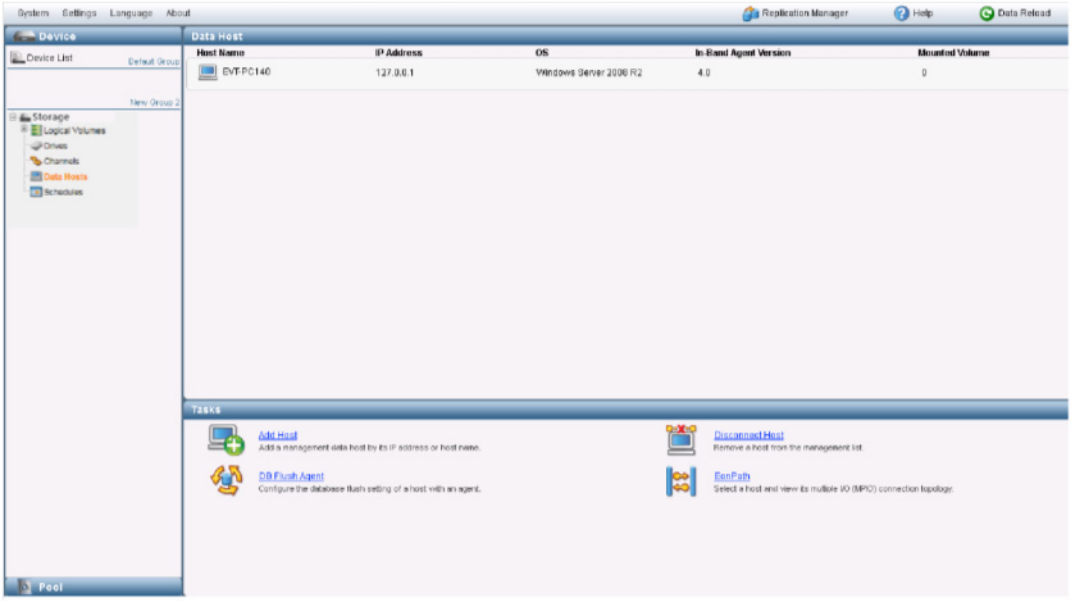
- If users click “Yes”, the Health Check link will be disabled and the connection marked normal.
- If users click “No”, suggestions for improving connectivity will appear.



Chapter 7

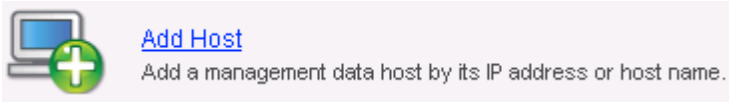
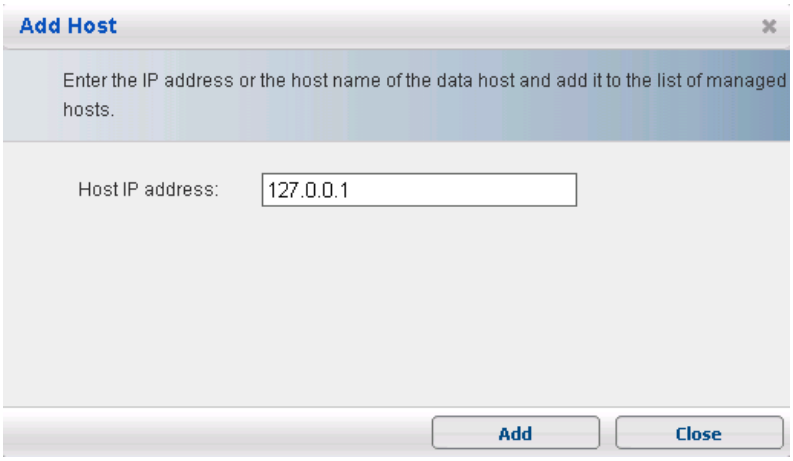
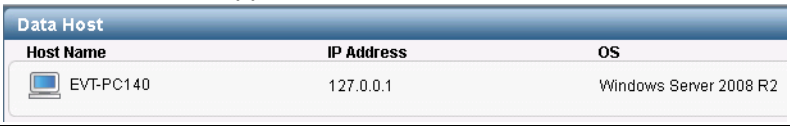
Working with Hosts

7.1 Introduction

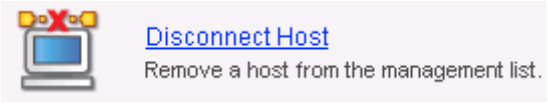
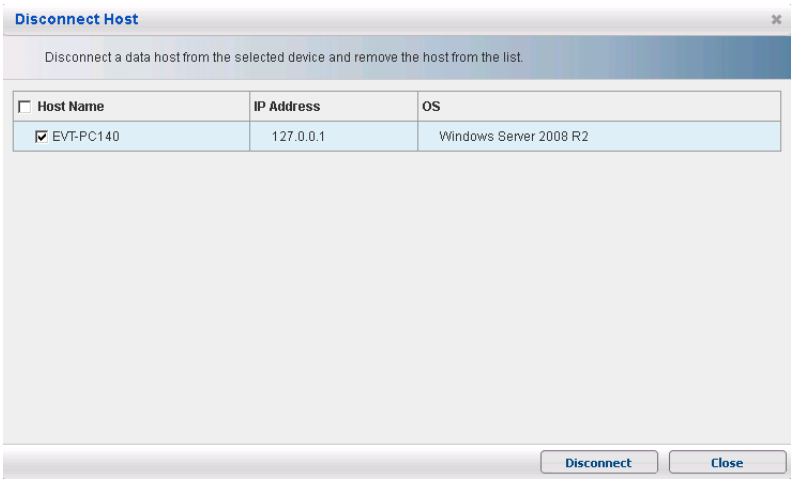


This chapter describes how to add or disconnect a host computer to/from the current system, configure database flush settings, and configure an MPIO system topology.

7.2 Adding a Host

Go to	SANWatch Home > Device sidebar > Device List > device name > Data Hosts > Tasks section
Steps	Click on the Add Host link.  Add Host Add a management data host by its IP address or host name. Enter the IP address of the new host, then click “Add”.  Add Host Enter the IP address or the host name of the data host and add it to the list of managed hosts. Host IP address: 127.0.0.1 Add Close The new host will appear in the Data Host section.  Data Host Host Name / IP Address / OS EVT-PC140 / 127.0.0.1 / Windows Server 2008 R2

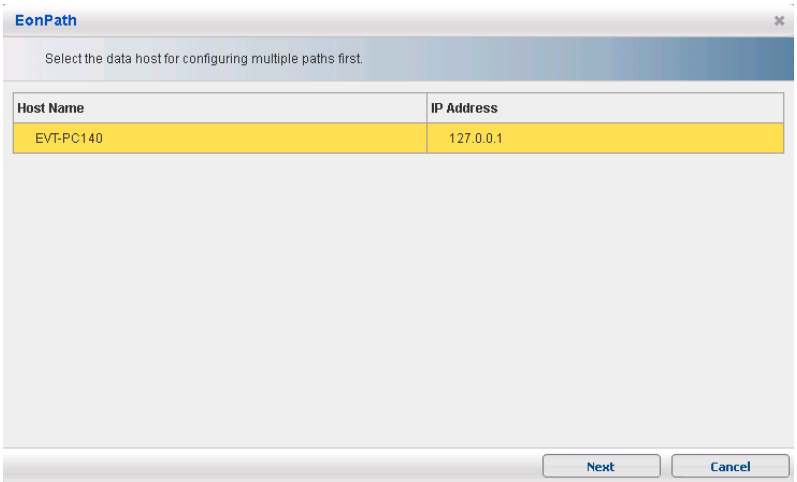
7.3 Removing (Disconnecting) a Host

Go to	SANWatch Home > Device sidebar > Device List > device name > Data Hosts > Tasks section
Steps	Click on the Disconnect Host link.  Select the host to be disconnected and click “Disconnect”.  The host will be removed from the list.  Disconnecting the host will not affect its configurations. When the host is reconnected to the device, its prior configurations will be reestablished.

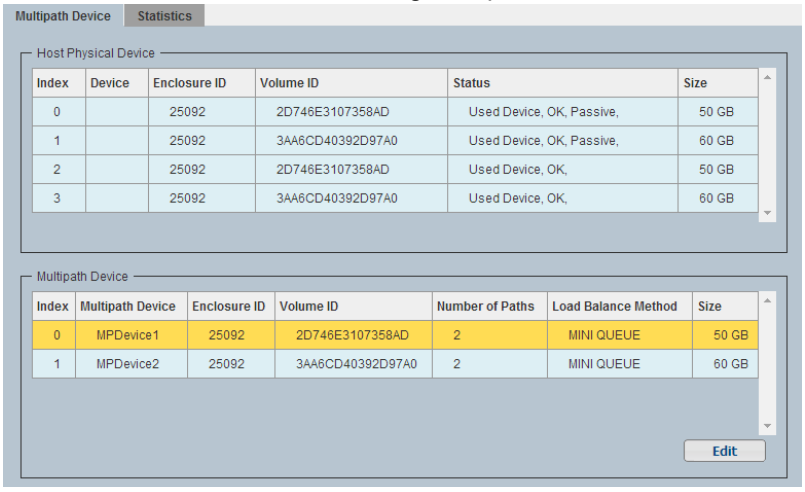
7.4 Editing Multipath Devices through EonPath

Go To	SANWatch Home > Device sidebar > Device List > device name > Data Hosts > Tasks section
Steps	Click on the EonPath link in the Tasks section.

The list of current hosts will appear. Highlight the host to configure and click “Next”.



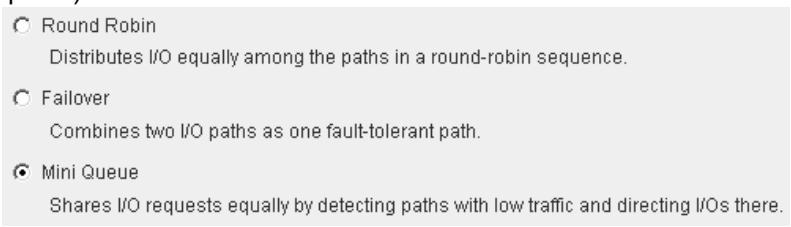
Users can view a list of the existing multipath devices.



Users can edit the list of existing multipath devices.

Select the load balancing policy.

Load balancing is only applicable to active paths (not passive paths).



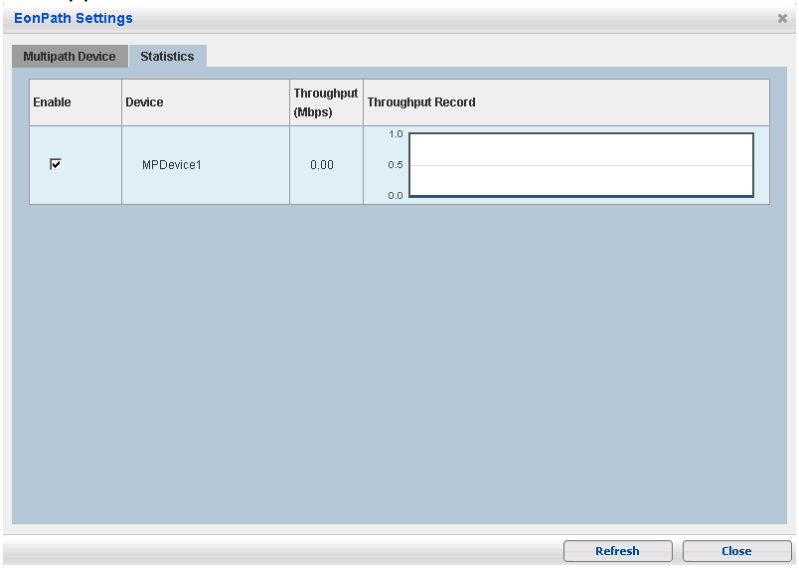
Click “OK” to finish editing the multipath pair, and click “Close” to close the Information window.

Click “Refresh” at the bottom to update the status if the device does not appear.

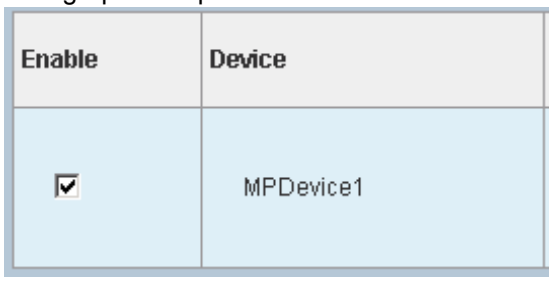
Parameters	**Failover**	Loads cannot be balanced between multiple paths. One dedicated path will be used for all data transactions. If the main path fails, the remaining path will assume the role of main path.
	Mini Queue	Data transactions are shared with all paths. The data load will be dynamically distributed according to the length of the job queue.
	Round Robin	Data transactions are shared with all paths. The data load will be equally distributed in a round-robin fashion.

7.5 Monitoring Multipath Devices in EonPath

Go To	SANWatch Home > Device sidebar > Device List > device name > Data Hosts > Tasks section
Steps	Click on the EonPath menu in the Tasks section. The list of current hosts will appear. Highlight the host to configure and click “Next”. Select the Statistics tab. The list of multipath device statistics chart will appear.



Select the checkbox next to the multipath device to be monitored. The graph will update the I/O statistics in real time.



To refresh the plot, click “Refresh”.

7.6 Flushing the Database Host Cache

When database applications (SQL, Oracle, etc.) are running on the host computer, user data is temporarily stored on the host computer’s memory (cache memory) before being transferred to the RAID subsystem. When conducting a replication operation (such as a snapshot or volume mirror), ensure the cache memory content is transferred to the RAID subsystem before initiating a data backup. Otherwise, data inconsistencies between the RAID subsystem and host computer may occur.

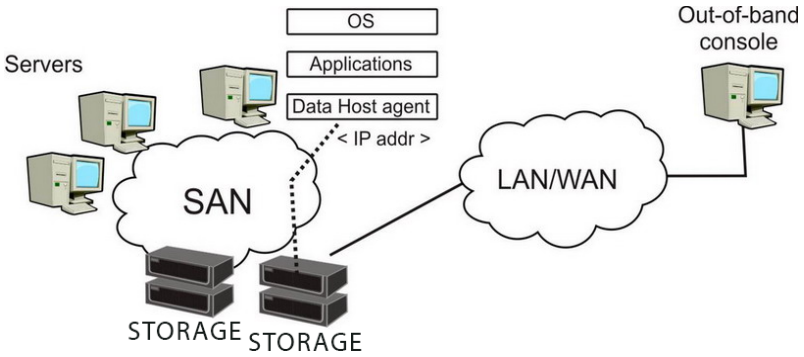
The database flush mechanism ensures that all cache data on the host computer is flushed (transferred) to the RAID system before a replication job is initiated.

In-Band Versus Out-of-Band

There are two methods used to flush cache memory depending on the connection between the host computer and the subsystem.

In-Band Flushing

For this method, flushing of the cache memory is triggered by the host computer, which is connected to the subsystem via an in-band connection. This is the standard flush method when only one data host computer exists or is not installed with Windows Virtual Machine (VM).



Out-of-Band Flushing

For this method, flushing of the cache memory is triggered by an out-of-band host computer. This method is required in the following cases:

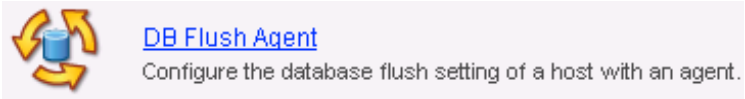
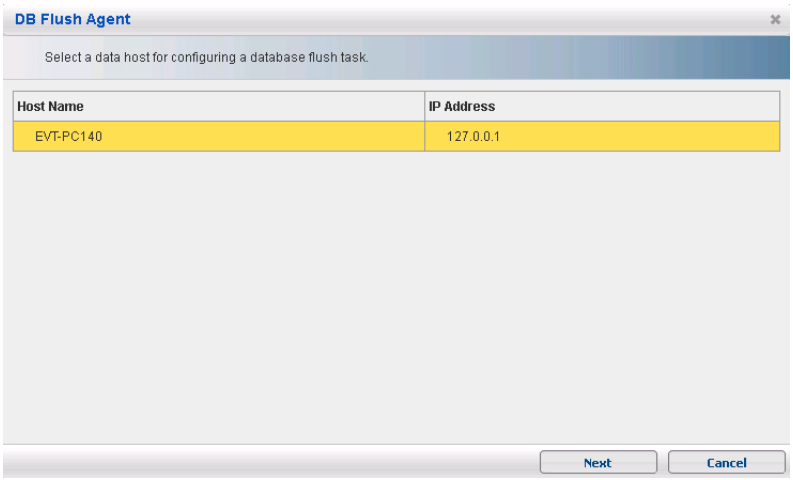
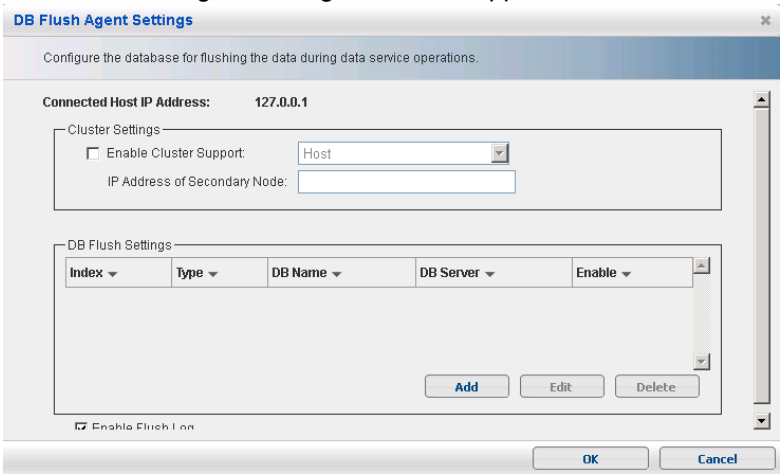
- Multiple host computers with database applications are connected to the subsystem. In-band flushing may cause conflict if more than one host computer simultaneously attempts to backup user data. In such cases, out-of-band flushing allows multiple servers to perform data flushing sequentially without conflict.
- Windows Virtual Machine (VM), installed on an ESX server, is in operation on the host computer. Because a VM cannot initiate cache flush commands, the host computer must use an out-of-band connection to trigger flushing.

7.7 Configuring In-Band Flushing Using a DB Flush Agent

For data held in database forms, all data must be flushed into the storage subsystem before conducting data backups. The DB Flush module in SANWatch enables users to automate this process.

DB Flush is compatible for the following databases:

- SQL
- Microsoft Exchange
- Oracle

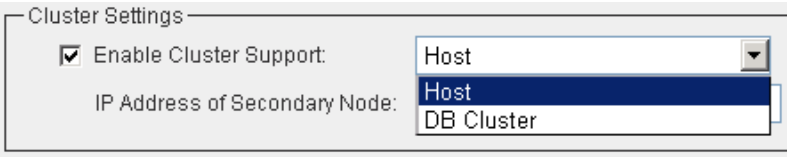
Go To	SANWatch Home > Device sidebar > Device List > device name > Data Hosts > Tasks section
Step 1: Activating DB Flush Agent	Click on the DB Flush Agent link in the Tasks section.  The list of current hosts will appear. Highlight the host to configure and click “Next”.  The DB Flush Agent setting screen will appear. 

Step 2: Enabling Database Clustering

Changing the database clustering settings resets all DB Flush Agent settings.

Database clustering refers to storing sequential rows of a database table on a disk. For server-centric database systems, this boosts database performance because the server can directly access the disk during database operations.

To enable database clustering, check the Enable Cluster Support checkbox and select “DB Cluster”. To add an additional node, select “Host” and enter the IP address.



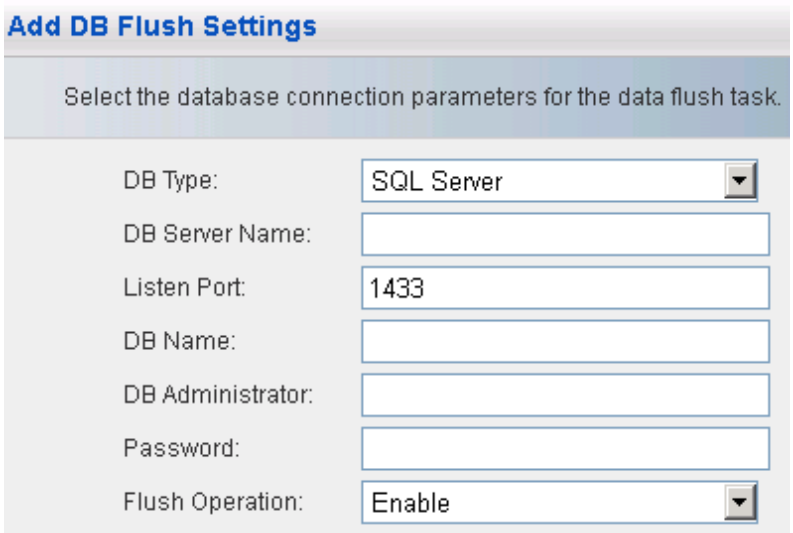
Step 3: Enabling Flush Logs

Flush logs can be enabled to achieve the following:

- Event logs for clustered nodes stored directly on the machine.
- Events reported in the following locations:
  Windows: Event Viewer
  Linux: /var/log/messages
  Solaris: /var/adm/messages

Step 4: Configuring Database Flush Settings

Click “Add”. The DB Flush setting window will appear.



Enter the parameters and click “OK”.

The new database flush setting will appear in the DB Flush Agent screen.

Click “OK” and close DB Flush Agent.

Parameters	**DB Type**	Specifies the database type, such as Oracle, SQL Server, and MS Exchange.
	DB Server Name	Specifies the user-defined name of the database server.
	DB Listen Port	Specifies the network port (default 1433) from which the database listener (software that manages network traffic between the database and client) monitors.
	DB Name	Specifies the user-defined name of the database.
	DB Administrator	Specifies the database administrator user name. Enter a “SA” (system administrator) login name. The “SA” name can be disabled when setting the database security level. If “SA” access is disabled, the only way to access a database system is by logging in as the Windows Administrator. For further details, refer to the section on how to enable an “SA” login.
	DB Password	Specifies the database password.
	Enable DB Flush	Allows database cache memory to be flushed to a local file before snapshot images are taken.

7.8 Viewing DB Flush Events (Windows)

The default path to view system events can be found in C:\app\Administrator\product\11.1.0\db_1

From there, users can also check related events. To examine event messages, go to *Windows Computer Management -> System Tools -> Event Viewer -> Application*

Event messages generated by the DB Flush agent are listed below.

List of Events	Message	Description
	`unsupported platform`	The OS platform is not supported
	`config file not exist or damaged`	No associated DBFlush configuration file exists or the file is missing.
	`config file io error`	Could not access the DBFlush configuration file.
	`dbflush no config, do nothing`	No valid DBflush configuration.
	`begin suspend database diskno=xx`	Starts DBFlush operation on partition or virtual volume index #.
	`dbflush x: is disabled, do nothing`	DBFlush configuration profile index X is manually disabled.
	`server x suspend fail`	DBFlush on server X operation failed.
	`suspend database fail`	DBFlush operation failed.

`end suspend database`	DBFlush operation completed.
`enter resume database`	DBFlush operation ended, resuming normal database operation
`server x: resume database fail`	DBFlush operation ended, failed to resume normal database operation.
`end resume database`	DBFlush operation ended, resumed normal database operation.

7.9 Using DB Flush Agent in Oracle 10g

To protect the integrity of snapshot copies, before taking a database snapshot, users should ensure that all data in cache memory is flushed to the storage system. For databases, a dedicated DB Flush Agent can perform flushing automatically. However, for other databases, flushing must be conducted manually.

Note	In the configuration example provided below, the Oracle database, including its data, log, and control files, are assumed to be stored in partitions on the storage system. SQL*PLUS is an Oracle command-line utility program.

Step 1: Suspend or Shutdown the Database	The database can be suspended or shutdown depending on whether snapshot protection is to be performed online or offline.
	
	To perform snapshot operations online, the database should be suspended using the following SQL*PLUS2 commands:
	`c:\sqlplus /nolog`
	`SQL>conn / as sysdba`
	`SQL>alter system suspend;`
	To perform snapshot operations offline, the database should be shutdown using the following SQL*PLUS commands:
	`c:\sqlplus /nolog`
	`SQL>conn / as sysdba`
	`SQL>shutdown immediate;`
	`SQL>startup mount`
	`SQL>exit`

Step 2: Take Snapshots	In SANWatch GUI, take snapshots of the partitions storing the database. If Oracle database files are stored in multiple partitions, to ensure data consistency, use the Group Snapshot feature to take simultaneous snapshots.

Step 3: Resume or Restart Database Service

To resume the service of a suspended database, input the following SQL*PLUS commands:

```
c:\sqlplus /nolog
SQL>conn / as sysdba
SQL>alter system resume;
```

To restart the service of a shutdown database, input the following SQL*PLUS commands:

```
c:\sqlplus /nolog
SQL>conn / as sysdba
SQL>shutdown immediate;
SQL>startup;
SQL>exit
```

Then restart the service on the host server.
When necessary, use the database snapshots to rollback data or restore files.

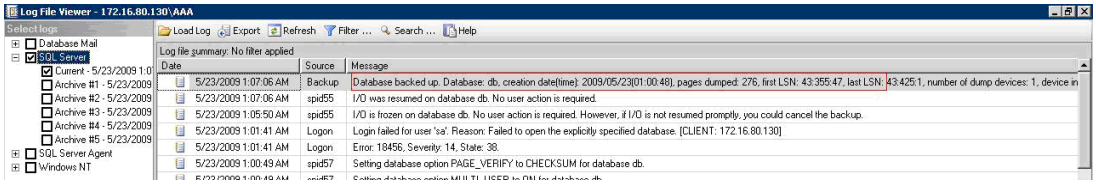
Test Script

Below is a sample script that tests growing databases in Oracle.

```
create table student
(id int,
name varchar(10),
english int,
math int,
chinese int
)
tablespace users;

create or replace procedure loopinsert as
i int:=1;
begin

for i in 1..500000 loop
INSERT INTO student
      (id, name, english, math, chinese)
SELECT max(id)+1,
   'sk', max(english) + 1,
   max(math) + 1, max(chinese) + 1
from student;
commit;
end loop;

end;
/

exec loopinsert;
commit;
```

Examining the Backup Process

Users can schedule snapshot backups that verify database accuracy by performing a rollback of an active database.
The backup process can be examined via Oracle Log File Viewer.



7.10 Using DB Flush Agent in MS SQL

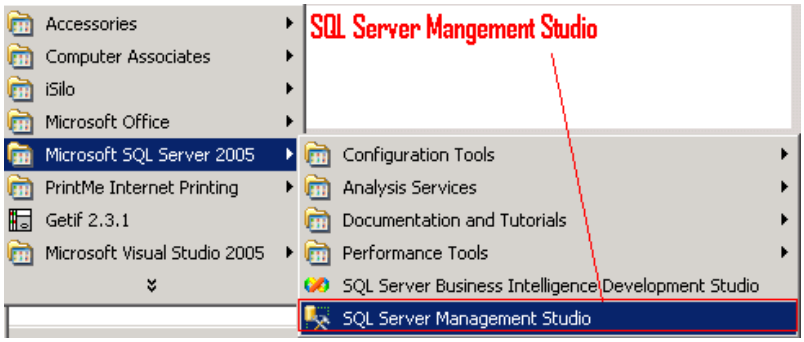
To protect the integrity of snapshot copies, before taking a database snapshot, users should ensure that all data in cache memory is flushed to the storage system.

Sample Database Configuration Using SQL Server 2005

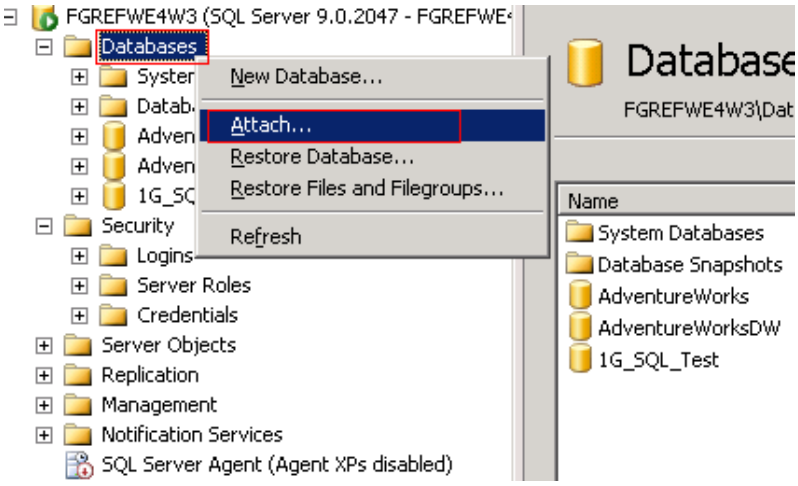
Create volumes. Reserve sufficient unallocated storage space in volumes for performing snapshot backups. Depending on the amount and frequency of data changes, a partition capacity of 2 to 3 times the snapshot is typically required for snapshot backups.

When taking snapshots for database applications, such as Oracle, use “Group Snapshot” in the scheduler. The Group Snapshots function ensures consistency between database volumes and logs. For group snapshots, users must select multiple source volumes.

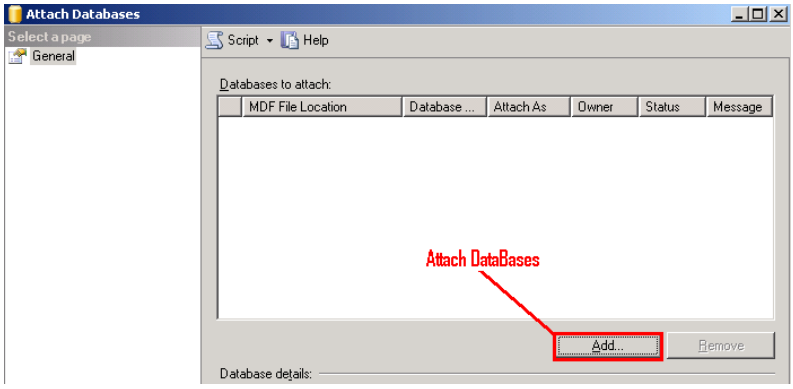
1. Map virtual volumes to hosts.
2. To test backups, copy data files to a virtual volume.
3. Start Microsoft SQL Server 2005.



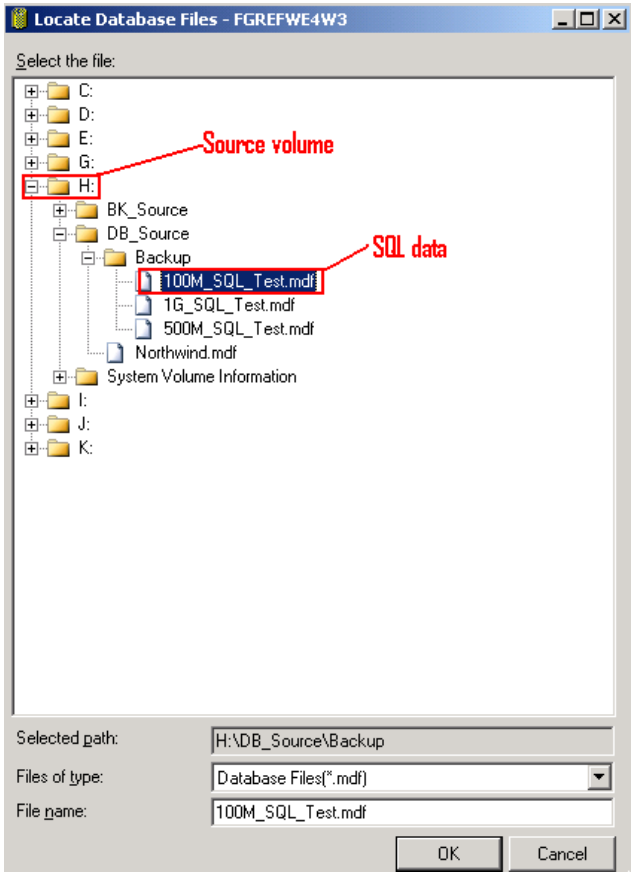
4. Use the Attach function to assign a virtual volume as the database location.



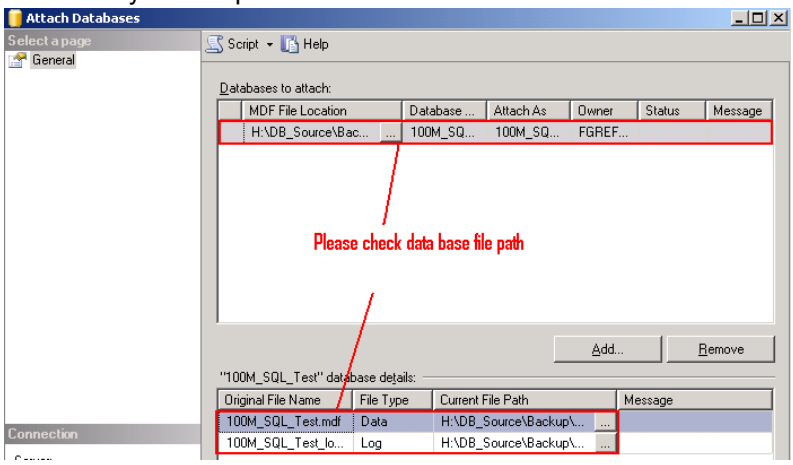
5. On the next screen, click “Add” to attach databases.



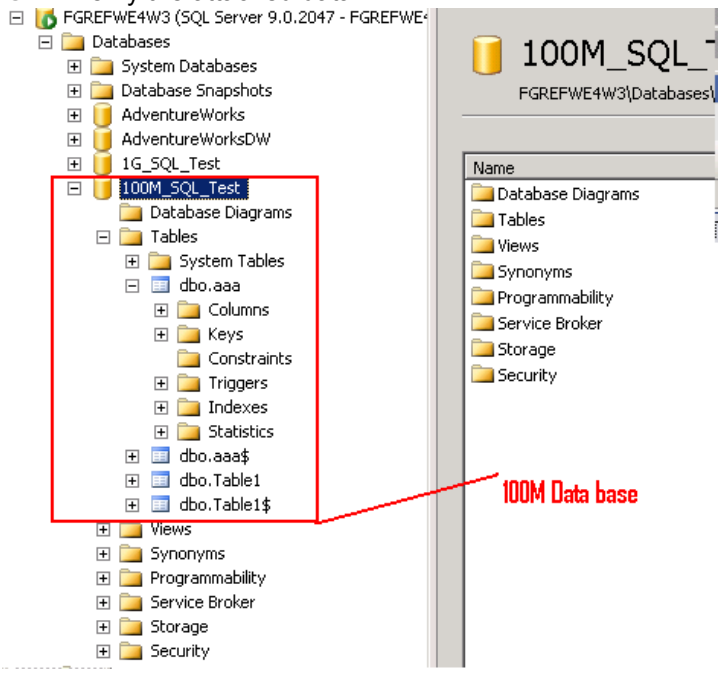
6. Select the previously copied database files.



7. Verify the file paths are correct.



8. Verify the attached data.

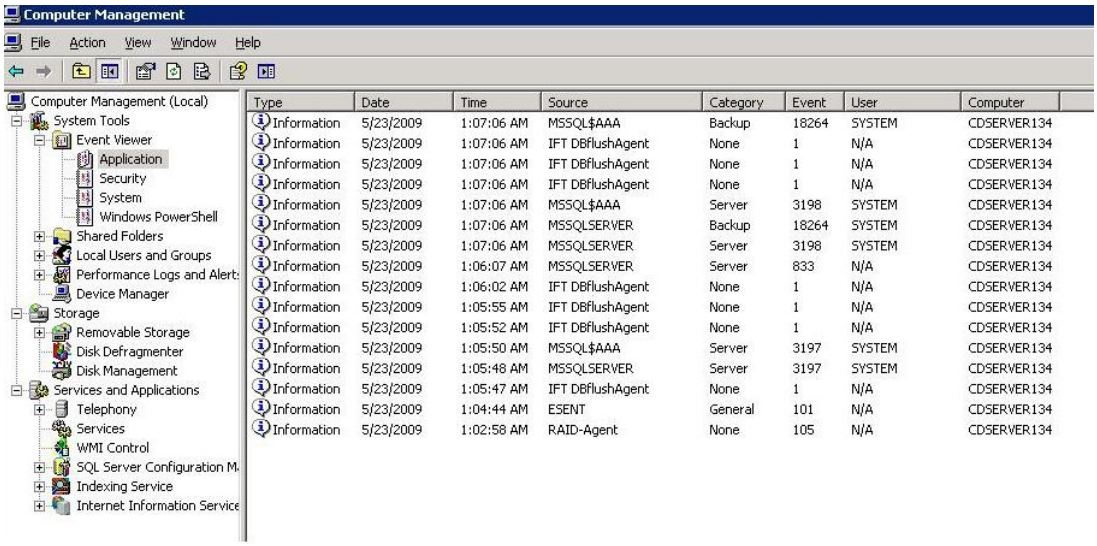


Test Script

Below is a sample script that tests growing databases in SQL.

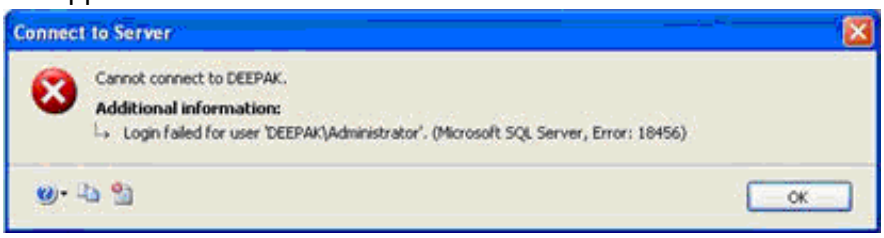
```
create table DBFlush.dbo.DBtest
(ID bigint,
 Rrd_Name char(20),
 Math float,
 English float,
 Chinese float,
 physical float
);

use DBflush
GO
declare @a int,@Temp_Name varchar(10),@c int ,@d
int,@e int, @f int, @Out_String varchar(30)
set @a=1
set @Temp_Name='sk'
set @c=99
set @d=99
set @e=99
set @f=99
while @a<=1000000
begin
             insert    into    DBflush.dbo.DBtest
(ID,Rrd_Name,Math,English,Chinease,physical) val-
ues
   (@a,@Temp_Name,@c,@d,@e,@f)
   set @a=@a+1
     set  @Out_String  =  'This  Record  NO  is:'  +
Str(@a)
   PRINT @Out_String;
end
```

Examining the Backup Process	You may perform snapshot backup using schedules that start from an active database and verify correctness of backup by performing the rollback function. Check *Windows Computer Management -> System Tools -> Event Viewer -> and Application.*

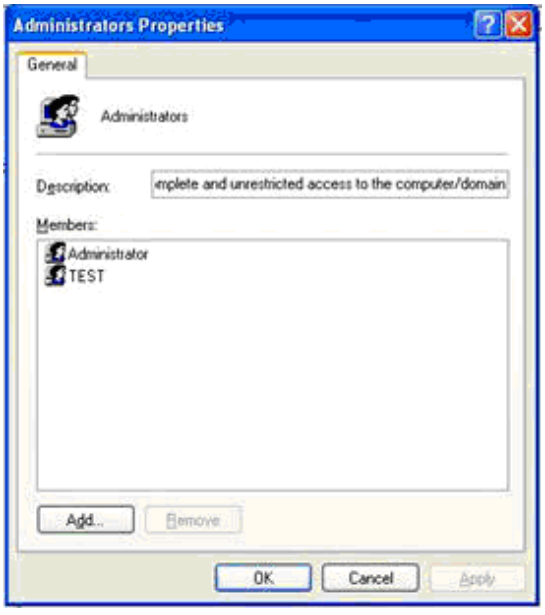


7.11 Enabling SA Login in MS SQL

If SA login is disabled or the SA login password is forgotten, the following message will appear.:

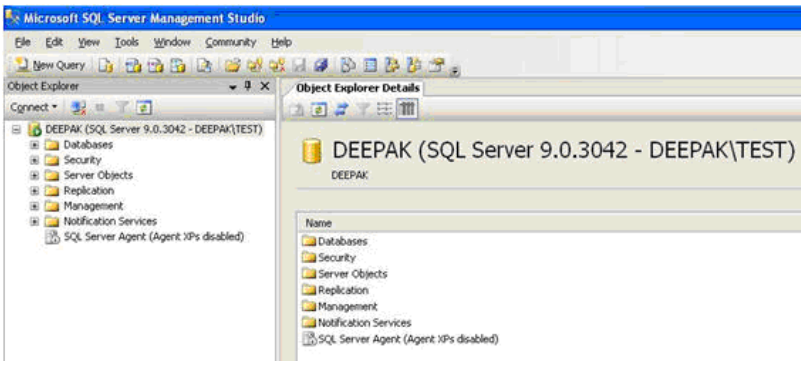


The screenshot below shows the members of the Windows Administrators group.

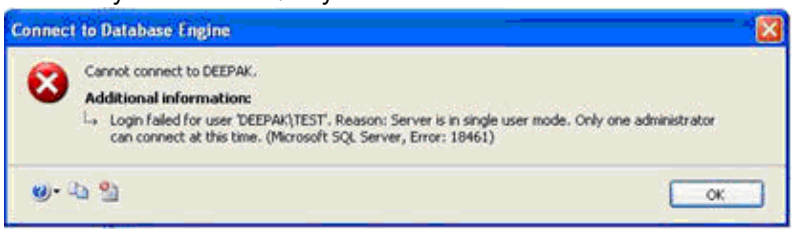


Note	MSSQLSERVER is for default instances. If proceeding in a named instance, use MSSQL$Instancename instead of MSSQLSERVER.

Steps	1. Login with the ID Test @OS Level.
	2. Stop SQL Server 2005 using the following command:
	`NET STOP MSSQLSERVER`
	3. Start SQL Server 2005 in Single User mode using the following command:
	`NET START MSSQLSERVER /m`
	4. Log into SQL Server 2005 using the ID Test as shown in the below screenshot.

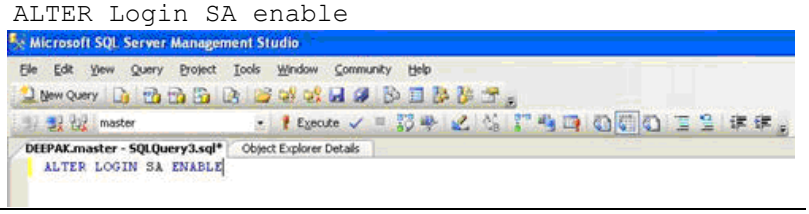


5. Because SQL Server is started in Single User mode, only one connection is allowed. Users will receive the following error if they click “New Query“.

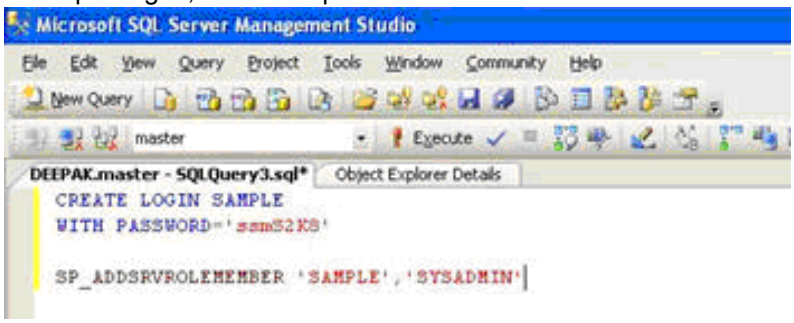


6. Disconnect and close Object Explorer. Reconnect using “New Query”, as shown below, and then enable SA login by inputting the following command:

```
ALTER Login SA enable
```



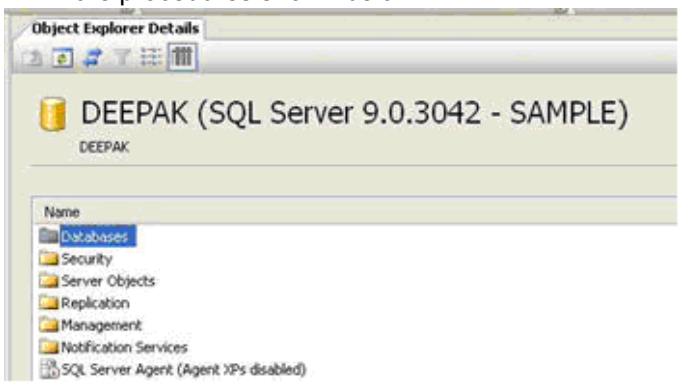
7. To create a new SQL Level login with system administrator privileges, follow the process shown in the screenshot below.

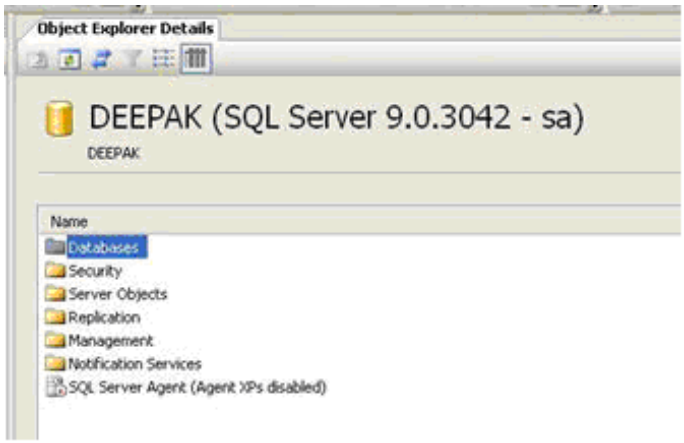


8. Now, users must stop and restart SQL Server normally using the following command:

```
NET START MSSQLSERVER
```

9. Connect using the SA login or newly created login and follow the procedures shown below.

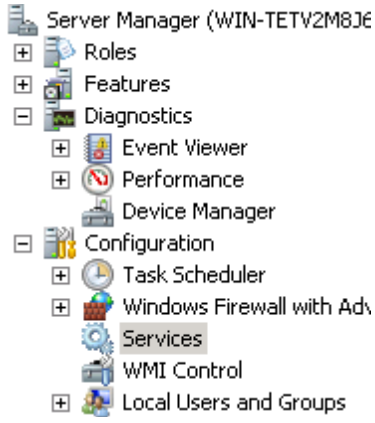




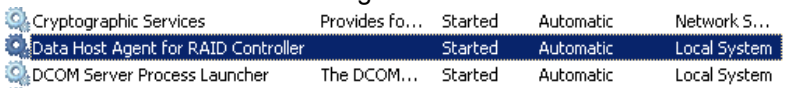
7.12 Configuring Out-of-Band Flushing

Steps (Windows Environment)

1. In Windows, open Server Manager > Configuration > Services.



2. Ensure that Data Host Agent for RAID Controller is initiated.



3. Go to Server Manager > Storage > Disk Management.

4. Select the disk with the volume to be flushed. If labeled Disk 1, “1” will become the disk ID for SANWatch flush agent configuration.

5. Refer to the section titled “Configuring Out-of-Band Flushing Using a DB Flush Agent” for information on how to configure SANWatch to perform data flushing.

Steps (Linux and Solaris Environment)

1. In Linux, start the data host agent.

```
[root@tsdRHL55 /]# ps -ef | grep newAgent
root      2675     1  0 09:06 ?        00:00:03 /usr/local/jre1
 -cp newAgent.jar:jconn3.jar:log4j.jar newagent.Agent /usr/loca
root      3707  2927  0 09:36 pts/1    00:00:00 grep newAgent
[root@tsdRHL55 /]#
```

2. Select the device to be flushed. For example, users may select the device named “sdb” located at the end of the list.

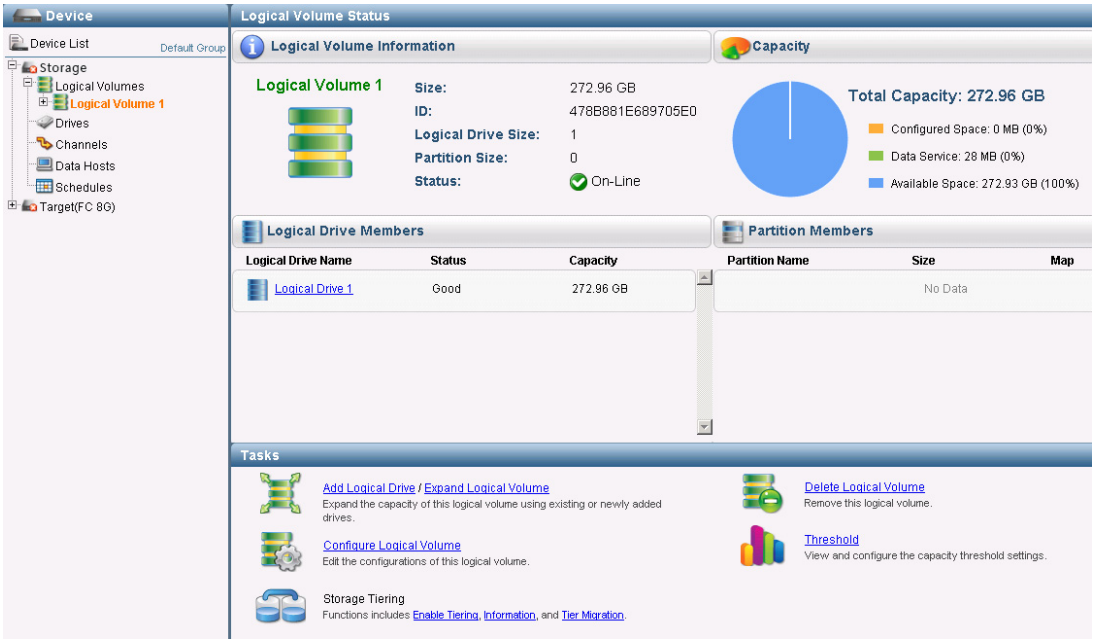
```
[root@tsdRHL55 ~]# more /proc/partitions
major minor  #blocks  name

   8     0  245117376 sda
   8     1     104391 sda1
   8     2  245007315 sda2
 253     0  242909184 dm-0
 253     1    2064384 dm-1
   8    16   52428800 sdb
[root@tsdRHL55 ~]# cd /
```

3. Using a web browser, open SANWatch and locate the partition that contains the database by going to
SANWatch Home > Device sidebar > Device List > device name > Logical Volumes > LV name > Partitions > partition name
Click the Help icon at the top-right corner, and look for the section titled “Configuring Out-of-Band Flushing Using a DB Flush Agent” to configure SANWatch to automatically perform data flushing.

Chapter 8

Working with Logical Volumes

8.1 Introduction

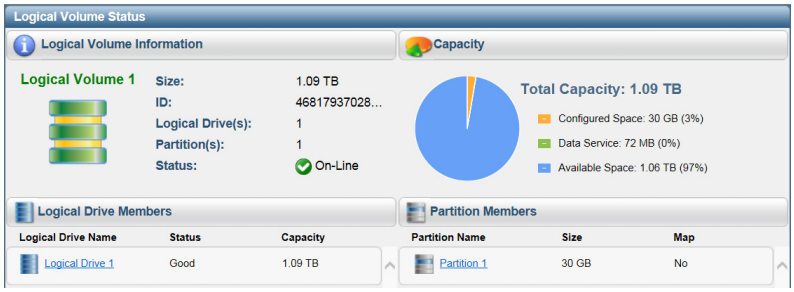


This chapter describes the parameters of a logical volume.

8.2 Viewing the Logical Volume Status

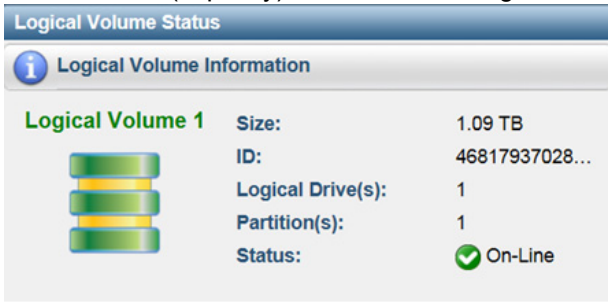
The status of each volume is summarized in the Information page, providing details of their configuration, performance, and storage capacity.

Go To	SANWatch Home > Device sidebar > Device List > device name > Logical Volumes > LV name
Viewing Volume Information	The volume status will be summarized in the Status section.



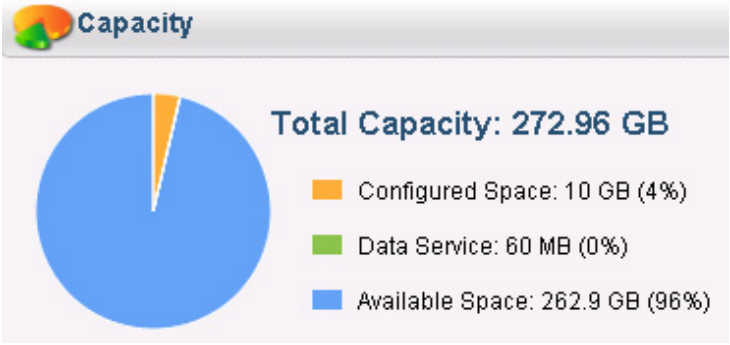
Volume Configurations

The basic configurations and overall status of each volume is listed in the Volume Information or Pool Information section. Users can view the size (capacity), ID, status, and logical drive information.



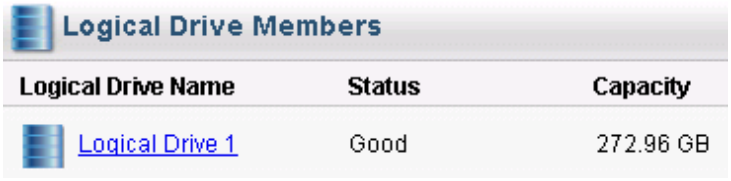
Volume Capacity

Users can view the amount and ratio of used (configured) capacity versus remaining (available) capacity, as well as the used capacity ratio for data services (snapshots, remote replications).



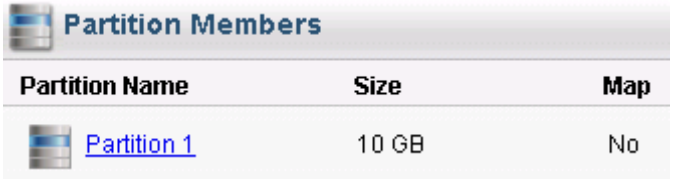
Logical Drive Information

Users can view a list of member logical drives and their detailed configurations (available after clicking the link).

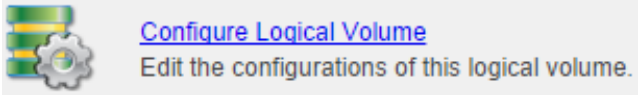
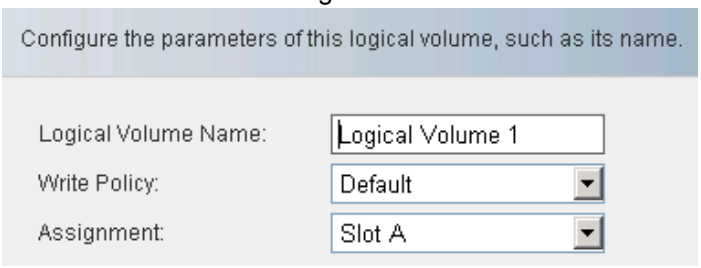


Partition Information

Users can view a list of LUN mappings and their detailed configurations (available after clicking the link).



8.3 Configuring Logical Volume Properties

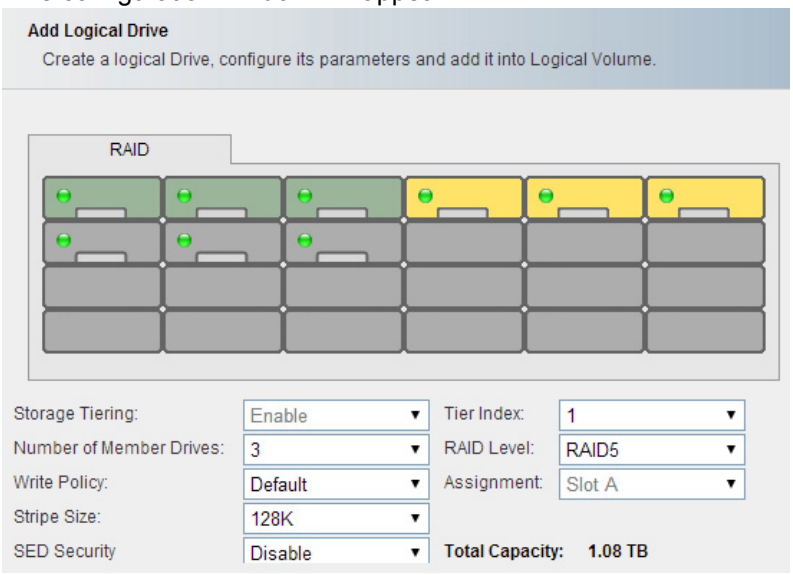
Go To	SANWatch Home > Device sidebar > Device List > device name > Logical Volumes > LV name > Tasks section
Steps	Click on the Configure Logical Volume link in the Tasks section.  Change the parameters in the Logical Volume Parameters section. Click “OK” to confirm changes. 
Parameters	**Name**: Specifies the logical volume name. **Write Policy**: ■ When Write Back (default) is enabled, write requests from the host are held in cache memory and distributed to disk drives later. Write-Back caching can dramatically improve write performance by caching unfinished writes in memory to more efficiently commit them to drives. In the event of a power failure, a battery backup module can hold cached data for a few days (usually 72 hours). ■ When Write Back is disabled (i.e., Write Through is adopted), write tasks from the host will be directly distributed to individual disk drives. If the controller is not in a redundant pair and no battery backup or UPS device exists to protect cached data, enabling Write Through mode is the safer option. **Assignment**: Specifies the controller to which the logical drive belongs. Do not change this setting except when switching the controller.
Controller Reassignment Procedure	To reassign a logical volume to a different controller, follow the steps below. 1. List the logical volume and all its logical drives 2. Shutdown the controller 3. Change the assignment through the command terminal (typically connected through the RS-232 interface) using the Set Logical Drive/Volume command. Note that a logical volume and all its logical drives must be assigned to the same controller. Users cannot partially change assignments even using the above procedure.

8.4 Adding a Logical Drive to an Existing Logical Volume

By default, when a logical volume is created, a logical drive is also created on the logical volume. However, a logical drive can be added to an existing logical volume using the procedures outlined below.

Go To	SANWatch Home > Device sidebar > Device List > device name > Logical Volumes > LV name > Tasks section
Steps	Click “Add Logical Drive” in the Tasks section.

The configuration window will appear.

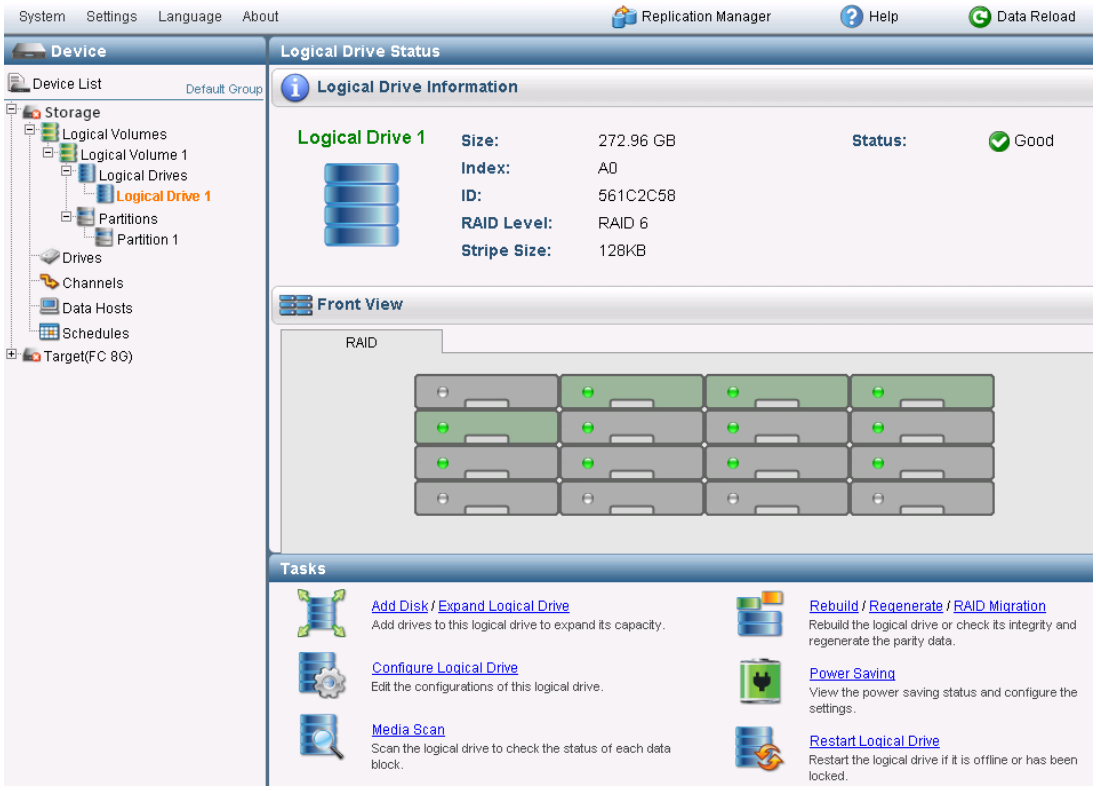


For more details regarding the options presented in the window, refer to the section “Creating a Logical Volume”.

Chapter 9

Working with Logical Drives

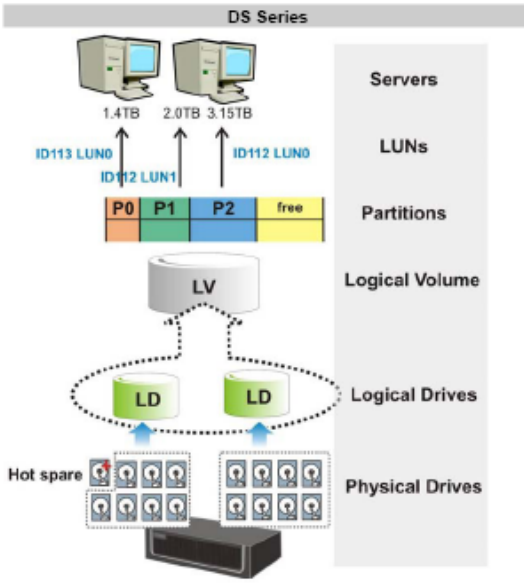
9.1 Introduction



This chapter describes how to view and change logical drive parameters, configure power saving settings, and add a logical drive to a remote hardware device. If a logical drive is offline or locked, restart the drive manually.

9.2 From Physical Drive to Logical Drive to Logical Volume

The diagram shows the hierarchy from physical drives to the host computer.

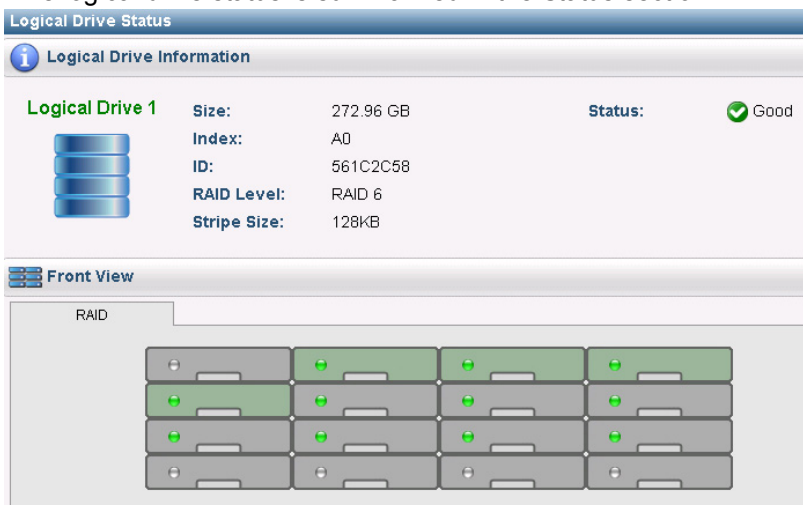


- A collection of physical drives forms a logical drive.
- A collection of logical drives forms a logical volume.
- A logical volume can be separated into partitions.
- Each partition is assigned an LUN (logical unit number) by the host computer.

9.3 Viewing the Logical Drive Status

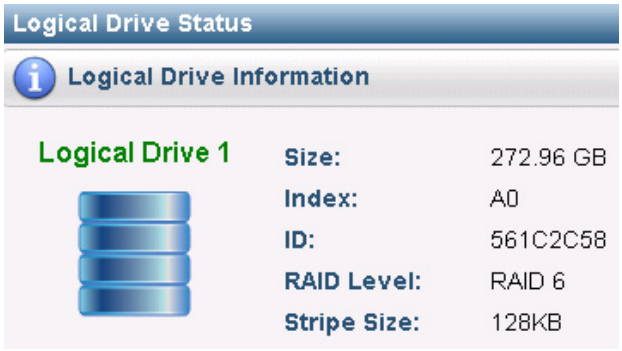
The status of each logical drive is summarized in the Logical Drive Information page, enabling users to quickly view the element configuration and locations of member hard disk drives.

Go To	SANWatch Home > Device sidebar > Device List > device name > Logical Volumes > LV name > Logical Drives
Viewing the Logical Drive Information	The logical drive status is summarized in the Status section.



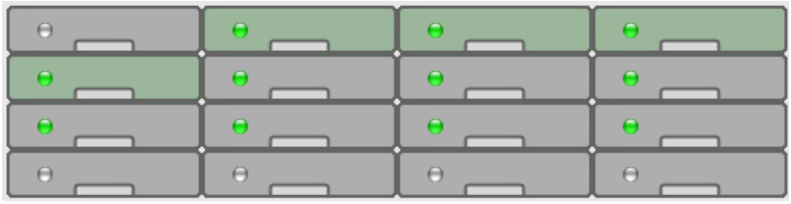
Logical Drive Configurations

The basic system configurations and overall system status are detailed in the Logical Drive Information section. Users can view the size (capacity), logical drive ID, RAID level, and controller module location.



Hard Drive Locations

The front view corner shows the hard drive configurations of the device the logical drive belongs to.



A green Status LED indicates that the hard drive is online.

The location of logical drive is denoted using different colors.

9.4 Adding Disk Drives to a Logical Drive

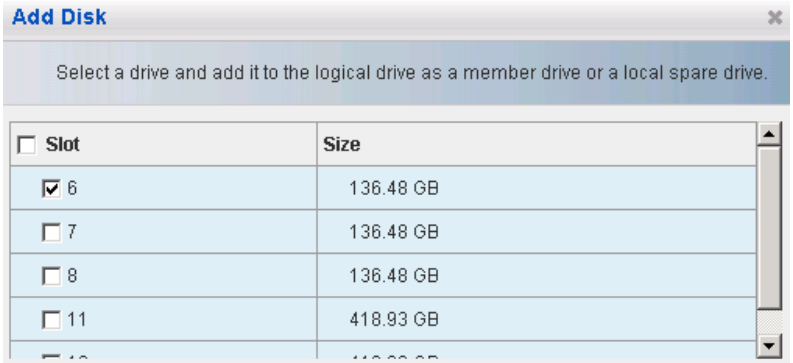
Add additional member drives or spare drive(s) to expand the size of the logical drive.

Before attempting to expand a logical drive, ensure available (unused) disk drives have been inserted into the enclosure.

Warning! *We strongly recommend assigning a spare drive. Without a spare drive, the risk of data losses increases.*

Go To	SANWatch Home > Device sidebar > Device List > device name > Logical Volumes > LV name > Logical Drives > Tasks section
Steps	Click Add Disk in the Tasks section.

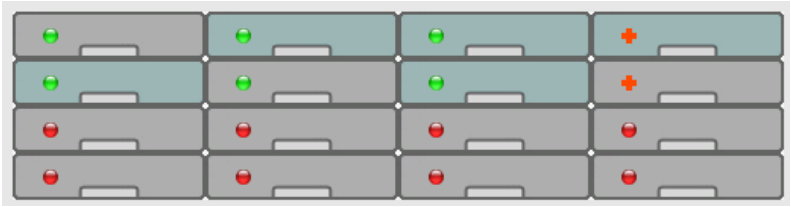
Select the drive to add from the list provided.



Select whether to add the drive as a spare or part of the logical drive.

If a local spare drive has been added

The spare drive will be marked in the front view.



Depending on the RAID level of the logical drive, users may need to add more than one drive at a time.

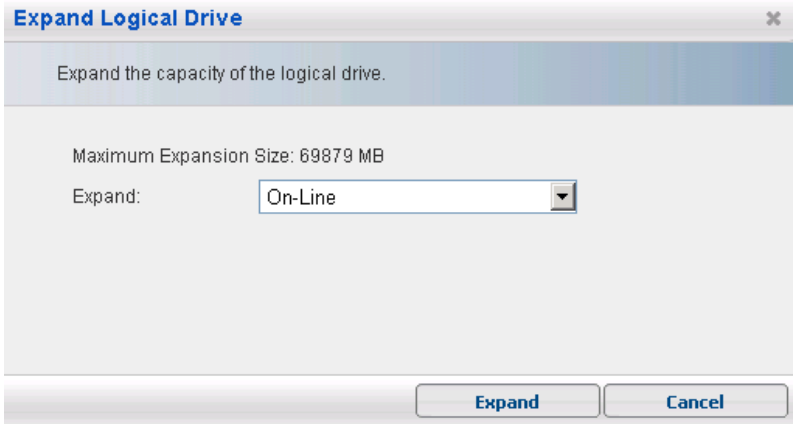
If member drives have been added

The drive will be added and the progress will appear in the Status section.

9.5 Expanding the Size of a Logical Drive

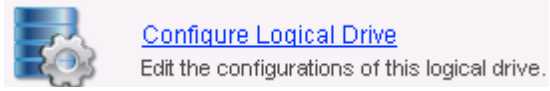
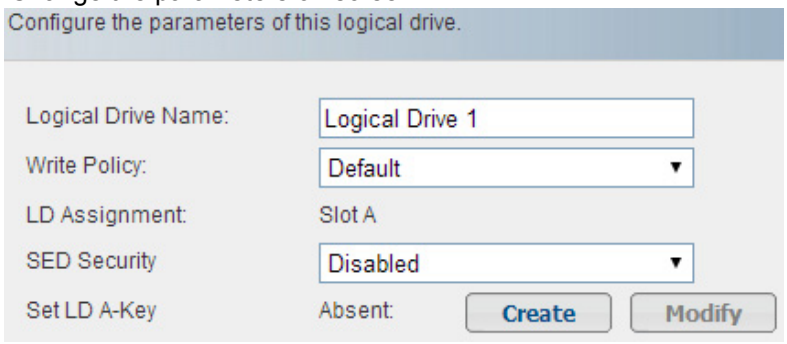
Expand a logical drive by adding unused space in the disk drives.

When All Disk Capacity Has Been Used	Logical drives cannot be expanded if all the disk drive capacity is already used for the logical drive. In such cases, the following two strategies can be implemented: ■ Add additional disk drives. ■ Copy and replace member disk drives with drive with greater capacity, and use the additional capacity to expand the logical drive by following the steps detailed in this section. All member drives must be replaced.
Go To	SANWatch Home > Device sidebar > Device List > device name > Logical Volumes > LV name > Logical Drives > Tasks section

Steps	Click on the Expand Logical Drive option in the Tasks section. The Expansion screen will appear.  Select the initialization mode and click “Expand”.

Expand Size	The available size is automatically calculated (total capacity – current logical drive capacity).
Execute Expand (Initialization)	Specifies whether the logical drive can be accessed during initialization (online) or not (offline). During online initialization, read/write performance to the logical drive will decrease because of the background initialization process.

9.6 Configuring Logical Drives

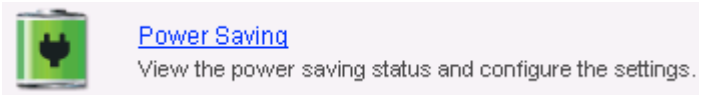
Go To	SANWatch Home > Device sidebar > Device List > device name > Logical Volumes > LV name > Logical Drives > LD name > Tasks section
Configuring Properties	Click on the Configure Logical Drive link in the Tasks section.  Change the parameters on screen. 

Logical Drive Name	Specifies the name of the logical drive.
Write Policy	Changes the write policy: Write Back (default) or Write Through. For detailed descriptions, see below.

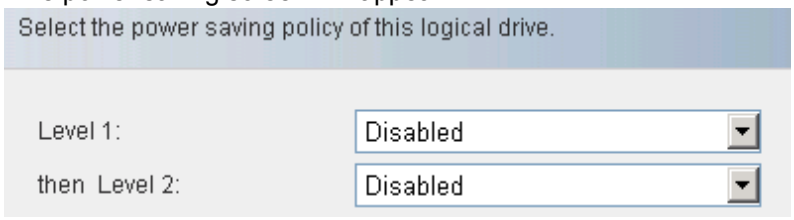
	Logical Drive Assignment	This option cannot be modified because logical drives and their logical volumes should be managed by the same controller. To change the logical volume controller, select the controller in the Device sidebar, and click “Configure Logical Volume”.
	SED Security	Enhances data security with SED for all logical drives on the subsystem. Once enabled, all logical drives will be SED-protected; therefore, this mechanism is known as a “global key”. Before enabling this option, create an SED authentication key at SANWatch Home > Device sidebar > Device List > device name > Tasks section > System Settings > Drive-Side tab
		Creating a global key (at SANWatch Home > Device sidebar > Device List > device name > Tasks section > System Settings > Drive-Side tab > SED Authentication Key) will disable and hide this option.
	Set Logical Drive A-Key	Enhances data security with SED using a “local key” for this logical drive. SED security will be enabled whenever a “local key” is created and imported. SED security using local keys will become ineffective after system reboots. To enable this function, users must import the key file or password every time the subsystem reboots.
Write Back Versus Write Through	■ When Write Back is enabled, write requests from the host are held in cache memory and distributed to disk drives later. Write-Back caching can dramatically improve write performance by caching unfinished write tasks in memory and more efficiently committing them to drives. In the event of a power failure, a battery backup module can retain cached data for a few days (usually 72 hours). ■ When Write Back is disabled (i.e., Write Through is adopted), write tasks initiated by the host are directly distributed to individual disk drives. If the controller is not in a redundant pair and no battery backup or UPS device exists to protect cached data, Write Through mode is the safer option.	

Configuring Power Savings

Click on the Power Saving link in the Tasks section.



The power saving screen will appear.



Power Saving Level

Select the Drive-Side tab and configure the power saving mode.

Three options are available: **Disabled, Level 1 only**, and **Level 1 then Level 2**.

Waiting Period

Users can also configure the waiting period before the system switches into power saving mode.

- Level 1: 1 to 60 minutes without I/O requests
- Level 2: 1 to 60 minutes of Level 1 state

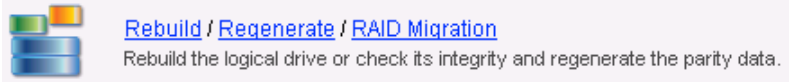
To configure the power saving levels for the entire device, go to SANWatch Home > Device sidebar > Device List > device name > Tasks section > System Settings > Drive-Side tab > Power Saving

Level	Power Saving	Recovery	ATA	SCSI
1	15-20%	1 sec	Idle	Idle
2	80%	30 to 40 sec	Standby	Stop

Regenerating Parities

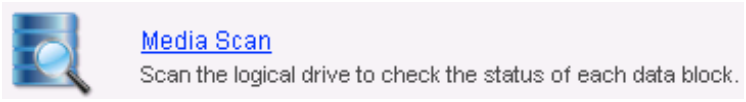
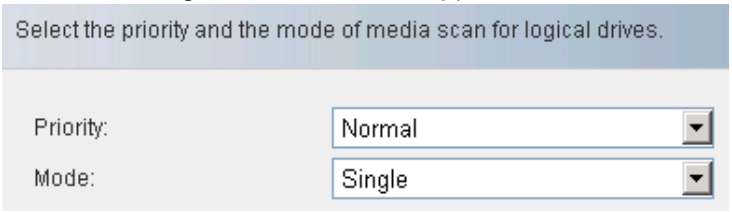
Parity regeneration is only applicable to RAID level 1 and above. This function enables user to check whether data inconsistencies or errors have occurred with data parities.

Click “Regenerate” in the Tasks section.



The parity data will be regenerated.

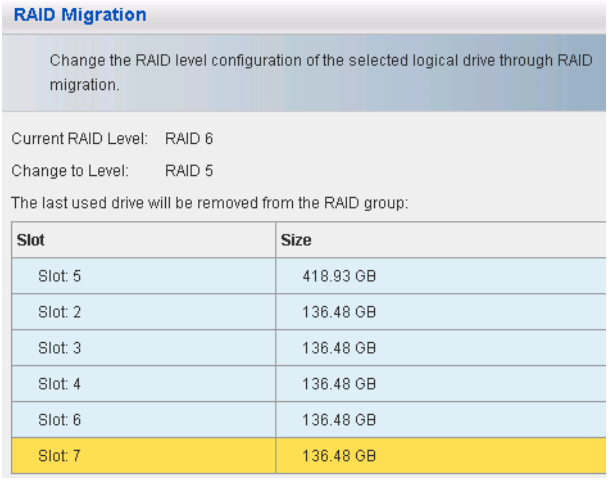
9.7 Scanning Logical Drives

Go To	SANWatch Home > Device sidebar > Device List > device name > Logical Volumes > LV name > Logical Drives > LD name > Tasks section	
Steps	Click on the Media Scan link in the Tasks section.  The scan configuration window will appear. 	
Parameters	**Priority**	The higher the priority, the faster the scanning. However, system performance will decrease.
	Mode	Scans once (Execution Once) or continuously.

9.8 Migrating a Logical Drive Between RAID 5 and RAID 6

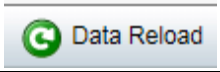
Migration allows the RAID level of a logical drive to be changed. Users may need to add or delete member drives according to the required drive minimum of each RAID level.

Migrating is only applicable to logical drives with RAID 5 or RAID 6 level. A logical drive cannot be migrated if already part of a logical volume. To migrate a drive from RAID 5 to RAID 6, at least one available drive is necessary.

Go To	SANWatch Home > Device sidebar > Device List > device name > Logical Volumes > LV name > Logical Drives > LD name > Tasks section
Steps	Click on the RAID Migration option. The current RAID levels will be shown. 

Click “Migrate”.

Then click “Data Reload” to refresh drive statuses.



9.9 Rebuilding a Logical Drive

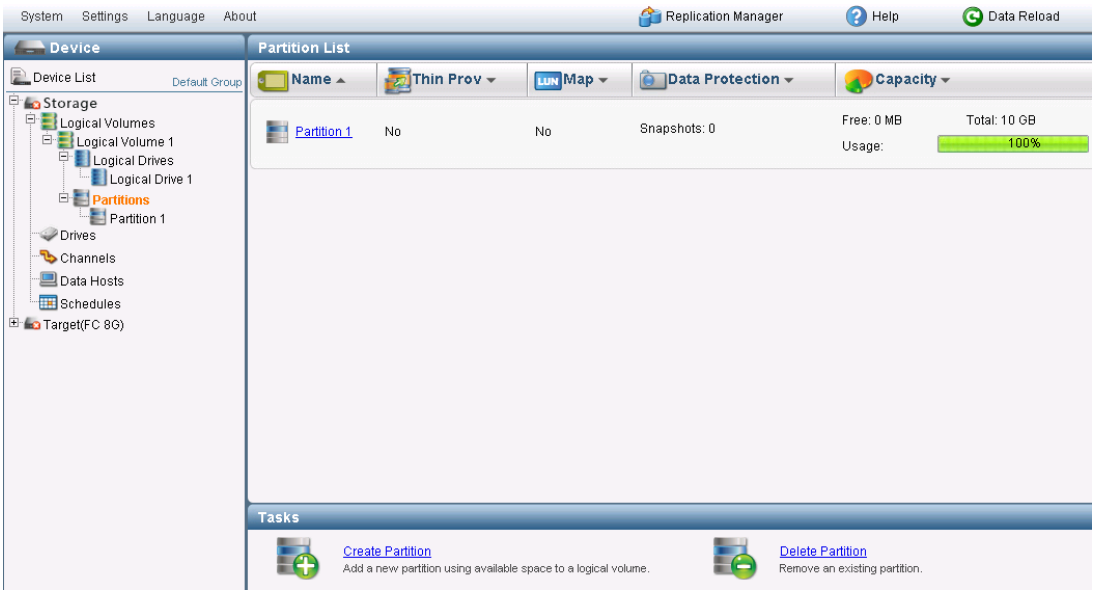
The Rebuild menu is available only when a logical drive is in a Degraded state due to drive failure(s).

Go To	SANWatch Home > Device sidebar > Device List > device name > Logical Volumes > LV name > Logical Drives > LD name > Tasks section
Steps	Click on the Rebuild option in the Tasks section. Select the logical drive currently in a degraded state and click “Rebuild”. If the logical drive does not return to a healthy state, remove the drive and create a new one.

Chapter 10

Working with the Partitions View

10.1 Introduction



This chapter describes the overall parameters of partitions included in a logical volume.

10.2 General Rules

Maximum Number	The maximum number of partitions are ■ Per RAID: 80 ■ Per JBOD: 40
Note on Over-Provisioning	Over-provisioning is a situation that may occur with a thin-provisioned storage system. This means that the available physical capacity is less than the logical capacity allocated for applications. Over-provisioning provides the advantage of maximizing capacity utilization, but also carries the risk of I/O failure when actual usage reaches the physical limits (this may result in the application or even the host crashing). Over-provisioning is allowed but not recommended. If the potential for allocating all space (over-provisioning) is detected, a warning message will be generated. However, users may still be able to create partitions.

10.3 Viewing the List of Partitions

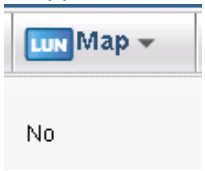
All partition information can be accessed via the sidebar of the user interface.

Go To	SANWatch Home > Device sidebar > Device List > device name > Logical Volumes > LV name > Partitions
Steps	Click on the Partitions tab in the left sidebar to view the list of partitions and the parameters recognized by the system.

Click on the name of a partition to access a detailed configuration page for the volume.

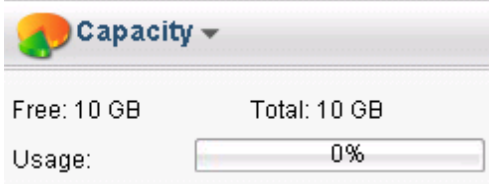
The Thin Prov tab shows whether thin provisioning is enabled on the partition.

The LUN Mapping tab shows whether the partition has been mapped to the host.



The Data Protection section shows the number of snapshot images taken of the partition.

The capacity section shows the total and available (free) capacity allocated to the partition.

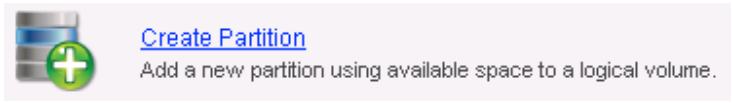


To refresh the status (to ensure the status has been updated), click the Data Reload option on the top bar.

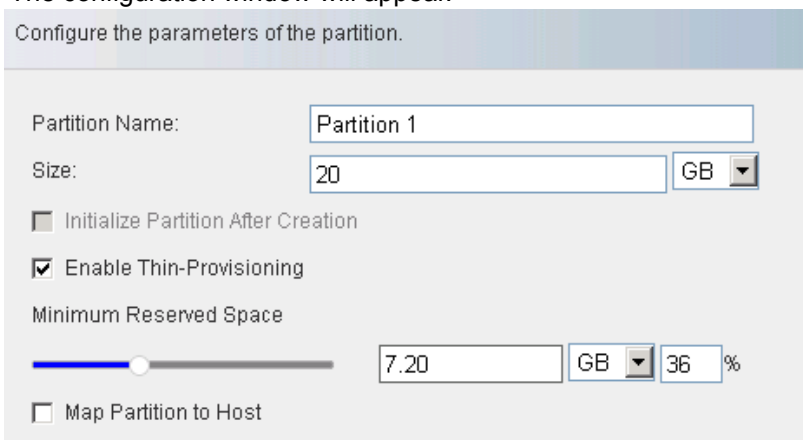
Note	If the Help screen does not appear, check whether pop-up windows are enabled by accessing the browser configuration options.

10.4 Creating a Partition

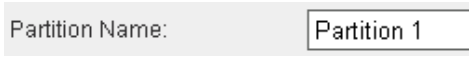
Note	The maximum size of a single partition is 256TB (before firmware version 3.88) and 512TB (after firmware version 3.88). Ensure that the size of the logical volume is appropriate (the size of the partition cannot exceed that of the logical volume). For the latest status information, check with technical support.
Go To	SANWatch Home > Device sidebar > Device List > device name > Logical Volumes > LV name > Partitions > Tasks section
Steps	Click on the Create Partition link in the Tasks section.



The configuration window will appear.



Enter the name of the partition.



Enter the size and select the unit.

The size of a partition must be multiples of 2 MB.

Enable Initialization or Thin Provisioning (mutually exclusive).

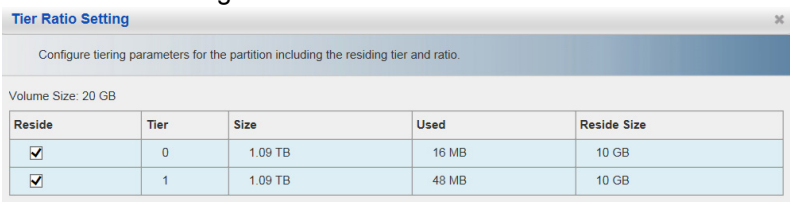
For a more detailed description of thin provisioning, refer to the following section.

Set the minimum reserved amount.

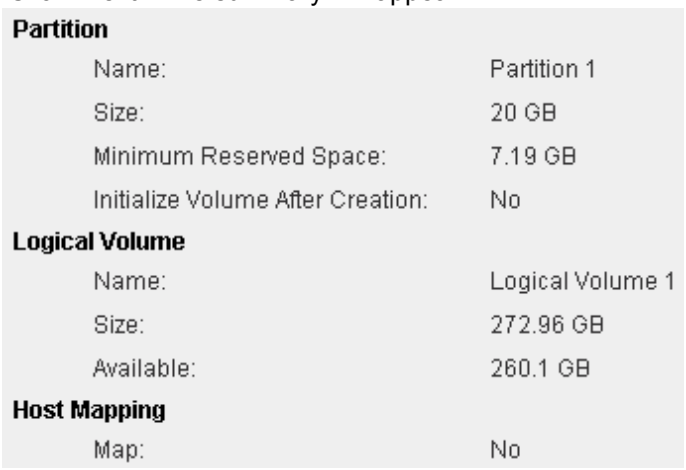
Users can map the partition to the host here or later.

For more detail regarding mapping, refer to the instructions provided below.

Click “Next”. If creating a partition on a tiered logical volume, decide the residing tier and ratio.



Click “Next”. The summary will appear.



The partition will appear in a list.

Size	Specifies the size and unit of the partition. If Thin Provisioning is enabled, the total size of partitions can exceed the size of the logical volume.
	The minimum size of a partition is 10 GB.
Initialize Partition After Creation	When this option is enabled, the partition's LBA addresses will be allocated sequentially for large and/or sequential I/Os. This is ideal for audio/video applications such as post-editing media and on-demand video.
Thin Provisioning	Enables thin provisioning. Move the slide bar to set the percentage of the partition capacity that will be physically allocated as a safe reserve. If the reserve reaches 100%, the partition becomes fully provisioned (all space is allocated from the virtual pool). For more information, refer to subsequent sections of this manual.
Map Partition to Host	Maps the partition to all host ports. The host port can also be mapped manually at a later time. For more information, refer to subsequent sections of this manual.

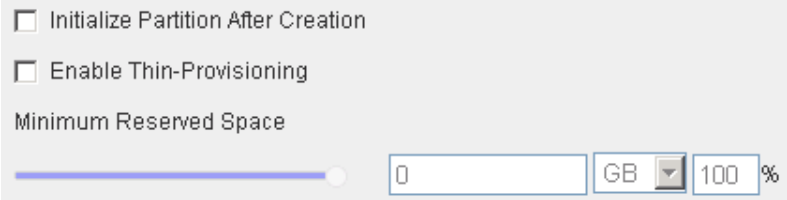
10.5 About Thin Provisioning

Thin provisioning allows users to allocate substantial virtual capacity to a logical volume, regardless of the physical capacity actually available. Actual space is only used for data write tasks. By automatically allocating system capacity to applications as required, thin provisioning technology can significantly increase storage utilization. Thin provisioning also greatly simplifies capacity planning and management tasks.

Advanced licensing may be required to access thin provisioning. Dynamically allocating capacity affects the overall system performance. If performance is a top priority (such as in AV applications), we recommend disabling thin provisioning (i.e., use full provisioning).

Thin Provisioning Settings

Thin provisioning is configured during the creation of a partition on a logical volume.
Thin provisioning options appear in the lower half of the Creation screen.

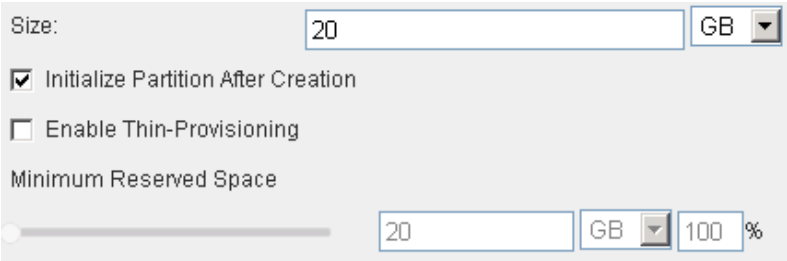


After the new partition is created, create one or more notification thresholds to ensure that the administrator receives warning/critical messages before all logical volume space is used. This will ensure sufficient time to expand the size of the logical volume.

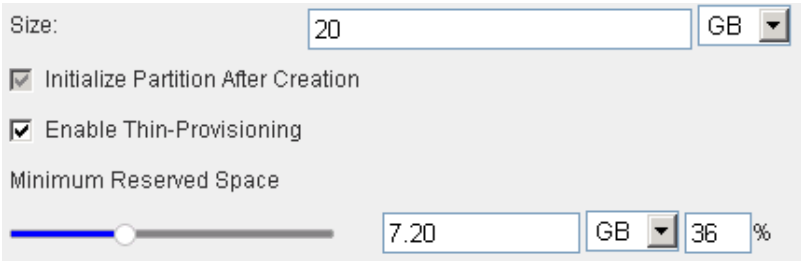
We recommend creating multiple thresholds for maximum security (for example, notification for 70%, warning for 90%, critical for 95%, critical and purge snapshot images for 99%).

Case 1: Full Provisioning (Thin Provisioning Disabled)

If the “Enable Thin Provisioning” option is unchecked, thin provisioning will be disabled and the capacity of the configured logical volume (14 GB in the example provided below) will be based on the capacity actually available. The partition will be created as a continuous physical space reserved only for the target application and initialized if the “Initialize Partition After Creation” box is checked (this option can also be disabled).

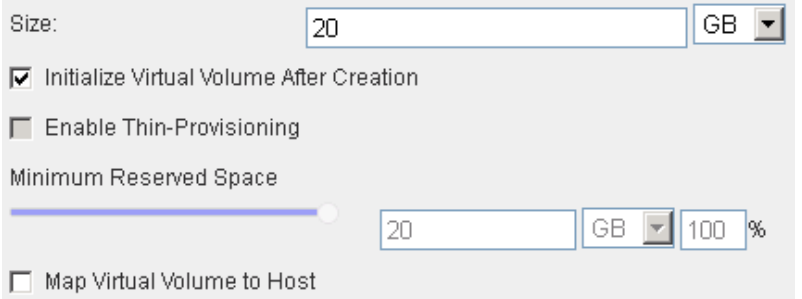


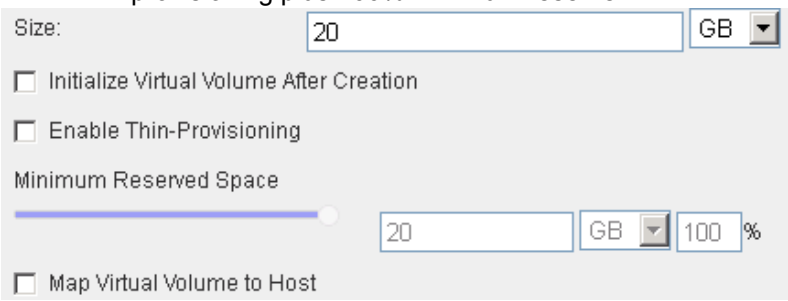
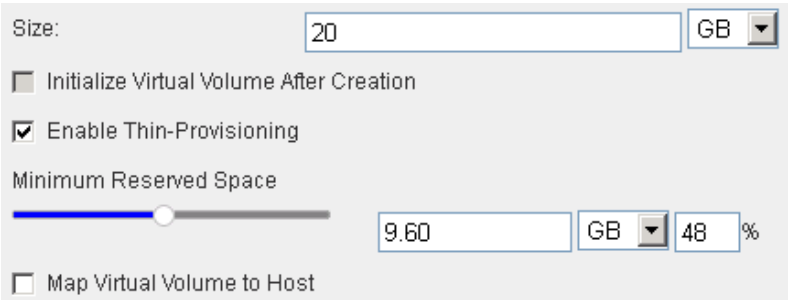
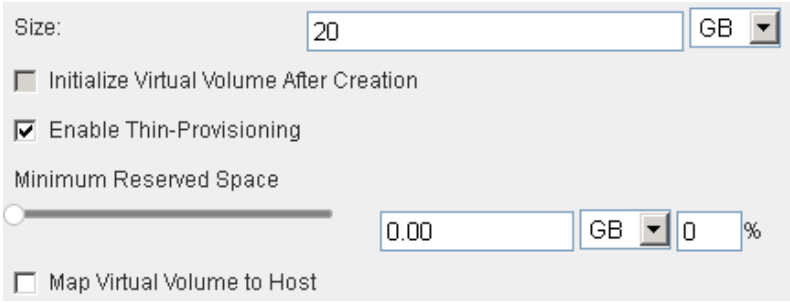
Full provisioning is suitable for mission-critical applications with substantial amounts of uninterrupted data, such as audio/video streams. Dynamically allocating space and expanding the usable area reduces I/O performance. Allocating a high physical capacity from the outset optimizes performance.

Case 2: Thin Provisioning	To enable thin provisioning, check the “Enable Thin Provisioning” option and set the Minimum Reserved Space using the slider. When the application uses the minimum reserved space, additional space will be taken from the rest of the logical volume space and dynamically added to the partition. In this example, the actual logical volume size is 10 GB but the partition is set at 20 GB, larger than the available size. This is acceptable providing the minimum reserved space (the actual physical space) is smaller than the size of the logical volume, which is 7.20 GB in this case.  The reserved space cannot exceed the actual available capacity.

10.6 Provisioning and Reserved Space

Below the three provisioning/initialization combinations are explained.

Options	■ Initialize Partition After Creation: Initializes the partition content. This option is only available when Thin Provisioning is disabled (i.e, Full Provisioning is enabled), because the full capacity of a partition must be in physical storage space for the partition to be initialized. ■ Enable Thin Provisioning: When checked, Thin Provisioning (physical partition capacity provided as required) will be enabled. When unchecked, Full Provisioning (all partition capacity is provided physically) will be enabled. ■ Minimum Reserve: The minimum physical capacity always allocated to the partition. If the minimum reserve is set at 0%, the partition is not allocated any real capacity by default. When the minimum reserve is set at 100%, the real capacity of the partition always matches the theoretical maximum (i.e., is equal to full provisioning).
Full Provisioning With Initialization	■ Initialization plus 100% minimum reserve  This configuration can only be applied to one storage tier.

Full Provisioning Without Initialization	■ Thin provisioning plus 100% minimum reserve  This configuration is not allowed in multi-tiered logical volumes.
Thin Provisioning with Minimum Reserve Space	■ Thin provisioning plus 1 ~ 99% minimum reserve  This configuration is not allowed in multi-tiered logical volumes.
Thin-Provisioning Without Minimum Reserve Space	Thin provisioning plus 0% minimum reserve 

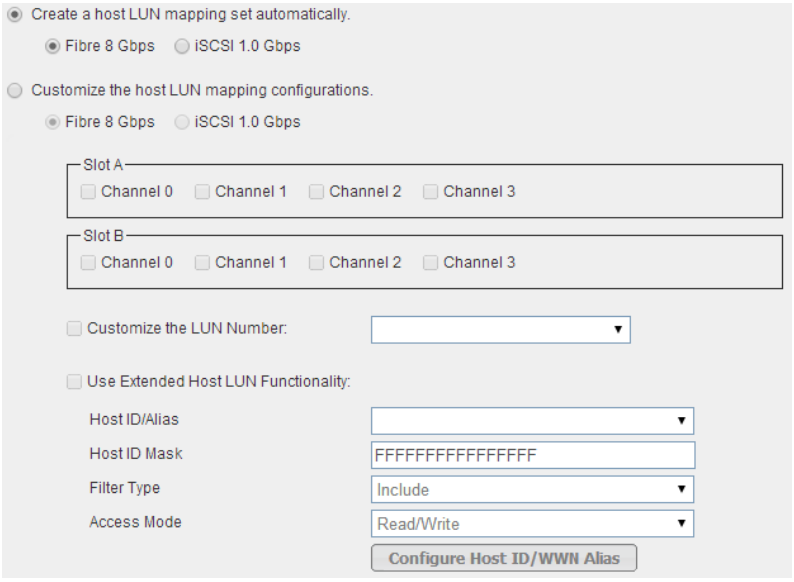
10.7 Mapping/Unmapping Partitions to a Host

Host LUN mapping is involved in the creation of partitions.

Mapping Host LUN

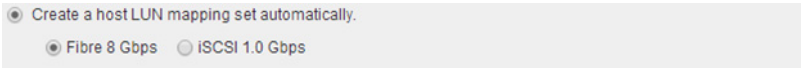
The Host Mapping Configuration Window
The prompt for Fibre channel models is shown below. For hybrid (Fibre and iSCSI) host models, users must configure both settings.

Example: Hybrid model



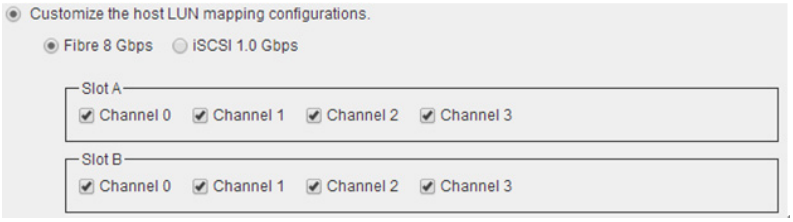
Automatic Configuration

Select this option to enable the system to automatically perform LUN mapping. For hybrid models, the host type must be selected.



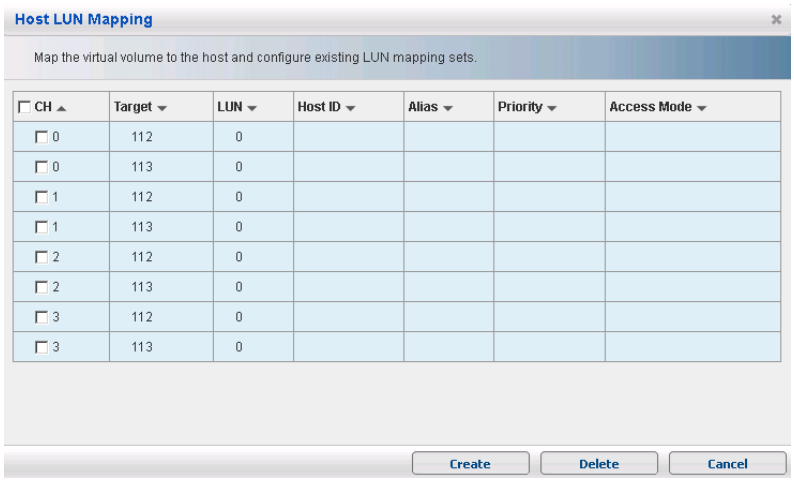
Manual Configuration

If manually conducting LUN mapping, check the Customize option and select the target channels.



Select a LUN number from the drop-down list.

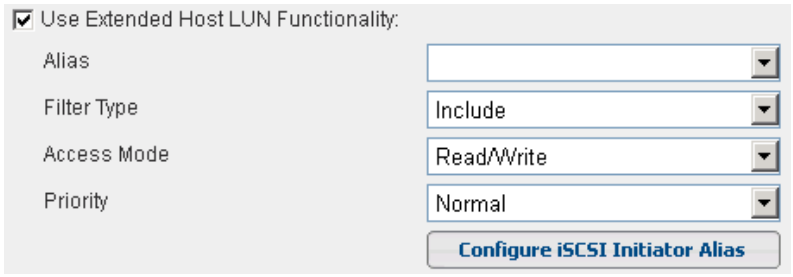
Click “OK”. A list of host LUN mapping configurations will appear in the window.



Using Extended LUN Mapping (Fibre Channel)

Extended LUN mapping is only available with manual configuration.

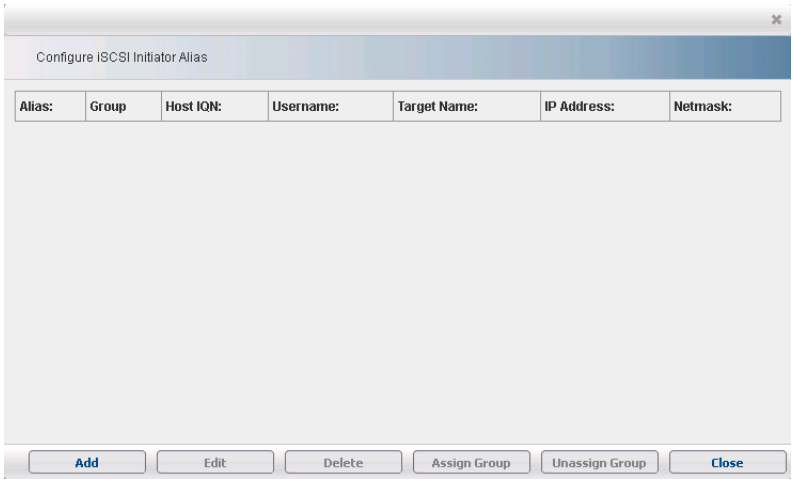
Click “Use Extended LUN Functionality” and specify parameters.



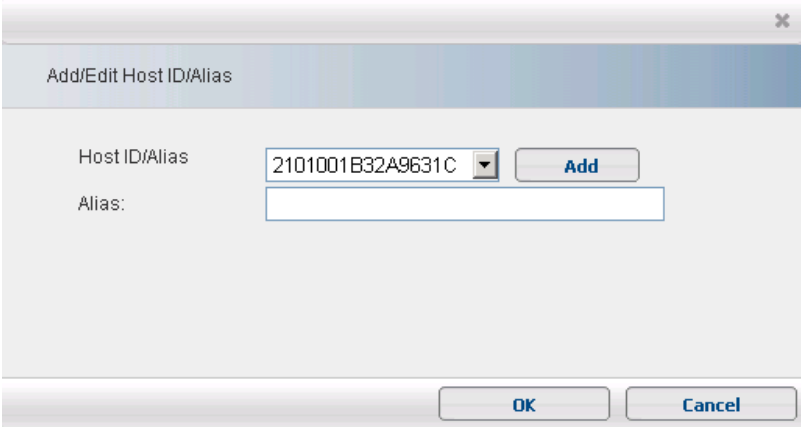
- Alias: Specifies a preconfigured iSCSI initiator instance. To create a new initiator alias, select the Configure iSCSI Initiator Alias option.
- Filter Type: Specifies whether initiators are allowed (included) or forbidden (excluded) from access after filtering.
- Access Mode: Specifies the access rights to LUN mapping for the host: read-only or read-write.
- Priority: Specifies access priority. For example, high priority can be assigned to volumes that serve applications, and low priority assigned to volumes that store archives or user data.

Configuring iSCSI Initiator Alias

Click on the Configure iSCSI Initiator Alias option.



In the Edit Host-ID/WWN List window, click “Add” to create a new entry and enter the node name (WWN Name) for identifying HBA ports in SAN. An HBA card may have one node name and multiple port names. The node name can be a nickname, such as “SQLserver_port,” instead of a real name.



Click “OK”. Repeat the process above to create additional LUN mappings, especially if there are multiple HBA ports accessing the same virtual volume (e.g., in high-availability applications).

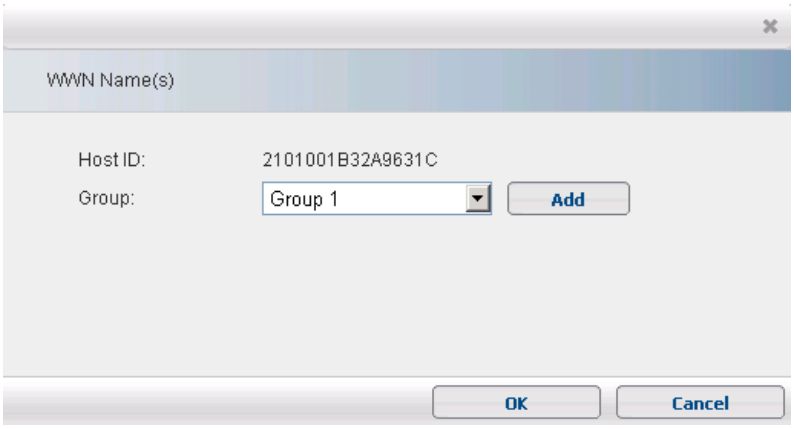
Assigning a WWN to a Group

A WWN group allows multiple hosts to be accessed in a single mask, a function that is useful for clustered storage server environments.

To create a group and assign it a WWN, highlight a WWN (yellow).

Alias	Group	Host ID / WWN	Controller
Alias		2101001B32A9631C	Slot A

Click “Assign Group” and select the group from the drop-down menu.



To add a new group, click “Add” and enter the group name.

The group name will appear in the list.

Alias	Group	Host ID / WWN	Controller
Alias	Group1	2101001B32A9631C	Slot A
Alias	Group1	2101001B32A9631C	Slot A
Alias	Group 1	2101001B32A9631C	Slot A

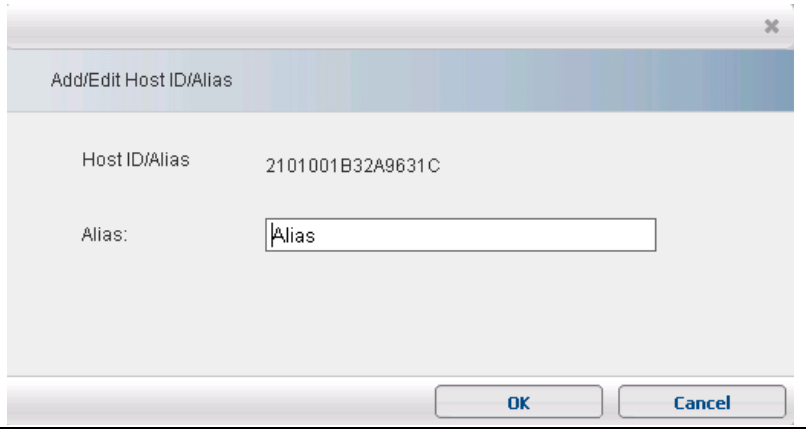
To unassign a WWN from a group, click “Unassign Group”.

Deleting a WWN Name from the List

Highlight a WWN in the list and click “Delete”.

Changing the Alias Name

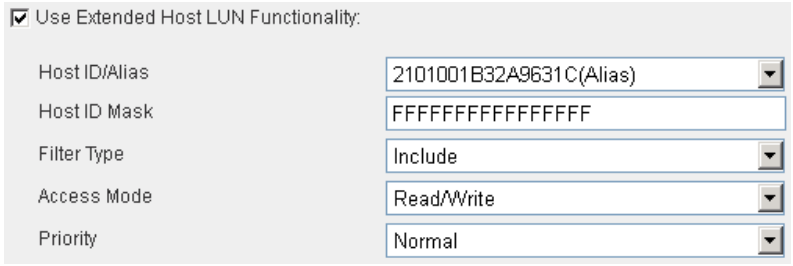
To edit the alias name of the WWN, click “Edit” and enter a new name.



Using Extended LUN Mapping (iSCSI Channel)

Extended LUN mapping is only available with manual configuration.

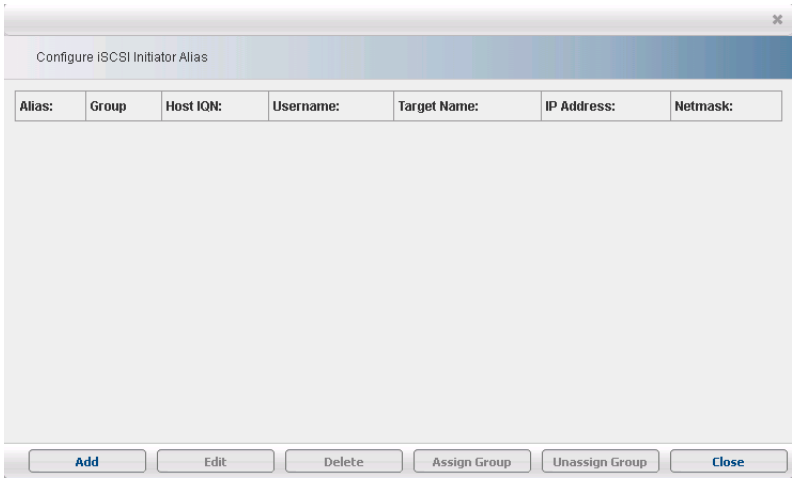
Click “Use Extended LUN Functionality” and specify parameters.



- Host ID/Alias: Specifies the host ID by referring to the WWPN port name. Users can also obtain the organizationally unique identifier (OUI) of a system: “00:D0:23” OUI. Avoid checking the OUI when mapping host LUN.
- Host ID Mask: This functions as a prefix mask in hexadecimal format.
- Filter Type: Specifies whether to allow (include) or forbid (exclude) WWNs from access after filtering.
- Access Mode: Specifies the access rights to LUN mapping for the host: read-only or read-write.
- Priority: Specifies access priority. For example, high priority can be assigned to volumes that serve applications, and low priority assigned to volumes that store archives or user data.

Configuring the iSCSI Initiator Alias

Click “Configure iSCSI Initiator Alias”.



Click “Add” to create an entry, then specify the parameters.

- Host IQN: Advantech’s storage IQN comprises the system serial number and three additional digits in the following format:
  iqn.2002-10.com.advantech:raid.snXXXXXX.XXX
  Six digits of the serial number follow “sn.”
  The next 3 digits denote the channel number, host ID, and LD ownership.
  The LD ownership digit is either “1” or “2”, where “1” indicates Controller A and “2” indicates Controller B. The IQN is determined by how the logical drive is mapped to the host ID/LUN. For example, if a logical drive is mapped to host channel 0 and AID1, the last three digits will be 011.
- Alias: Assign the iSCSI initiator an easily remembered name.
- Username/Password: Specifies the user name and password for CHAP authentication. This information is the same as the CHAP target node name and CHAP secret in the OS settings. The User Password (one way, from initiator) must be at least 12 bytes.
- Target Name/Password: Specifies the target name and password for CHAP authentication. This information is the same as the CHAP initiator node name and CHAP secret in the OS setting. The Target Password (two way, outbound from storage) must be at least 14 bytes.
- IP Address/Netmask: Specifies the IP address and subnet mask, if necessary. Multiple initiator ports on an application server can occasionally share the same IQN.

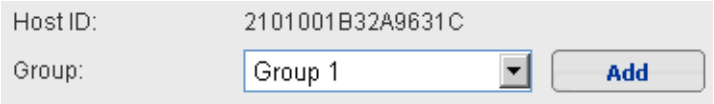
Click “OK”. Repeat the above process to create additional LUN mappings, especially if multiple HBA ports are accessing the same virtual volume (e.g., in high-availability applications).

Assigning an Initiator to a Group

A group allows multiple host LUNs to be accessed in a single mask, which is a useful function in clustered storage server environments.

To create a group and assign it an initiator, highlight an initiator (yellow).

Click “Assign Group” and select the group from the drop-down menu.



To add a new group, click “Add” and enter the group name.

The group name will appear in the list.

To unassign an initiator from a group, click “Unassign Group”.

Deleting an Initiator Name from the List

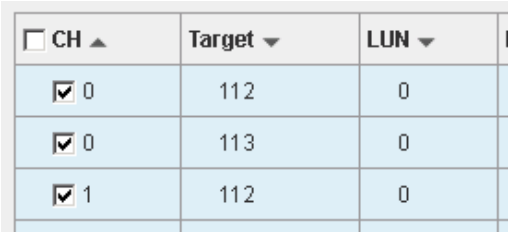
Highlight an initiator in the list and click “Delete”.

Editing Initiators

To edit the configuration of an initiator, click “Edit”.

Unmapping Host LUN

Select the host LUN to unmap.



Click “Delete”.

Managing LUN Mapping on the Host Side

Select the partition with the LUN mappings to be managed, click the Help icon at the top-right corner, and access the “Managing LUN Mapping on the Host Side” option for detailed instructions.

Notes

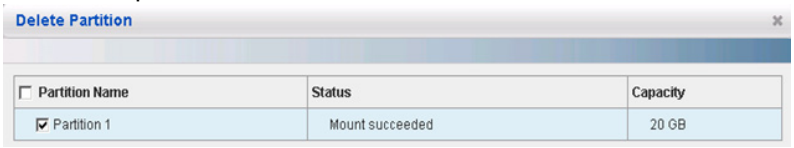
- By mapping a partition to multiple ports on multiple HBAs, path redundancy is achieved. To manage fault-tolerant paths on a single volume, users must install EonPath driver (for Windows servers), Device Mapper (for Linux), and Solaris MPXIO (for Solaris platforms and Sparc machines).
- To acquire HBA port names, access the utility software or website of the HBA vendor.
- In hybrid models, iSCSI host channels are, by default, used for remote replication.

10.8 Deleting Partitions

Before deleting a partition, the following features, if applied, must be deleted:

- Snapshot images
- Partition pair or volume pair relationships
- LUN mappings

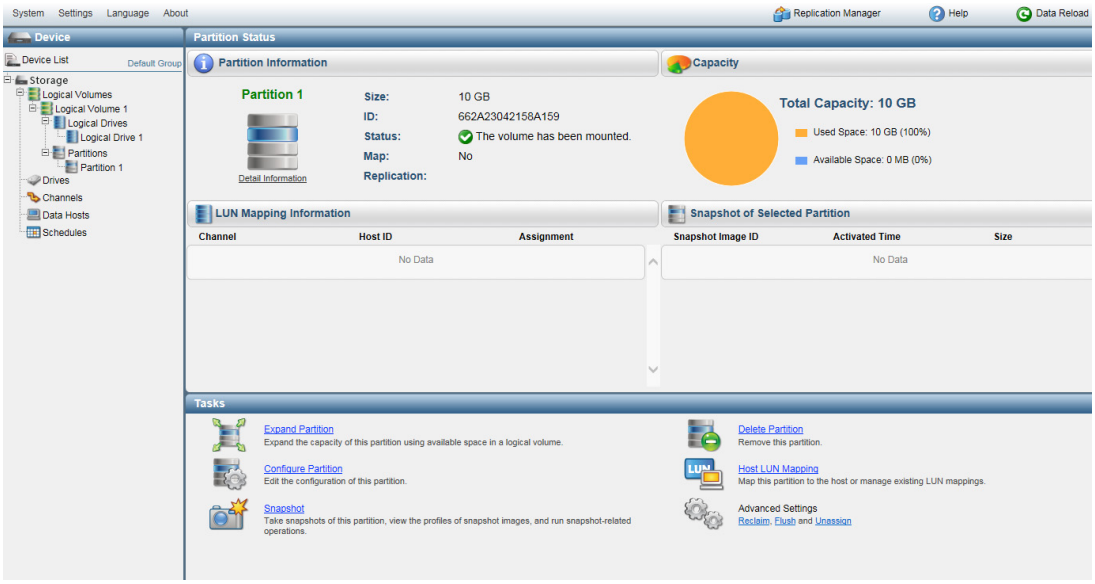
Deleting a partition will also delete all its data.

Go To	SANWatch Home > Device sidebar > Device List > device name > Logical Volumes > LV name > Partitions > Tasks section
Steps	Click on the Delete Partition link in the Tasks section.  Select the partition and click “Delete”.  A warning message will appear. Click “Yes” to proceed.

Chapter 11

Working with Partitions

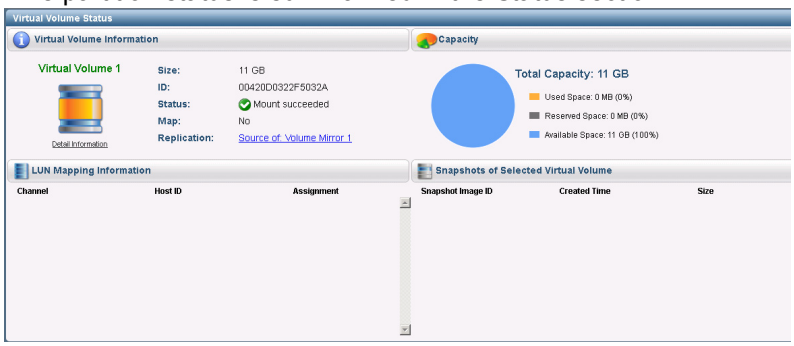
11.1 Introduction



This chapter explains how to view the status and parameters of a partition, expand or shrink a partition, configure host LUN, take snapshot images, and configure advanced settings, such as database flushing and unused space reclaiming.

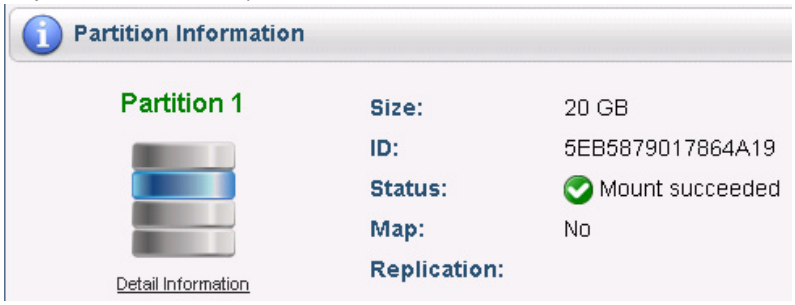
11.2 Viewing Partition Status

The status of each partition is summarized in the Partition Information page, ensuring users can quickly understand the configuration, performance, and storage capacity of any partition.

Go To	SANWatch Home > Device sidebar > Device List > device name > Logical Volumes > LV name > Partitions > partition name
Viewing the Partition Information	The partition status is summarized in the Status section. 

Partition Configurations

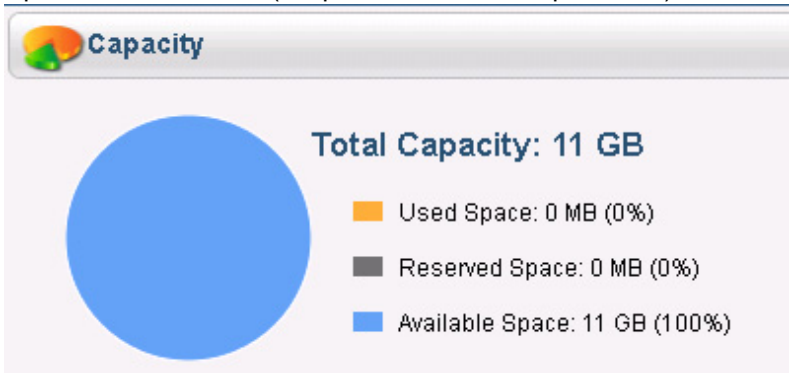
The basic partition configurations and overall system status are provided in the Partition Information section. From this page, users can obtain information regarding the size (capacity), ID, status, mapping, and replication settings of any partition (click on the link provided to access the Replication Manager and configure data replication functions).



Click on the Detail Information link below the partition icon to view additional parameters, such as Created Time, Current Tasks in Progress, and Storage Tiering Status. Click “Refresh” to update the status.

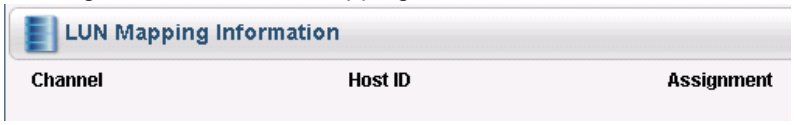
Capacity

This shows the amount and ratio of used (configured) and remaining (available) capacity. Users can also view the capacity used for specific data services (snapshots or remote replications).



LUN Mapping Information

Shows the current LUN mapping status (if available). Users can create or configure host LUN mapping from the Tasks section by clicking on the Host LUN Mapping icon.



Snapshot Information

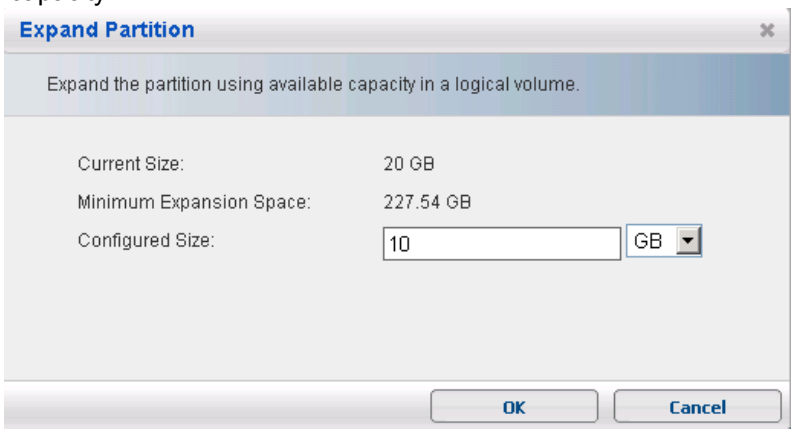
Lists the existing snapshot images taken of the partition. Users can create a new snapshot image from the Tasks section by clicking on the Snapshot icon.

11.3 Expanding Partitions

A partition can only be expanded if the partition or volume has available capacity.

Go To	SANWatch Home > Device sidebar > Device List > device name > Logical Volumes > LV name > Partitions > partition name > Tasks section
Steps	Click on the Expand Partition link in the Tasks section.

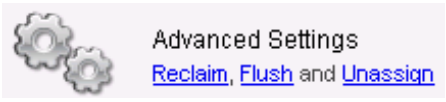
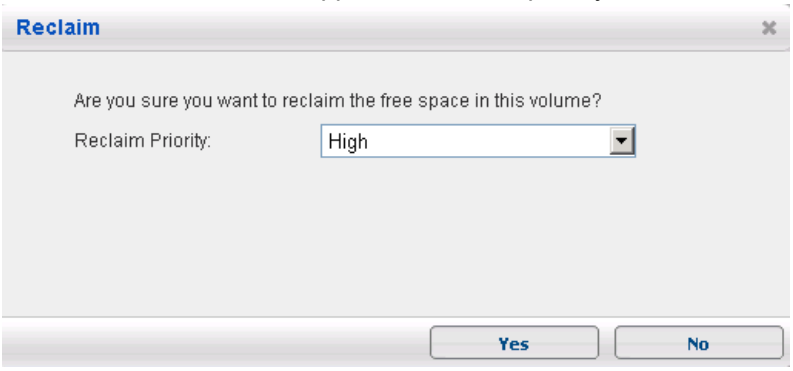
The expansion setting window will appear. Specify the expansion capacity.



After the expansion operation is complete, check that the size of the partition has increased by the specified amount.

11.4 Reclaiming Unused Partition Space

In thin-provisioned partitions, the space vacated by deleting data cannot be used unless manually reclaimed. The storage subsystem is aware of the actual host space usage and optimizes data allocation in the subsystem accordingly.

Note	■ To reclaim unused space, the partition must be mapped to the host. ■ The Partition Space Reclaim function is only supported in Microsoft Windows or Linux environments.
Go To	SANWatch Home > Device sidebar > Device List > device name > Logical Volumes > LV name > Partitions > partition name > Tasks section
Steps	Click on the Reclaim link in the Advanced Settings options in the Tasks section.  The Reclaim window will appear. Select the priority and click “OK”.  ■ High Priority: Reclaim will be efficiently processed but may affect system performance. ■ Normal Priority: Follows standard reclaim settings. The task may be processed more slowly but has a lower likelihood of affecting the system performance. If a reclaim operation is already in process, users must wait until the operation is complete, or stop and restart the process to run simultaneously with the second reclaim task.

11.5 Configuring Host LUN Maps

A partition is a division of the logical drive that appears as a physical drive to any host with access to that partition. To ensure that partitions are recognized when the host bus adaptors are reinitialized, each partition must be mapped to a host LUN.

Go To	SANWatch Home > Device sidebar > Device List > device name > Logical Volumes > LV name > Partitions > partition name > Tasks section
Mapping/Unmapping Host LUN	Before configuring LUN mapping, go to SANWatch Home > Device sidebar > Device List > device name > Logical Volumes > LV name > Partitions Click on the Help icon at the top-right corner and access the “Mapping/Unmapping Partitions or Virtual Volumes to Host” section for detailed instructions on LUN mapping configurations.

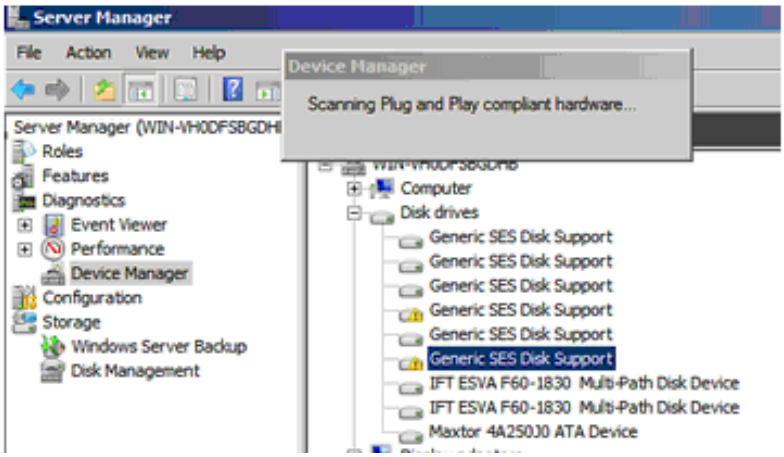
11.6 Managing LUN Mapping on the Host Side

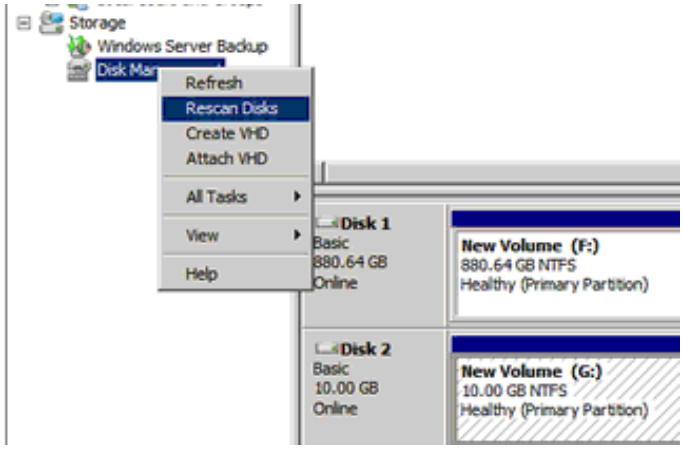
This section provides an example that demonstrates the process for configuring LUNs on the host side in a Windows, Linux, or Solaris environment.

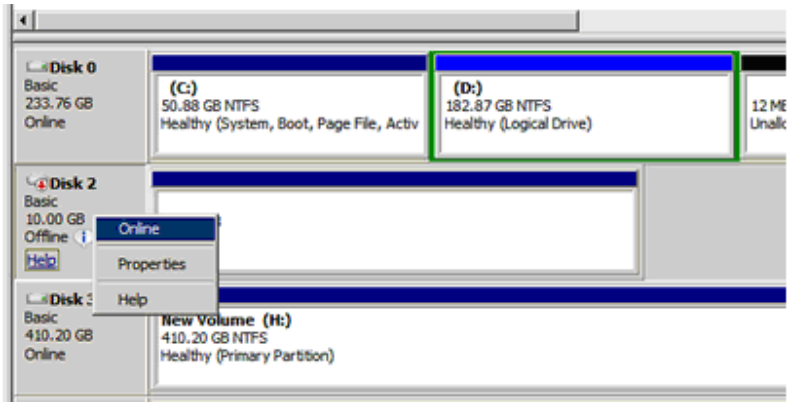
Notes	If LUNs cannot be located from the host side, change the type of SES device by doing the following: Go to SANWatch Home > Device sidebar > Device List > device name > Tasks section > System Settings > Host-side tab From the Peripheral Device Type drop-down menu, choose the “No Device Present (Type= 0x7F)” option. Restart the subsystem for the change to take effect.

Managing LUNs on Windows Server

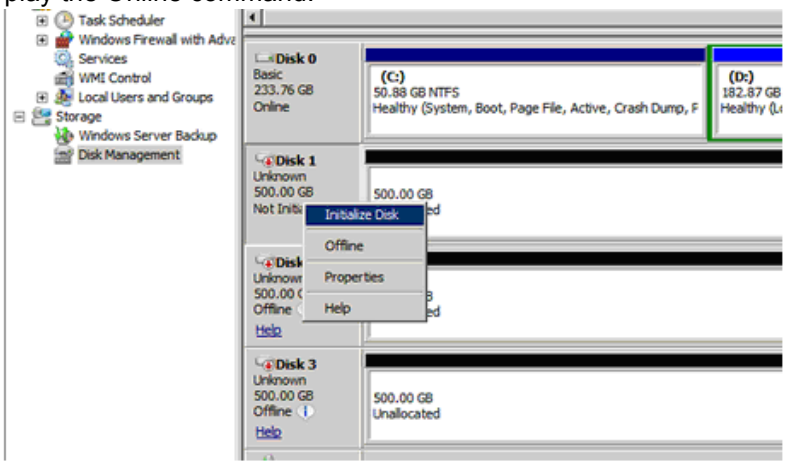
The screenshots shown below are of Windows Server 2008 R2, Server Manager. Once partitions are mapped, users can then scan, initialize, and format the partitions.



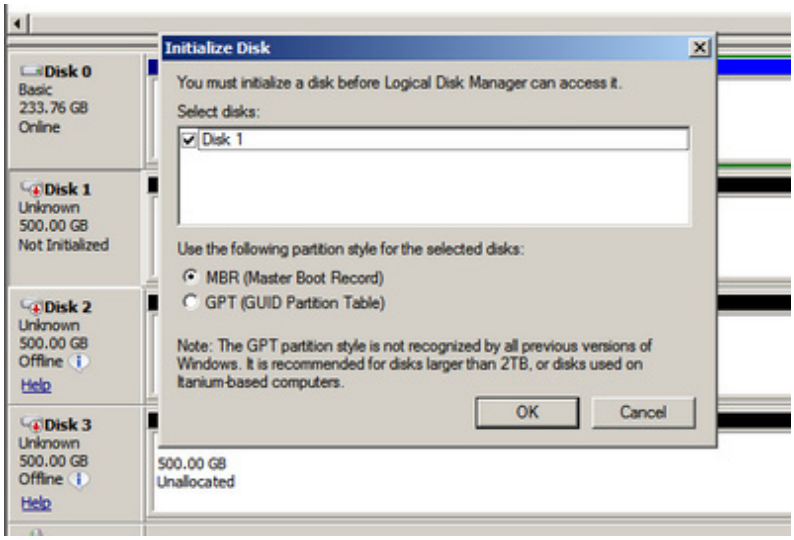




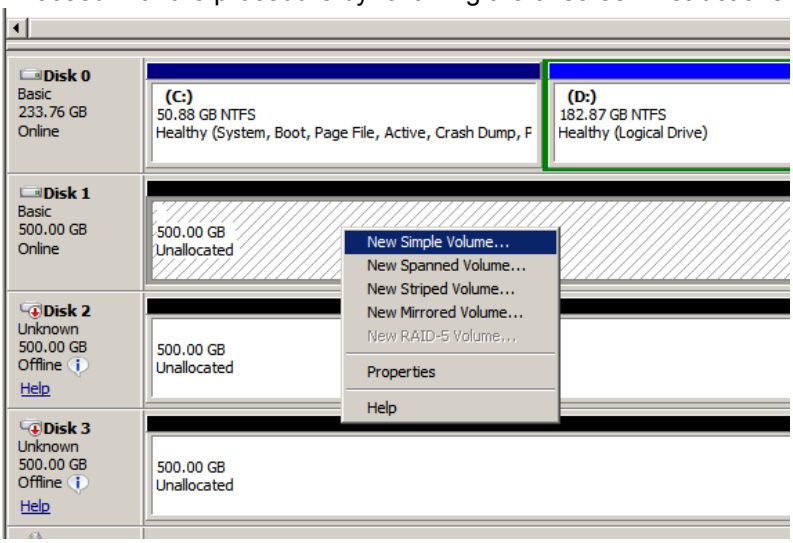
Left click on the mouse to select a disk, and then right click to display the Online command.



Next, right click the mouse to display and execute the Initialize Disk command.

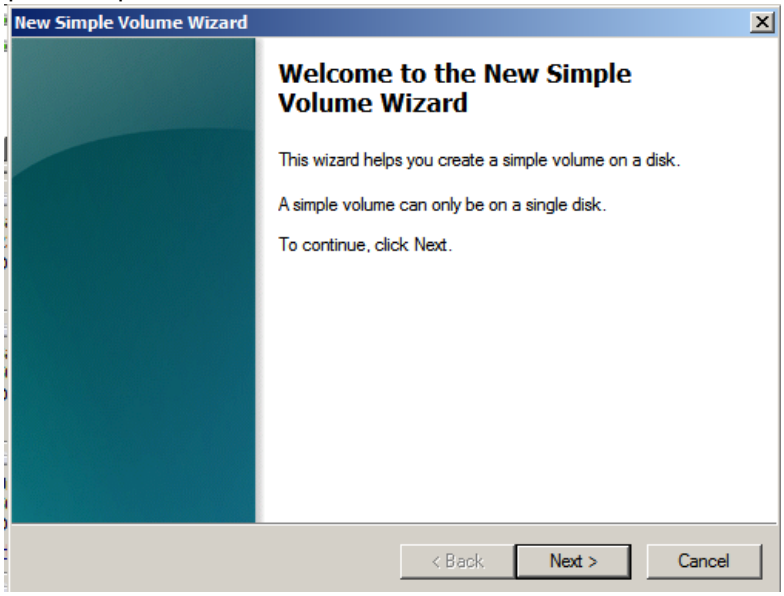


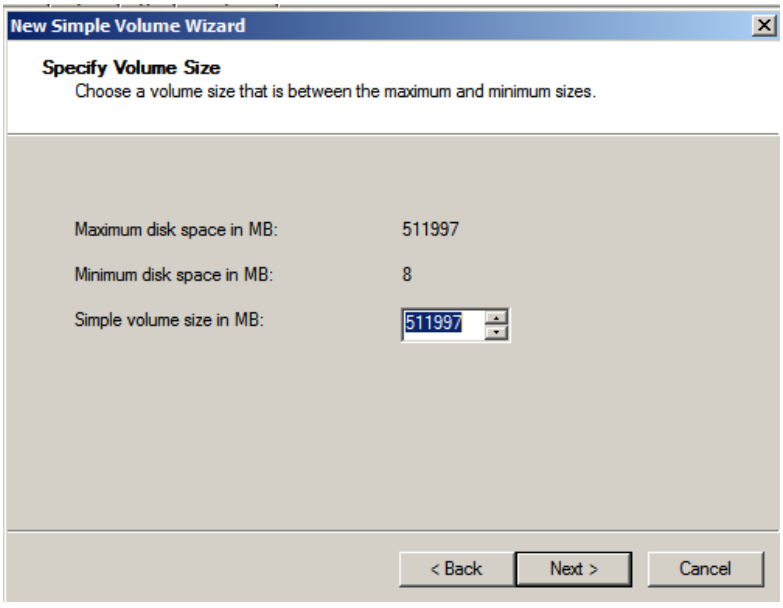
Proceed with the procedure by following the onscreen instructions.

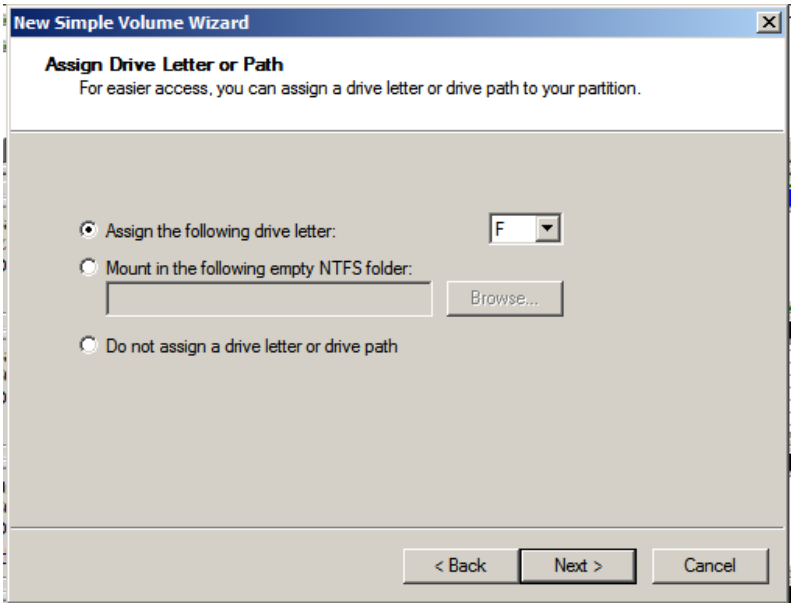


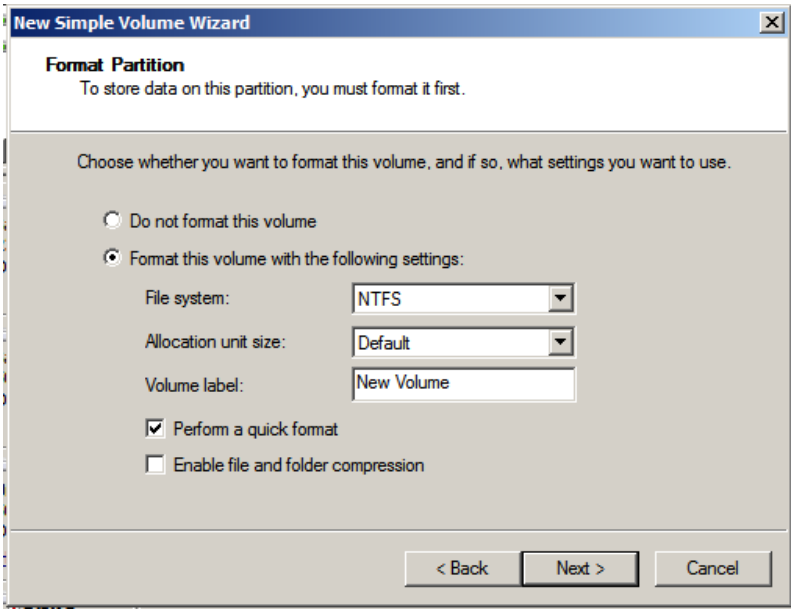
Right click the mouse on an unallocated partition to create a new simple partition.

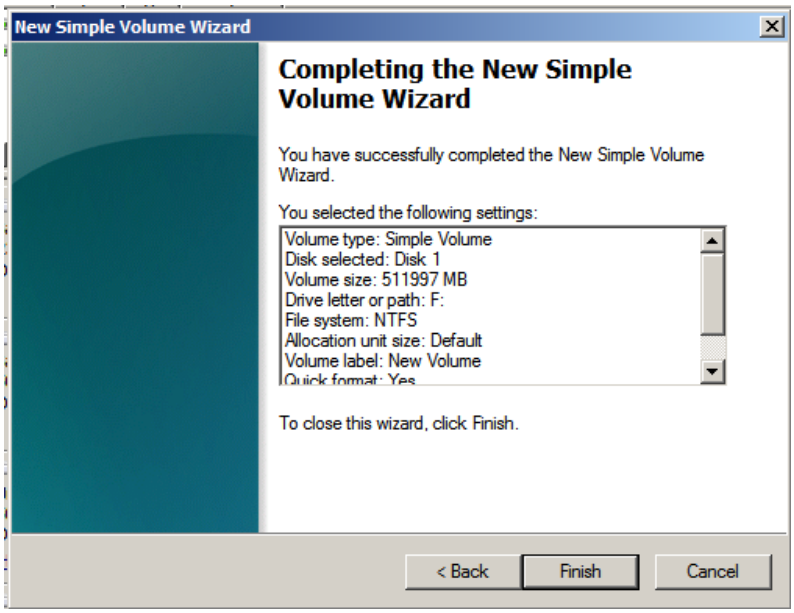
Follow the instructions provided by the Partition Wizard to complete the procedure.






New Simple Volume Wizard
Assign Drive Letter or Path
For easier access, you can assign a drive letter or drive path to your partition.
Assign the following drive letter:
F
Mount in the following empty NTFS folder:
Browse...
Do not assign a drive letter or drive path
< Back
Next >
Cancel


New Simple Volume Wizard
Format Partition
To store data on this partition, you must format it first.
Choose whether you want to format this volume, and if so, what settings you want to use.
Do not format this volume
Format this volume with the following settings:
File system:
NTFS
Allocation unit size:
Default
Volume label:
New Volume
Perform a quick format
Enable file and folder compression
< Back
Next >
Cancel


New Simple Volume Wizard
Completing the New Simple Volume Wizard
You have successfully completed the New Simple Volume Wizard.
You selected the following settings:
Volume type: Simple Volume
Disk selected: Disk 1
Volume size: 511997 MB
Drive letter or path: F:
File system: NTFS
Allocation unit size: Default
Volume label: New Volume
Quick format: Yes
To close this wizard, click Finish.
< Back
Finish
Cancel

Managing LUNs on Linux

Below are example shell commands for managing LUNs in a Linux environment.

```
[root@rh53-admin    ~]#    /etc/init.d/multipathd
restart
Stopping             multipathd             dae-
mon:                                [FAILED]
Starting             multipathd             dae-
mon:                                [  OK  ]
[root@rh53-admin ~]# cd /proc
[root@rh53-admin  proc]#  /etc/init.d/multipathd
restart
Stopping             multipathd             dae-
mon:                                [  OK  ]
Starting             multipathd             dae-
mon:                                [  OK  ]
[root@rh53-admin proc]#
[root@rh53-admin proc]# cat partitions
major minor  #blocks  name
   8     0   78150744 sda
   8     1     104391 sda1
   8     2   78043770 sda2
   8    16   20971520 sdb
   8    17   10482688 sdb1
   8    32   20971520 sdc
   8    33   10482688 sdc1
   8    48   20971520 sdd
   8    49   10482688 sdd1
   8    64   20971520 sde
   8    65   10482688 sde1
 253     0   73891840 dm-0
 253     1    4128768 dm-1
 253     2   20971520 dm-2
 253     3   10482688 dm-3
[root@rh53-admin proc]#
[root@rh53-admin ~]# ls
anaconda-ks.cfg  install.log         scsidev-2.37
Desktop             install.log.syslog   scsidev-
2.37.tar.tar
[root@rh53-admin ~]# cd /
[root@rh53-admin /]# ls
bin  dev  home  lost+found  misc  net  proc  sbin   srv  tftpboot  usr
boot  etc  lib  media     mnt   opt  root  selinux  sys  tmp     var
[root@rh53-admin /]# cdd home/
bash: cdd: command not found
[root@rh53-admin /]# cd home/
[root@rh53-admin home]# ls
1.4  peggy  SANWatch_2.1.a.06
[root@rh53-admin home]# cd 1.4/
[root@rh53-admin 1.4]# ls
README                        virtual1.4.tar.gz
```

```
Virtual_1.4_Release_Note.txt
Virtual_Linux_1.4_PVR.txt
[root@rh53-admin 1.4]# tar -xzf virtual1.4.tar.gz
[root@rh53-admin 1.4]# ls
README                Virtual_1.4_Release_Note.txt
Virtual_Linux_1.4_PVR.txt
virtual1.4  virtual1.4.tar.gz
[root@rh53-admin 1.4]# cd virtual1.4
[root@rh53-admin virtual1.4]# ls
INSTALL  LICENSE  objs  UNINSTALL  virtuald
[root@rh53-admin virtual1.4]# chmod 777 INSTALL
[root@rh53-admin virtual1.4]# ./INSTALL
                     DRIVER DISCLAIMER

PLEASE CAREFULLY READ THE FOLLOWING TERMS AND
CONDITIONS
BEFORE YOU USE OR LOAD THIS SOFTWARE:
```

1. This driver software is created by Advantech and is provided “as is” and Advantech cautions users to determine for themselves the suitability of the software version.
2. Advantech disclaims any express or implied warranty, relating to sale and/or use of Advantech products, including, liability or warranties relating to fitness for a particular purpose, merchantability or infringement of any patent, copyright or other intellectual property right.
3. Advantech assumes no responsibility for loss of use, loss of data, equipment malfunctions, or damages arising from the installation or use of this software. In no event is Advantech liable for any loss of profit or commercial damages including, but not limited to, indirect, special, incidental, consequential, or other damages.
4. Advantech reserves the right to revise or change the software at any time, without notice.

- Brands, product names and website addresses herein are trademarks or registered trademarks of their respective owners.
- If problems arise with the use of this software, please visit our website at www.advantech.com.tw or contact our technical support team at http://www.Advantech.com/support/.

By loading or using the software, you agree to the above disclaimer.

```
Accept? (Y/N): y

Install virtual Driver for Kernel  2.6.18-128.el5
./INSTALL: line 67: insserv: command not found
call depmod
Load module...
load virtual for dm
Starting virtual:
[root@rh53-peggy virtual1.4]# modinfo virtual
filename:        /lib/modules/2.6.18-128.el5/ker-
nel/drivers/virtual/virtual.ko
version:        1.4
author:         Advantech Inc.
license:        GPL
srcversion:     B890F953F061460C34430B9
depends:        scsi_mod
vermagic:       2.6.18-128.el5 SMP mod_unload 686
REGPARM 4KSTACKS gcc-4.1
parm:           masterTarget:charp
parm:           cacheCoverSizeInGB:int
parm:           cachePercentage:int
[root@rh53-peggy virtual1.4]# cd /proc
[root@rh53-peggy proc]# cat partitions
major minor  #blocks  name

   8     0   78150744 sda
   8     1     104391 sda1
   8     2   78043770 sda2
   8    16   20971520 sdb
   8    17   10482688 sdb1
   8    32   20971520 sdc
   8    33   10482688 sdc1
   8    48   20971520 sdd
   8    49   10482688 sdd1
   8    64   20971520 sde
   8    65   10482688 sde1
 253     0   73891840 dm-0
 253     1    4128768 dm-1
 253     2   20971520 dm-2
 253     3   10482688 dm-3
   8    80    2015231 sdf
   8    81    2015200 sdf1
 231     0   10482688 virtual0
[root@rh53-admin proc]# reboot

[root@rh53-admin ~]# cd /proc
[root@rh53-admin proc]# cat partitions
major minor  #blocks  name
```

```
   8     0   78150744 sda
   8     1     104391 sda1
   8     2   78043770 sda2
   8    16   31457280 sdb
   8    32   31457280 sdc
   8    48   31457280 sdd
   8    64   31457280 sde
 253     0   73891840 dm-0
 253     1    4128768 dm-1
 253     2   31457280 dm-2
 231     0   31457280 virtual0
[root@rh53-admin proc]#

[root@rh53-admin ~]# cd /proc
[root@rh53-admin proc]# cat partitions
major minor  #blocks  name

   8     0   78150744 sda
   8     1     104391 sda1
   8     2   78043770 sda2
   8    16   31457280 sdb
   8    32   31457280 sdc
   8    48   31457280 sdd
   8    64   31457280 sde
 253     0   73891840 dm-0
 253     1    4128768 dm-1
 253     2   31457280 dm-2
 231     0   31457280 virtual0
[root@rh53-admin  proc]#  mkfs  -t  ext.  /dev/
virtual0
mkfs.ext.: No such file or directory
[root@rh53-admin  proc]#  mkfs  -t  ext3  /dev/
virtual0
mke2fs 1.39 (29-May-2006)
Filesystem label=
OS type: Linux
Block size=4096 (log=2)
Fragment size=4096 (log=2)
3932160 inodes, 7864320 blocks
393216 blocks (5.00%) reserved for the super user
First data block=0
Maximum filesystem blocks=0
240 block groups
32768 blocks per group, 32768 fragments per group
16384 inodes per group
Superblock backups stored on blocks:
          32768, 98304, 163840, 229376, 294912,
819200, 884736, 1605632, 2654208,
        4096000
```

```
Writing inode tables: done
Creating journal (32768 blocks): done

This filesystem will be automatically checked every 20 mounts or
180 days, whichever comes first.  Use tune2fs -c or -i to override.
[root@rh53-admin proc]#
[root@rh53-admin proc]# mount /dev/virtual0 /mnt/vv
[root@rh53-admin proc]# cd /mnt\/vv
[root@rh53-admin vv]# ls
lost+found
[root@rh53-admin vv]#

==========

[root@rh53-admin ~]# cd /proc
[root@rh53-admin proc]# cat partitions
major minor  #blocks  name

   8     0   78150744 sda
   8     1     104391 sda1
   8     2   78043770 sda2
   8    16   41943040 sdb
   8    32   41943040 sdc
   8    48   41943040 sdd
   8    64   41943040 sde
 253     0   73891840 dm-0
 253     1    4128768 dm-1
 253     2   41943040 dm-2
 231     0   41943040 virtual0
[root@rh53-admin proc]# fdisk

Usage: fdisk [-l] [-b SSZ] [-u] device
E.g.: fdisk /dev/hda  (for the first IDE disk)
  or: fdisk /dev/sdc  (for the third SCSI disk)
   or: fdisk /dev/eda  (for the first PS/2 ESDI drive)
  or: fdisk /dev/rd/c0d0  or: fdisk /dev/ida/c0d0 (for RAID devices)
  ...
[root@rh53-admin proc]# fdisk -l

Disk /dev/sda: 80.0 GB, 80026361856 bytes
255 heads, 63 sectors/track, 9729 cylinders
Units = cylinders of 16065 * 512 = 8225280 bytes
```

```
   Device Boot      Start         End      Blocks
Id  System
/dev/sda1   *           1          13      104391
83  Linux
/dev/sda2              14        9729    78043770
8e  Linux LVM

Disk /dev/sdb: 42.9 GB, 42949672960 bytes
64 heads, 32 sectors/track, 40960 cylinders
Units = cylinders of 2048 * 512 = 1048576 bytes

Disk /dev/sdb doesn't contain a valid partition
table

Disk /dev/sdc: 42.9 GB, 42949672960 bytes
64 heads, 32 sectors/track, 40960 cylinders
Units = cylinders of 2048 * 512 = 1048576 bytes

Disk /dev/sdc doesn't contain a valid partition
table

Disk /dev/sdd: 42.9 GB, 42949672960 bytes
64 heads, 32 sectors/track, 40960 cylinders
Units = cylinders of 2048 * 512 = 1048576 bytes

Disk /dev/sdd doesn't contain a valid partition
table

Disk /dev/sde: 42.9 GB, 42949672960 bytes
64 heads, 32 sectors/track, 40960 cylinders
Units = cylinders of 2048 * 512 = 1048576 bytes

Disk /dev/sde doesn't contain a valid partition
table

Disk /dev/dm-2: 42.9 GB, 42949672960 bytes
255 heads, 63 sectors/track, 5221 cylinders
Units = cylinders of 16065 * 512 = 8225280 bytes

Disk /dev/dm-2 doesn't contain a valid partition
table
[root@rh53-admin proc]# cd /home/
[root@rh53-admin home]# ls
1.4  peggy  SANWatch_2.1.a.06
[root@rh53-admin home]# cd 1.4/
[root@rh53-admin 1.4]# ls
README               Virtual_1.4_Release_Note.txt
Virtual_Linux_1.4_PVR.txt
virtual1.4  virtual1.4.tar.gz
[root@rh53-admin 1.4]# cd virtual1.4
[root@rh53-admin virtual1.4]# ls
INSTALL  LICENSE  objs  UNINSTALL  virtuald  vir-
tual.ko
```

```
[root@rh53-admin virtual1.4]# chmod 777 UNINSTALL
[root@rh53-admin virtual1.4]# ./UNINSTALL
uninstall     /lib/modules/2.6.18-128.el5/kernel/
drivers/virtual
[root@rh53-admin virtual1.4]# cd /pro
bash: cd: /pro: No such file or directory
[root@rh53-admin virtual1.4]# cd /proc
[root@rh53-admin proc]# cat partitions
major minor  #blocks  name
   8     0   78150744 sda
   8     1     104391 sda1
   8     2   78043770 sda2
   8    16   41943040 sdb
   8    32   41943040 sdc
   8    48   41943040 sdd
   8    64   41943040 sde
 253     0   73891840 dm-0
 253     1    4128768 dm-1
 253     2   41943040 dm-2
[root@rh53-admin proc]#
```

Managing LUNs on Solaris (Enabling iSCSI initiators)

- **Required Solaris iSCSI Software and Hardware**

Solaris iSCSI software and devices

- The Solaris10 1/06 or later release for Solaris iSCSI initiator software
- The Solaris10 8/07 or later release for Solaris iSCSI target software

The following software packages:

- SUNWiscsir–Sun iSCSI Device Driver (root)
- SUNWiscsiu–Sun iSCSI Management Utilities (usr)
- SUNWiscsitgtr–Sun iSCSI Target Device Driver (root)
- SUNWiscsitgtu–Sun iSCSI Target Management Utilities (usr)
- Any supported NIC
- To verify the availability of initiator and target service:
- Become super user.
- Verify that the iSCSI software packages are installed.
- `# pkginfo SUNWiscsiu SUNWiscsir`
- System SUNWiscsir Sun iSCSI Device Driver (root)
- System SUNWiscsir Sun iSCSI Management Utilities (usr)
- Verify that you are running a Solaris10 1/06 or later release.
- Confirm that your TCP/IP network is setup by telneting an iSCSI target using port 3260.

- Configure iSCSI Target Discovery
  Become super user.
  To configure the target device to be discovered dynamically or statically, see the instructions below.
  Configure the device for dynamic discovery (SendTargets).
  - `# iscsiadm add discovery-address10.0.0.1:3260`
  - The iSCSI connection is not initiated until the discovery method is enabled. See the next step.

  Configure the device for static discovery.
  - `# iscsiadm add static-config eui.5000ABCD78945E2B,10.0.0.1`
  - The iSCSI connection is not initiated until the discovery method is enabled. See the next step

  Enable the iSCSI target discovery method by executing one of the following:
  - For devices configured to be dynamically discovered (SendTargets), enable the Send Targets discovery method.
  - `# iscsiadm modify discovery --sendtargets enable`
  - For devices configured to be statically discovered, enable the static target discovery method.
  - `# iscsiadm modify discovery --static enable`

  Create iSCSI device links for the local system.
  - `# devfsadm -i iscsi`

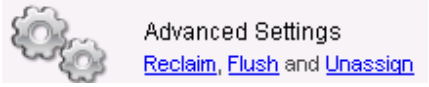
11.7 Configuring Out-of-Band Flushing Using a DB Flush Agent

If data is held in database forms, all data must be flushed into the storage subsystem before any backup operation. The DB Flush module in SANWatch supports automatic flushing.

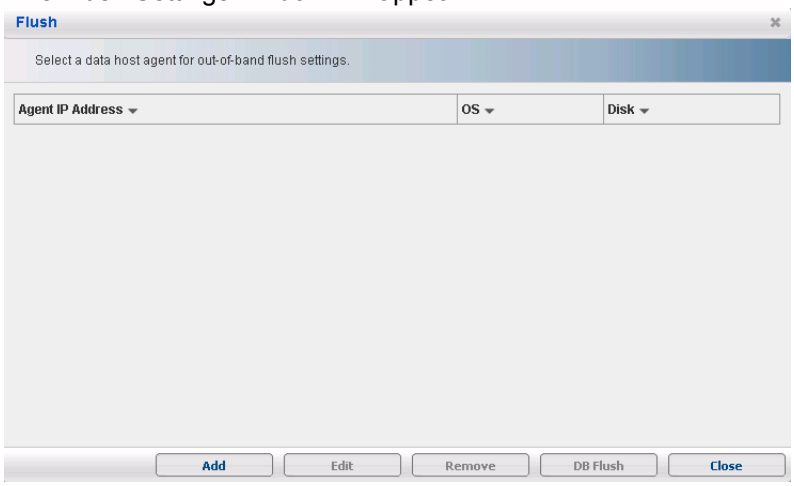
DB Flush is compatible with the following databases:

- SQL
- Microsoft Exchange
- Oracle

For more information regarding configuring out-of-band flushing on the host side, refer to the section titled “Configuring Out-of-Band Flushing.”

Go To	SANWatch Home > Device sidebar > Device List > device name > Logical Volumes > LV name > Partitions > Tasks section
Step 1: Activating the DB Flush Agent	Click on the Flush link in the Tasks section. 

The Flush Settings window will appear.

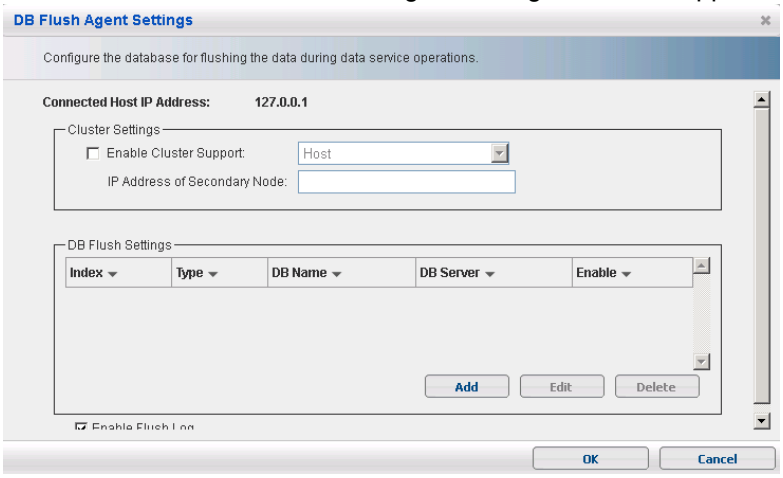


Click “Add” to add a setting. In the Flush Agent Setting, enter the host agent IP address, select the OS type, and enter the following in the Disk field:

- For Windows, the Disk ID (the “1” in “Disk 1”, for example)
- For Linux, /dev/ID (such as /dev/sdb in the above case)
- For Solaris, /dev/dsk/ID (such as /dev/dsk/sdb in the above case)

A list of flush agents will appear. Select the target item for out-of-band flushing.

Click “DB Flush”. The DB Flush Agent setting screen will appear.

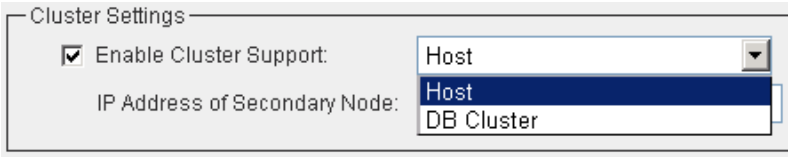


Step 2: Enabling Database Clustering

Changing the database clustering settings will reset other DB Flush Agent settings.

Database clustering refers to the storing of sequential rows of a database table on a disk. This boosts database performance for server-centric database systems because the server can perform database operations by directly accessing the disk.

To enable database clustering, check the Enable Cluster Support checkbox and select “DB Cluster”. To add another node, select “Host” and enter the IP address.



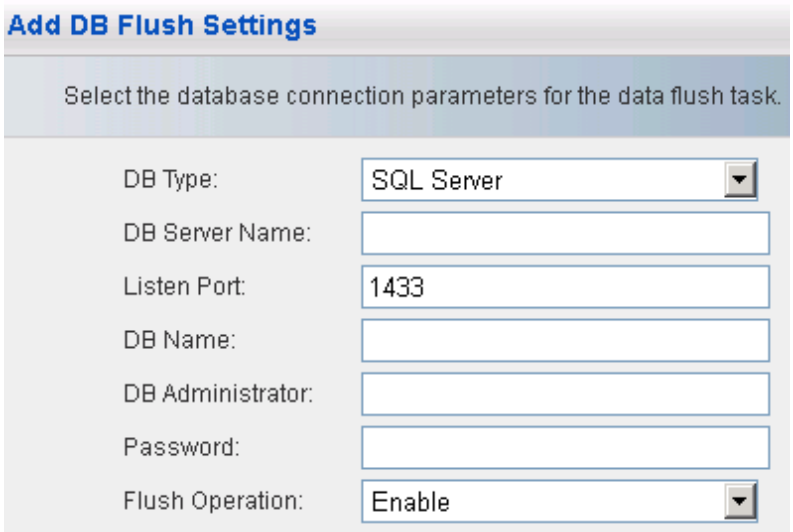
Step 3: Enabling Flush Log

Enable the flush log to initiate the following:

- Event logs for clustered nodes to be stored on the machine.
- Events to be reported in the following locations:
  Windows: Event Viewer
  Linux: /var/log/messages
  Solaris: /var/adm/messages

Step 4: Configuring Database Flush Settings

Click “Add”. The DB Flush setting window will appear.



Enter the parameters and click “OK”.

The new database flush setting will appear in the DB Flush Agent screen.

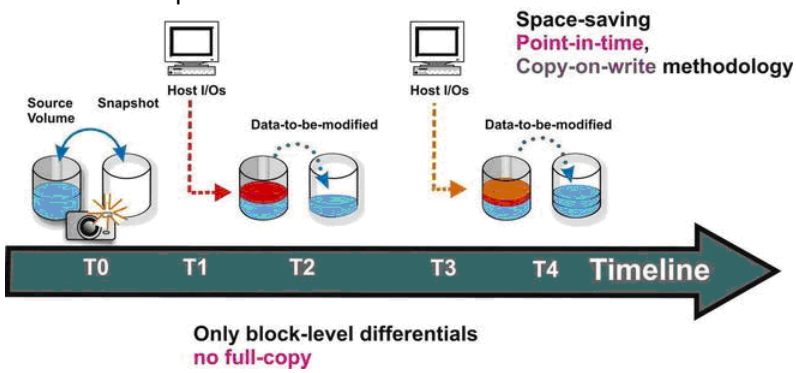
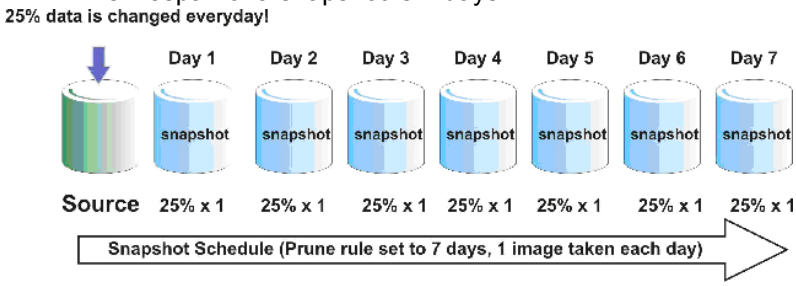
Click “OK” and close DB Flush Agent.

Parameters	**DB Type**	Specifies the database from Oracle, SQL Server, and MS Exchange.
	DB Server Name	Specifies the user-defined name of the database server.
	DB Listen Port	Specifies the network port (default 1433) that is monitored by the database listener (a software that manages the network traffic between the database and client).
	DB Name	Specifies the user-defined name of the database.
	DB Administrator	Specifies the database administrator user name. Enter a system administrator login name. Access permission for the SA name can be disabled when configuring the database security level. By disabling “SA” access, users must login as the Windows Administrator to access a database system.
	DB Password	Specifies the database password.
	Enable DB Flush	Allows database flushing of cache memory to a local file before taking snapshot images.

Chapter 12

Working with Snapshots

12.1 General Snapshot Rules

Number of Snapshots	■ The maximum number of snapshots in a partition is 1024. ■ The maximum number of snapshots in a logical volume is 16000. ■ The maximum number of online snapshots (snapshot images mapped to hosts) is 1024.
Space Concerns	■ Space for storing snapshot images is automatically allocated by the logical volume. ■ When a logical volume or pool is created in SANWatch, 30% of the available space will be reserved. The system notifies users when more than 70% of the available space is filled. Ensure there is always sufficient storage space. ■ The space required for snapshots depends on how frequently data is updated.  ■ Use the prune rule option in the snapshot scheduler window to limit the maximum number and lifespan of snapshots.
Database Concerns	When taking snapshots for database applications such as Oracle, use “Group Snapshot” in the scheduler. Users can select multiple source partitions when creating a snapshot schedule. Using Group Snapshots ensure the integrity of backup data between database and log partitions.
What to Evaluate When Planning	When planning snapshots, evaluate the following concerns: ■ How many data changes will occur within the time frame? ■ How many snapshots may need to be recovered? ■ How long can data losses be tolerated (= how frequently are snapshots needed)?
Case Study: Calculating the Required Space	Here the required data space is calculated based on the following assumptions: ■ 25% of data is expected to change every day. ■ A snapshot is taken every day. ■ 7 snapshots are necessary for data protection. ■ The lifespan of a snapshot is 7 days.  The required logical partition storage space measures (25% x 1) + (25% x 1) + (25% x 1) + (25% x 1) + (25% x 1) + (25% x 1) + (25% x 1) = 1.75 times the source partition size.

Pruning vs. Purging Snapshot Images

For effective use of the storage space, two mechanisms known as pruning and purging are provided for automatically removing older snapshot images.

Pruning

Pruning refers to removing old snapshot images once certain threshold specifications are reached or the retention period is expired. Pruning occurs according to the threshold conditions, regardless of the availability of storage space. Pruning can be configured when creating snapshot images.

Purging

Purging refers to removing old snapshot images when the used storage space reaches the threshold (i.e., the available space is insufficient). Purging continues until the used storage space is below the threshold setting or all snapshot images are deleted or marked as invalid (the original data will always remain intact). Purging can be configured when creating notification thresholds for virtual pools.

Purging takes priority over pruning and is considered a critical issue for the overall system. When purging occurs, users can apply either of the following actions:

- Increase the size of the logical volume or pool to expand the available storage space
- Remove unnecessary data from existing LVs or reconfigure LVs for more efficient storage
- Increase the pruning threshold (not recommended)

If a snapshot image is marked as invalid during a purging operation, the image can no longer be used and must be deleted immediately.

12.2 Taking Snapshots

Go To

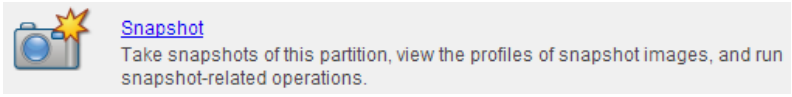
SANWatch Home > Device sidebar > Device List > device name > Logical Volumes > LV name > Partitions > Tasks section

Snapshots can also be executed according to a schedule. For more information, visit the following location and click the Help icon at the top-right corner:

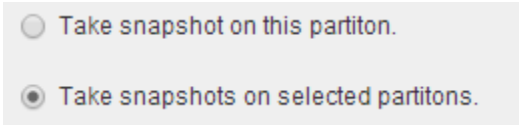
SANWatch Home > Device sidebar > Device List > device name > Schedules

Steps

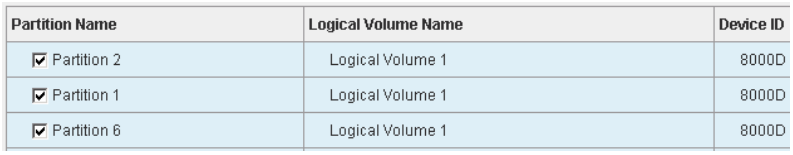
Click on the Snapshot link in the Tasks section.



Select the partition for taking snapshots



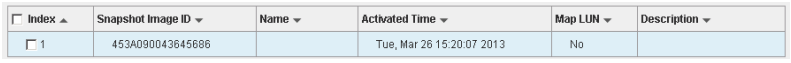
To select other partitions, click the “Take snapshots on selected partitions” option and specify the partition(s) to take snapshot images of.



Partition Name	Logical Volume Name	Device ID
Partition 2	Logical Volume 1	8000D
Partition 1	Logical Volume 1	8000D
Partition 6	Logical Volume 1	8000D

Click “Take Snapshot” to execute.

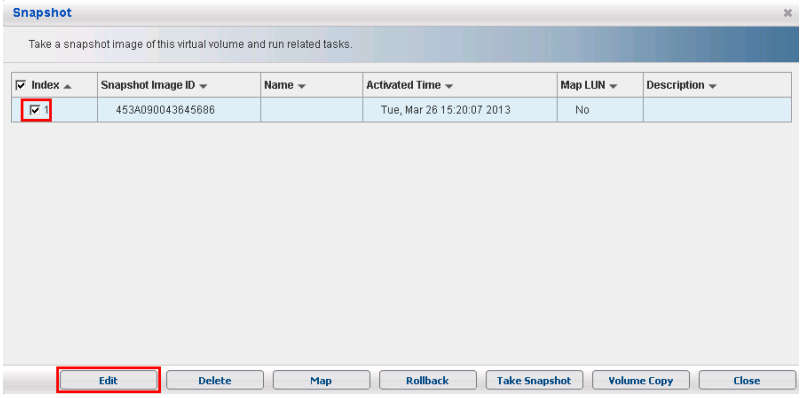
The snapshot image will be taken immediately and the result will appear in the list.



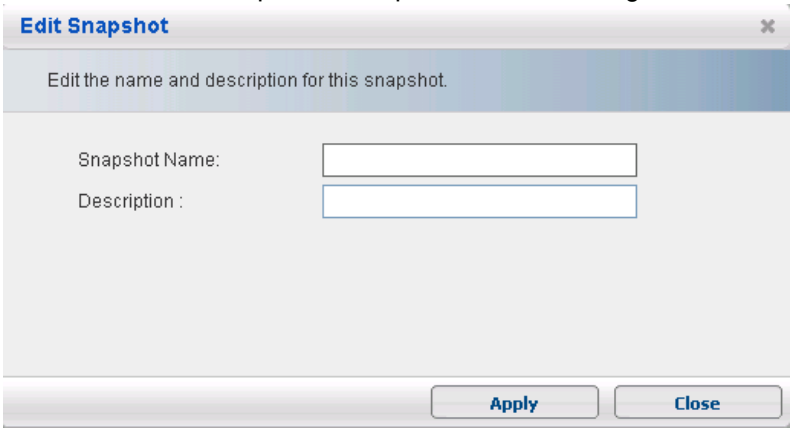
Index	Snapshot Image ID	Name	Activated Time	Map LUN	Description
1	453A090043645686		Tue, Mar 26 15:20:07 2013	No	

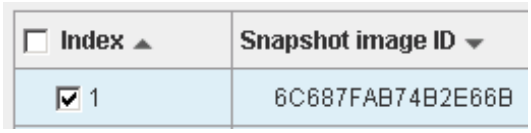
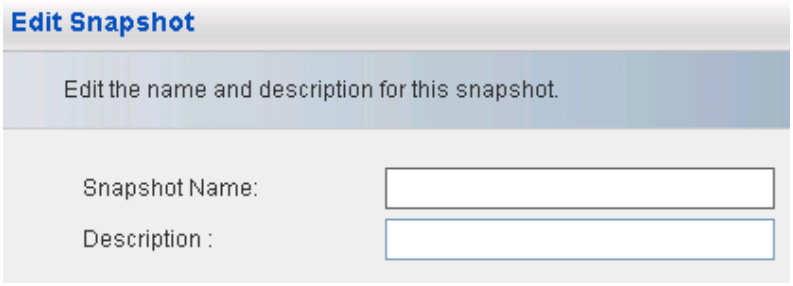
Configuring Snapshots

Select a snapshot image and click “Edit”.



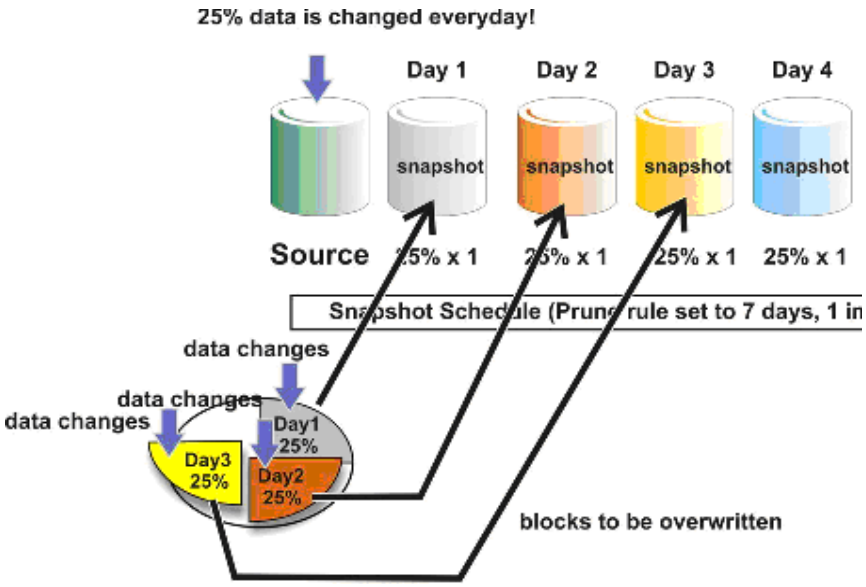
The name and description of snapshots can be changed.



Configuring Snapshots	Navigate to the partition with the snapshots for modification, and click “Snapshot” in the Tasks section. Click “Next”. Check the box next to the snapshot image ID, and click “Edit”.  Edit the name and description of the snapshot image and click “OK”. 
Deleting Snapshots	Select the partition with the snapshots for modification, and click “Snapshot” in the Tasks section. Click “Next”. Check the box next to the snapshot image ID, and click “Edit”. Click “Delete” and then click “Yes”.
Note	Taking multiple snapshots simultaneously is useful for database applications that require uniform backups of multiple partitions.

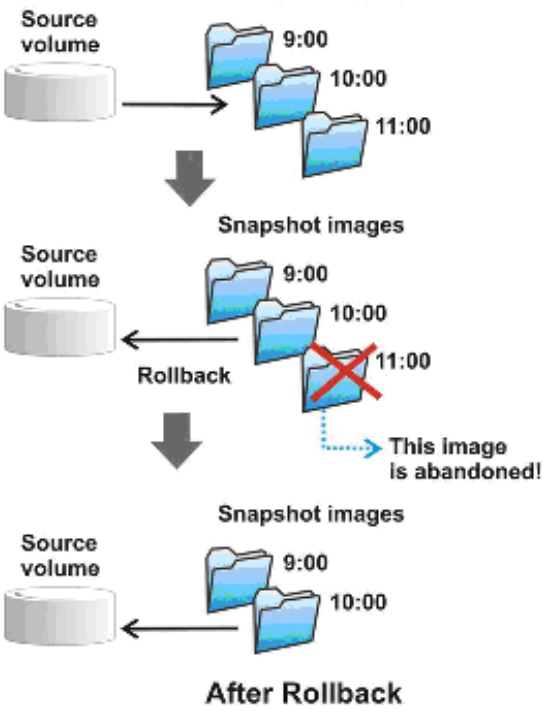
12.3 Recovering a Source Partition from a Snapshot (Rollback)

If a source partition is rolled back to a specific state, all images must remain intact because data is stored in sequential snapshot images. The example below shows a source partition with three daily snapshots. To rollback to Day 1, all three images must be intact and available for reference in order to reconstruct past data.



Go To	SANWatch Home > Device sidebar > Device List > device name > Logical Volumes > LV name > Partitions > partition name > Tasks section
Steps	If a partition is mapped, the partition must be unmapped before it can be rolled back using a snapshot image.
	Click “Snapshot” in the Tasks section. Click “Next” and select the snapshot image to rollback to. Click “Rollback”, and click “Yes” in the confirmation dialog. The source partition will be rolled back.
	The process can take up to several minutes depending on the size of the source partition.
	Users can re-establish host LUN mappings for the source partition.

Note on Rollback Timing	If a snapshot image is used to rollback a source partition, any and all snapshot images taken after that image will be erased. In the example below, the snapshot image taken at 11:00 will be erased because the source partition it referred to was replaced by an image taken at 10:00.



12.4 Mapping a Snapshot Image to the Host

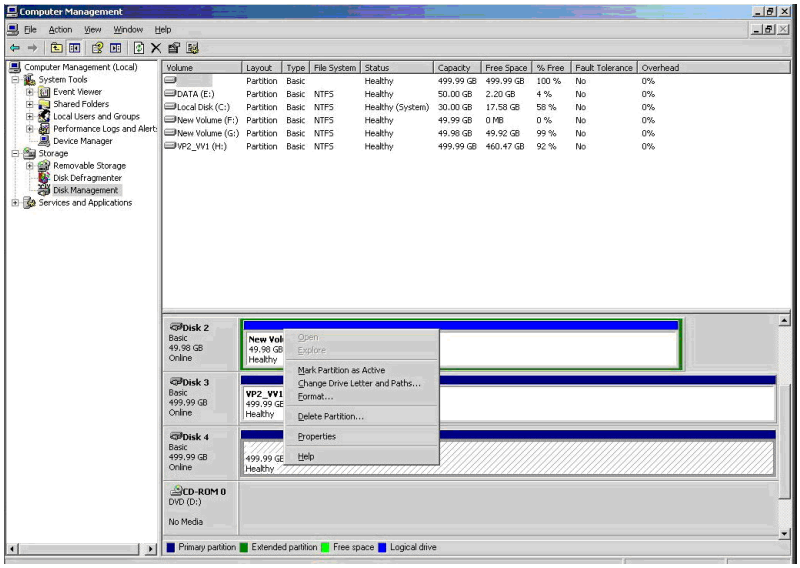
The mapping process is twofold. After mapping a snapshot in SANWatch, users must assign a drive letter to the snapshot in the host computer environment.

Go To	SANWatch Home > Device sidebar > Device List > device name > Logical Volumes > LV name > Partitions > partition name > Tasks section
Steps	Click “Snapshot” in the Tasks section. Click “Next” and check the box next to the snapshot image ID. Click “Map”. The Host LUN Mapping window will appear. The process is the same as that for mapping a partition to a host. For detailed instructions, go to ■ SANWatch Home > Device sidebar > Device List > device name > Logical Volumes > LV name > Partitions Click the Help icon at the top-right corner, and search for “Mapping/Unmapping Partitions or Virtual Volumes to Host”.

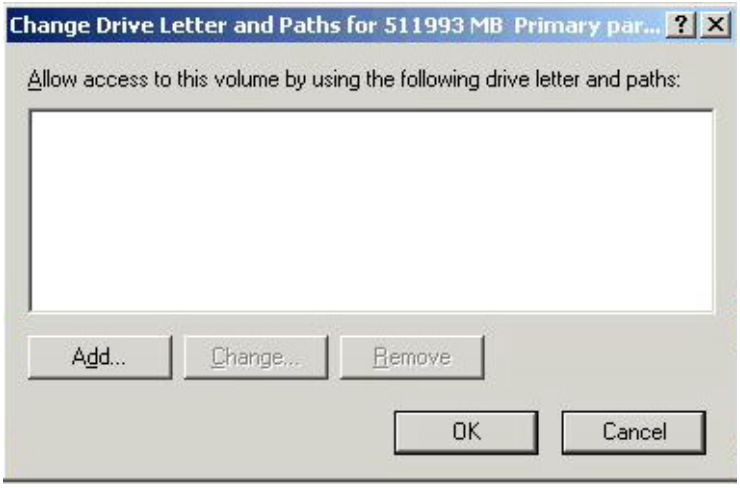
Assigning a Drive Letter to the Snapshot

Before accessing data in the snapshot, the snapshot must be assigned a drive letter. The procedures for assigning a drive letter in a Windows Server environment, are provided below.

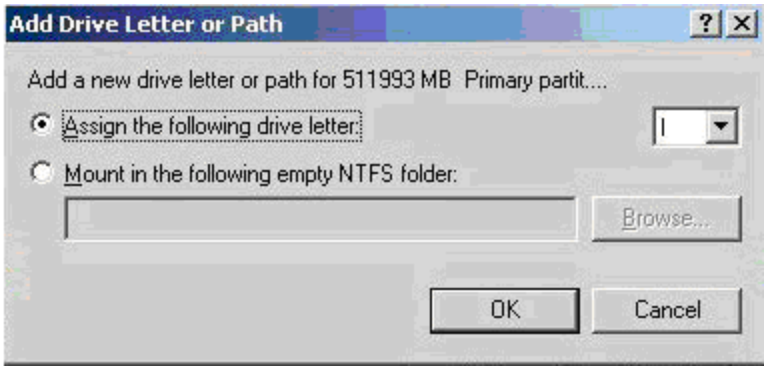
1. When an image is mapped, the image appears as a new drive.



2. Right click on the disk and select the “Change Drive Letters and Path” option.
3. Click “Add” in the prompt.



4. Select the drive letter and click “OK”.

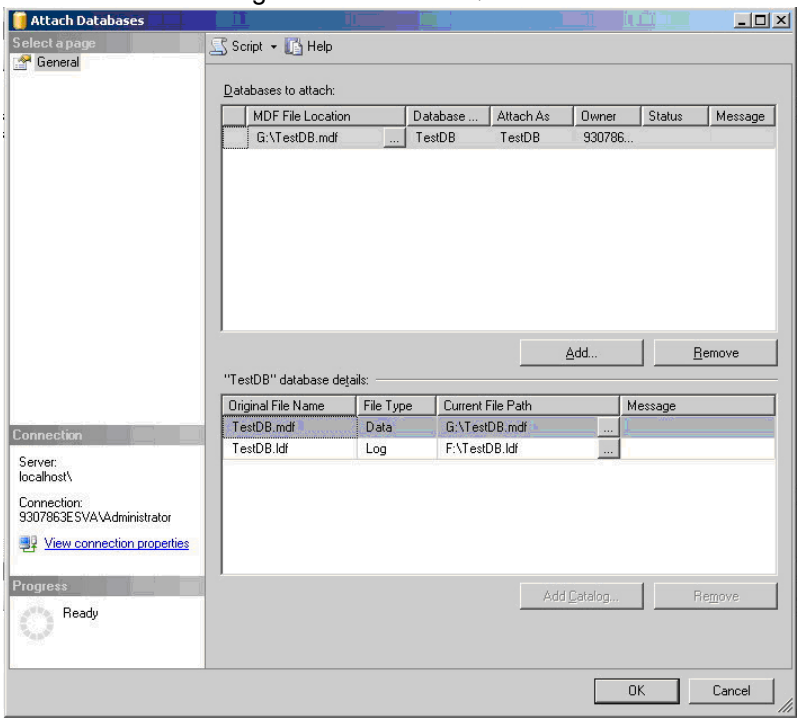


5. The data in the snapshot should be accessible.

12.5 Recovering a Database Volume from Grouped Snapshots

Background

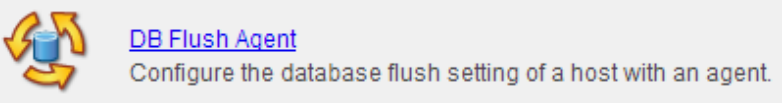
The procedure below is based on a simple configuration. That is, two virtual volumes presented to the host, one as a data volume and the other as a log volume for an SQL server.



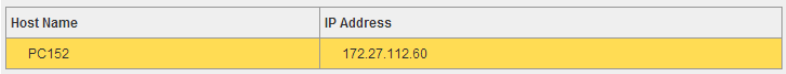
Step 1: Configuring SANWatch

Go to SANWatch Home > Device sidebar > Device List > device name > Data Hosts > Tasks section

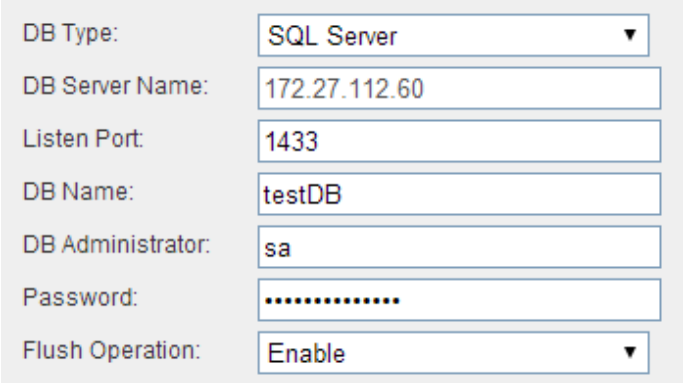
Click “DB Flush Agent”.



Select a host for configuring database flushing, and click “Next”.

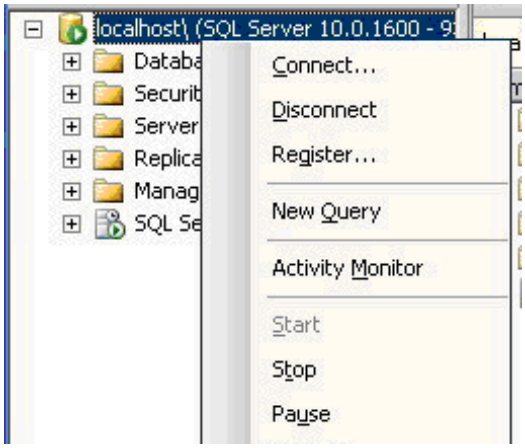


Click “Add”. A configuration prompt will appear.



Configure the parameters, click “OK”, and wait for the configuring progress to complete.

Open SANWatch Manager and create a snapshot schedule.

Parameters	**DB Type**	Select the database type from Oracle, SQL, and MS Exchange.
	DB Server Name	Shows the IP address of the in-band server.
	Listen Port	Specifies the database listen port. A default value is given.
	DB Name	Specifies the name of the database.
	DB Administrator	Specifies the name of the database administrator. A default value is given.
	Password	Specifies the password for the database administrator.
	Flush Operation	Flushes the database when a snapshot image is taken. To enable this procedure, check this option.
Step 2: Rollback Snapshot Images	Here the database is assumed to be corrupted and must be recovered to a certain point. Stop the database service. In Microsoft SQL server, right click and select “Stop”.  In SANWatch Manager, unmap the database volume. Refer to the section titled “Recovering a Source Volume from a Snapshot (Rollback)” for more information.	

12.6 Creating a Volume Copy from a Snapshot Image

To create a volume copy, at least one snapshot image must be available.

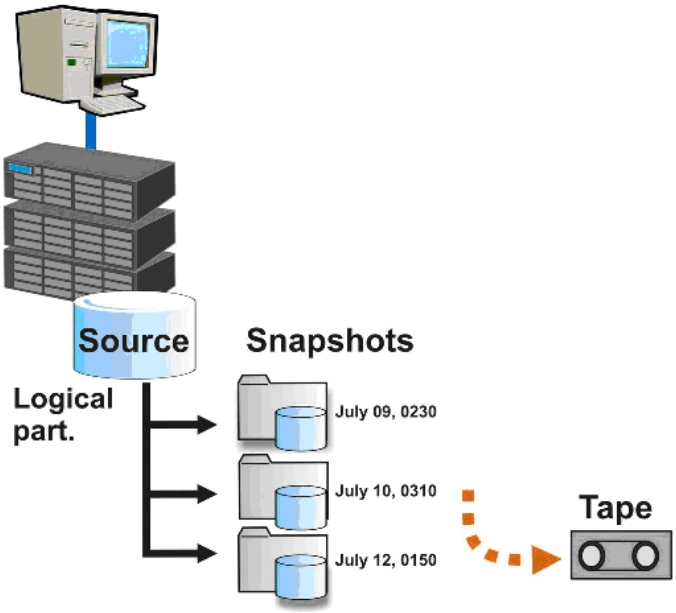
Go To	SANWatch Home > Device sidebar > Device List > device name > Logical Volumes > LV name > Partitions > partition name > Tasks section
Steps	Click “Snapshot” in the Tasks section. Click “Next”, check the box next to the snapshot image ID, and click “Volume Copy”. Follow the instructions.

12.7 Making Backups of Snapshot Images

This section explains the three methods for making backups of snapshot images using tape storage and/or volume copy/mirror functions.

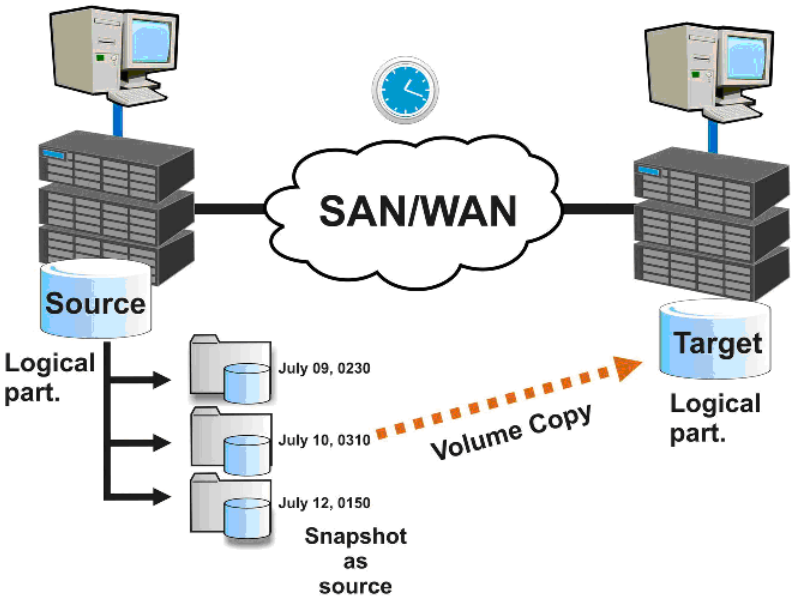
Using Tape Backup

Snapshots are saved to tape media during system low time.



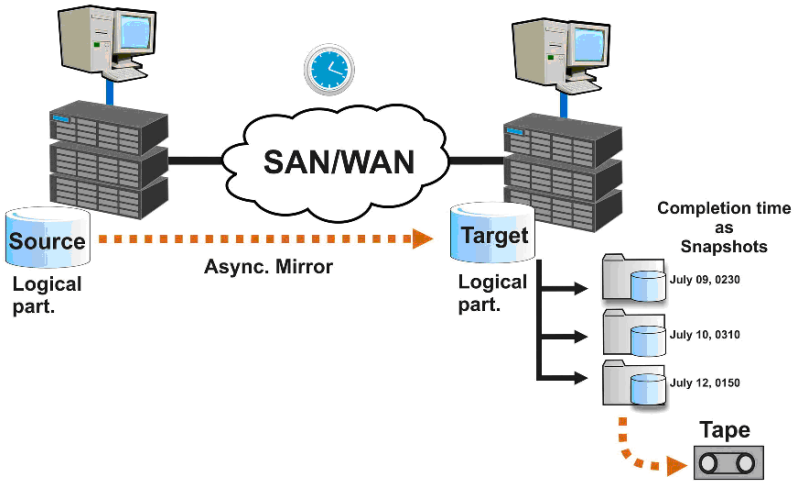
Using Volume Copy

After snapshot images are taken, the images are copied to another location using the volume copy function.



Using an Asynchronous Mirror

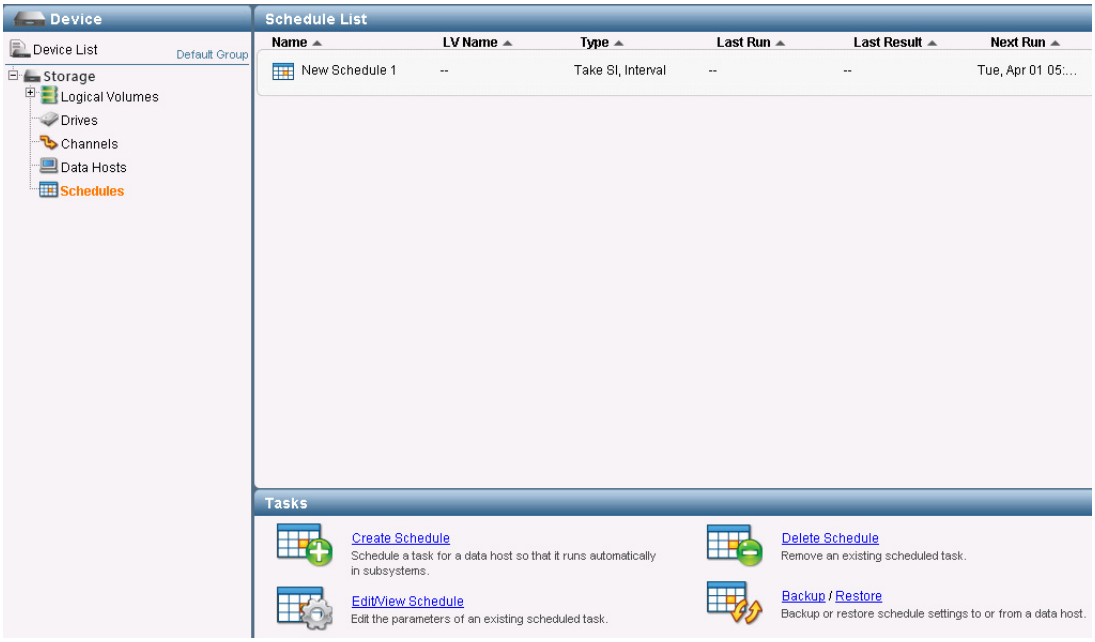
Snapshots can be saved (mirrored) to a remote location using the asynchronous mirror function. The other backup methods, such as tape media, can be used in remote site situations.



Chapter 13

Working with Schedules

13.1 Introduction

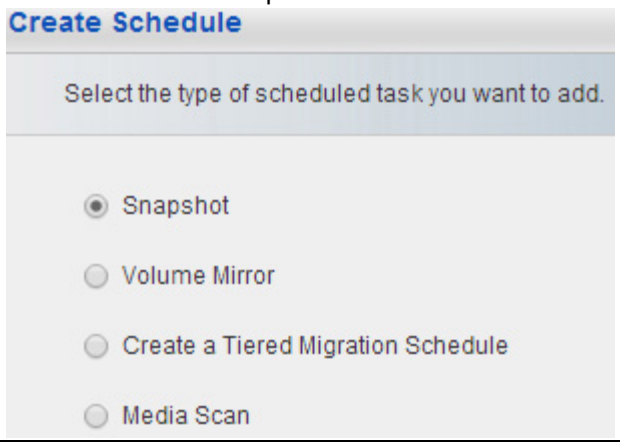


This chapter describes how to create a scheduled task (snapshot, volume mirror) and backup or restore schedule settings.

13.2 Viewing Schedules

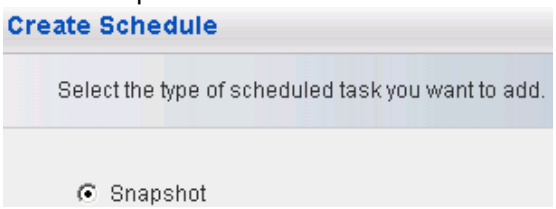
Go To	SANWatch Home > Device sidebar > Device List > device name > Schedules	
View	The list of scheduled tasks will appear in the Schedule List section.	
Parameters	**Name**	Shows the name of the scheduled task.
	LV Name	Shows the name of logical volume where the scheduled task is executed.
	Type	Shows the type of the task (snapshot, volume mirror, remote replication, and tiered migration) and associated parameters.
	Last Run	Shows the date and time when the scheduled task was last executed.
	Last Result	Shows the result of the last execution of the scheduled task.
	Next Run	Shows the date and time when the scheduled task will be next executed.

13.3 Creating Schedules: General Rules

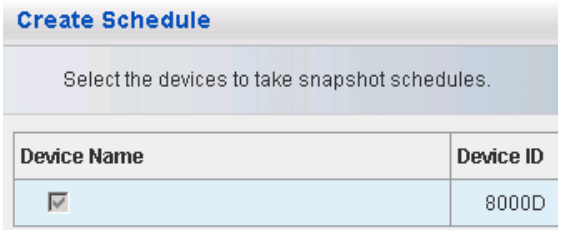
Go To	SANWatch Home > Device sidebar > Device List > device name > Schedules > Tasks section
Steps	Click “Create Schedule” in the Tasks section.  Select the schedule option. 
Changing the IP Address	Scheduled asynchronous volume mirroring will fail if the remote IP (host server IP for in-band or subsystem IP for out-of-band) changes between (a) and (b). ■ (a) When the volume pair is created ■ (b) When the scheduled asynchronous volume mirror begins Ideally, the IP address should remain fixed after the volume pair is created. However, if the IP address must be changed, follow the steps below. 1. Restart SANWatch. 2. Rediscover or add a new IP address manually. 3. Open SANWatch Manager from the subsystem using the updated IP address. 4. Remove the existing schedule. 5. Synchronize/asynchronize the volume pair to fix the broken link caused by changing the IP address. 6. Create a new schedule with the updated IP address. The remote IP address can be changed from the firmware after a volume mirror (remote replication) pair is created. However, this will break the remote pair. To remove a broken pair, the target must first be unassigned in SANWatch. Changing the remote IP after a remote replication pair is created is not permitted in SANWatch. To change the IP, first unassign the target volume of the remote replication pair. After changing the IP, reassign the pair by syncing/asyncing it manually.

13.4 Taking Snapshots by Schedule

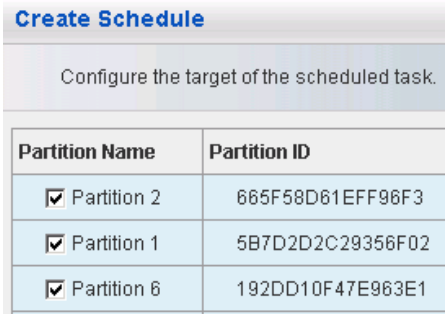
Notes	■ The interval between two snapshots must be 10 minutes or more. ■ If a snapshot taking process takes longer than the interval, the next snapshot will be abandoned and the first snapshot will be completed instead. ■ If multiple schedules occur simultaneously, both schedules will fail.
Go To	SANWatch Home > Device sidebar > Device List > device name > Schedules
Steps	Click “Create Schedule” in the Tasks section. Select Snapshot and click “Next”.



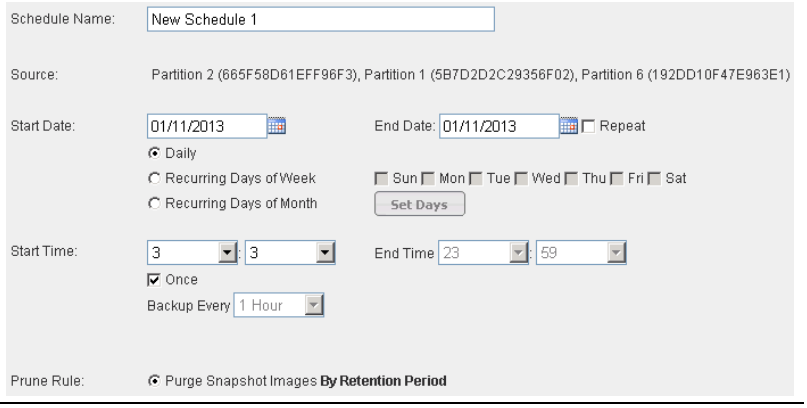
Check the box next to the device that contains the partition(s) for snapshotting and click “Next”.

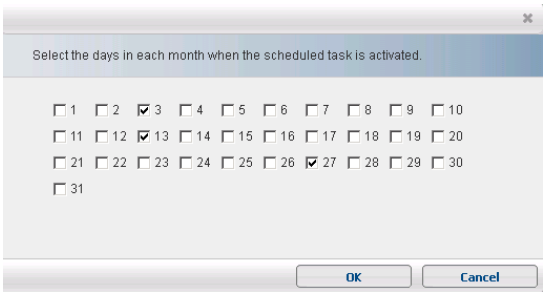
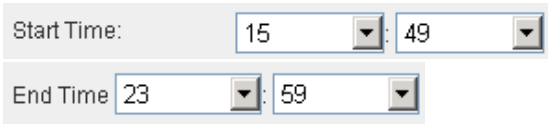
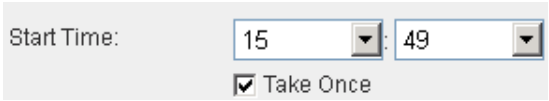


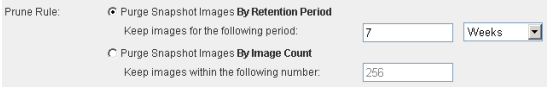
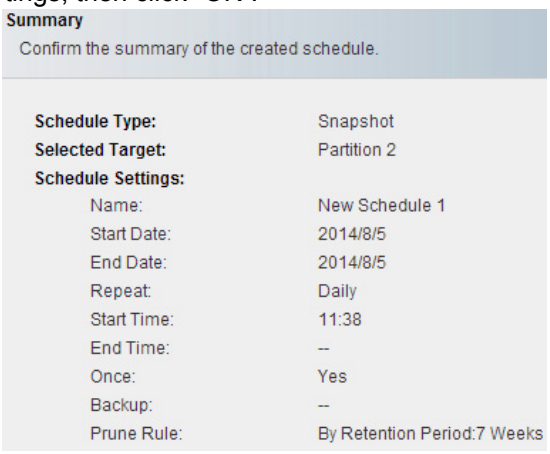
Select partition(s), and click “Next”.



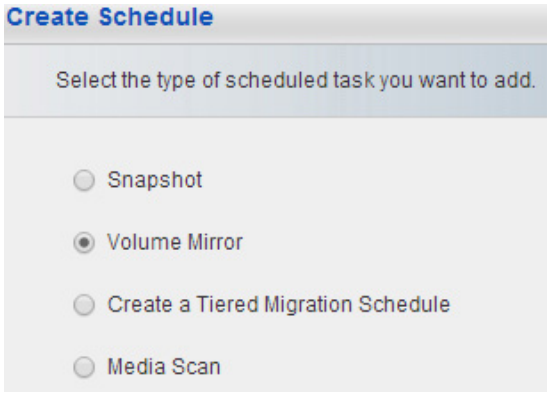
Input the schedule parameters.



Parameters	**Schedule Name**	Enter a name for the snapshot schedule.
	Source	Shows the selected source for the snapshot.
	Start/End Date	Specifies the duration of this schedule. To configure, click the part to be configured (for example, the year). If there is no stop date, check the “Repeat” option.
	Daily/Recurring Week Day/Recurring Days of the Month	Specifies the recurrence of this schedule. **Daily** If the “Daily” checkbox is selected, the scheduled task will be executed every day.  **Weekly** Select the days on which the scheduled task will be executed.  **Monthly** Click “Set Days”.  Select the days of each month on which the scheduled task will be executed. 
	Start/End Time	Specifies the start and end hour/minute of the scheduled task.  Configure the interval (frequency) using options from the drop-down list.  If the task is only executed once, check the “Take Once” option. The task will be executed at the set start time. 

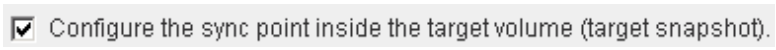
Prune Rule	Specifies the snapshot storage amount (snapshot image count) or period (retention period).  Click “Next” and confirm the summary settings, then click “OK”.  The snapshot schedule should appear in the Schedule List section. 
Exporting/Importing Scheduled Backup Tasks	Click the Help icon at the top-right corner and look for “Backing Up or Restoring Schedule Settings”.

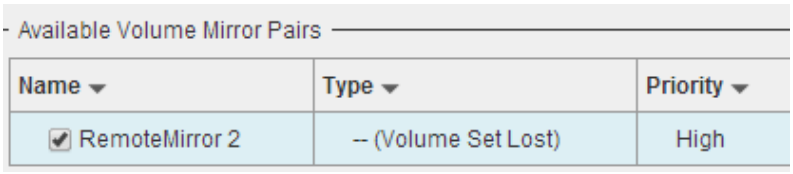
13.5 Creating a Volume Mirror by Schedule

Note	At least one volume mirror pair must exist to create a volume mirror schedule task. Go to SANWatch Home > Device sidebar > Device List, click the Help icon at the top-right corner, and look for a section titled “Creating a Volume Mirror” for more information about volume mirrors.
Go To	SANWatch Home > Device sidebar > Device List > device name > Schedules > Tasks section
Steps	Click “Create Schedule” in the Tasks corner. The list of tasks will appear. Check “Volume Mirror” and click “Next”. 

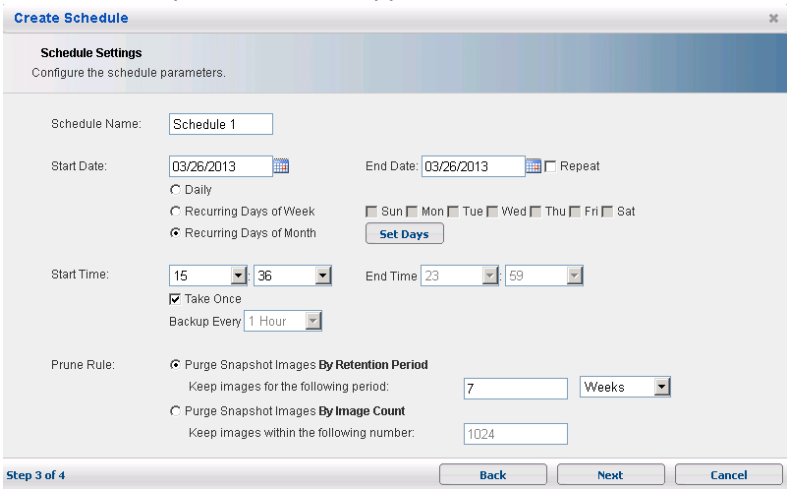
The list of volume mirror pairs will appear. Select a pair and click “Next”.

The sync point can be located inside the target volume.



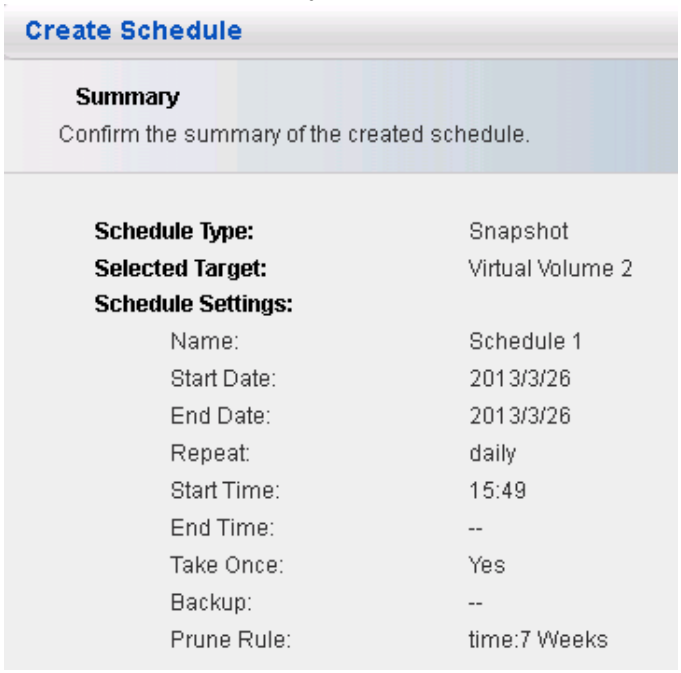


The schedule parameters will appear.

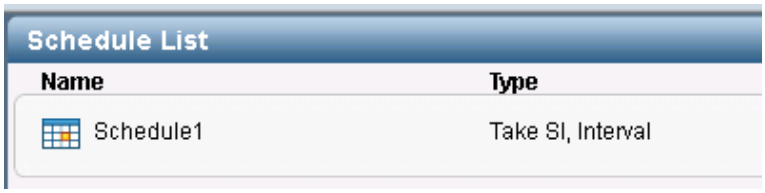


Parameters	**Name**	Enter the name of the scheduled task. Schedule Name: Schedule 1
	Start/End Date	Specifies the duration of this schedule. To configure, click the calendar icon and select the date. If there is no end date, check the “Repeat” option.
	Daily/Recurring Week Day/ Recurring Days of the Month	Specifies the recurrence of this schedule. **Daily** If the “Daily” checkbox is selected, the scheduled task will be executed every day. **Weekly** Select days on which the scheduled task will be executed. **Monthly** Click “Set Days”. Select the days of each month on which the scheduled task will be executed.
	Start Time/End Time	Specifies the start and end hour/minute of the scheduled task. Configure the interval (frequency) using the options in the drop-down list. If the task is executed only once, check the “Take Once” option. The task will be executed at the specified start time.

Click “Next”. A summary of the scheduled task will appear.



Click “OK”. The scheduled task will appear in the list.



Changing the IP Address

Scheduled asynchronous volume mirroring will fail if the remote IP (host server IP for in-band or subsystem IP for out-of-band) changes between (a) and (b).

- (a) When the volume pair is created
- (b) When the scheduled asynchronous volume mirror begins

Ideally, the IP address should remain fixed after the creation of a volume pair. However, if a volume pair must be changed, follow the steps below.

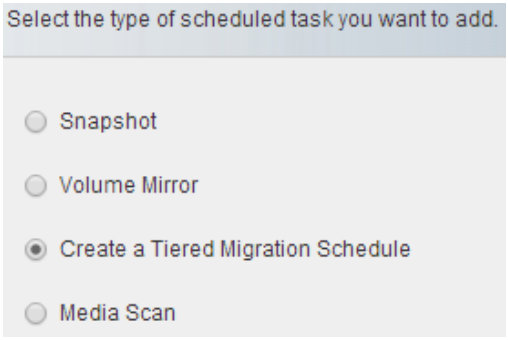
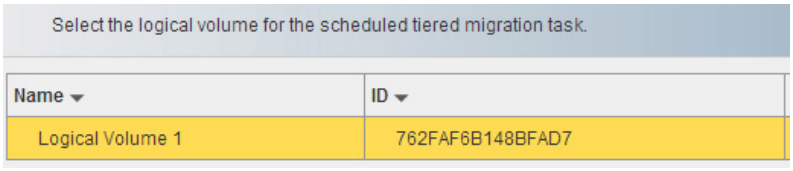
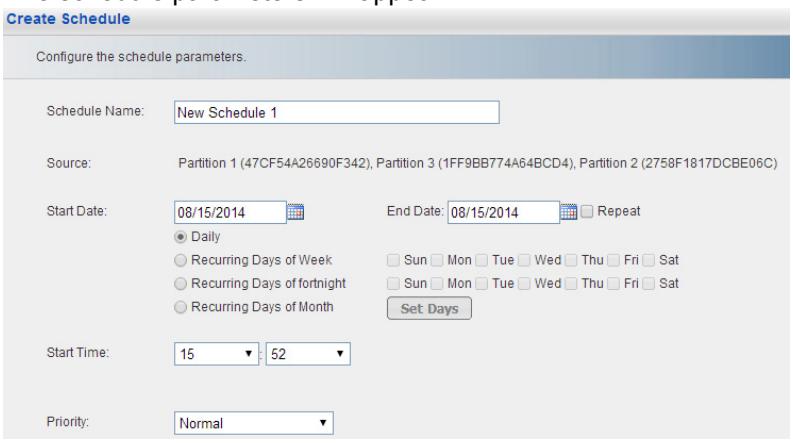
1. Restart SANWatch.
2. Rediscover or add a new IP address manually.
3. Open SANWatch Manager from the subsystem using the updated IP address.
4. Remove the existing schedule.
5. Synchronize/asynchronize the volume pair to fix the broken link caused by the changed IP address.
6. Create a new schedule with the updated IP address.

The remote IP address can be changed from the firmware after a volume mirror (remote replication) pair is created. However, this will break the remote pair. To remove a broken pair, the target must first be unassigned in SANWatch.

Changing the remote IP after a remote replication pair is created is not permitted in SANWatch. To change the IP, first unassign the target volume of the remote replication pair. After changing the IP, reassign the pair by syncing/asyncing it manually.

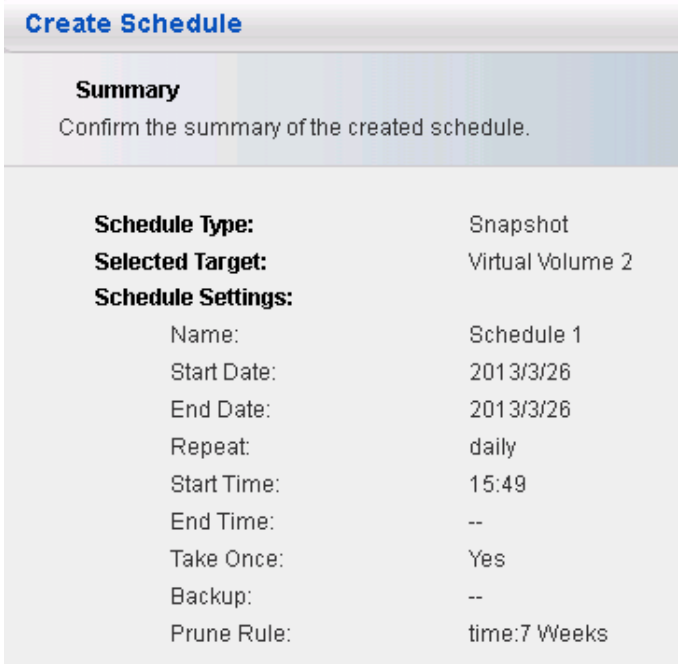
13.6 Creating Tiered Data Migration by Schedule

This feature is only available when one or more logical volumes residing in multiple tiers exist in the subsystem.

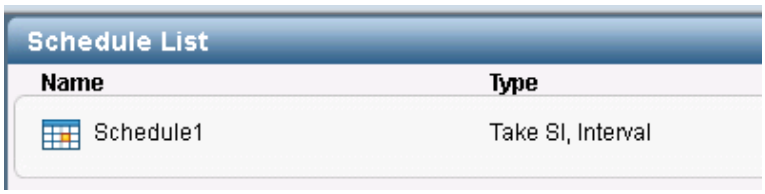
Go To	SANWatch Home > Device sidebar > Device List > device name > Schedules > Tasks section
Steps	Click “Create Schedule” in the Tasks section. The list of tasks will appear. Select “Create a Tiered Migration Schedule” and click “Next”.  The list of tiered logical volumes or pools will appear. Select one and click “Next”.  The schedule parameters will appear. 

Parameters	**Name**	Enter the name of the scheduled task. Schedule Name: Schedule 1
	Start/End Date	Specifies the duration of this schedule. To configure, click the calendar icon and select the date. If there is no end date, check the “Repeat” option.
	Daily/Recurring Week Day/ Recurring Days of the Month	Specifies the recurrence of this schedule. **Daily** If the “Daily” checkbox is selected, the scheduled task will be executed every day. **Weekly** Select the day on which the scheduled task will be executed. **Monthly** Click “Set Days”. Select the days of each month on which the scheduled task will be executed.
	Start Time/End Time	Specifies the start and end hour/minute of the scheduled task. Configure the interval (frequency) using the items in the drop-down list. If the task is executed only once, check the “Once” option. The task will be executed at the specified start time.

Click “Next”. A summary of the scheduled task will appear.

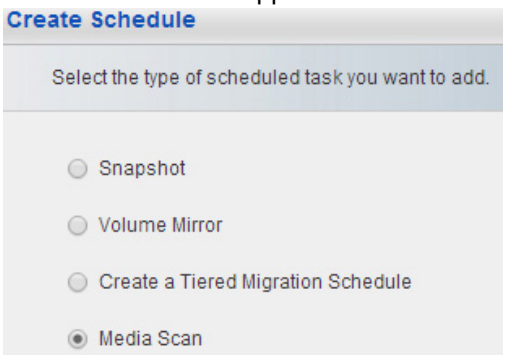


Click “OK”. The scheduled task will appear in the list.

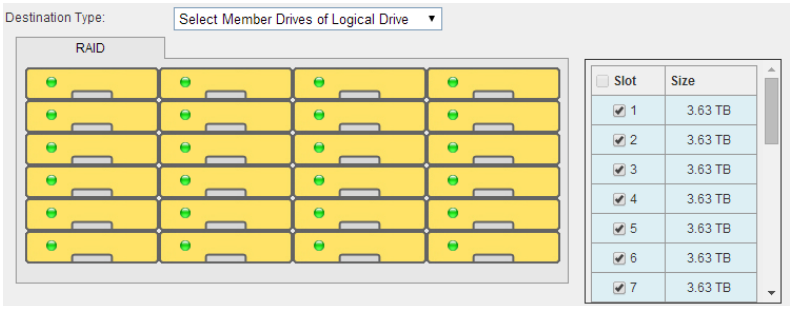


13.7 Scanning Disk Drives by Schedule

Go To	SANWatch Home > Device sidebar > Device List > device name > Schedules > Tasks section
Steps	Click “Create Schedule” in the Tasks section. The list of tasks will appear. Check “Media Scan” and click “Next”.

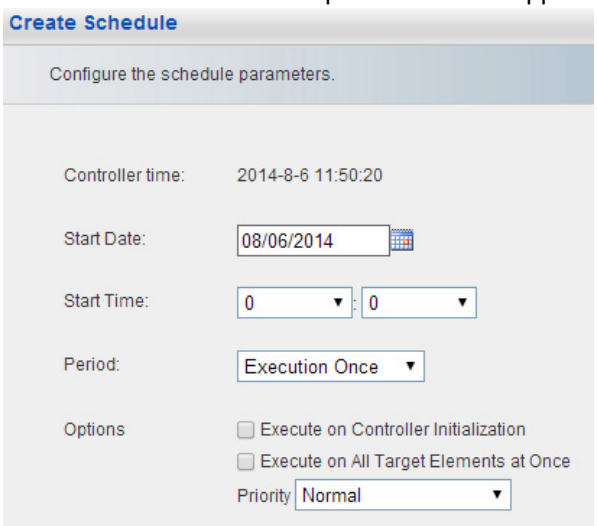


The front view of the device will appear. Select the drives to be scanned.

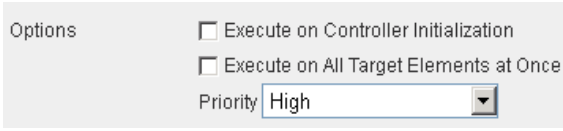


- Select Member Drives of a Logical Drive: Click a drive that belongs to a logical drive in the front panel, and all member drives (including local spare drives) of that logical drive will be selected.
- Select All Logical Drives: All drives that are members of logical drives will be selected.
- All Global/Enclosure Spare Drives: Only global/enclosure spare drives will be selected.
- All Assigned Drives: All drives that are part of a logical drive, logical volume, and partition will be selected.
- All Eligible Drives: All healthy drives, regardless of whether part of a logical drive, will be selected.

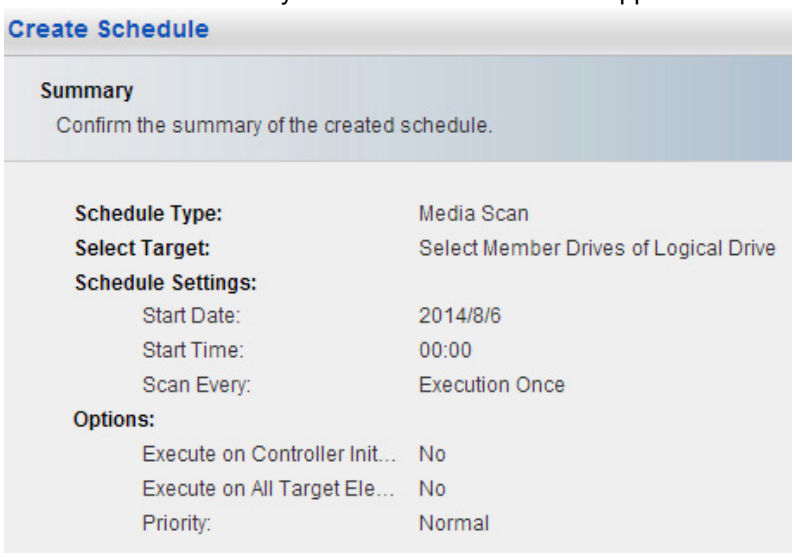
Click “Next”. The schedule parameters will appear.



Parameters	**Start Date/Start Time/Period**	Specifies the start date, start time, and period of this schedule.
	Options	Choose whether to scan ■ When the controller is initialized ■ All drives at once (if the priority is set to “high”, scanning will be conducted rapidly but the system performance may be affected)



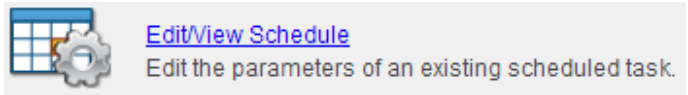
Click “Next”. A summary of the scheduled task will appear.



Click “OK”. The scheduled task will appear in the list.

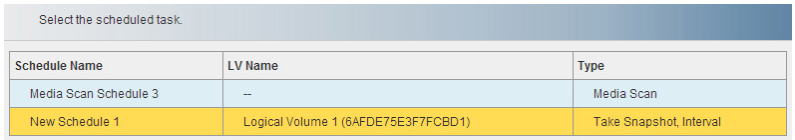
13.8 Editing/Deleting Schedules

Go To	SANWatch Home > Device sidebar > Device List > device name > Schedules > Tasks section
Editing a Schedule	Click “Edit/View Schedule” in the Tasks section.

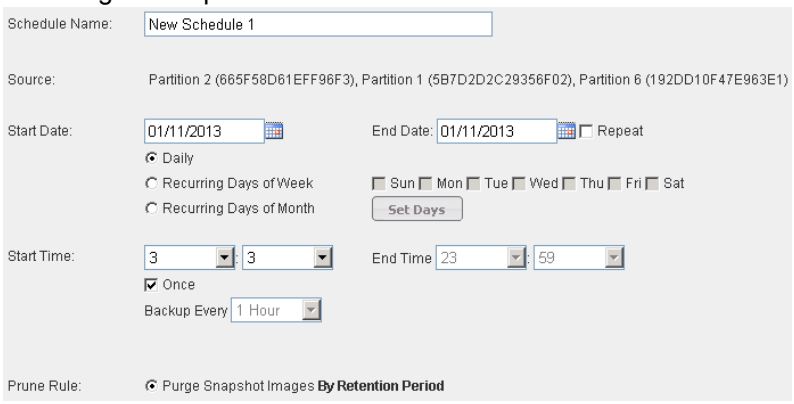


A list of the scheduled tasks will appear. Highlight the task to be edited and click “Next”.

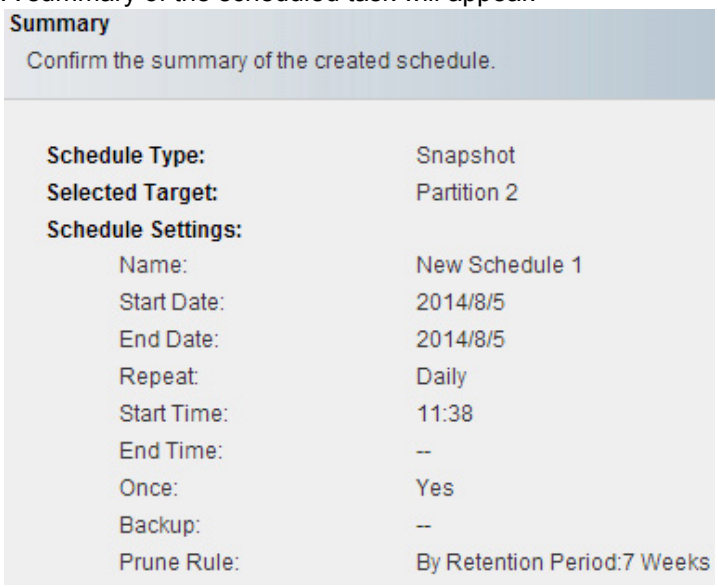
For scheduled tasks related to media scans, users can only click “View” to review summary information.



The schedule parameters will appear. These parameters are the same as those configured when the scheduled task was created. Reconfigure the parameters and click “Next”.



A summary of the scheduled task will appear.



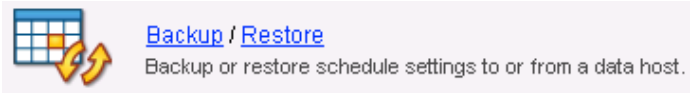
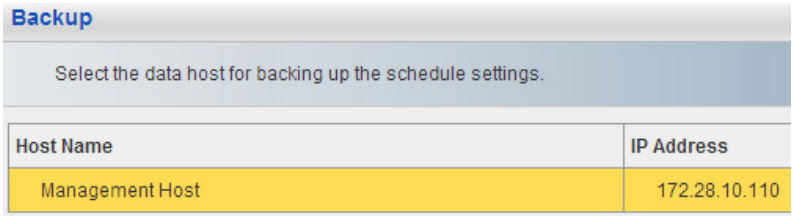
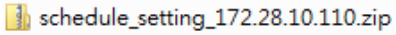
Click “OK” to close. The scheduled task will reappear in the list.

Deleting a Scheduled Task	Click “Delete Schedule” in the Tasks section. A list of scheduled tasks will appear. Highlight the task to be deleted and click “Delete”. The selected task will be removed from the list.

13.9 Backing Up or Restoring Schedule Settings

Users can save schedule configurations to a local file or import existing settings to the subsystem. This feature is useful for moving a RAID environment from one subsystem (or controller) to another.

To use this feature, SANWatch must be connected to the subsystem via an in-band connection, and at least one backup schedule (snapshot or mirror) must exist.

Go To	SANWatch Home > Device sidebar > Device List > device name > Schedules
Backing Up Settings	Click “Backup” in the Tasks section.  A list of available hosts will appear. Highlight a specific host and click “OK”.  The scheduled tasks settings will be exported as a zip file for download to a computer. 
Restoring Settings	Click “Restore” in the Tasks section. A list of available hosts will appear. Highlight the host and click “Browse”. Select the settings file (*.zip) from a local folder. The settings will be uploaded and restored on the selected host.
Note	The configuration data is in a proprietary format and packed in zip format (*.zip). When importing configuration data, do not unpack the zip file. Instead, select and import the original zip file.

Appendix A

TCP/IP and UDP Port Assignments

A.1 TCP/IP and UDP Port Assignments

The following ports are provided for manually configuring secure access to SAN-Watch. If management access must span protected networks, users should contact their network administrators.

Software	58630	SSL port for connecting RAID subsystems.
	58632	Non-SSL port for connecting RAID subsystems.
	58641	Port for receiving automatic discovery responses.
Management Host Agent	58634	Port for receiving requests from the notification manager.
	58635	Port for redundant configurations when synchronizing the management host agent.
	58641	Port for receiving automatic discovery responses.
	58699	Port for receiving requests for port access to SANWatch.
In-Band Data Host Agent	58630	SSL port for a console to connect to the data host agent.
	58632	Non-SSL port for a console to connect to the data host agent.
	58640	Port for receiving automatic discovery requests.
VSS Agent	58650	Port for receiving VSS requests.
MPIO Agent	58670	Port for receiving MPIO requests.
UDP Port Assignments	58640	Should be enabled for all modules.
	58641	Should be enabled for all modules.

ADVANTECH

Enabling an Intelligent Planet

www.advantech.com