User Manual

SANWatch Web-Based Interface

Version 6.7 (November 2018)

Legal Information

All Infortrend products, including the product customers have purchased from Infortrend, shall be subject to the latest Standard Warranty Policy available on the Infortrend website: http://www.infortrend.com/global/Support/Warranty

Infortrend may from time to time modify, update or upgrade the software, firmware or any accompanying user documentation without any prior notice. Infortrend will provide access to these new software, firmware or documentation releases from certain download sections of our website or through our service partners. Customer shall be responsible for maintaining updated version of the software, firmware or other documentation by downloading or obtaining from Infortrend, and installing designated updated code, including but not limited to firmware, microcode, basic input/out system code, utility programs, device drivers, and diagnostics delivered with Infortrend product.

Before installing any software, applications or components provided by a third party, customer should ensure that they are compatible and interoperable with Infortrend product by checking in advance with Infortrend. Customer is solely responsible for ensuring the compatibility and interoperability of the third party's products with Infortrend product. Customer is further solely responsible for ensuring its systems, software, and data are adequately backed up as a precaution against possible failures, alternation, or loss.

For any questions of hardware/ software compatibility, and the update/ upgrade code, customer should contact Infortrend sales representative or technical support for assistance.

To the extent permitted by applicable laws, Infortrend shall NOT be responsible for any interoperability or compatibility issues that may arise when (1) products, software, or options not certified and supported by Infortrend are used; (2) configurations not certified and supported by Infortrend are used; (3) parts intended for one system are installed in another system of different make or model.

Contact Information

Customer Support

Contact your system vendor or visit Infortrend's website
http://infortrend.com/global/About/Worldwide

for the contact information of support offices worldwide.

About This Manual

This manual describes how to access and use the browser-based interface version of SANWatch software suite for EonStor, EonStor DS, ESVA, and EonServ series.

For the following subjects, consult other resources for more information:

- Desktop software application version of SANWatch: Consult the SANWatch manual version 4.x or earlier.
- Components that are not user-serviceable: Contact our support sites.
- Hardware operation: Consult the Hardware Manual in the CD-ROM.

Version 5.0	➢ Initial release for the browser-based interface version of SANWatch.
Version 5.1	➢ Updated contact information
Version 5.2	➢ Added Data Replication ➢ Added Storage Tiering
Version 5.3	➢ Updated descriptions to match GUI
Version 5.4	➢ Added SANWatch installation
Version 5.5	➢ Incorporated and updated ESVA user manual contents ➢ Rearranged chapter order ➢ Added new features: SED Security, Storage Tiering enhancement, Host Channel Group enhancement, etc
Version 5.6	➢ Added new feature: SSD Cache Pool ➢ Added firmware update ➢ Added miscellaneous notes and warning information
Version 5.7	➢ Removed Load Balancing related information ➢ Added reserved IP information ➢ Added description for converged host board ➢ Added notes regarding EonServ models
Version 5.8	➢ Removed Installing EonPath (Multipathing) Driver ➢ Added Working with Multipath ➢ Added Eonpath limitation – only for Windows server 2003 & before

Version 5.9	➢ Added compatibility notice of disk roaming and remote duplication. ➢ Updated language, system tab, UI, etc.
Version 6.0	➢ Updated link to Oracle SQL utility ➢ Updated links to Link Activation and Provisioning and reserved space
Version 6.1	➢ Added InfiniBand channel configurations ➢ Updated the installation folder name in the installation CD
Version 6.2	➢ Updated the section Exporting System Settings ➢ Add the section Creating a Logical Volume with RAID Level 30/50/60 ➢ Correct that Thin Provisioning is available with standard license (no need for advanced license)
Version 6.3	➢ Updated license related procedures
Version 6.4	➢ Update Data Replication
Version 6.5	➢ Updated Logical Volume
Version 6.6	➢ Updated Appendix
Version 6.7	➢ Updated Summary of System Configurations; Adding a Host; Data Replication; Configuring Automatic Failover for Remote Replication

Table of Contents

Working with Channels (NOT Supported by EonServ)

Working with Hosts

Working with the Logical Volumes or Pools View

Working with Logical Volumes or Pools

Working with the Logical Drives or Pool Elements View

Working with Logical Drives or Pool Elements

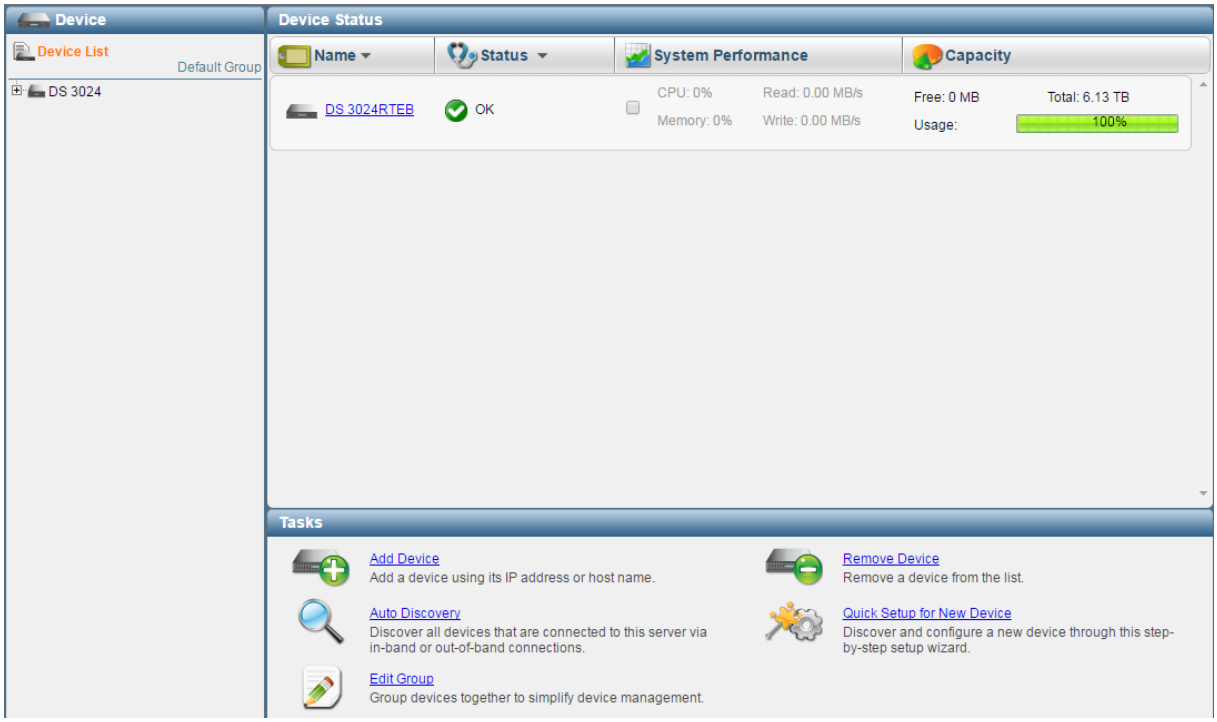
Working with the Partitions or Virtual Volumes View

Working with Partitions or Virtual Volumes

Working with Schedules

Appendix

Introduction



SANWatch Browser Interface is the proprietary software suite for the Infortrend storage systems. SANWatch can be accessed through a web browser as long as both the computer and the subsystems are online. You are no longer required to install complex desktop application to your local computer: everything is always available over the network.

Connecting SANWatch to Storage Subsystems

SANWatch, storage subsystems and the host computers can be connected in either in-band (connection through host links) or out-of-band (connection through LAN management port). Because SANWatch is web-based, you may access the GUI from anywhere on the network. The flexible connection schemes allow you to manage SANWatch according to your needs and system configurations, notably the following two factors:

- Local management vs. Remote management
- Full configuration vs. Monitoring & notification

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.

Computer Requirements

Computer Requirements

Hardware

- Broadband access

OS

- Microsoft Windows XP, Vista, 7, 8 (32/ 64 bit), Windows Server 2003 R2, 2008 (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 you cannot access the browser-based interface in a Windows environment (such as Windows Server 2003), it is probably because the default network firewall setting of the OS is set to "High," forbidding users from entering the user interface as admin. Please change the network settings in the OS.

Installation

This section lists the installation procedures for SANWatch and other software modules included in the CD-ROM. Refer to the previous section to determine which modules apply to your environment.

Installing Java

SANWatch installation requires Java version 6 or later. When you install SANWatch on your computer (refer to the next section), the installation wizard or scripts that come with your SANWatch installation CD will help you install Java 6 along the way, but you can also install a newer version manually using the installation package downloaded from http://java.com/download.

For users wanting to install Java 6 provided by SANWatch Installation CD, you can jump to the next section directly.

For Windows

You can install the JAVA installation package downloaded from http://java.com/download.

For Mac OS X

Before installing Java on a Mac, make sure 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, you can install Java using Software Update (at the Apple icon > Software Update); For OS X 10.7 Lion or later, you can install it using the installation package downloaded from http://java.com/download.

For Linux

Here is a brief instruction on how to download and install Java for Linux, and then enable it in Firefox. For more options and details, visit here.

Download 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 sub-directory 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

Here is a brief instruction on how to download and install Java 6 self-extracting binary file for 32-bit Solaris, and then enable it in Firefox. For more options and details, see: installation package overview, JRE installation procedures, JRE plug-in installation procedures for Firefox.

Download 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.

Initiating SANWatch Installation

Initially, ways and tools to launch SANWatch installation vary depending on the operating system (OS) you are using, but they are basically helping you install Java 6 (optionally) and launch the SANWatch Installation Wizard.

> If you choose NOT to install the Java provided by the installation CD, make sure you already have Java 6 or later installed on your computer. Refer to the previous section for details.

For Windows

From the installation CD, open SANWatch.exe, and from the navigation menu that appears, choose SANWatch GUI Software Installation, and then select Windows Platform under SANWatch Management Tool. 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: If you want to install the data host only instead of the GUI-based SANWatch. Skip to the next section directly.

Locate the "SANWatch" folder on the installation CD and copy it 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 then browse its contents to make sure the "linux.sh" script is in the folder. If you are using Solaris, make sure "unix.sh" is in the folder.

```
[root@localhost ~]# cd <computer_path>/SANWatch/
[root@localhost <computer_path>/SANWatch]# 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 you are using Linux, make "linux.sh" executable, and then execute it.

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

If you are using Solaris, do the same to "unix.sh."

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

The first two sections of the script will take you through Java installation. If you already have Java 6 or later 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 Procedure
  ************************************************************
  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 will ask you whether you want to install SANWatch. Just type "yes" and press Enter to proceed to the next section.

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

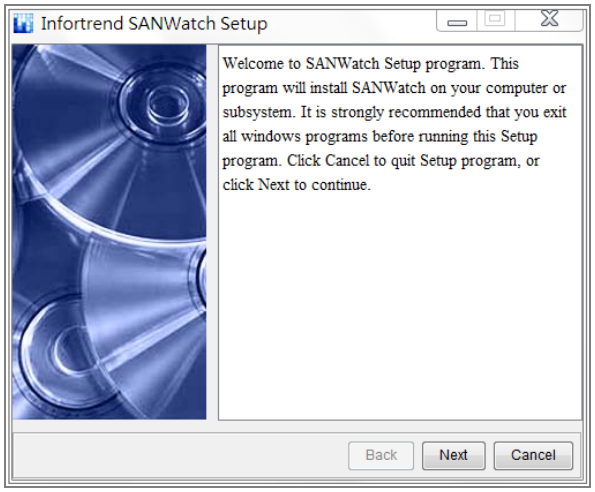
Installing SANWatch

This section introduces how to install the whole GUI-based SANWatch on various OS platforms.

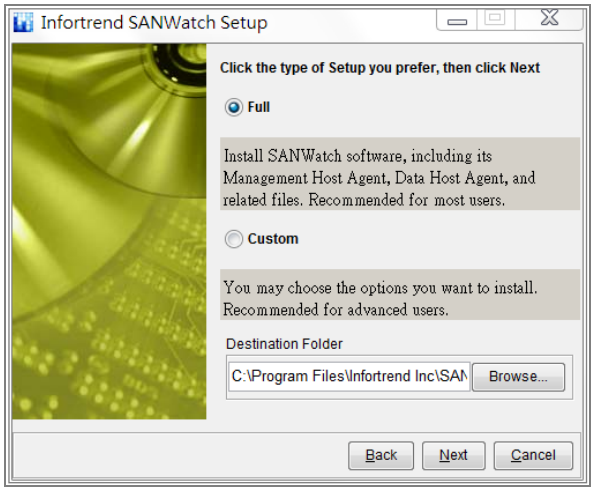
For the Linux platform, you can also install the data host agent only to save reserve system resources.

Installing GUI-based SANWatch

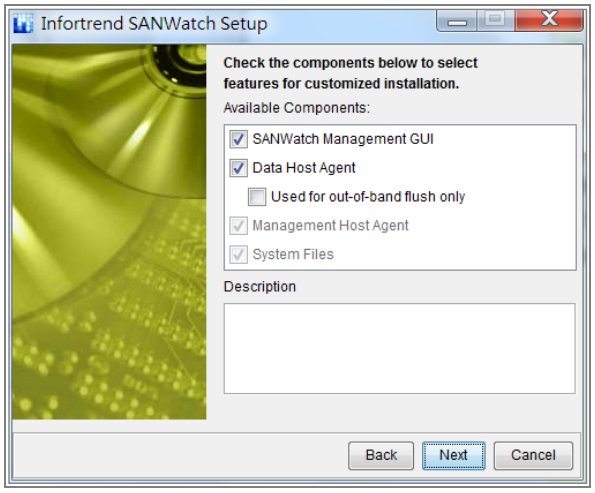
1. After installation is initiated, you will be guided to the Infortrend SANWatch Setup wizard. Click Next to continue.



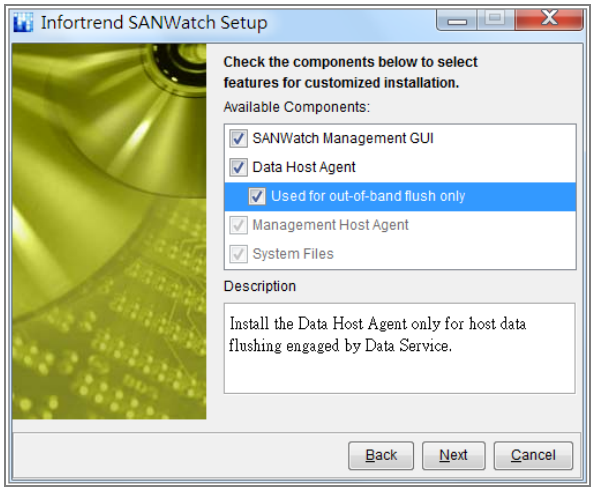
2. The installation program asks for Full or Custom installation. You can also select the installation folder here.
   Choose Full installation if you intend to manage SANWatch directly from the host computer. Then skip to Step 4.



3. Otherwise, choose Custom installation, and in the component list corner, select the module(s) you need based on the computer on which you are installing SANWatch.

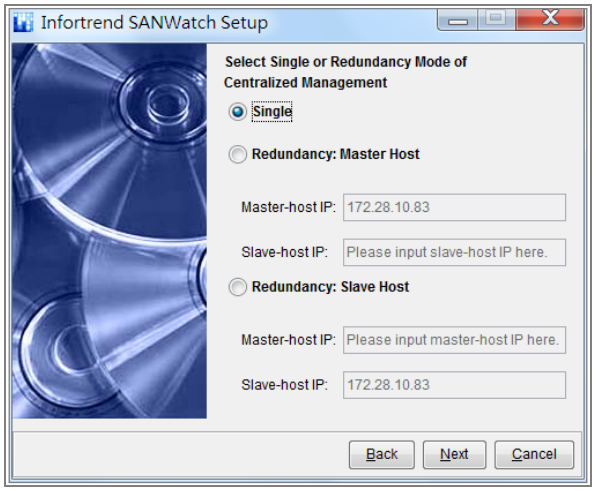


If you are using DB Flush Agent for taking snapshot images with database applications, select Data Host Agent and/or Out-of-Band Flush Only. Click Next to continue.

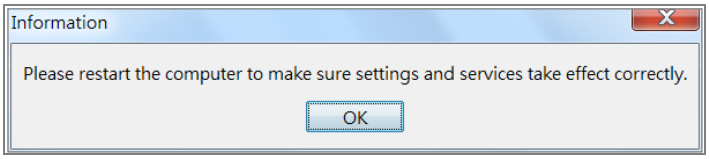


4. Select if you want to install SANWatch in a single host computer or

redundant host computers. For the redundancy mode, specify the IP addresses of the master and slave host computers. If you choose to manage your RAID subsystem network using dual computers, it is strongly recommended you install and log in to SANWatch on the master host first, and make sure it's online before installing SANWatch on the slave-host.



When the installation has completed, 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 you are prompted with the question "Would you like to install Java-based RAID Manager now?"

```
        ************************************************************
            Java-based GUI RAID Manager Installation Procedure
        ************************************************************

        SECTION I : JRE v1.6.0_25 Installation
*NOTE: 1.Before you can run Java-based program successfully, you should have
         installed JRE(Java Runtime Enviroment).
       2.JRE v1.6.0_25 will be installed on /usr/local/jre1.6.0_25 .
Would you like to install JRE v1.6.0_25 now?
Please type yes or no.
yes
```

6. When you are asked whether to install all agents or selected agents only, use the "**`-s /usr/local dataHost`**" command to install the data host agent:

```
Install JRE v1.6.0_25 finished!

-------------------------------------------------------------------------------
SECTION II : Java-based RAID Manager Installing by GUI or Command

*NOTE: Selecting which installing method you preferred, GUI or command line.

Would you like to install Java-based RAID Manager now?
Please type yes or no.
yes
---------- Install Command Information ----------
Installing all agents => command format: -a (install direction)
Example: -a /usr/local

Installing selected agents => command format: -s (install direction) hostType
Example: -s /usr/local dataHost managementHost(one of the agents or both)
-s /usr/local dataHost
```

The data host agent is now installed successfully. It will be activated automatically during system startup, saving you the trouble of having to manually start the service.

Installing 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. You need VSS if you intend to take snapshot images while using database applications (Oracle, SQL, MS Exchange).

Installation procedures

Activate SANWatch.exe and click VSS in the SANWatch installation corner or enter the VSS directory in the SANWatch 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

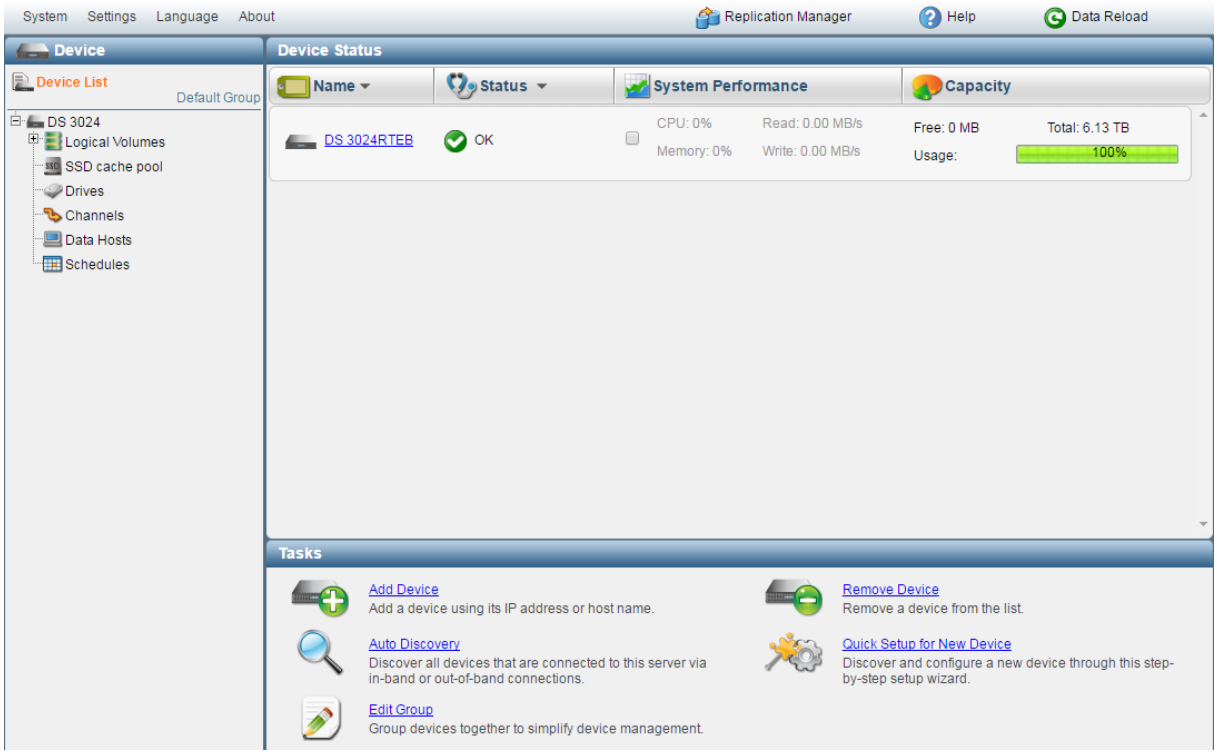
The Setup Wizard will appear. Follow the instructions to complete the installation.

Reboot the computer when the installation is complete.

Uninstalling/Upgrading SANWatch

Uninstalling SANWatch	Uninstall SANWatch just as you would with any other applications. For example in Windows, go to Start > All Programs > Infortrend Inc > Uninstall SANWatch.
Upgrading SANWatch	In order to upgrade SANWatch into a new version, you need to uninstall the current version and then install the new version. Visit the Support site for the latest version of SANWatch.

SANWatch Interface



This chapter describes how to navigate the SANWatch Home interface and use the functions available from there. You can learn about basic GUI elements, how to find online help tools, adding and configuring hardware devices (RAID subsystems or JBODs), configuring data replication (volume mirror and volume copy) and automatic event notification.

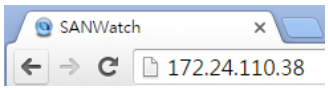
Navigating the User Interface

Logging into the User Interface

Logging into the SANWatch Browser Interface is easy and straightforward: type in the IP address of the host computer into the browser.

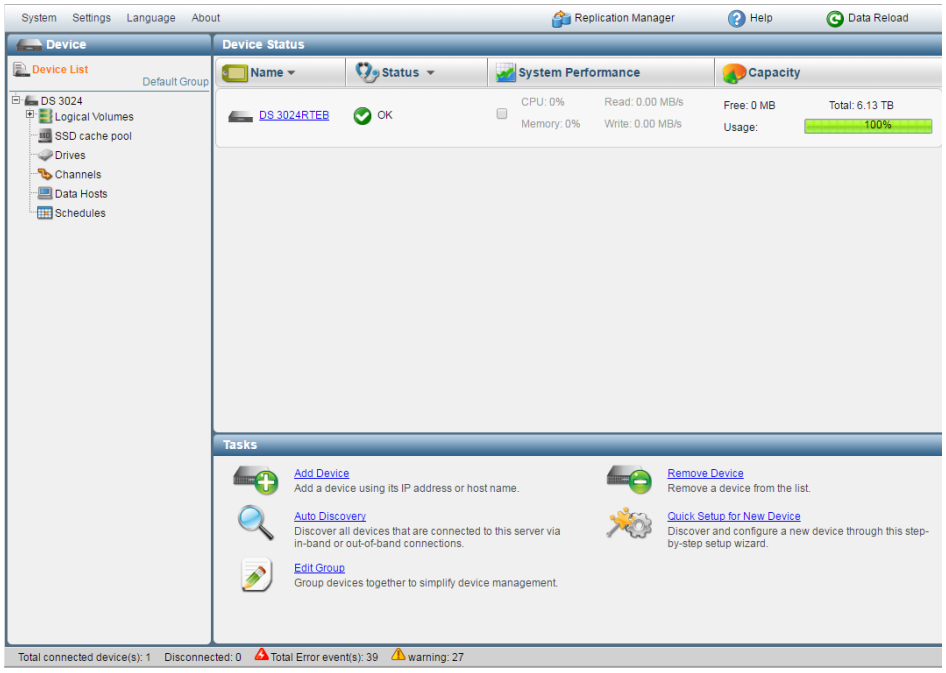
Log In

Enter the IP address of the host computer into the browser and press the Enter key.



The login screen will appear. Enter the password (the default password is **root**) and click Login. (You may check Remember Password if you prefer automatically logging into the interface in the future)

The user interface will appear.



Log Off

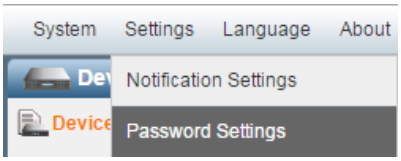
Select the System > Log Off menu. The user interface will return to the Log In screen.

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

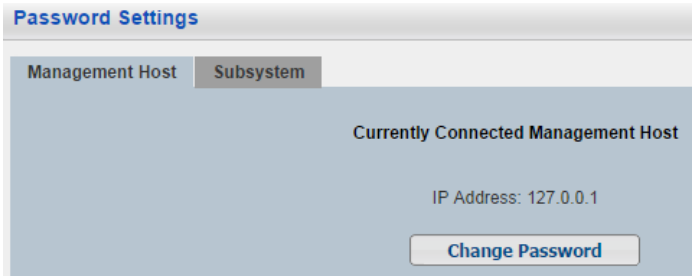


Changing SANWatch Login

Select the Management Host tab, click Change Password, and enter the existing password and new password (twice for confirmation). The default login

Password

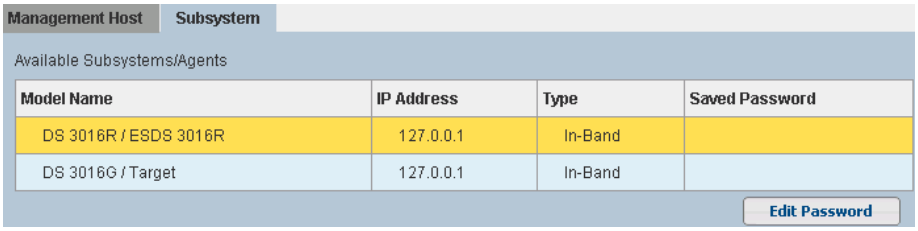
password is **root**.



Assigning a Password to a Subsystem

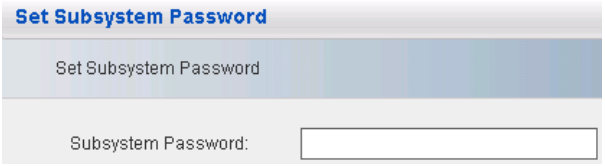
Once you set up a password for the subsystem, you need to enter it whenever you try to access or configure the hardware setting for that subsystem.

Select the Subsystem tab to view the list of subsystems and their passwords.



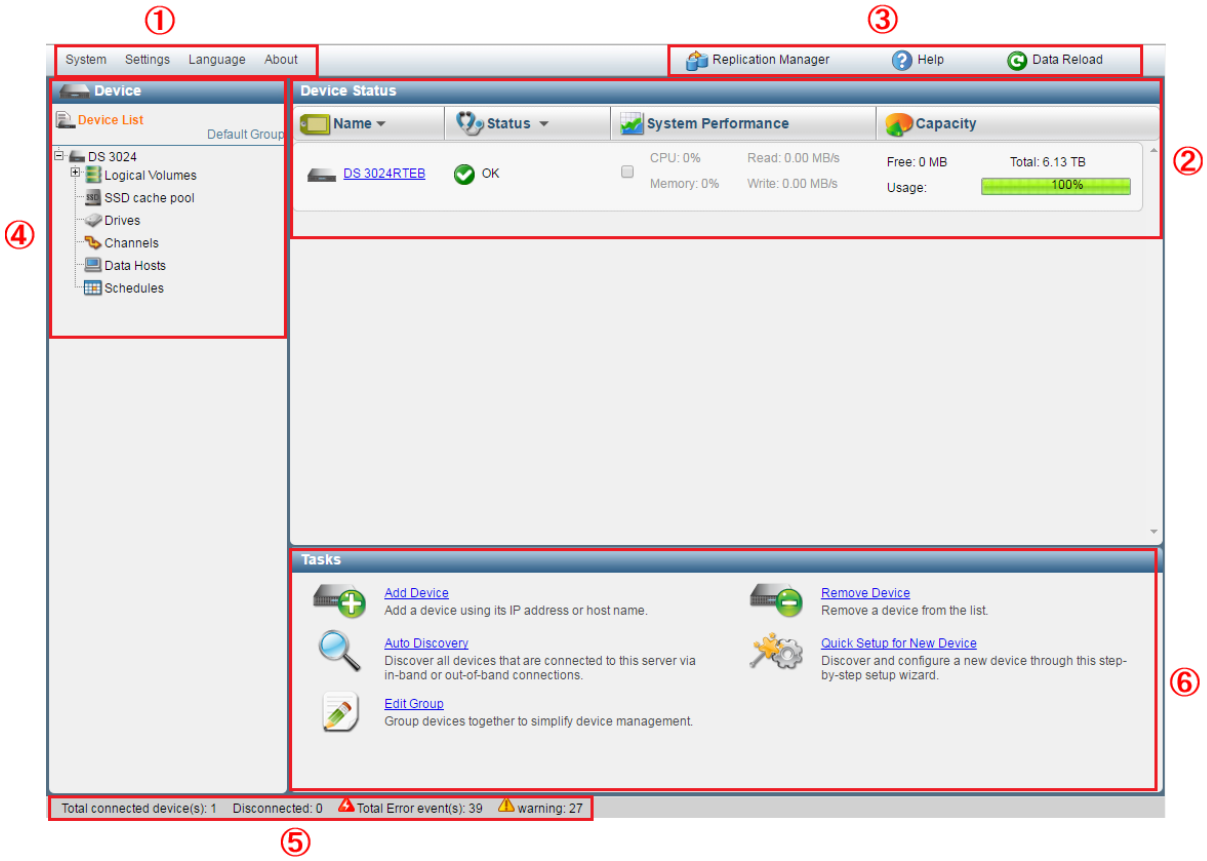
Highlight the storage subsystem from the list and click the Edit Password button.

Enter the new password.



After specifying a password, when you try to access the hardware device page, you will be asked to enter the password.

Getting to Know the User Interface

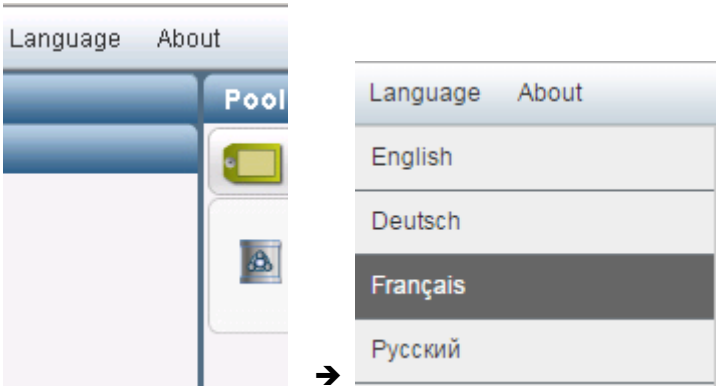


Display Element	Description
1: Top menu bar (Left)	The menu items at the top left allow you to export system settings, log off / shutdown the subsystem (NOT supported by EonServ), configure notifications and passwords, change the display language, and view the SANWatch version information.

2: Main window	The current status and the configurations of the item chosen in the left sidebar will appear in this area.
3: Top menu bar (Right)	You may access the Replication Manager for configuring and running data replications, Online Help (this help document), and refresh the screen contents.
4: Side Column	You may view the system configurations (Device sidebar) or the storage configurations (Pool sidebar) in a tree structure to have an overview of the overall 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 corner	Convenient shortcuts to major functionalities are available for the item that is currently highlighted in the sidebar / main window area.

Navigating the Interface

	Although SANWatch is a browser-based software, most operations are designed as intuitive, desktop-like features.
Selecting an Item	You may click an item if the mouse cursor shape turns into a pointing device. The text color may also change as shown in this example. (Example: Pool List > Pool 1)  Depending on selection, a drop down list may appear by hovering the mouse cursor 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 requires the user's attention.

Using Help Tools

Changing the Display Language

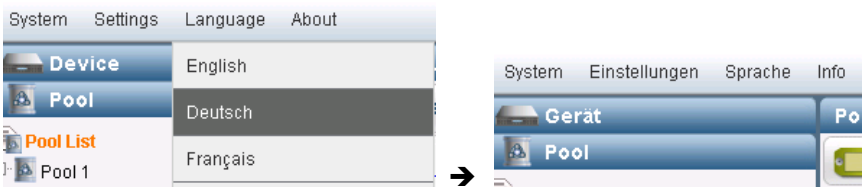
Switch the display language from the default English to your preferred language in an instant.

Go To

SANWatch Home > Top menu bar > Language

Steps

Select the desire language from the drop-down menu to change the interface displayed language. (Example: from English to German)



Available Languages

- English (default)
- German
- French
- Japanese
- Simplified Chinese
- Traditional Chinese
- Korean

Notes

- Some texts might not be translated (for example, texts that are embedded in a diagram or the official license agreement). In those cases, the texts will remain English, the default language.
- In case you have accidentally changed the language (and thus lost sight of the “Language” menu), the Language menu tab is the third tab from the right (or second from the left) on the menu bar.

Viewing the SANWatch Version Information

View the current version number of SANWatch and/or the end user license agreement.

Go To

SANWatch Home > Top menu bar > About

Steps

Click the About menu from the top menu bar. The version information window will appear.

Viewing the License Agreement

Click the *License Agreement Details* link in the window to view the end user license agreement contents.

For legal considerations, the license agreement is not necessarily translated into non-English languages.

Accessing Infortrend Website

Clicking the *Infortrend Technology, Inc.* link takes you to the official website of Infortrend.

Viewing Online Help

View the help contents (this document) when you need descriptions/instructions for complicated or unfamiliar features.

Go To

SANWatch Home > Top menu bar > Help

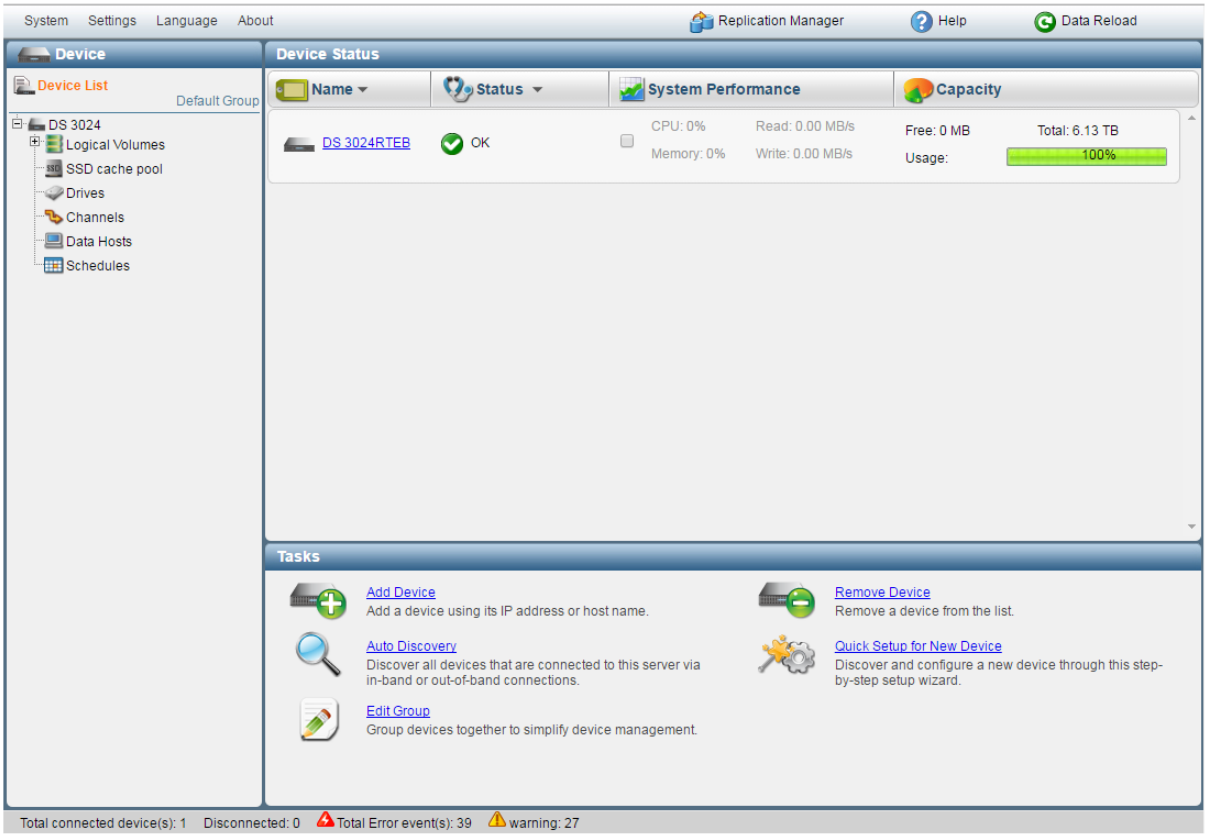
Steps

The Online Help will appear in a separate screen in a new tab or a pop-up window. The contents are organized in the same manner as the PDF version of the help document.

Note

If the Help screen does not appear, you might need to enable pop-up windows from the browser's configuration options.

Working with the Devices View



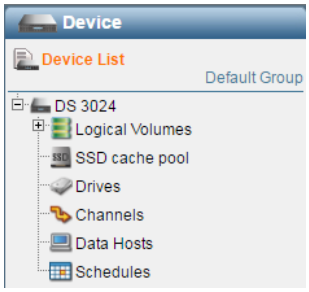
This chapter describes how to monitor and configure the hardware: RAID subsystems, JBOD expansion enclosures, hard drives, and so on.

Viewing the List of Hardware and the Status

All hardware information can be accessed from the Device Sidebar in the user interface.

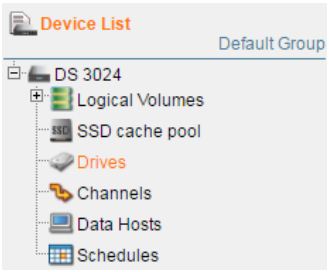
Go To

SANWatch Home > Device sidebar > Device List

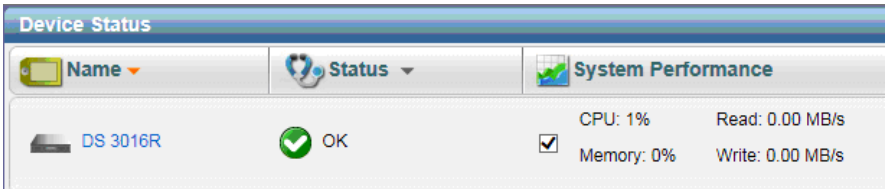


Steps

When you click the *Device* tab in the left sidebar, the list of hardware recognized by the system will appear.

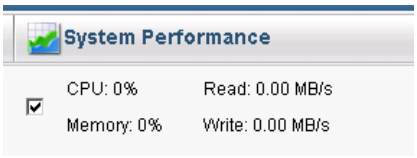


The hardware status summary will appear to the right, in the main screen.



System Performance

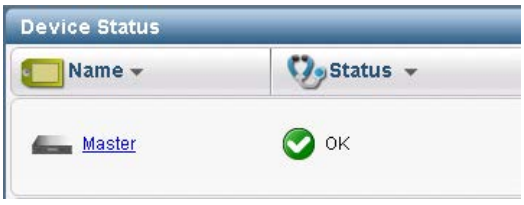
To enable monitoring system performance, check the System Performance checkbox.



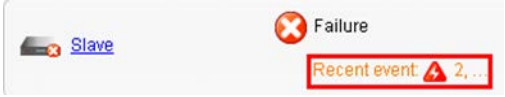
Because the monitoring function affects system performance and it is therefore disabled by default.

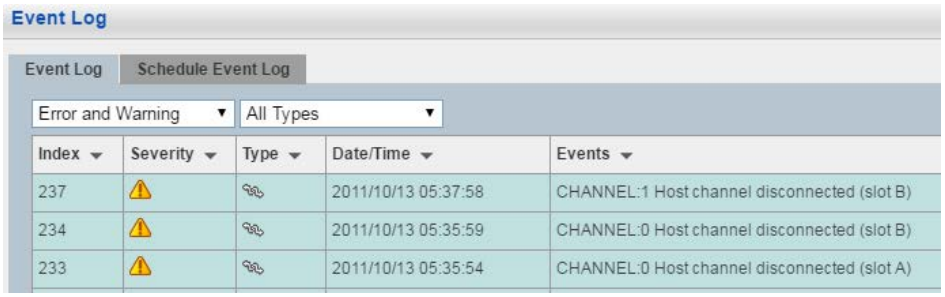
System Status

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



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





To refresh the status (in case you want to make sure that the hardware status has been updated), click *Data Reload* on the top menu bar.

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

To start configuring your RAID subsystem or JBOD expansion enclosure through the SANWatch Browser Interface, all you have to do is to connect the device to the network and then use the one-touch device discovery functionalities introduced here.

Prerequisites

Before adding a subsystem/JBOD to the user interface, make sure that the subsystem has already been connected to the network and a valid IP address has been assigned to it.

If you are using Internet Explorer, go to Tools > Internet Options > Security, and then do the following 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 corner

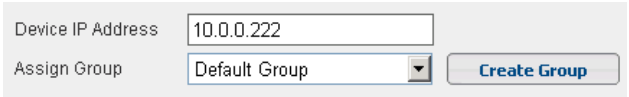
Steps

You can add (discover) a device in two ways: specify a known IP address or search a range of IP addresses.

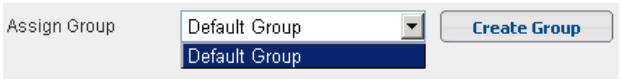
Specifying an IP Address

Click *Add Device* in the *Tasks* pane.

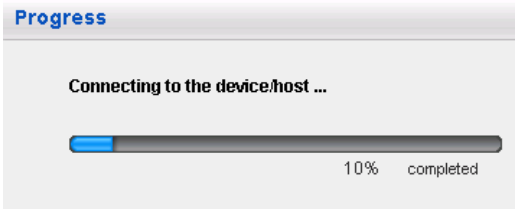
Enter the IP address of the device.



By default, the device will be added to a device group called Default Group. You can assign the device to a different group or even create a new group. (To learn more about device groups, see the next section in this help document.)



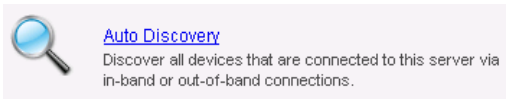
The device will be added to the host computer. Click *Cancel* to stop the process.



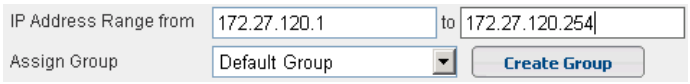
The new device will appear in the sidebar when done.

Searching for a range of IP addresses

You may use the Auto Discovery function to search for your device if you do not know its specific IP address but its subnet range. (You may also use this function 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. You can assign the device to a different group or even create a new group. (To learn more about device groups, see the next section in this help document.)

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

Removing a Device (RAID Subsystem or JBOD Expansion Enclosure)

You may remove a device from your system easily. User data and device configurations will not be affected; the device will be simply deregistered from your system.

Go To

SANWatch Home > Sidebar > Device List > Tasks corner

Steps

Click Remove Device.

Check the device you wish to remove.

Click on "Remove" at the bottom to remove the device.

Editing Groups and Group Assignments

You can organize the list of devices into groups to easily manage complicated network with clusters of devices, especially when there are multiple instances of same models.

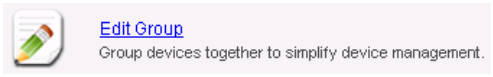
Notes

- All devices must be assigned to a group. (By default, they are assigned to a group called Default Group.)
- A device cannot be assigned to multiple groups.
- List of groups are directly visible in the sidebar.

Creating a Group

Go to SANWatch Home > Sidebar > Device List > Tasks corner.

Click Edit Group.



Check the box next to the device you wish to add to the new group and click on "Create Group" at the bottom.

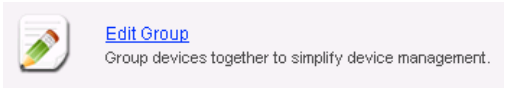
Enter the group name and click OK.

The new group will appear in the list.

Renaming a Group

Go to SANWatch Home > Sidebar > Device List > Tasks corner.

Click Edit Group.



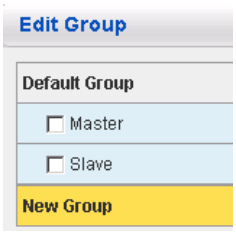
Click to highlight the group that you want to rename and click Rename Group.

You are not allowed to rename Default Group.

Click Rename Group.

Enter the new name and click OK.

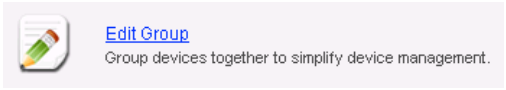
The new group name will appear in the list.



Reassigning a Device to another Group

Go to SANWatch Home > Sidebar > Device List > Tasks corner.

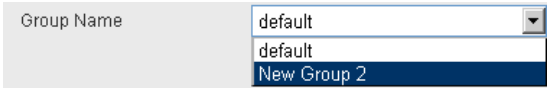
Click the Edit Group icon.



Check the device that you want to reassign to a different group.

Click on "Move Device".

Select a group in the drop-down list.

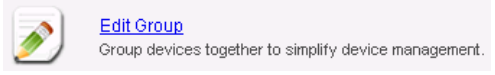


Click "OK" and the device will be assigned to a different group.

Remove a Group

Go to SANWatch Home > Sidebar > Device List > Tasks corner.

Click Edit Group.



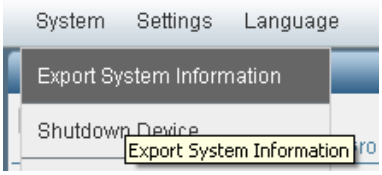
Click the name of the group you want to remove, click Delete Group, and click Yes in the confirmation message that appears.

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

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) whose system information you wish to export. Then click the button **With core dump** if you wish to export the system information with memory core dump. Click the button **W/o core dump** if you only want to export system information without memory core dump.

The system information will be archived in a package of Zip file, including text (.txt) and Microsoft Excel (.xlsx) format files) and downloaded to a folder on your computer.

Export event log

The exported data includes log files for all events, actions and unhandled events in text and Excel formats. The user can make use of the functions such as “filter,” “sort” and “search” provided by Microsoft Excel on the event log data.

Unhandled event(s): Because the latest exported event will be marked, when exporting unhandled events, the exporting event will begin from the first un-exported event.

The filename of all events and action logs in Excel format should be “*ctrlID*_**SupportEvent.xlsx**.”

The filename of unhandled events in Excel format should be “*ctrlID*_**Unhandled_SupportEvent.xlsx**.”

The event log file contains the following columns:

- **Device**: Device name
- **Index**: The order of event occurrences
- **Severity**: Severity is categorized into the following four levels.
  (1) Information: There is no subsystem issue. Users do not have to be informed of the operation result.
  (2) Warning: Some issues occurred and users have to be informed. However, the system has no malfunction risk.
  (3) Error: An error occurred and the system is still operational. However, the system has a malfunction risk if another error occurs.
  (4) Critical: System failure occurred and resulted in serious malfunction.
- **Date/Time**: The date and time of the event occurrence
- **Code**: Event code for looking up entries in the event service guideline
- **Event**: This is the exported message. In the text file, this is the message for general users. In the Excel file, this is the message for first line support personnel.
- **Hyperlink**: This is a hyperlink to content in "Event-Service_Guide_Table.docx" (the troubleshooting guide) related to the event provided to help users easily find information on how to handle the event.

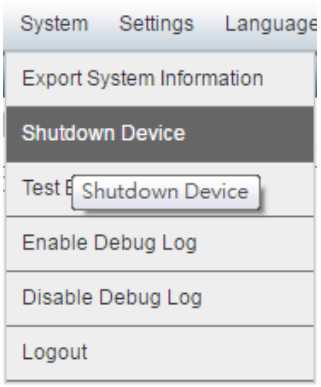
Action log	User actions are also logged for audit purposes. The action log data is exported to the file "*ctrlID*_**ActionLog.txt**" and contains the following columns: ● **Index**: Serial number ● **Date/Time**: The issue date and time of the user action ● **Operation**: The type of the user action ● **Target**: The target of the user action ● **Code**: Operation ID ● **Events**: Descriptions of user actions
Export system configuration	The exported data includes system configuration information in the file "ctrlID_Conf.html," which presents the device and configuration in a tree structure. Each node can be collapsed or expanded. You can use the "find" function provided by the browser to search for keywords.
Export memory dump	When exporting system information, the user can choose whether to also export core dump files. Click the button **With core dump** or **W/o core dump** for the corresponding action. The memory dump will create 4 files (maximum). The maximum size of each file is 512 MB.

Troubleshooting guide	The exported data also includes a file "**Event-Service_Guide_Table.docx**" which is a troubleshooting guide containing all information about error events and handling procedures. Each event includes three entries: ● **Basic Information**: Event ID & severity. ● **Detail**: Event message, root cause and all information about the problem. ● **Recovery procedure**: Steps to take to resolve the problem.
Exported data size limit	The log records include: ● Internal events ● External events ● Act logs (EI command for "**set**") The size limit of each file is 15MB.

Resetting/Shutting Down the System (NOT supported by EonServ)

> Before resetting or upgrading the subsystem, make sure you finish all current tasks and export the system information if necessary.
> This feature is NOT supported by EonServ models.

Go to SANWatch Home > Top menu bar > System, and select Shutdown Device from the menu.

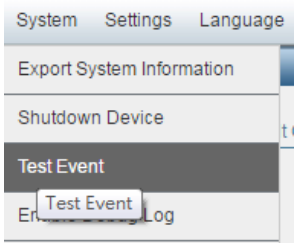


The list of connected devices (RAID or JBOD) will appear. Check the device you want to shut down and click OK.

Currently used storage volumes will become unavailable for hosts and users after shutting down the device. (The user data inside the device will remain intact.)

Test Event

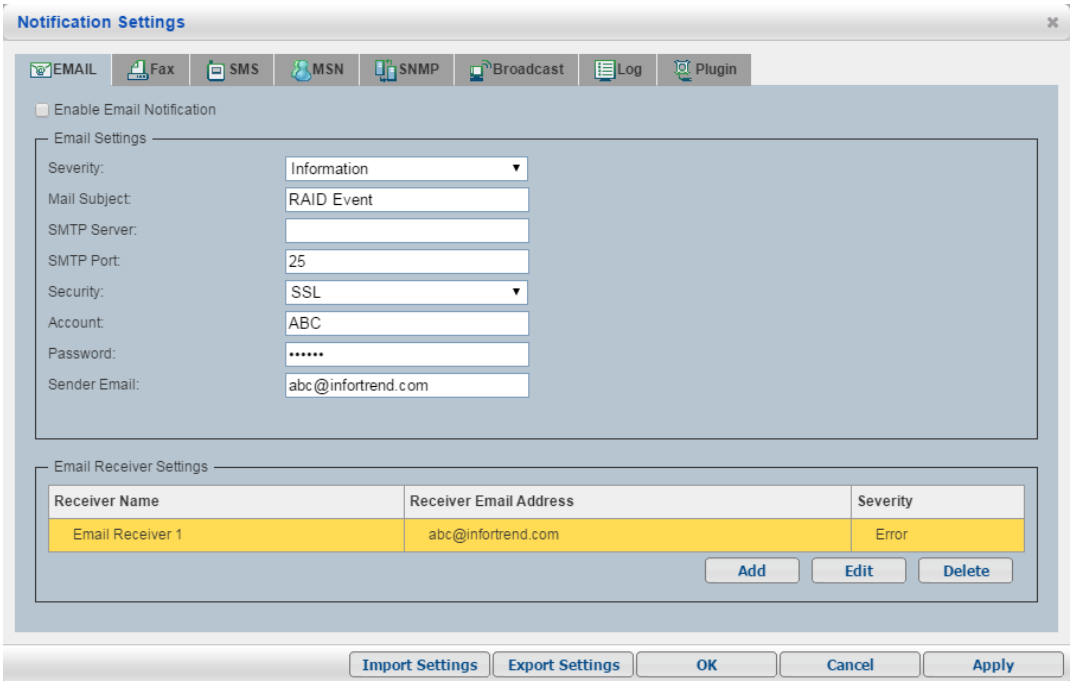
Go to SANWatch Home > Top menu bar > System > Test Event



Steps The confirmation pop-up window will appear to ensure the action of testing being generated.

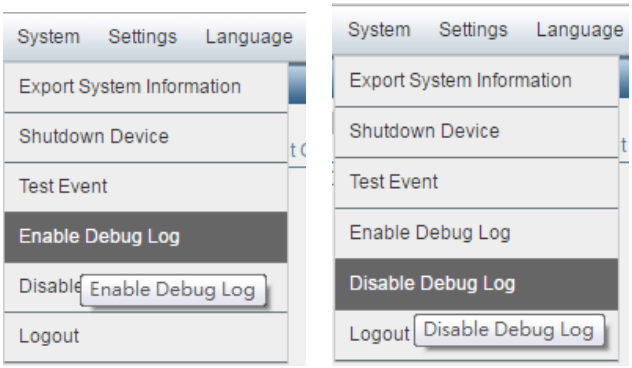
Go to: SANWatch Home > Top menu bar > Setting > Notification Settings

The function is used to check Notification Settings. Before testing this event, check Notification Setting correct or not. The function tab will test settings based on Notification Settings.

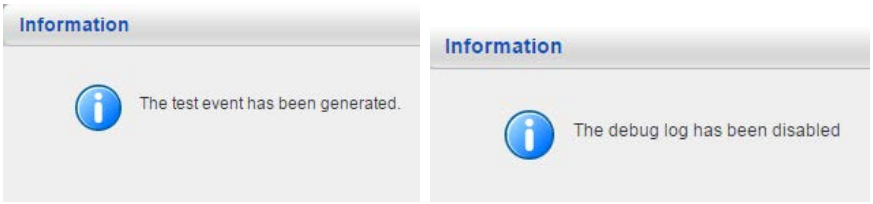


Enable or Disable Debug Log

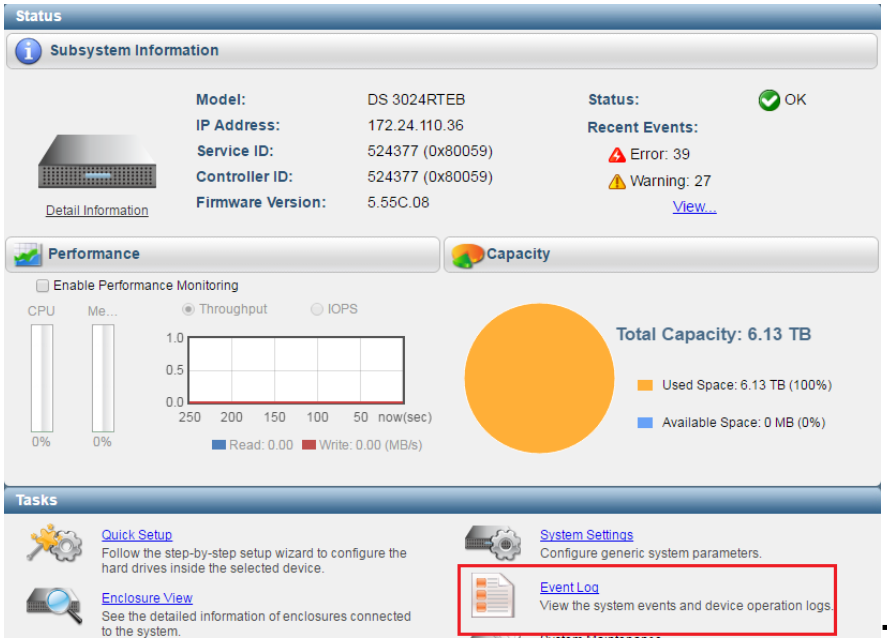
Go to SANWatch Home > Top menu bar > System > Enable Debug Log / Disable Debug Log



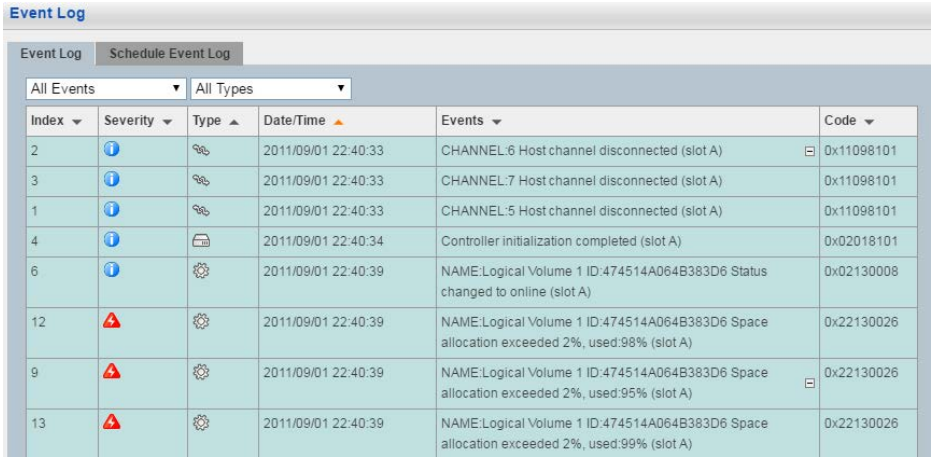
Steps Select from drop-down menu either to enable or disable recording debug logs. The confirmation pop-up window will appear to ensure the action of log recording enabled or disabled.



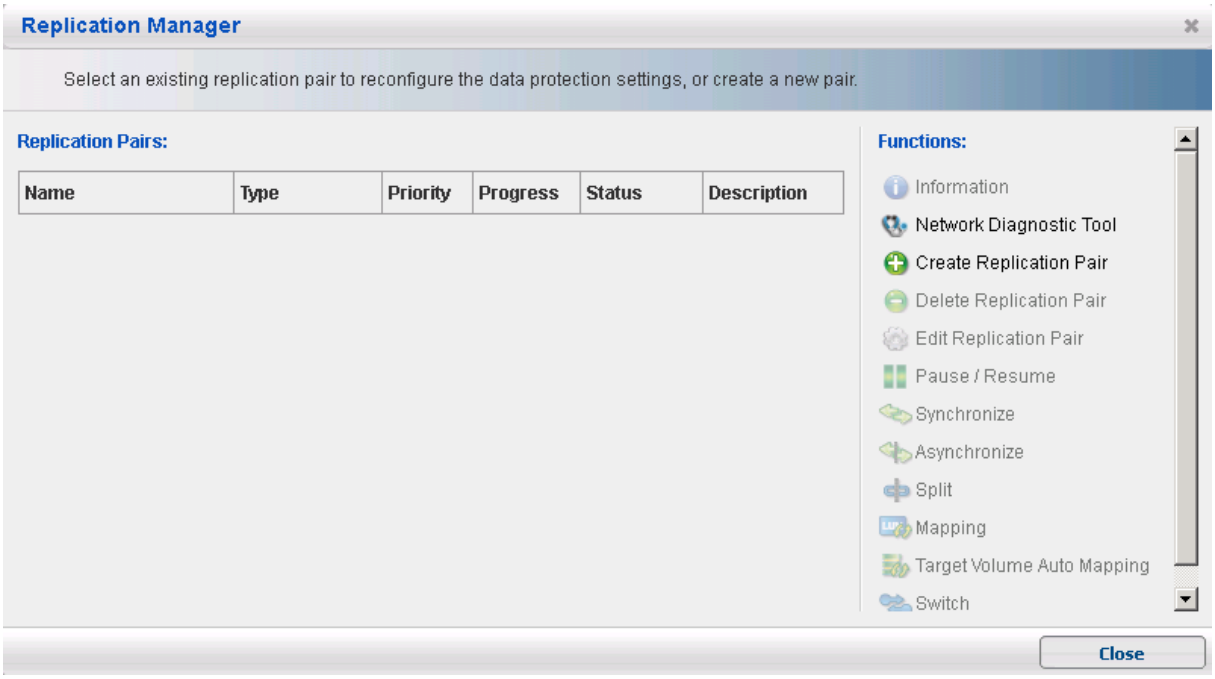
If enabled the logs recording, check Event logs from the list. Go to: Device > Tasks > Event Log.



Click on Event Log to check if debug logs appeared on the list or no debug event shown. If select debug logs disabled, the system will stop recording.



Data Replication



Volume copy and mirror can be done inside the same subsystem or across physically distant locations. For RAID systems, there is no difference between local replication and remote replication in terms of usage but the license is separated. Make sure you have acquired the correct license (local replication or remote replication).

Note

When setting up a copy or mirror task involving volumes in different networks:

- Open TCP/IP ports on the firewall to allow communication between SANWatch and the subsystems. Check TCP/IP and UDP Port Assignments to avoid using default ports.
- You cannot create a remote replication or disk roaming task between EonStor DS and EonStor GS devices.
- To set up an asynchronous volume mirror or volume copy task, activate the DB Flush Agent first. Check Configuring Out-of-Band Flush Using DB Flush Agent for reference.

Firmware Version on Remote Replication

It is strongly recommended to run remote replication only if the same firmware version is shared among the subsystems involved (source and target devices)

Opening the Replication Manager

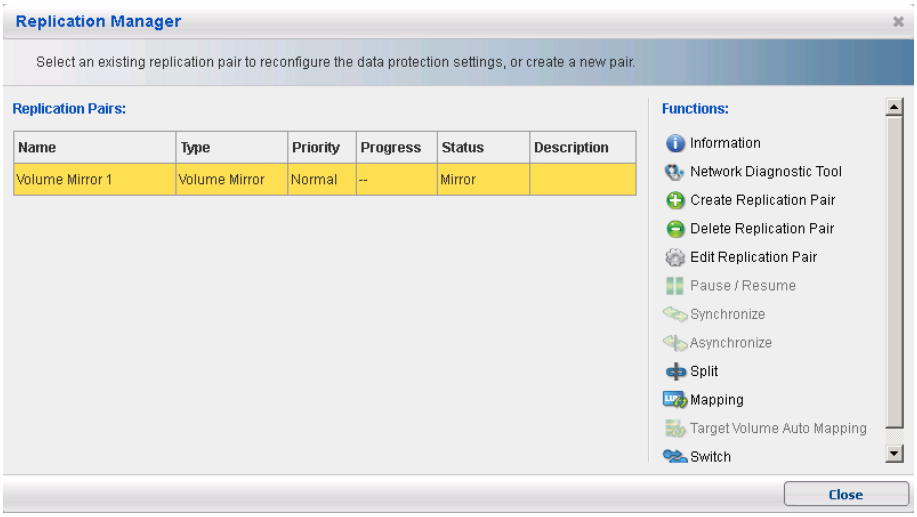
All replication-related operations can be accessed from the Replication Manager window. You may create a new replication pair, view the progress, and reconfigure the settings.

Go to

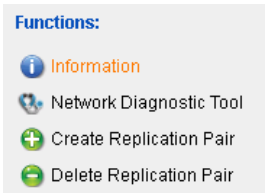
SANWatch Home > Top menu bar > Replication Manager

Steps

When the Replication Manager window opens, the 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 on the replication pair will appear.


Replication Pair Information
Pair Details
Pair ID: 762F073911419D37
Created Time: 03/26/2013 19:20 PM
Completed Time: 03/26/2013 21:20 PM
Split Time: The pair has not been split yet.
Sync Commenced Time: 03/26/2013 21:20 PM
Source Details
Name: Virtual Volume 1
Pool: Pool 2
Volume Set ID: 4FAFAA3E35B045A3
Mapped: No

Diagnosing the Network Status for Replication

You may check the current devices available on the network to see if remote replication pairs can be created safely between devices.

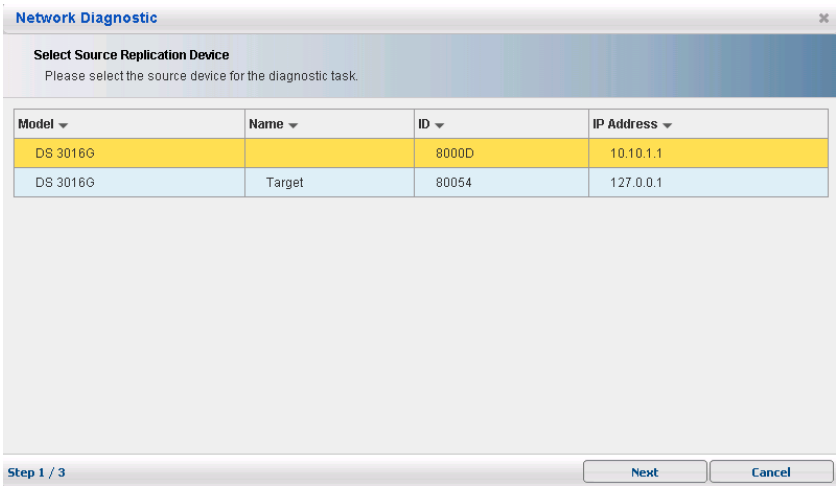
Go to

SANWatch Home > Top menu bar > Replication Manager

Steps

Click Network Diagnostic Tool.

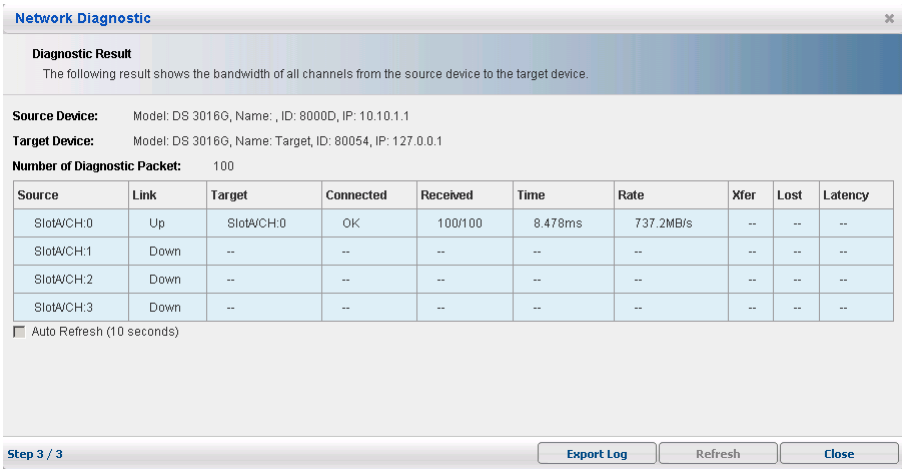
Highlight the source device you wish to diagnose and click Next.



Highlight the system you wish to diagnose and click Next.

Specify the amount of diagnostic data packet (64K per each). Valid values: 1-10000.

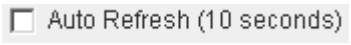
Click Diagnose. The diagnose result will appear.



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

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 result to a local folder, click the Export button.

Creating a Volume Copy

If the target partition (for EonStor DS subsystems) or virtual volume (for ESVA subsystems) has snapshot image(s), you cannot create a volume copy.

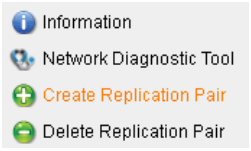
For more information about snapshots, go to the following location and click the Help icon at the top-right corner:
EonStor DS subsystems: SANWatch Home > Device sidebar > Device List > device name > Logical Volumes > LV name > Partitions
ESVA subsystems: SANWatch Home > Pool sidebar > Pool List > pool name > Virtual Volumes

Go to

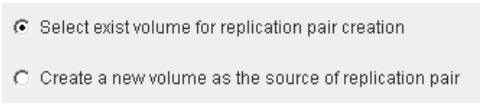
SANWatch Home > Top menu Bar > Replication Manager

Steps

Click Create Replication Pair in the Functions area.

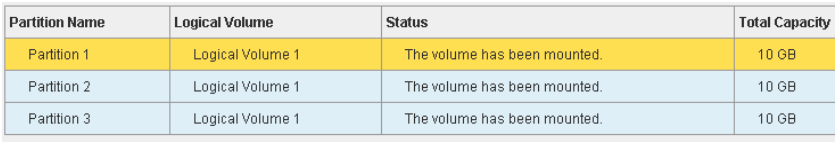


Method 1: Select your source from an existing partition or virtual volume and click on Next.



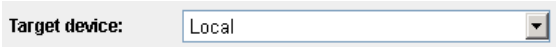
Select your source device and click on Next.

The list of available partitions or virtual volumes will appear. Highlight (yellow) the source and click Next.

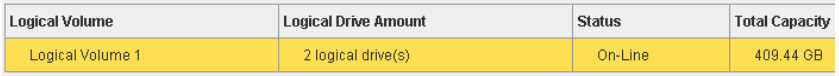


Partition Name	Logical Volume	Status	Total Capacity
Partition 1	Logical Volume 1	The volume has been mounted.	10 GB
Partition 2	Logical Volume 1	The volume has been mounted.	10 GB
Partition 3	Logical Volume 1	The volume has been mounted.	10 GB

Select the target device (hardware) from the drop-down list. If you select Local, then the source and target partitions or virtual volumes are located on the same subsystem.

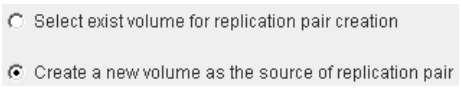


The list of available logical volumes or pools will appear. Highlight (yellow) the target logical volume or pool and click Next.

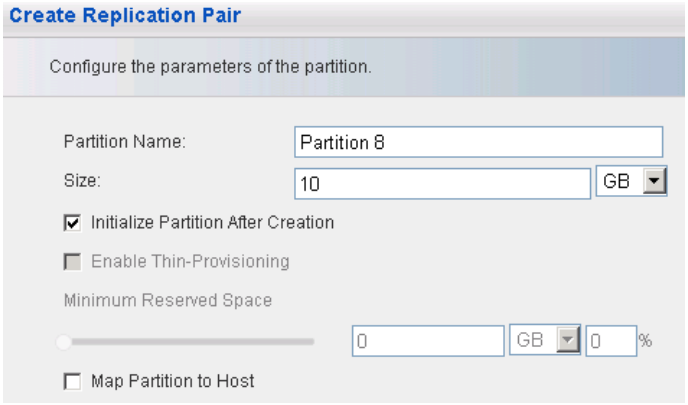


Logical Volume	Logical Drive Amount	Status	Total Capacity
Logical Volume 1	2 logical drive(s)	On-Line	409.44 GB

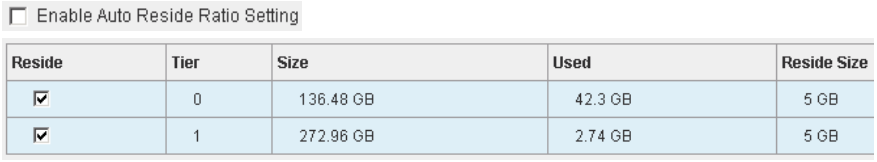
Method 2: Create a new partition or virtual volume as the source.



Click on Next to create a new partition or virtual volume.

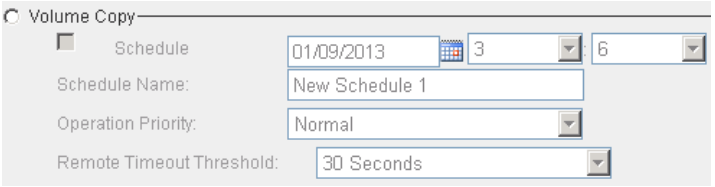


Check the “Enable Auto Reside Ratio Setting” box (for ESVA subsystems only) if you wish and click on Next.

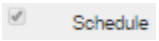


Enter the name of the volume copy.

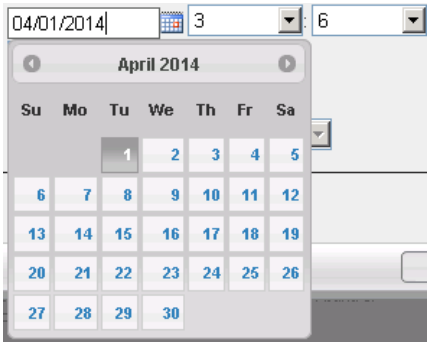
Setup Volume Copy schedule.



If you select Volume Copy, the option “Schedule” will automatically be checked by default.



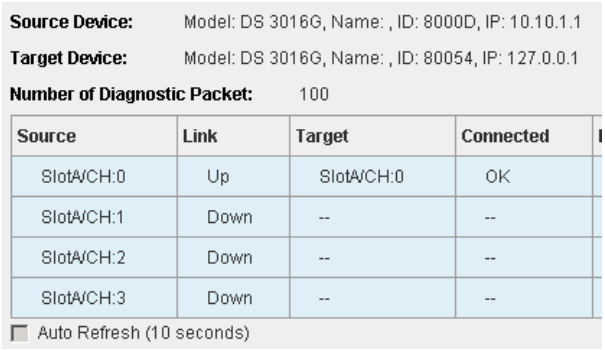
Click in the schedule box and select the date, time (24hr format) and priority by clicking the date in the calendar, choose time and priority from the drop down boxes, then click on Next.



If the source and target partitions or virtual volumes are on located on different subsystems, user may click Diagnose Network to check on the network connection status.

Set the number of diagnostic packets

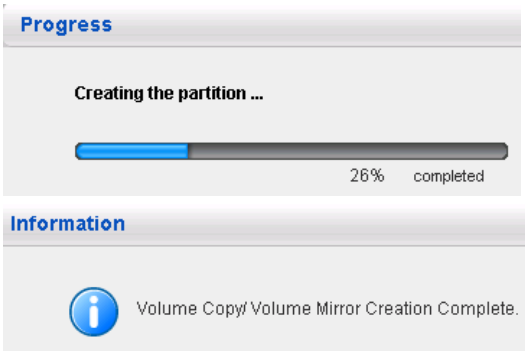
Click Diagnose for connection status.



A summary will appear.

Confirm all settings and click on OK to create the Replication Pair.

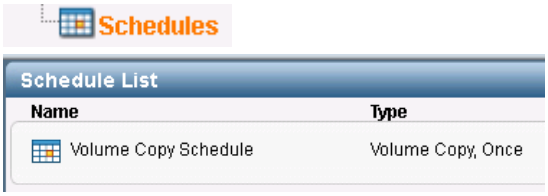
A progress window will show creation progress.



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

Priority

Specifies access priority. For example, higher priority can be assigned to volumes serving applications and lower priority to volumes storing archives or user data.

Remote Timeout Threshold

The remote timeout threshold option allows you to avoid breaking a remote replication pair when the network connection between the source and the target becomes unstable or too slow. You may choose how long the controller will wait (timeout). The replication pair will receive better protection if the timeout period is long, 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 the volume mirror when there is no network activity for the length of the timeout period.

Disabled:

Host I/O may be impacted seriously 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 stopped for the Wait (timeout) period (default: 30 seconds) and will be retried.

Stage 2: Fails to sync to the remote target.

If the target volume cannot be found, the un-synced 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 for several times. If target volume is still not found, sync will be aborted and uncompleted sync 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.

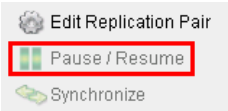
Stage 4: Replication pair will be marked as abnormal

The status of the split replication pair will be updated as abnormal so that users can avoid creating host LUN mapping via such target volume.

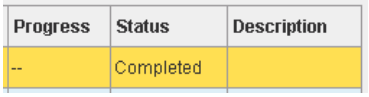
Viewing the Progress

The newly created replication pair will be initialized upon creation or according to the schedule. You may 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 into Completed.



Progress	Status	Description
--	Completed	

If network connection is lost during the process, the status of the replication pair will change into Non-Complete.

Creating a Volume Mirror

Notes

- If the target volume has snapshot image(s), you cannot create a volume mirror.
- Synchronous mirror is NOT recommended over WAN connections as high I/O latency may cause the process to fail.

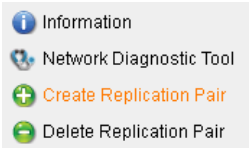
Go to

SANWatch Home > Top menu bar > Replication Manager

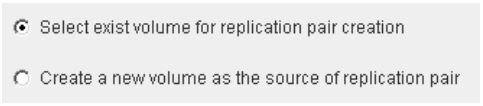
You can also create volume mirrors by schedule. For more information, go to the following location and click the Help icon at the top-right corner:
EonStor DS subsystems: SANWatch Home > Device sidebar > Device List > device name > Schedules
ESVA subsystems: SANWatch Home > Pool sidebar > Pool List > pool name > Schedules

Steps

Click Create Replication Pair in the Sidebar.



Select your source from an existing volume or create a new source volume and click on Next.

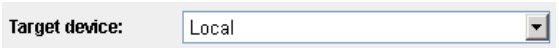


Select your source device and click on Next.

The list of available virtual volumes (for ESVA subsystems) or partitions (for EonStor DS subsystems) will appear. Highlight (yellow) the source volume or partition 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

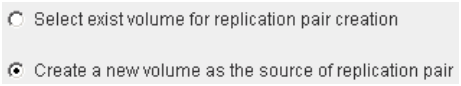
Select the target device (hardware) from the drop-down list.



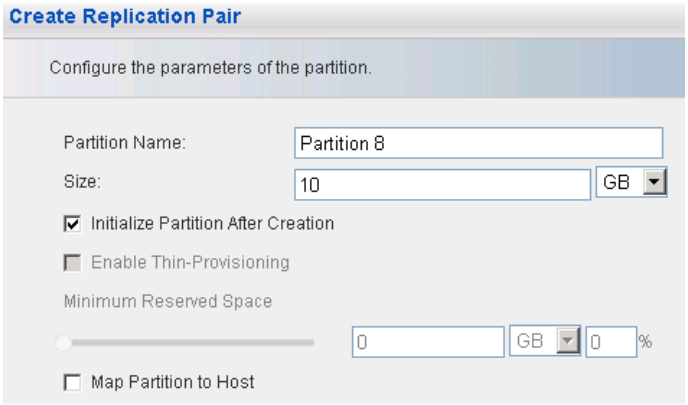
The list of available virtual pools (for ESVA subsystems) or logical volumes (for EonStor DS subsystems) will appear. Highlight (yellow) the target volume and click Next.

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

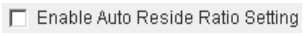
Create a new partition or virtual volume as the source



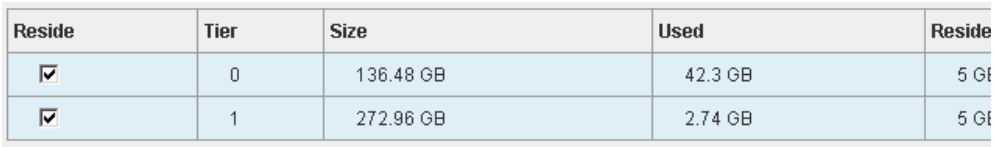
Click on Next to create a new partition or virtual volume.



Check the “Enable Auto Reside Ratio Setting” box if you wish and click on Next.



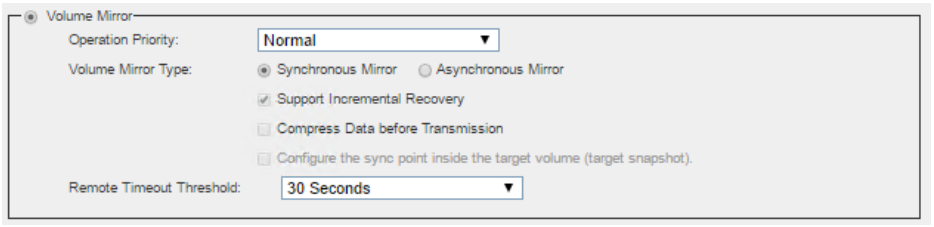
This option is available for ESVA subsystems only.



Reside	Tier	Size	Used	Reside
☑	0	136.48 GB	42.3 GB	5 GB
☑	1	272.96 GB	2.74 GB	5 GB

Enter the name of the volume mirror.

Select Volume Mirror priority and type.



"Support Incremental Recovery" and "Compress Data before Transmission" are available only when the source and the target reside in different locations (remote replication).
"Support Incremental Recovery" is always enabled for synchronous mirror; it is disabled by default for asynchronous mirror.
"Compress Data" is supported by ESVA subsystems only and available for asynchronous mirror only. Furthermore, enabling it requires licensing from Infortrend.

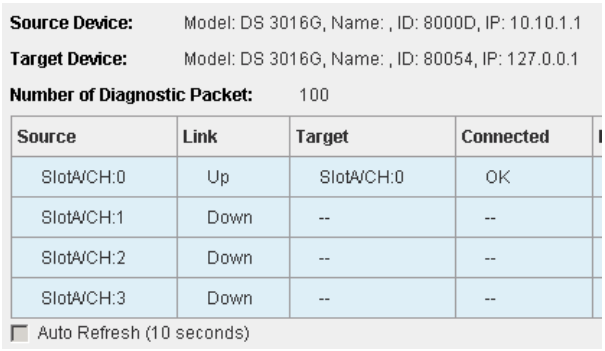
Select the remote timeout threshold. This option defines how long the system will continue to try connecting with the target device when establishing a remote replication connection. If the timeout period is longer, the remote replication connection will become more stable due to fewer disruptions, but system performance will be affected.

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

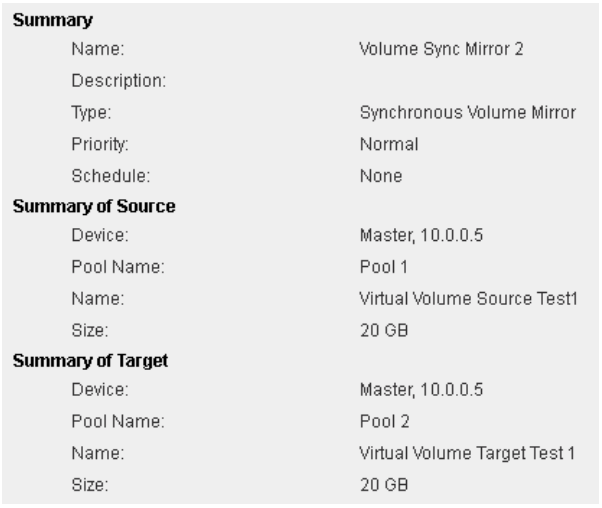
User may click "Diagnose Network" to check on the network connection status.

Set the number of diagnostic packets

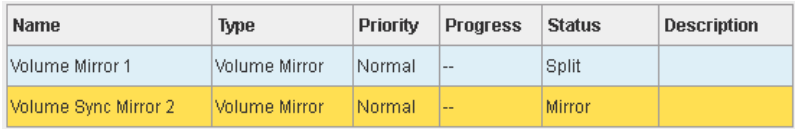
Click on Diagnose for connection status



Click Next. The summary will appear.



Click OK. 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	**Priority**	Specifies access priority. For example, higher priority can be assigned to volumes serving applications and lower priority to volumes storing archives or user data.
	Synchronous / Asynchronous	When the synchronous mode is enabled, the host will write data to both the source and target at the same time. In the asynchronous mode, the host I/O will be allocated to the source volume only, thus allowing higher bandwidth and optimized performance. New data will be written later into the target in batch, avoiding heavy I/O traffic.
	Incremental Recovery	Allows you to “move back” to the source volume if it recovers. The new data accumulated in the target volume during downtime will then be gradually copied to the source volume.
	Compress Data	If the bandwidth is not enough for asynchronous mirroring, compressing data reduces the amount of I/O. This option impacts the subsystem performance by taking up extra computing power.
	Target snapshot	For Asynchronous Mirror only. The system will take snapshots in the target volume for every asyncing task but only the latest snapshot of asyncing target volume will be kept.
	Remote Timeout Threshold	The remote timeout threshold option allows you to avoid breaking a remote replication pair when the network connection between the source and the target becomes unstable or too slow. You may choose how long the controller will wait (timeout). The replication pair will receive better protection if the timeout period is long, 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 the volume mirror when there is no network activity for the length of the timeout period. **Disabled:** Host I/O may be impacted seriously 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 stopped for the Wait (timeout) period (default: 30 seconds) and will be retried.

Stage 2: Fails to sync to the remote target.

If the target volume cannot be found, the un-synced 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 for several times. If the target volume is still not found, sync will be aborted and uncompleted sync 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.

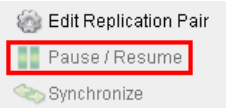
Stage 4: Replication pair will be marked as abnormal

The status of the split replication pair will be updated as abnormal so that users can avoid creating host LUN mapping via such 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 into Completed.

Progress	Status	Description
--	Completed	

If network connection is lost during the process, the status of the replication pair will change into Non-Complete.

Editing/Deleting a Replication Pair

Go to

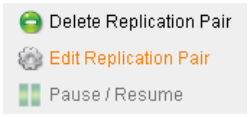
SANWatch Home > Top menu bar > Replication Manager

Editing a Pair

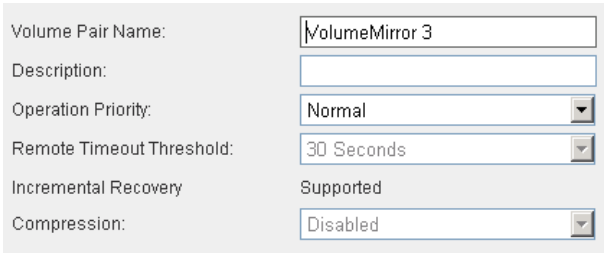
Highlight a replication pair (yellow) in the list.

Name	Type	Priority
VolumeMirror 3	Volume Mirror	Normal
VolumeMirror 3	Volume Mirror	Normal

Click Edit Replication Pair in the Sidebar.



You may change the name and priority of the replication pair and add a short description to it.



Deleting a Pair

Highlight a pair (yellow) in the list.

Name	Type	Priority
Volume Copy	N/A	Normal
Volume Mirror 1	Volume Mirror	Normal

Click Delete Replication Pair in the Sidebar.

Deleting a volume copy pair removes the relationship between the source and target volume: the logical volumes or pools themselves stay intact.

We recommend you to delete volume copy pairs once the volume copy task has been completed, since 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 you do so, the target volume data will become corrupted and thus unusable. Needless to say, the ongoing task will also be interrupted.

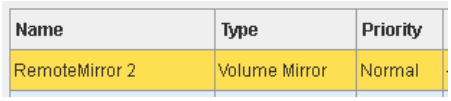
Mapping the Source or the Target to Host LUN

Go to

SANWatch Home > Top menu bar > Replication Manager

Steps

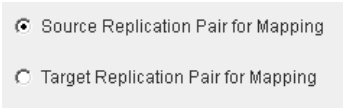
Highlight the replication pair (yellow).



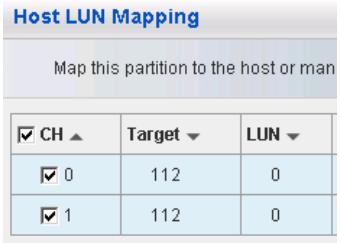
Name	Type	Priority
RemoteMirror 2	Volume Mirror	Normal

Click Mapping in the Sidebar.

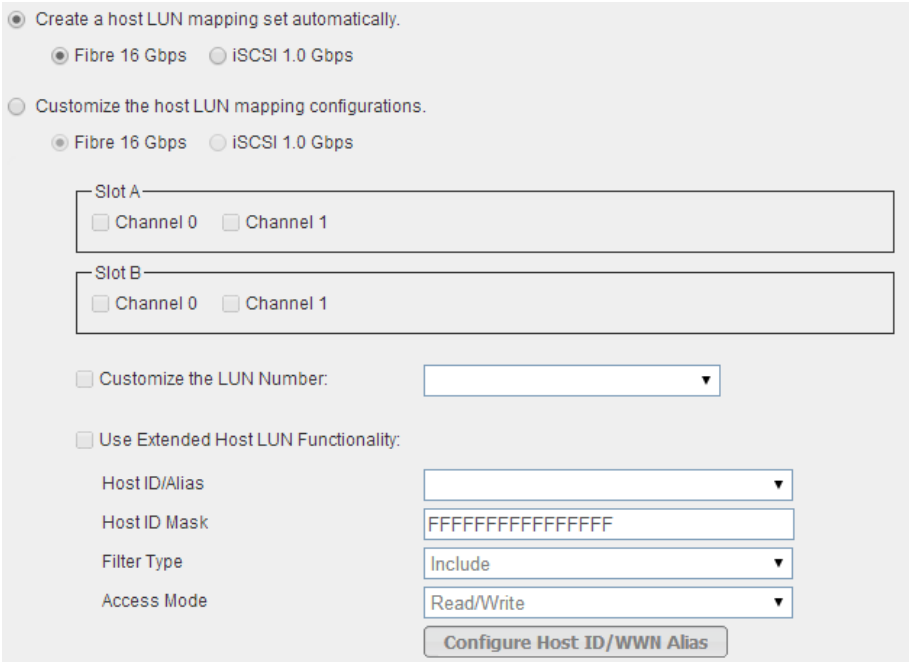
Select whether to map the source or the target (mapping to the target is not always available depending on the replication pair's conditions)



Click OK to select the channel and click on Create.

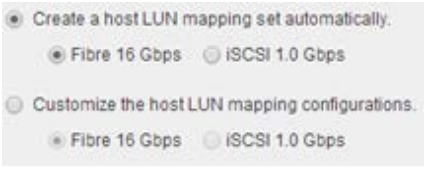


The mapping configuration window will appear.



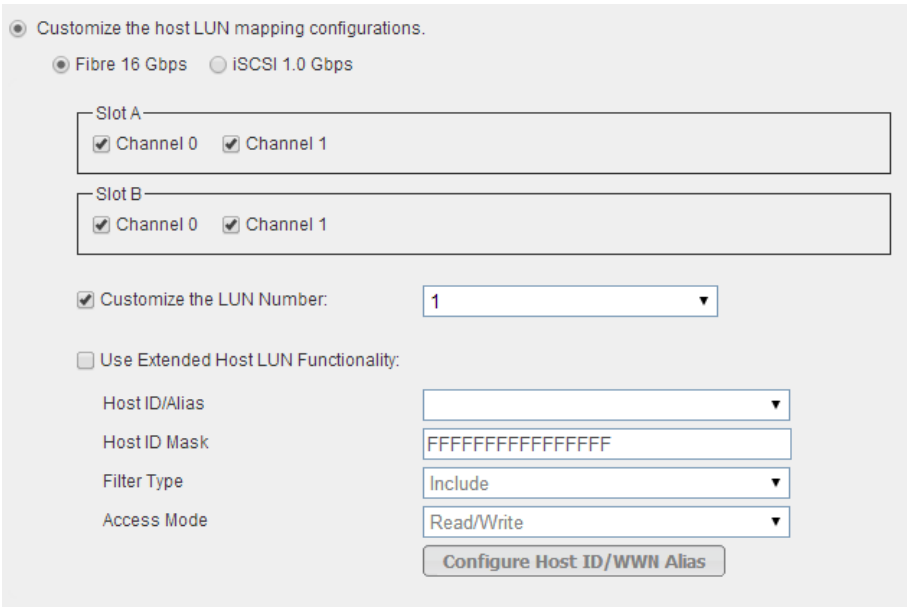
Automatic Configuration

If you let the system create LUN mapping automatically, check it. For hybrid models, you need to select the host type.



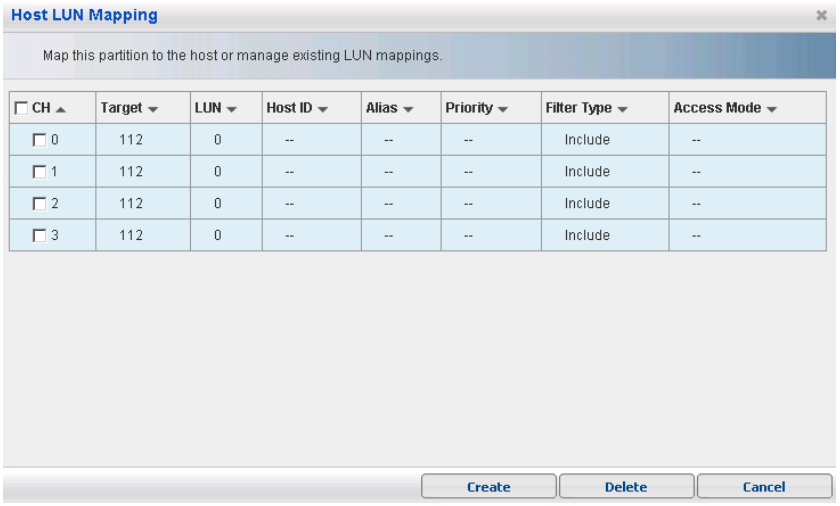
Manual Configuration

If you manually configure the LUN mapping, check the Customize option and select the Channels.



Select the LUN number from the drop-down list.

Click OK. The list of Host LUN Mapping configurations will appear in the window.

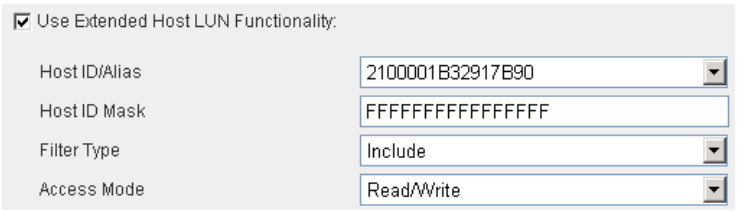


(To delete LUN mappings, you may check the Channels and click Delete).

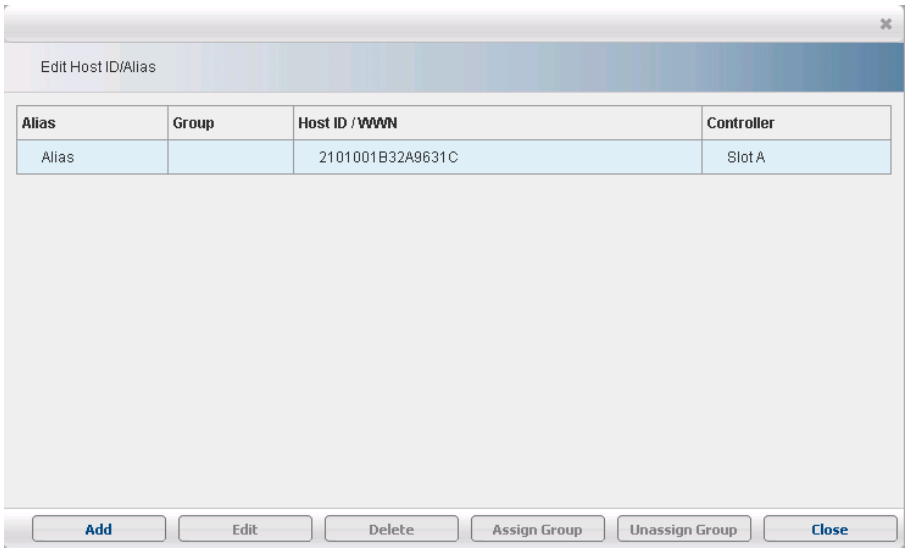
Using Extended LUN Mapping (Fibre Channel)

Extended LUN Mapping is available only for manual configuration.

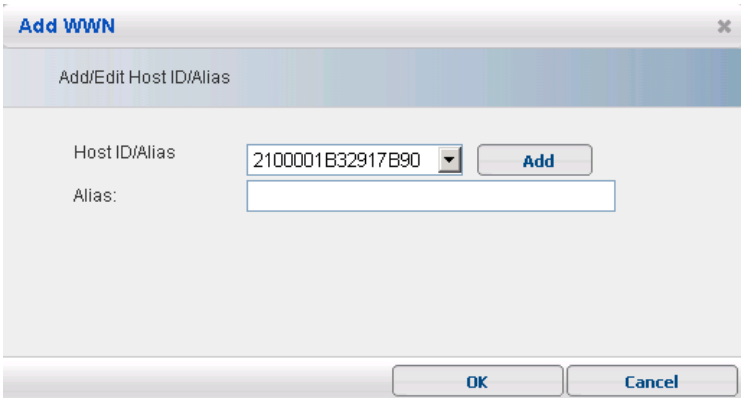
Click Use Extended LUN Functionality and enter or select the parameters.



- Host ID/Alias: Specifies the host ID, referring to WWPN port name. You can also see OUI (Organizationally Unique Identifier) of an ESVA: “00:D0:23” oui. Note: Avoid checking the OUI while mapping host LUN.
- Host ID Mask: Works as a prefix mask in hexadecimal format.
- Filter Type: Specifies whether to allow (include) WWNs or forbid (exclude) them from accessing after filtering.
- Access Mode: Specifies the access right of LUN mapping for the host: read-only or read-write.
- 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.

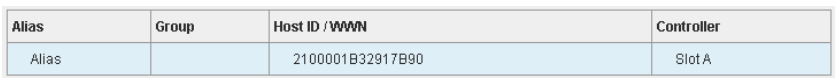


Click OK. Repeat the above process to create more LUN mappings especially if you have multiple HBA ports accessing the same virtual volume (e.g., in high-availability application).

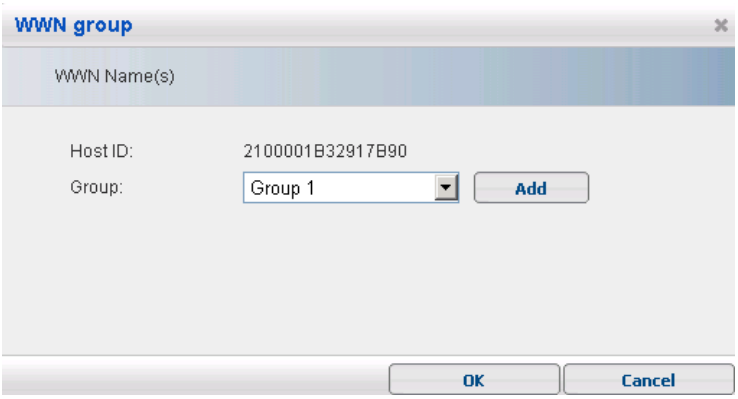
Assigning a WWN to a Group

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

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

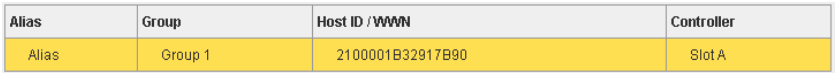


Click Assign Group and select the group from the drop-down menu.



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

The group name will appear in the list.



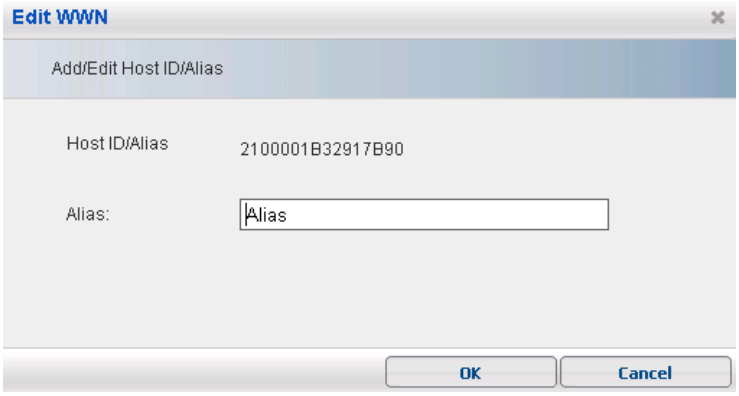
To unassign a WWN from a group, click Unassign Group.

Deleting a WWN Name from the List

Highlight a WWN in the list and click Delete.

Changing the Alias name

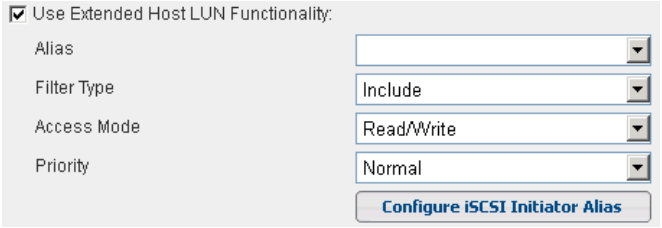
To edit the alias name of the WWN, click Edit and enter the new name.



Using Extended LUN Mapping (iSCSI Channel)

Extended LUN Mapping is available only for manual configuration.

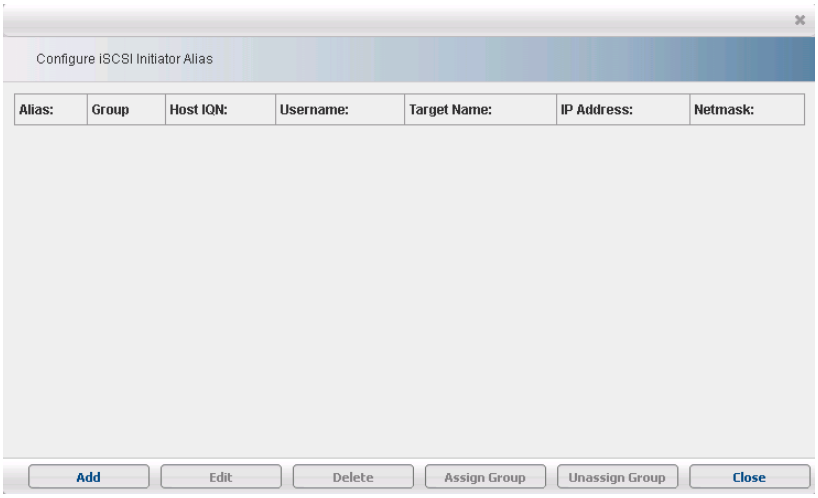
Click Use Extended LUN Functionality and enter the parameters.



- Alias: Specifies a pre-configured iSCSI initiator instance. To create a new initiator alias, click the Configure iSCSI Initiator Alias button.
- Filter Type: Specifies whether to allow (include) initiators or to forbid (exclude) them from accessing after filtering.
- Access Mode: Specifies the access right of LUN mapping for the host: read-only or read-write.
- Priority: Specifies access priority. For example, higher priority can be assigned to volumes serving applications and lower priority to volumes storing 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: Infortrend's storage IQN is composed of the system serial number and 3 more digits in the following format:
  iqn.2002-10.com.infortrend:raid.snXXXXXX.XXX
  6 digits of serial number follows "sn."
  The next 3 digits are: channel number, host ID, LD ownership.
  The LD ownership digit is either "1" or "2" where "1" indicates Controller A and"2" indicates Controller B. The IQN is in accordance with how you map your 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 easy to remember name for the iSCSI initiator.
- 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 setting. The User Password (One-way, from initiator) has to 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) has to 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 sometimes share the same IQN.

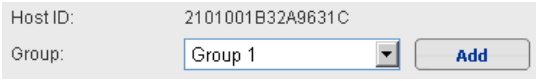
Click OK. Repeat the above process to create more LUN mappings especially if you have multiple HBA ports accessing the same virtual volume (e.g., in high-availability application).

Assigning an Initiator to a Group

A group allows multiple host LUNs to be accessed in a single mask, which becomes 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.

Switching the Roles of a Replication Pair

You may swap the roles (source and target) of a replication pair.

Notes

- To switch the roles, you need to split the replication pair. Make sure there is no important data transaction going at the moment.
- In a replication pair, the target must have the equal or more capacity than the source. Therefore, to switch the roles properly, it is best that the source and the target pair have the same amount of capacity.

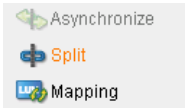
Go to

SANWatch Home > Top menu bar > Replication Manager

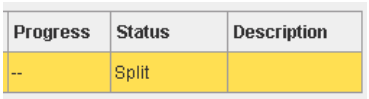
Step 1: Splitting the Replication Pair

Highlight a replication pair.

Click Split in the sidebar.

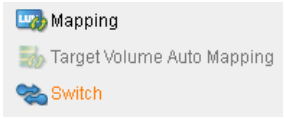


The replication pair status will change into Split.

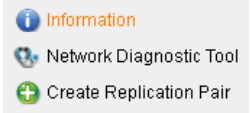


Step 2: Switching the Roles

While the highlighted pair has been split, click Switch in the Sidebar.



The source and the target will swap their roles. After completion, click Information to confirm the new parameters.



Syncing a Replication Pair

You may (manually) synchronize the replication pair when you have to perform incremental data recovery: to repair the damaged content of the source pair, the target data will be copied (synced) into the source.

Notes

- Sync/Async applies to a replication pair that has already been split. Make sure there is no important data transaction going at the moment.
- Synchronous mirror is NOT recommended over WAN connections as high I/O latency may cause the process to fail.

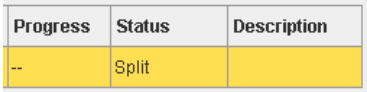
Go to

SANWatch Home > Top menu bar > Replication Manager

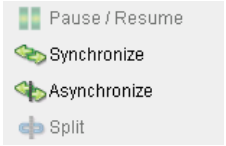
Syncing the Pair

Highlight a replication pair.

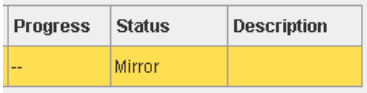
Confirm that the status has been Split.



Click Synchronize in the Sidebar.



The source and the target will be synced and the status will go back to normal.



Using the Incremental Recovery Option in Asynchronous Mirror

The Incremental Recovery option allows you to “move back” to the source volume if it recovers. The new data accumulated in the target volume during downtime will then be gradually copied to the source volume.

> This option affects the I/O performance and takes up extra space in the target volume due to the meta data 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.”

You also have to be remindful of the source volume condition:

- If the source volume is still missing, you 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, you have to switch the source and target role first, and then start asynchronous mirroring. See below for detailed steps.
- The target volume must be unmapped.

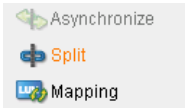
Go to

SANWatch Home > Top menu bar > Replication Manager

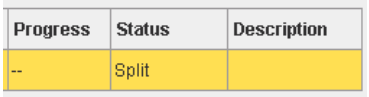
Step 1: Splitting the Replication Pair

Highlight a replication pair.

Click Split in the sidebar.

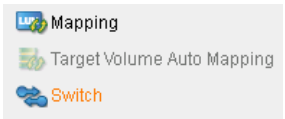


The replication pair status will change into Split.



Step 2: Switching the Roles

While the highlighted pair has been split, click Switch in the Sidebar.



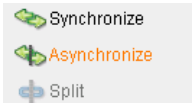
The source and the target will swap their roles. After completion, click

Information to confirm the new parameters.

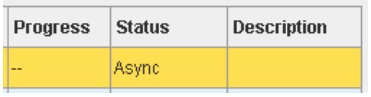
Step 3: Recovering the Pair

The source volume has become the target, and the target volume becomes the source.

Click Asynchronize in the Sidebar.



Wait until the status becomes Async.



Progress	Status	Description
--	Async	

Start the asynchronous volume mirror process. Then original source volume will receive the incremental difference form original target and keep each other synced.

Select the Role Switch function again. The original source volume will go back to the source of the volume pair, completing the recovery process.

The incremental recovery process can be applied only once per pair.

Configuring Automatic Failover for Remote Replication

The automatic failover function helps achieving continuous data transaction when a replication pair gets broken. When the host (recovery) agent fails to locate the source volume of a replication pair due to a disaster such as power outages, it will try to map the target volume to the host for failover. Because the target volume is a copy of the source, users can continue their operations using the data on the target side.

> Because the failover job is engaged by the agent and needs the mapping operation, it will still cause downtime on the host for seconds or even minutes (depends on the environment).

Note

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 being mapped
- This feature is available only for synchronous volume mirror tasks, with in-band configurations (in **Data hosts**) completed on both the source and target sites. Check Adding a Host for reference.

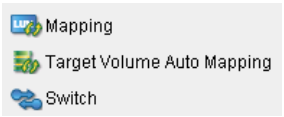
Go to

SANWatch Home > Top menu bar > Replication Manager

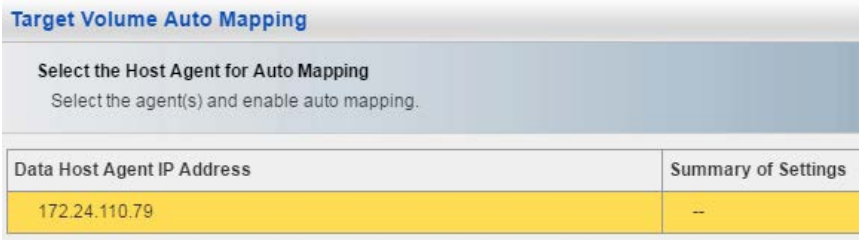
Steps

Highlight a replication pair.

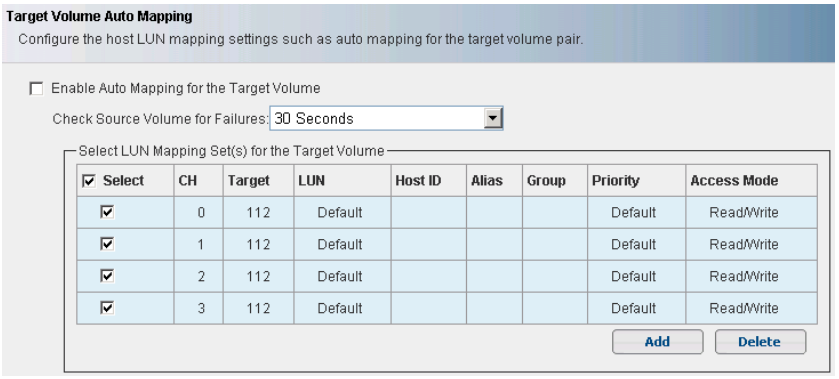
Click Target Volume Auto Mapping in the Sidebar.



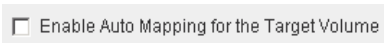
Select the host agent for configuring auto failover and click Next.



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 when it fails.

- LUN Mapping List: Select the LUN mapping for the target volume. You may create a new LUN mapping (see the next step) by clicking on Add.

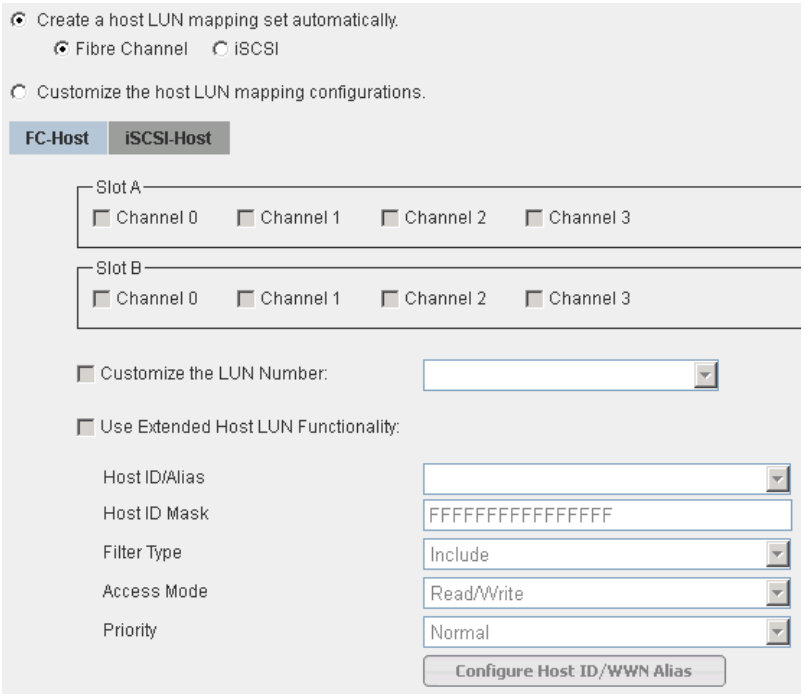
  

- Trigger a File (optional): Check this box to run a script or program after mapping the target volume to the host. For example, you may run a scanning script file.

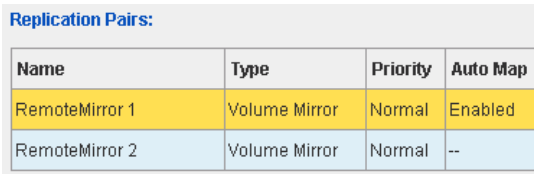
  

To add a new LUN mapping, click Add.

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



Click OK. The “Auto Map” column shows the current Auto Failover (Mapping) status of the replication pair. (Empty means no setting has been configured).



Replication Pairs:

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

Remote replication and disk roaming cannot be executed between EonStor DS and EonStor GS.

Notifying Users of System Events

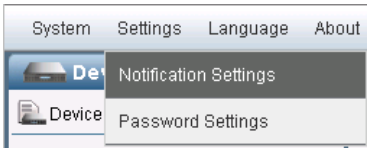
The following notification services are available:

- **Phone Home:** Notify Infortrend service center of critical events through an email message (ESVA subsystems only).
- **Email**: Notifies users through an email message.
- **Fax**: Notifies users through a fax message.
- **SMS**: Notifies users through an SMS mobile phone message.
- **MSN**: Notifies users through an MSN computer chat message.
- **SNMP**: Notifies users through SNMP protocol.
- **Broadcast**: Sends notifications via LAN networks.
- **Log**: Notifies users by sending system logs via email.
- **Plugin**: Activate user-specified applications when a system event occurs.

Activating Notification Settings

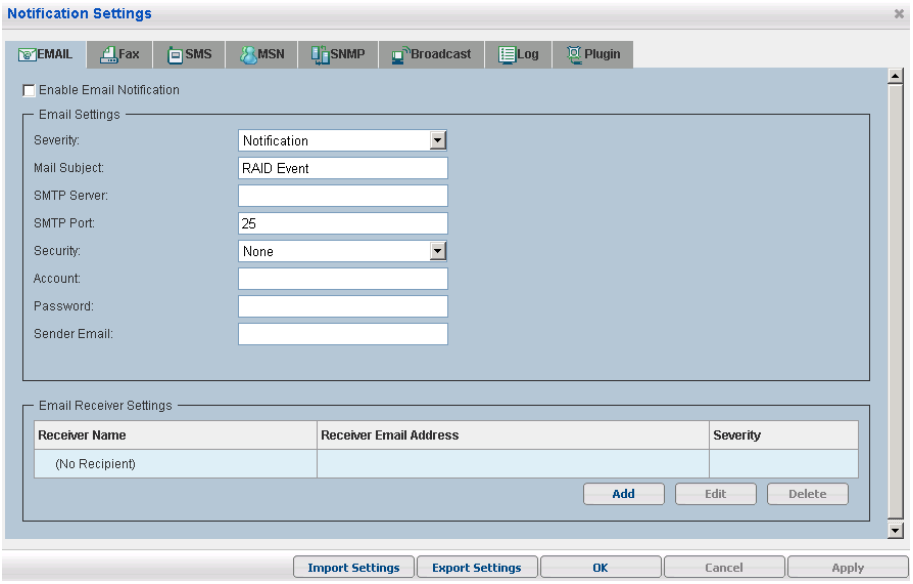
Go to

SANWatch Home > Top menu bar > Settings > Notification Settings



Steps

The Notification Settings will appear in the main window, showing email notification settings by default.



Notifying via Phone Home (ESVA subsystems only)

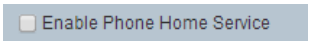
The Phone Home feature allows critical events will automatically be delivered to Infortrend service center.

Go to

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

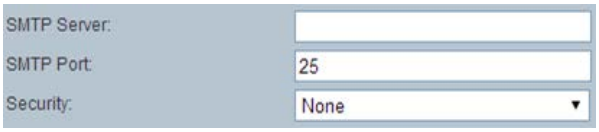
Configuring Phone Home

Check Enable Phone Home Service.



Choose Enabled from the Daily Heart-Beat Check drop-down menu if you want to deliver a system health report back to Infortrend on a daily basis.

Enter the SMTP server's IP address and port number through which you wish to deliver the Phone Home package. Choose SSL from the Security drop-down menu if you want Email to be transmitted in encrypted format.



Enter a valid email account, password, and address.

Fill in your company name, contact person (system administrator), and a phone number with which Infortrend can contact you.

Click Send Information Back to send the health report back to Infortrend immediately. Click Test Phone Home to test the validity of your Email account and the contact with Infortrend's service center. You should be able to receive an Email reply.

Infortrend does not have access to the data in your ESVA subsystem.

Notifying via Email

Email notification automatically sends an email message to users when a system event occurs.

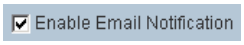
Go to

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

Adding a new email receiver

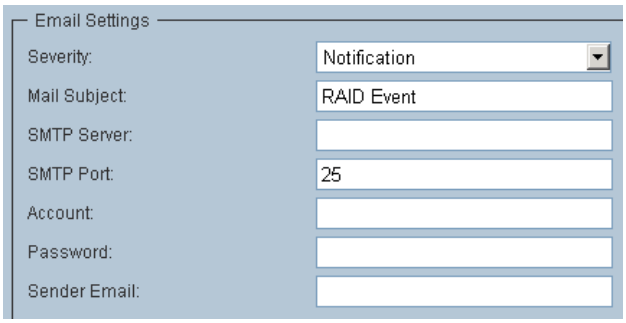
Enabling Notification

Check Enable Email Notification.



Configuring Email Sender Settings

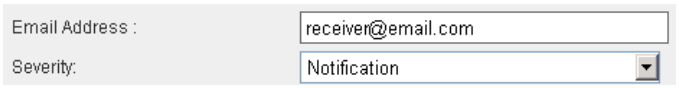
Enter the sender parameters in the Email Settings corner.



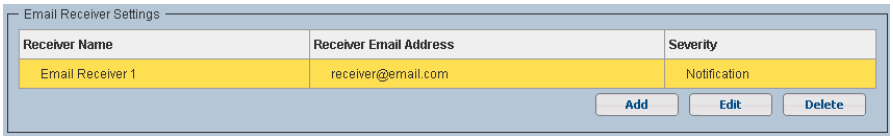
Configuring Email Receiver Settings

To add a new email receiver, click Add in the Email Receiver Settings corner.

Enter the parameters and click Add to confirm.



The new email receiver will appear in the *Email Receiver Setting* corner.



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	**Email Address**	Specifies the email address of the receiver.
	Severity > Notification	Notifies users whenever a system event occurs.
	Severity > Warning	Notifies users of all warning and critical messages.
	Severity > Critical	Notifies users only when critical issues occur.
	SMTP Server	Specifies the SMTP mail server name. Example: infortrend@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.

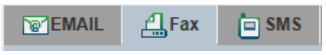
Notifying via Fax

You need to install the following modules to your computer before using 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 new FAX receiver

Enabling Notification

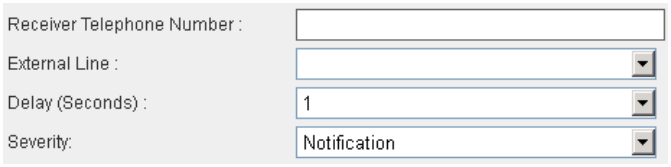
Check Enable Broadcast Notification.

Configuring Fax Settings

Specify the severity and the fax queue size in the Fax Settings corner.

Click Add in the Fax Receiver Setting corner.

Enter the parameters and click Add.



The new fax recipient will appear in the *SNMP Receiver Setting* corner.

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.

Notifying via SMS

You need to install one GSM modem to your computer for using this feature. The following modems are tested to comply with SANWatch.

- Siemens TC35
- Wavecom Fast Rack M1206

Go to

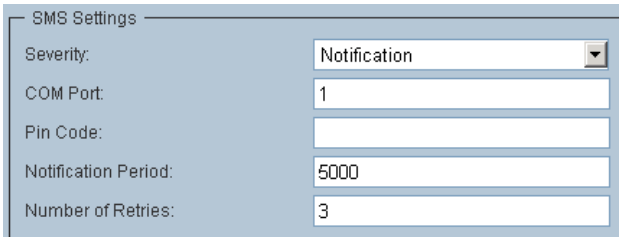
SANWatch Home > Top menu bar > Settings > Notification Settings > SMS tab

Enabling Notification

Check Enable SMS Notification.

Configuring SMS Sender Settings

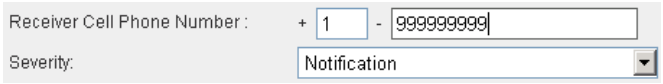
Enter the sender information and specify the severity.



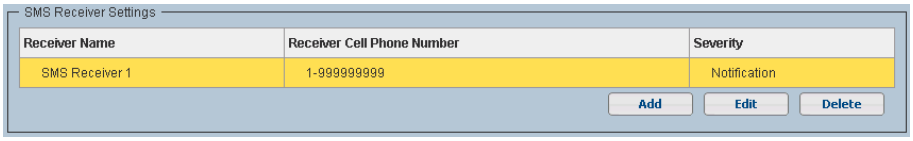
Configuring SMS Receiver Settings

Click Add in the SMS Receiver Setting corner.

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 message.
	Number of Retries	Specifies how many times the SMS will be resent in case it does not reach the receiver.

Notifying via MSN

You need to have a valid MSN or hotmail account to use this feature. Notices will be sent to a Skype installed device.

Go to

SANWatch Home > Top menu bar > Settings > Notification Settings > MSN icon

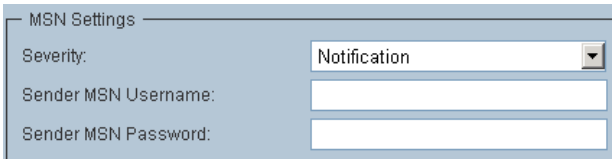
Adding a new MSN receiver

Enabling Notification

Check Enable MSN Notification.

Configuring MSN Sender Settings

Enter the sender account (username and password) and specify the severity.

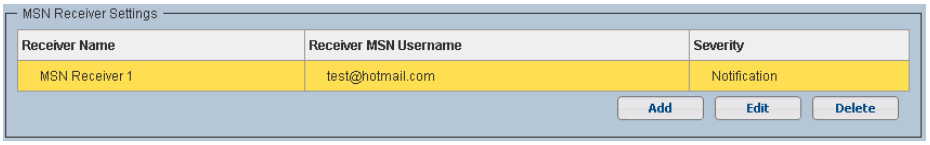


Configuring MSN Receiver Settings

Click Add in the MSN Receiver Setting corner.

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

MSN Account — Specifies the MSN chat account name. Example: Infortrend@hotmail.com.

Sender MSN Account	Specifies the MSN chat account name of the sender. Example: Infortrend@hotmail.com
Sender MSN Password	Specifies the password for the sender MSN account.
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.

Notifying 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

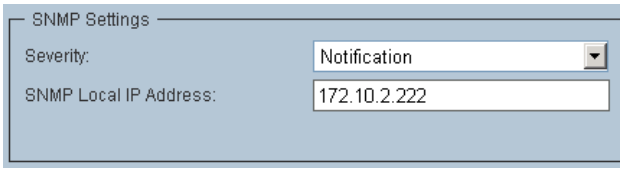
Adding a new SNMP receiver

Enabling Notification

Check Enable SNMP Notification.

Configuring the Local Side

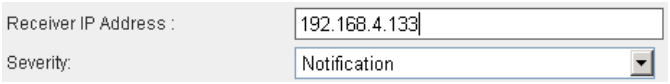
Select the severity and enter the IP address of the local side.



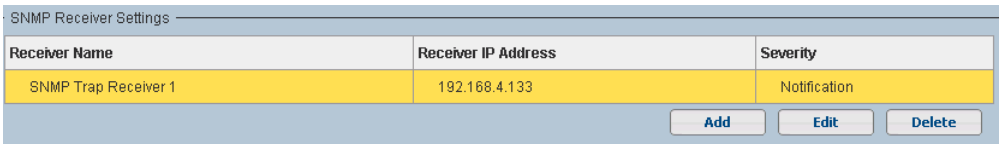
Configuring the Remote Side

Click *Add* to add a new 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.

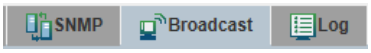
	Example: 192.168.4.133
Severity > Notification	Notifies users of all events.
Severity > Warning	Notifies users of all warnings and critical events.
Severity > Critical	Notifies users only when critical issues occur.
SNMP Local IP	Specifies the IP address of the SNMP sender. Example: 192.168.4.133

Notifying via Broadcasting

Broadcasting sends notifications via LAN networks.

Go to

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



Adding a new Broadcasting receiver

Enabling Notification

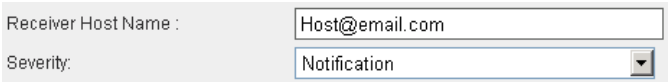
Check Enable Broadcast Notification.

Configuring Settings

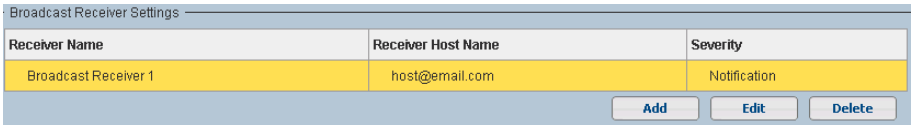
Click Add in the Broadcast Receiver Settings corner.

Enter the parameters and click *Add*.

The host name must be entered as an email address.



The new Broadcast 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 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.

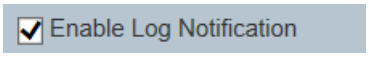
Sending System Log to Users

Users may periodically receive system log information by emails.

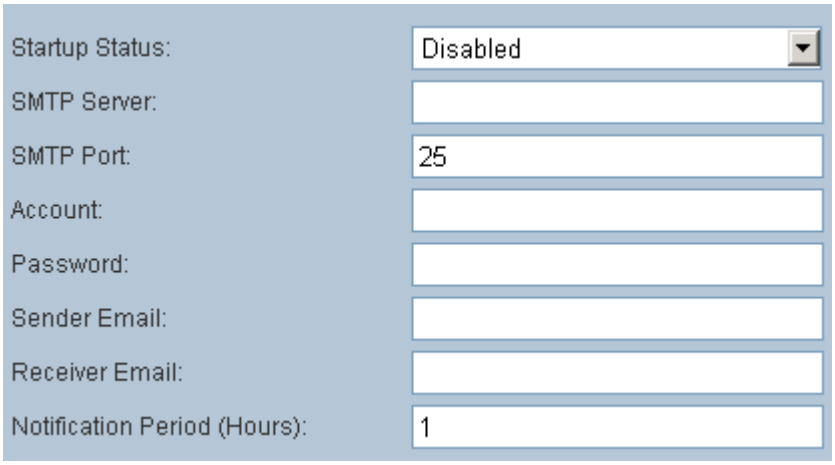
Steps

Click the Log tab in the Notification Settings menu. (The log notification setting appears by default when you activate the Notification Settings.)

Check Enable Log Notification.



Enter the notification parameters.



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

Startup Status	Enables or disables the log notification.
SMTP Server	Specifies the SMTP mail server name. Example: infortrend@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 receiver’s email address.
Notification Period	Specifies how frequently the log will be sent to the receiver.

Activating Applications upon Events

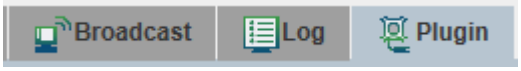
You may activate user-specified applications when a system event occurs.

Steps

Copy the plug-in executable file into the folder. Example: *Application.exe* (in case of Windows)

Activate the Notification Settings.

Click the Plugin tab in the Notification Settings menu. The Plugin setting will appear.

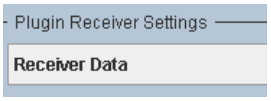


Creating the Plug-in

Click Create Plugin in the Plugin corner and enter the details of the plugin program.

Creating the Receiver

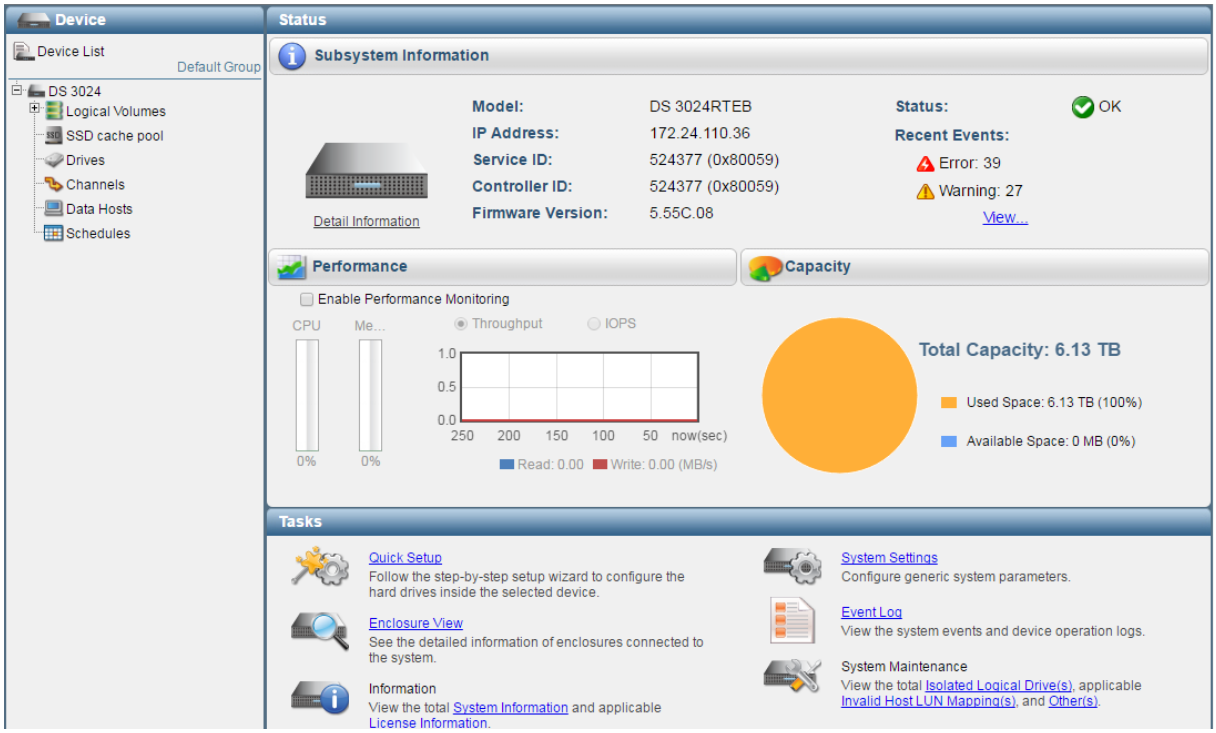
Click Add to show an input field dialog box. Enter the configuration string to be read when the application program starts. A configuration argument may look like this:
"\plugin\userprogram.exe uid=xx model=xxx-xxx ip=xxx.xxx.xxx.xxx ctrlrName=N/A severity=1 evtStr="Evt String" recv="customized string"



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 plug-in subfolder

Working with Devices



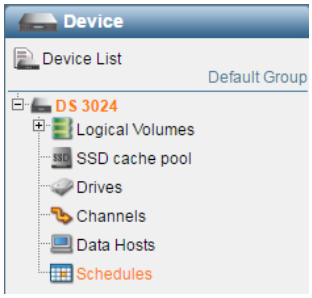
This chapter describes how to view and configure hardware parameters of a device, including system performance, event log, hard disk drive configuration, and invalid/isolated logical drive and host LUN settings.

Viewing the Overall Status

The status of each device (RAID system or JBOD expansion enclosure) is summarized in the Subsystem Information page, where you can quickly grasp the hardware configuration, performance, storage capacity.

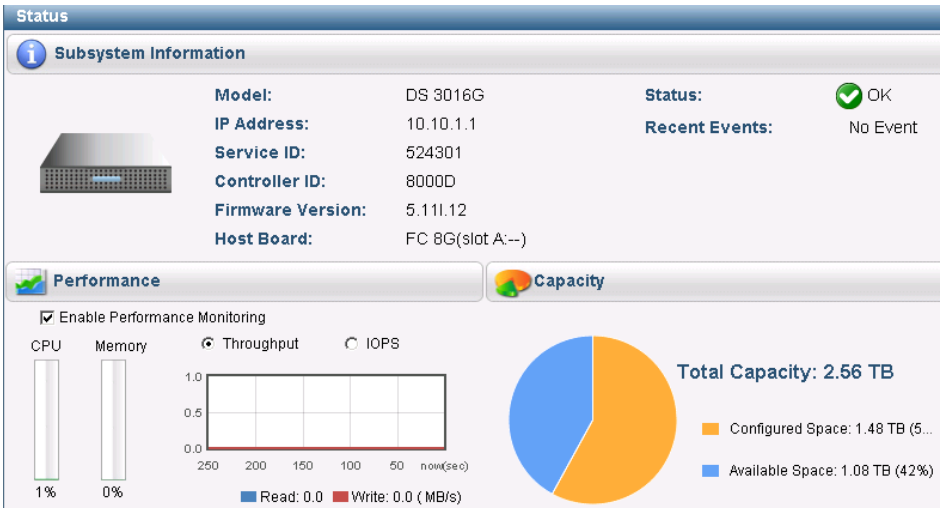
Go To

SANWatch Home > Device sidebar > device name



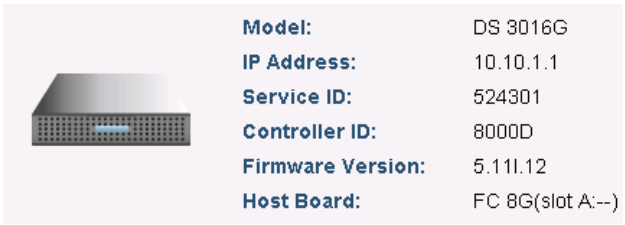
Viewing the Subsystem Information

The device status will be summarized in the Status corner.



Hardware Configurations

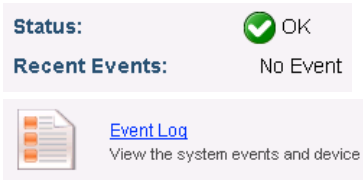
The basic system configurations and overall system status will be listed in the Subsystem information corner. You can see the model name, IP address, controller ID (might be required when receiving technical support), and firmware version.



Events

Most recent system events will be listed in the Recent Events corner. To view all

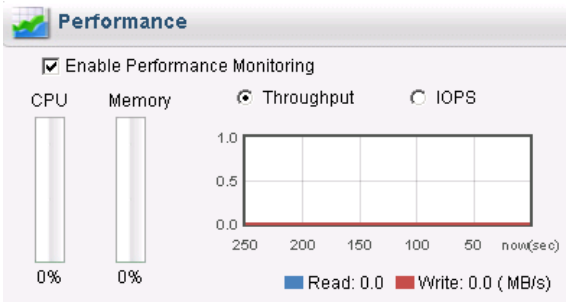
past events, click the Event Log menu in the Tasks corner.



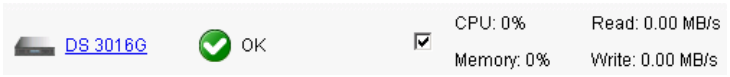
Performance Monitor

Check the Enable Performance Monitoring checkbox to see the CPU/memory usage and read/write throughput.

The Performance Monitor is disabled by default to save system resources.

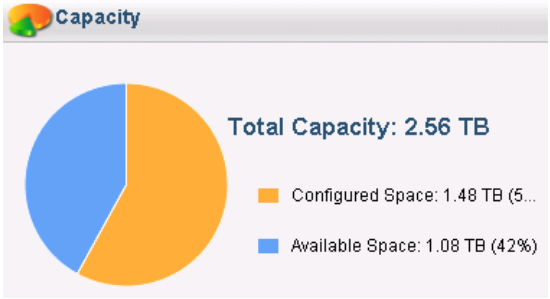


You may also click Device List in the top-left corner to view the summary of system performance in the Device Status list view.

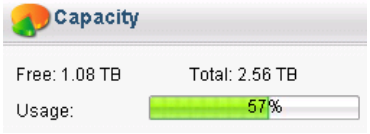


Storage Capacity

See the amount and ratio of used (configured) capacity and the remaining (available) capacity.



You may also view a quick summary in the Device Status list view.

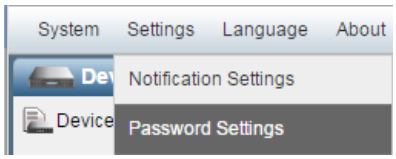


Changing Login Passwords

You can modify the default login password or set a new password for logging into SANWatch management host or accessing storage subsystems.

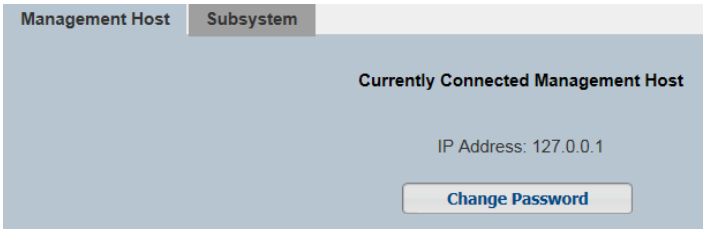
Go to

SANWatch Home > Top menu bar > Settings > Password Settings



Changing SANWatch Login Password

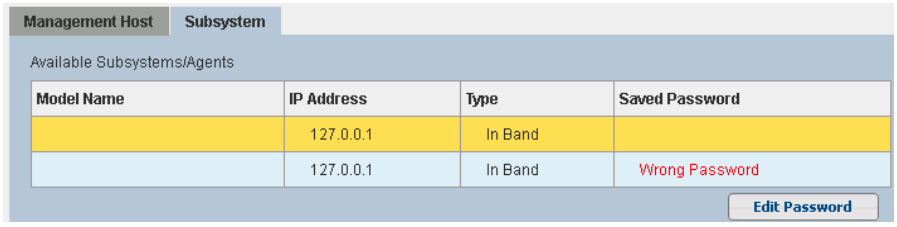
Select the Management Host tab, click Change Password, and then change the login password of the SANWatch management host.



Assigning a Password to a Subsystem

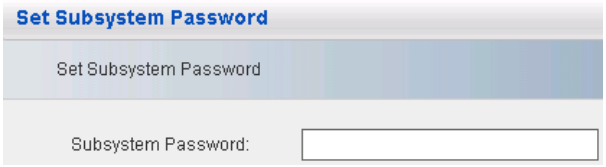
> Once you set up a password for the subsystem, you need to enter it whenever you try to access or configure the hardware setting for that subsystem.

Select the Subsystem tab. The list of subsystem passwords are listed.



Highlight the storage subsystem from the list and click the Edit Password button.

Enter the new password.



After specifying a password, when you try to access the hardware device page, you will be asked to enter the password.

Note To reset the passwords, restore factory settings.

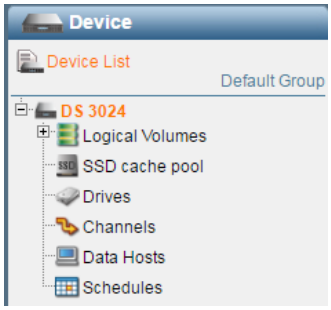
Monitoring System Performance

You can see the current system performance in a glance from the device home page. The System Information corner allows you to see further detailed information including controller throughput and cache usage.

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

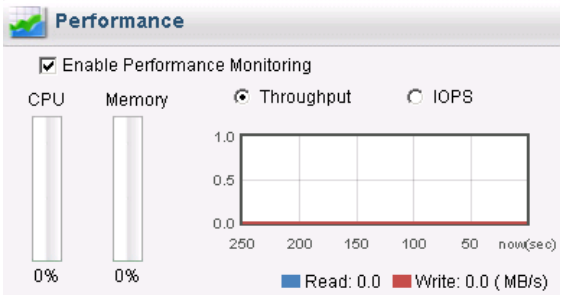
Overall System Performance

Go to SANWatch Home > Device sidebar > device name.



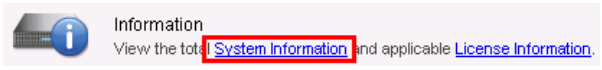
Check the Enable Performance Monitoring checkbox to see the CPU/memory usage and read/write throughput.

> The Performance Monitor is disabled by default to save system resources.



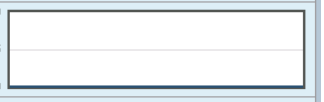
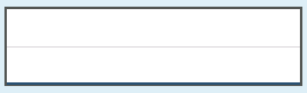
Controller Performance and Cache Usage

Click System Information in the Tasks corner.



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

Check the item you want to monitor: Controller Read/Write performance and cache usage (dirty cache).

Operation Description	Value	Graph
☑ Primary Controller Disk Read/Write Performance (MB/sec)	0.00	
☑ Secondary Controller Disk Read/Write Performance (MB/sec)	0.00	
☑ Dirty Cache (%)	0.00	

Viewing the Hardware Status LED

The Enclosure View gives you a quick overview of the currently installed hardware modules (hard drives, power supplies, controllers) in the device as well as the hardware status LEDs.

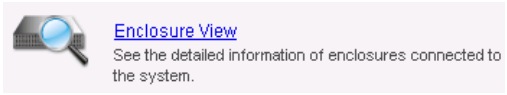
> For precise definition and status of the hardware modules and their LEDs, refer to the hardware manual.

Go To

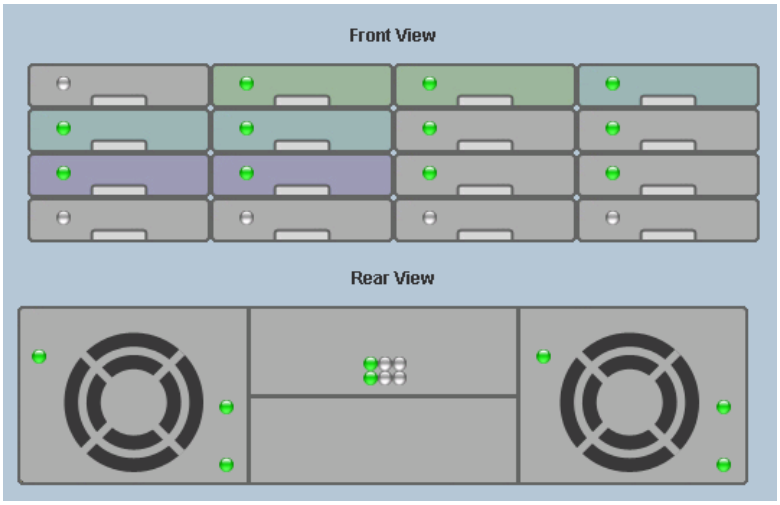
SANWatch Home > Device sidebar > Device List > device name> Tasks corner

Enclosure View

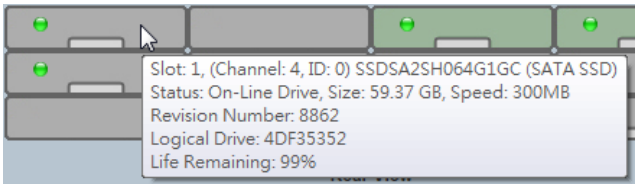
Click Enclosure View in the Tasks corner.



The front/rear view of the device will appear. Each circle (green/red) indicates an LED indicator.



To have a quick view of a hardware module's info, hover your mouse over the module, and the info will be displayed in a tooltip.



> "Life Remaining" is available for SSD drives only.

Hard Drives (Front View)

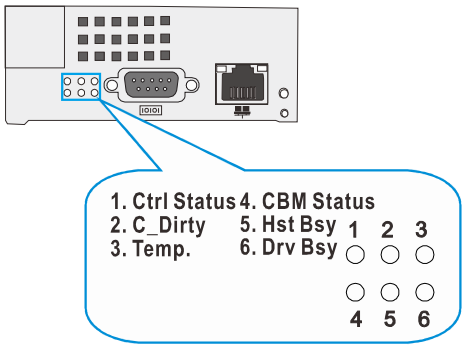
-  : Currently installed
-  : Currently uninstalled or in an error state

Power Supplies (Rear View)

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

Controllers (Rear View)

 : The six LEDs indicate controller status LEDs.



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. It is also lit during the initialization process.
2. C_Dirty	**Amber**	**Amber** indicates the following: - Cache Memory is dirty. - Data in flash backup module is being flushed to cache. - Errors occurred with cache memory (ECC errors). - Data is being flushed from flash backup module to drive (when power is restored). - Battery voltage is lower than 2.5V.

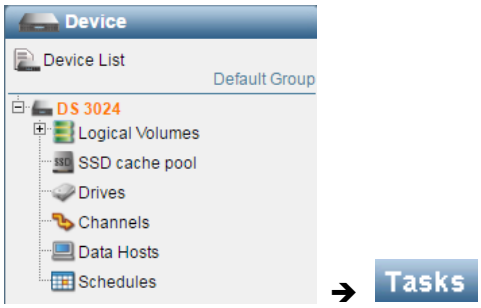
		- Battery temperature reading is abnormal (out of the 0 to 45°C range). - Battery is not present. **OFF** indicates that the cache is clean, and that the battery backup unit is capable of sustaining memory in case of power loss. **Blinking Amber** indicates cached data is being transferred to the flash 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 flash modules are present. **Amber** steady on indicates CBM failure, meaning either BBU or flash has failed. When lit, it also indicates either BBU or a 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** to indicate traffic on the host bus.
6. Drv Bsy	**Green**	**Blinking Green** to indicate traffic on the drive channels.

Viewing System Information

The System Information screen shows you the current status and configurations of the device (system).

Go To

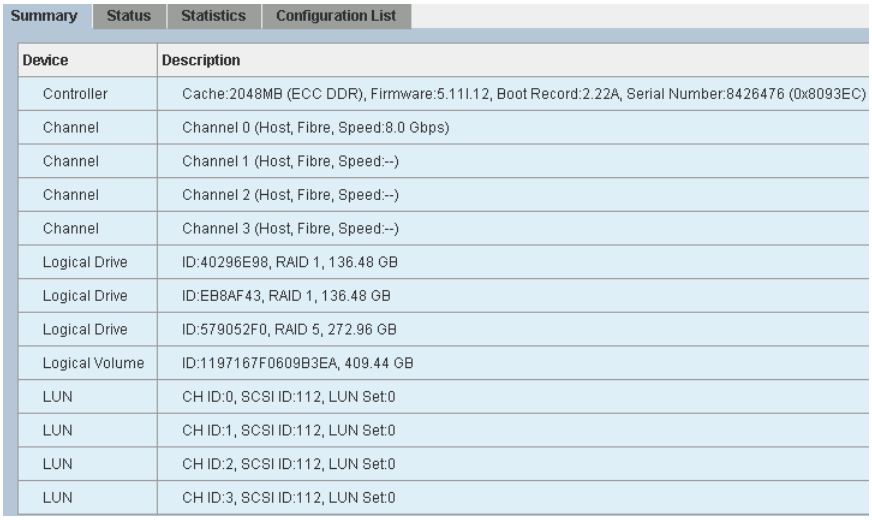
SANWatch Home > Device sidebar > Device List > device name> Tasks corner



Steps

Click System Information in the Tasks corner.

The system information screen will appear.



Device	Description
Controller	Cache:2048MB (ECC DDR), Firmware:5.11I.12, Boot Record:2.22A, Serial Number:8426476 (0x8093EC)
Channel	Channel 0 (Host, Fibre, Speed:8.0 Gbps)
Channel	Channel 1 (Host, Fibre, Speed:--)
Channel	Channel 2 (Host, Fibre, Speed:--)
Channel	Channel 3 (Host, Fibre, Speed:--)
Logical Drive	ID:40296E98, RAID 1, 136.48 GB
Logical Drive	ID:EB8AF43, RAID 1, 136.48 GB
Logical Drive	ID:579052F0, RAID 5, 272.96 GB
Logical Volume	ID:1197167F0609B3EA, 409.44 GB
LUN	CH ID:0, SCSI ID:112, LUN Set:0
LUN	CH ID:1, SCSI ID:112, LUN Set:0
LUN	CH ID:2, SCSI ID:112, LUN Set:0
LUN	CH ID:3, SCSI ID:112, LUN Set:0

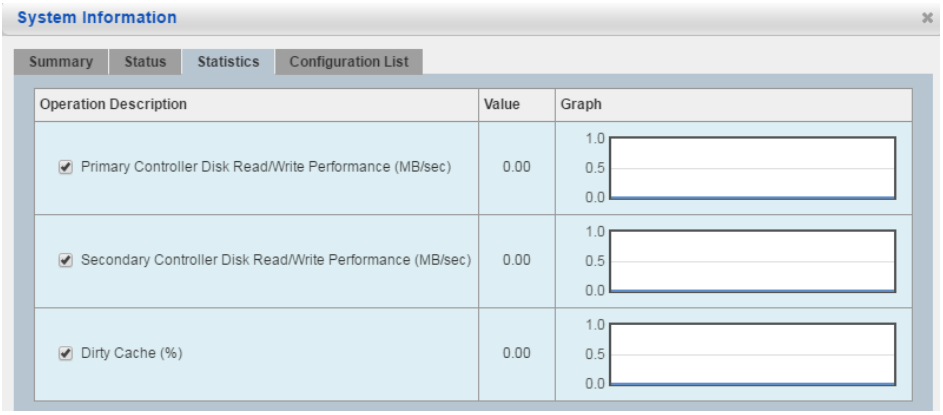
The Entire System Configuration

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

Controller/Cache Status

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

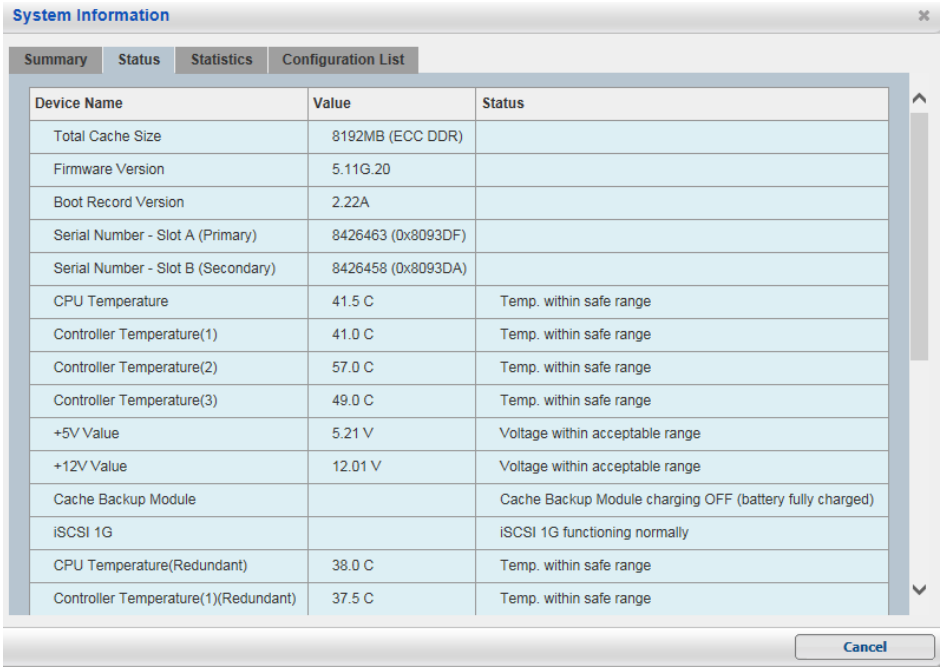
You can monitor the overall system throughput and storage capacity usage from the Device home page screen, in the Performance corner.



Temperature/Voltage

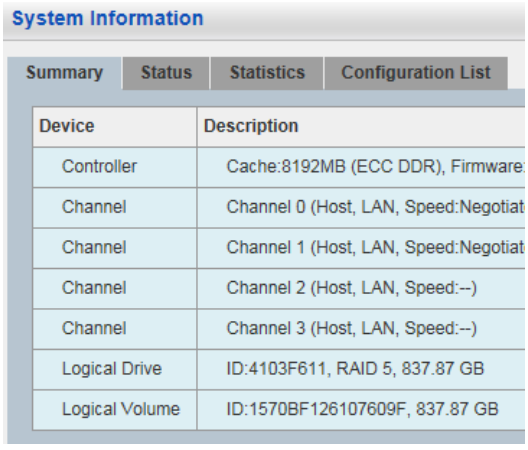
To monitor the voltage and temperature of the device, click the Status tab.

When the voltage/temperature reaches preconfigured thresholds, an event message will be sent to notify the user of potentially hazardous situation. You can change the threshold settings from the System Settings link in the Tasks corner.

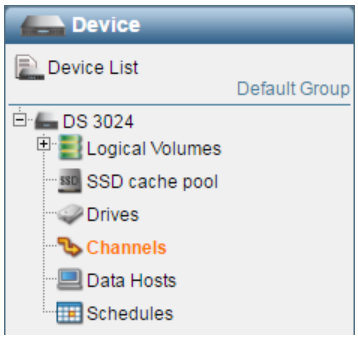


Controller and Channel Settings

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



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



Resetting/Shutting Down the System

Resetting/Shutting Down the System

There are several ways to reset all or part of the system (device).

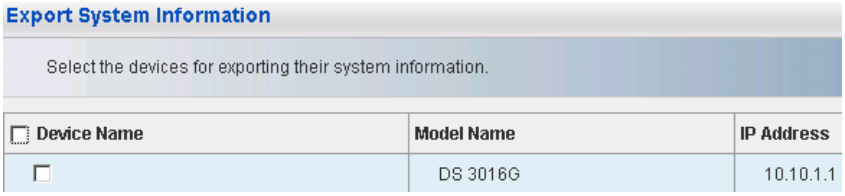
- Shutting down the device (RAID subsystem or JBOD)
- Shutting down the controller
- Resetting the controller

> Before resetting or upgrading the subsystem, make sure you finish all current tasks and save the configuration settings if necessary.

Saving System Settings

Go to SANWatch Home > top menu bar > System > Export System Information.

The list of connected devices (RAID or JBOD) will appear. Check the device and click OK.



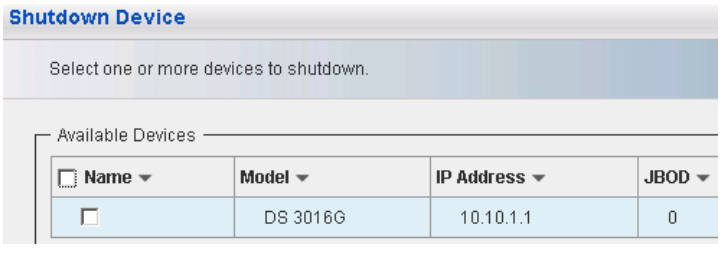
The system information can be downloaded into a local folder in Zip format (text format).

To view the system information on screen, click System Information in the Tasks corner.

Shutting Down the Device (Enclosure)

Go to SANWatch Home > top menu bar > System > Shutdown Device.

The list of connected devices (RAID or JBOD) will appear. Check the device you want to shut down and click OK.

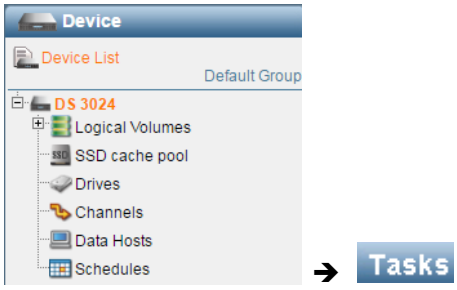


> Currently used storage volumes will become unavailable for hosts and users after shutting down the device (The user data inside the device will remain intact)

Shutting Down the Controller (NOT supported by EonServ)

As opposed to shutting down the device (the whole enclosure), shutting down only the controller does not power off the whole system.

Go to SANWatch Home > Device sidebar > Device List > device name > Tasks corner.



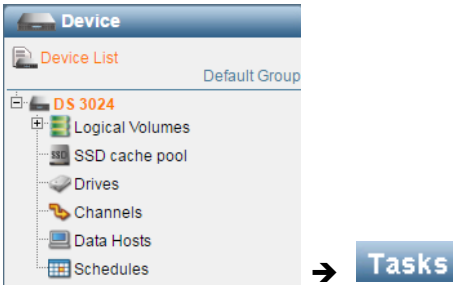
Click System Settings.

The System Settings screen will appear. Select the System tab.

Check Shutdown Controller and click Apply.

Resetting the Controller (NOT supported by EonServ)

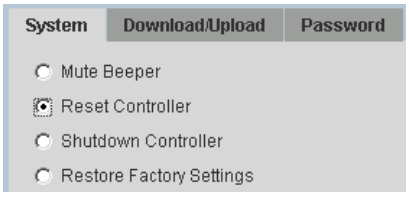
Go to SANWatch Home > Device sidebar > Device List > device name > Tasks corner.



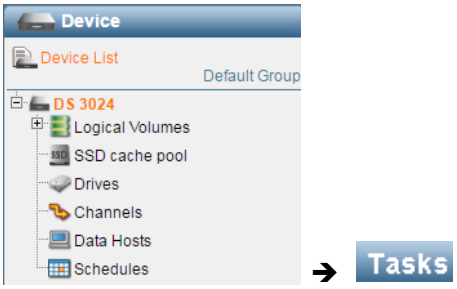
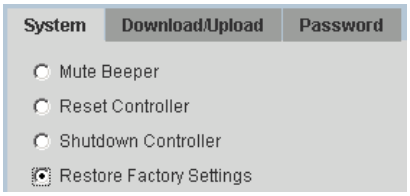
Click System Settings.

The System Settings screen will appear. Select the System tab.

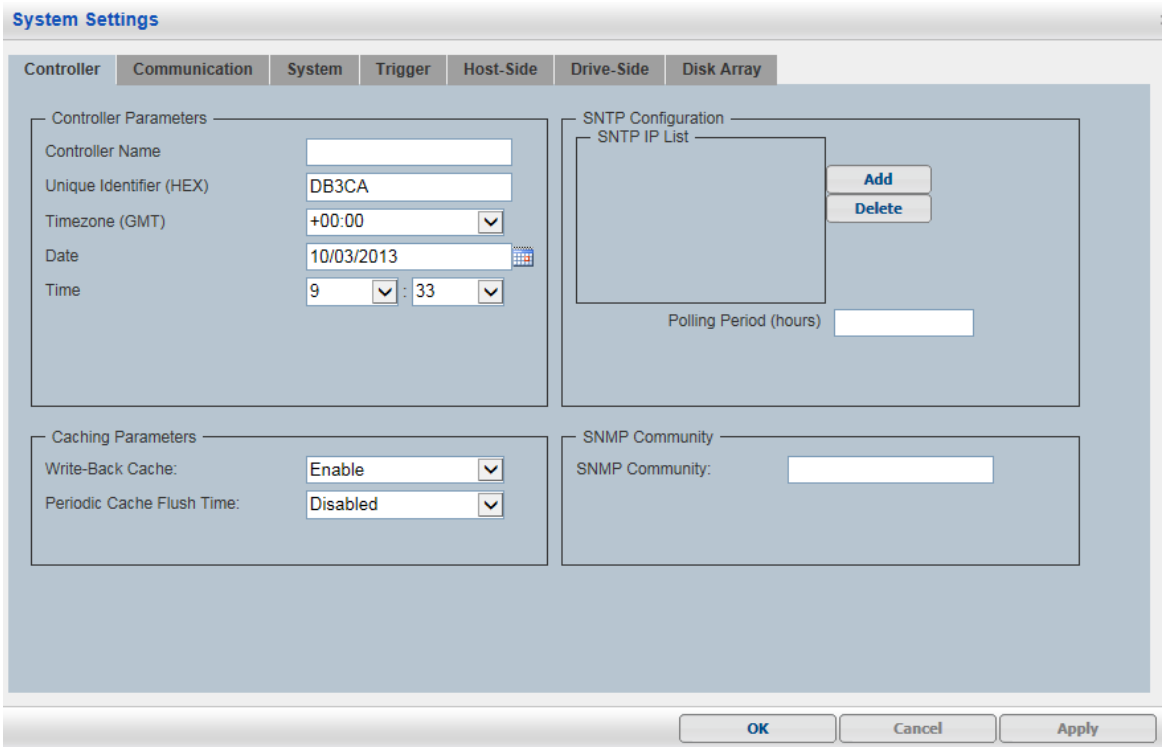
Check Reset Controller and click Apply.



Restoring Factory Default Settings (NOT supported by EonServ)

	Restoring the default settings is the last resort for solving system errors, since it erases all system configurations.
Pre-Restoration Works	Before you restore the default settings, save the current configurations: ➢ Stop all host IOs. ➢ Export system configurations. ➢ Make a list of host ID/LUN mapping information.
Go to	SANWatch Home > Device sidebar > Device List > device name > Tasks corner 
Steps	Click System Settings.  The System Settings screen will appear. Select the System tab. Check Restore Factory Settings and click Apply. 

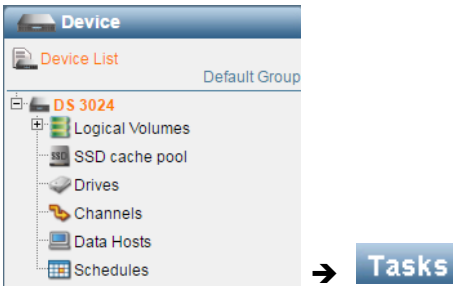
Configuring System Settings



Summary of System Configurations

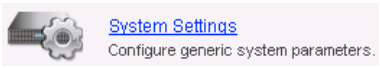
Go to

SANWatch Home > Device sidebar > Device List > device name > Tasks corner

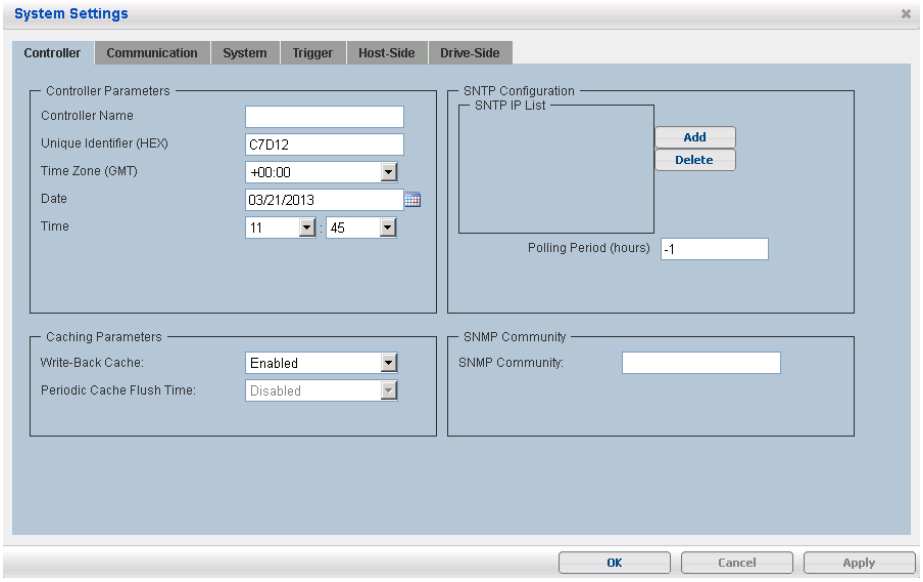


Steps

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 at the bottom. The following is the list of configurable items. Default values are marked in **bold** letters.

Controller

Here you can configure the controller parameters.

Item	Options	Configuration List
Controller Name: (user-defined, **empty**) Unique Identifier: (device-defined) Time Zone: -12:45 to **00:00** to +13:45 (NOT supported by EonServ) Date/Time: (computer-defined) (NOT supported by EonServ)	Controller Setting(s)	Controller Parameters
Caching Parameters	Write-Back Cache: **Enabled** / Disabled	

		Periodic Cache Flush Time (sec): **Disabled**
	SNTP Configuration (NOT supported by EonServ)	SNTP IP List: (user-defined, **empty**) Polling Period (hr): (user-defined, **empty**)
	SNMP Community	(user-defined)

Communication (Not on EonServ)

Here you can configure the network and serial communication settings.

Item	Options	Configuration List
Management Port	**IPV4**/IPV6	
RS232	Terminal Emulation: **Enabled** Baud Rate: 2400 ~ 38400	Communication > COM 1
Network Protocol Support	Enable network protocol support	
ISNS (for iSCSI-host models only)	Add/Delete Server IP	
Trunk Groups (iSCSI-host models only)	All channels except CH0	

System

Here you can perform 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

Here you can configure device upper / lower temperature and voltage thresholds and events to trigger notifications.

Highlight a threshold parameter and click on Configure to set 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

Here you can configure host computer and host interface settings.

Item	Options/Description
Maximum Number of Queued I/O	This setting determines the maximum I/O operations per host channel that are acceptable to connected servers. Consider the host's memory, number of drives, and drive capacity when changing this setting. With more resource, you can set a higher value. Note: Setting the value to **1024** generally provides the optimum performance.
LUN per Host SCSI ID	This setting determines the maximum number of LUNs per host SCSI ID. When users access the system through a host SCSI ID, they see the associated LUNs as drives. Note: Each controller can host up to 1,024 LUNs in terms of total host SCSI IDs. To check how many host SCSI IDs are set, go to **Channels > Host Channel Settings** and go to a SCSI channel to count checked IDs.
Login Authentication with CHAP	This setting determines whether the system should authenticate a user's identity with CHAP (Challenge-handshake authentication protocol). Note: This option is available to iSCSI-host models only.
Jumbo Frames	When enabled, this setting allows the system to increase an Ethernet frame's size and therefore the processing performance. All end devices in the iSCSI network must have their jumbo frame function activated, and share the same jumbo frame size setting. Note: This option is available to iSCSI-host models only.
Max Concurrent Host-LUN Connections	This setting determines the maximum concurrent host-LUN connections. Note: You can set a higher value only if the system has more than four logical drives or partitions.
Tags Reserved per Host-LUN Connection	This setting determines the minimum number of I/Os (i.e. tags) that each connection should process. Then, the system reserves resources accordingly for each connection. When you set a higher value, the system reserves more resources for your connections.

Peripheral Device Type	This setting allows the system to create a virtual peripheral device that users can access when the system does not have a LUN or storage space. The virtual peripheral device works as a portal between users and the system. Users can get needed system information through it.
Peripheral Device Qualifier	The setting determines the status of the virtual peripheral device. **Connected**: The virtual peripheral device is connected to the system. **Supported but not Connected**: The virtual peripheral device is supported by the system, but it is not connected to the system for access.
Device Supports Removable Media	This setting determines whether the system supports attached media sources like DVD and CD-ROM. Note: This setting only works in legacy versions of SANWatch.
LUN Applicability	This setting determines how a SCSI ID is mapped to a LUN. **First Undefined LUN**: Map the first available LUN to the SCSI ID. **Only Undefined LUN 0's**: When the system has no LUNs, create a virtual LUN and map it to the SCSI ID.
Cylinder/Head/Sector	This setting determines the size of a logical drive in units of cylinders, heads, and sectors. Specifying larger numbers increases a logical drive's size.

Drive-side

Here you can configure hard drive interface settings.

Item	Options	Configuration List
Auto-Assign Global Spare Drive	Enabled / **Disabled**	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	Enabled / **Disabled**	Drive-Side Parameters
Power Saving (Level 1 & Level 2)	**Disabled** / 1 min to 1 hour	Drive-Side Parameters
SED Authentication Key	**Create** / Modify	Drive-Side Parameters

Disk Array

Here you can configure hard drive array settings.

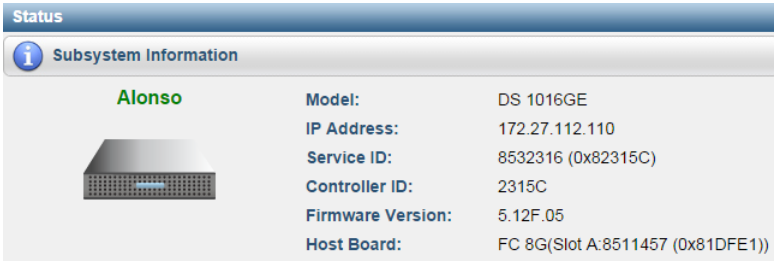
Item	Options	Configuration List
Rebuild Priority	**Normal** / Improved / High	Disk array parameters
Verify Write on LD Initialization	**Disable** / Enable	Disk array parameters
Verify Write on LD Rebuild	**Disable** / Enable	Disk array parameters
Verify Write on Normal Access	**Disable** / Enable	Disk 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

Updating the Firmware

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

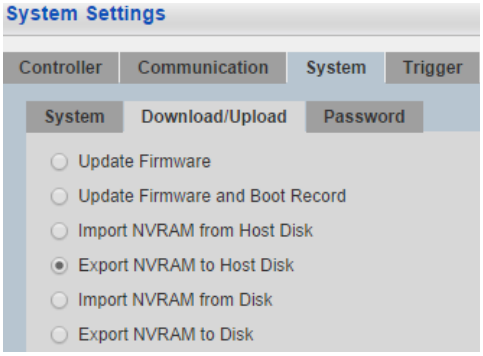
Prerequisite I: Checking Current Firmware Version

To check your current firmware version, go to SANWatch Home > Device sidebar > Device List > device name > Status corner. 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

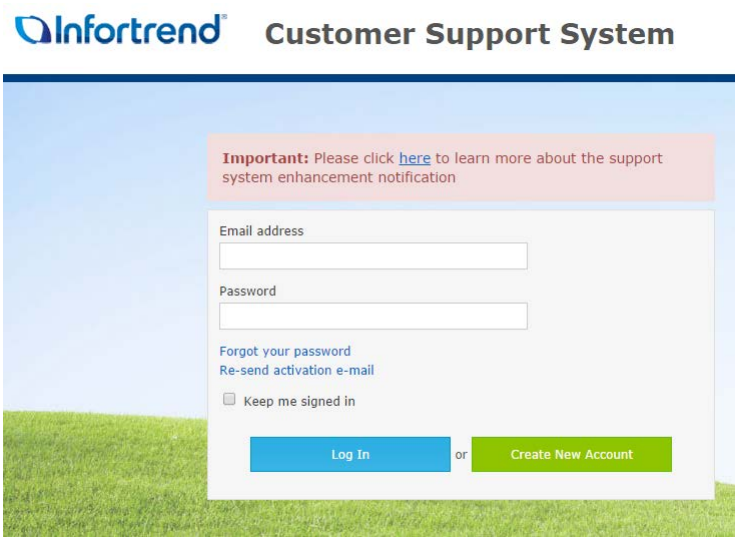


Select Export NVRAM to Host Disk and click OK. For more information, click the Help icon at the top-right corner and look for the Exporting /Importing NVRAM section.

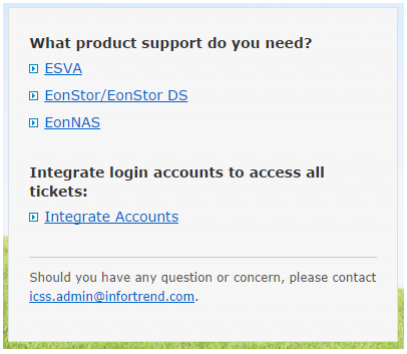
Prerequisite III: Obtaining the Firmware Package

Before retrieving the latest firmware from Infortrend, make sure you already have a user account at Infortrend's Customer Support System, which was created when you registered your subsystem online.

Go to http://support.infortrend.com, and then enter your account information to log in.



Select the type of subsystem you are using.
For ESVA users, click ESVA.
For EonStor/EonStor DS users, click EonStor/EonStor.

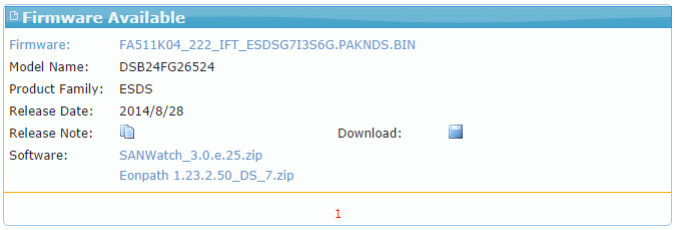


In the page that appears, choose Downloads > Firmware & Software from the top menu.

In the Firmware Search section that appears, enter either of the following serial numbers, and then click Search: "System S/N" or "Controller S/N"

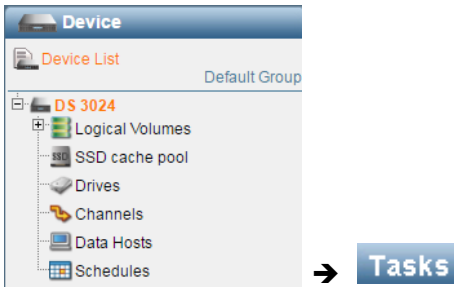
When the search is complete, firmware available for your subsystem will be shown in the Firmware Available section. Click Download to download it to

your computer.

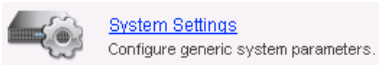


Updating the Firmware

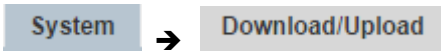
Go to SANWatch Home > Device sidebar > Device List > device name > Tasks corner.



Click System Settings.

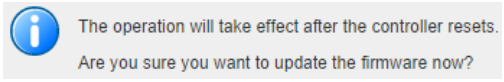


The System Settings screen will appear. Go to System > Download/Upload.



Click Browse under Update Firmware, locate the ".BIN" file you downloaded from Infortrend, and then click Open.

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



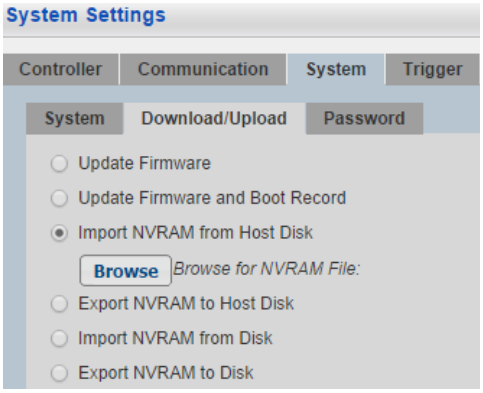
At the end of the updating process, you are required to reset your controller(s) for the operation to take effect:

For R-models, you can click Rolling Upgrade to reset the controllers one by one, thus decreasing system downtime; or, you can click Reset to reset the controllers simultaneously.

For other models, click Reset to reset the controller.

Importing System Configuration

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



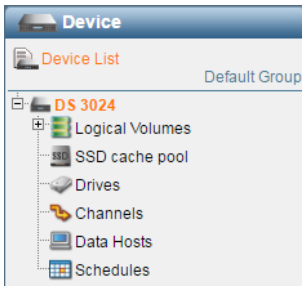
Select Import NVRAM from Host Disk and click Browse to locate the system configuration file you've exported before updating the firmware. For more information, click the Help icon at the top-right corner and look for the Exporting /Importing NVRAM section.

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 will be notified to the user to indicate potentially hazardous situation.

Go to

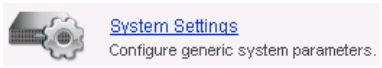
SANWatch Home > Device sidebar > Device List > device name > Tasks corner



➔ Tasks

Configuring the Temperature / Voltage Thresholds

Click System Settings.

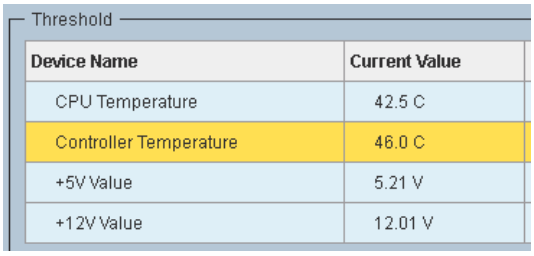


The System Settings screen will appear. Select the Trigger tab. The threshold settings will appear.

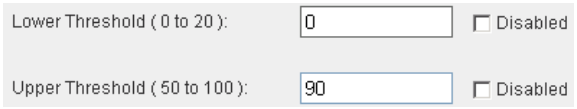
Trigger

Configuring the Voltage/Temperature Threshold

Highlight an item in the list.



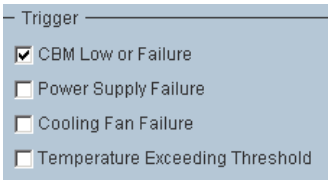
Click Configure. The configuration screen will appear. Enter the threshold value or you may click Disabled if you want to disable the threshold (and notification).



Selecting Triggered Item

You can select which events will trigger the subsystem to notify the user.

> To receive notifications when the temperature reaches the threshold, make sure that the Temperature Exceeding Threshold checkbox has been selected.


Trigger
CBM Low or Failure
Power Supply Failure
Cooling Fan Failure
Temperature Exceeding Threshold

Configuring the IP Address

You may change the IP address of the device, but doing so will disconnect the user interface in the old address. Make sure that you note down the new IP address and reconnect with the user interface using the new address.

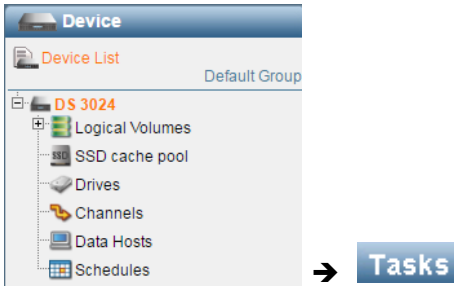
Notes

You are not allowed to assign any of the following system reserved IP addresses to your subsystem:

- 127.x.x.x
- 128.0.x.x
- 191.255.x.x
- 192.0.x.x
- 223.255.255.x

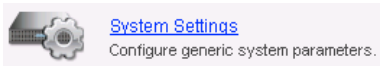
Go to

SANWatch Home > Device sidebar > Device List > device name > Tasks corner

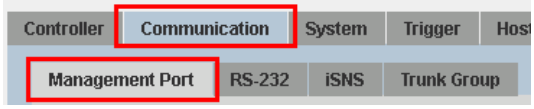


Steps

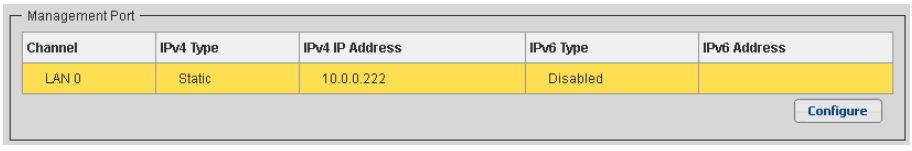
Click System Settings.



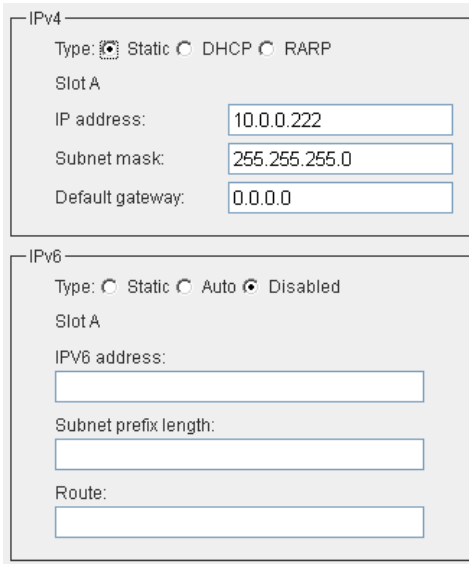
The System Settings screen will appear. Select the Communication > Management Port tab.



Highlight the management (LAN) port you wish to configure and click Configure.



You may configure the IP address (IPV4 or IPV6).



The following system reserved IP addresses should not be used for your subsystem: 169.254.1.1~169.254.254.254.

Parameters	**IPV4 Type**	➢ Static: Specifies a fixed address. ➢ DHCP: Allows the network router to pick an available address for the device. ➢ RARP: Reverse Address Resolution Protocol is an old type of 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 IPV4 address. The router will automatically pick an address for 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.

Create SED Authentication Key for LD/LV Protection (EonStor DS subsystems only)

The SED (Self-Encrypting Drive) authentication key allows you to protect logical drives or logical volumes with SED security using drive-level encryption. You can enable SED for your subsystem with a "global key" or "local key(s)."

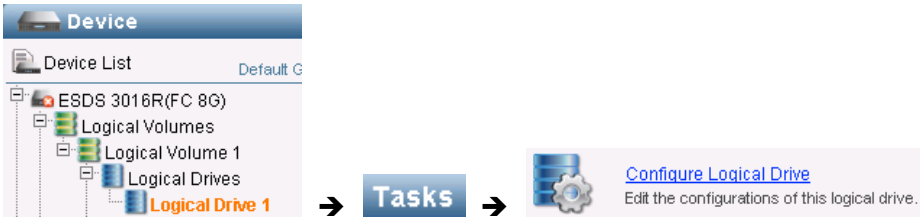
- **Global key**: This key can be used to encrypt all logical drives of your subsystem. Until you disable SED for a logical drive, SED encryption will always be effective.
- **Local key**: This key is used to encrypt a specified logical drive, and is available only when the global key is not created in the subsystem. In other words, creating a global key will overwrite the local key and hide its options in SANWatch. SED security using local keys will become ineffective after the system reboots; enabling it requires you to import the key file or password after each system reboot.

SED security only works on logical drives or logical volumes composed of SED drives only.

Go to

For global key: SANWatch Home > Device sidebar > Device List > device name > Tasks corner > System Settings > Drive-Side tab

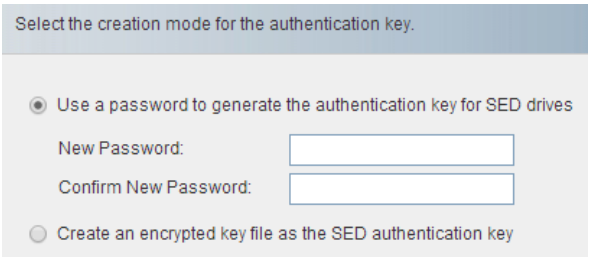
For local key: Navigate to a logical drive that supports SED, click Configure Logical Drive in the Tasks corner.



Steps (Global Key)

Click Create.

In the window that appears, use either of the following options to enable SED security.



- Use a password for SED authentication.
- Create an encrypted key file for SED authentication. You can either click Generate to create a new key, which will be downloaded and saved on your computer as a ".bin" file. Click Browse to locate and import the key file you just downloaded.

Click OK to generate the SED authentication key or password.

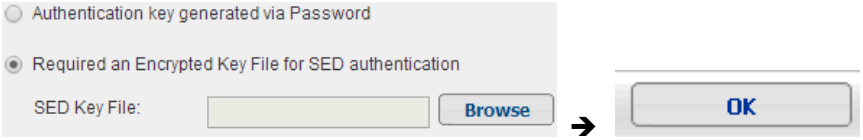
Now you can enable SED security for a logical drive or logical volume using the global key by doing the following:
Navigate to a logical drive or logical volume that supports SED, click Configure Logical Drive or Configure Logical Volume in the Tasks corner, and choose Enabled from the SED Security drop-down menu.

It is strongly recommended that you keep your SED authentication password or key file in a safe medium.

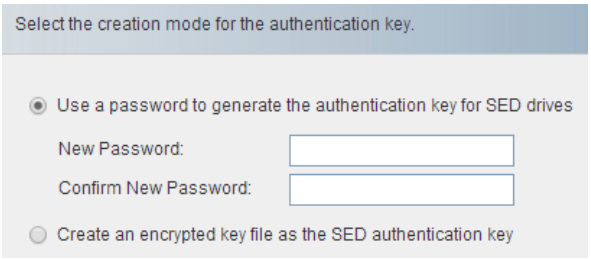
Modifying or Removing SED Authentication Key

Click Modify.

Use the SED password or key file you created while enabling SED password or key to unlock it, and click OK.



In the window that appears, do either of the following:



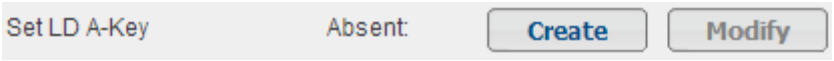
- To modify the SED key or password: Enter a new password or create a new key file to change the SED password or key, and then click OK.
- To remove the SED key or password: Leave the password fields blank and

click OK.

- To cancel changing the SED key or password, click Cancel.

Managing Local Keys for a Logical Drive

Click Create or Modify to enable SED security using a password or key file.



The process of creating a local key is mostly the same as that of a global key. The only difference is that SED security will be enabled once the key or password is generated.

Configuring Power Saving Settings

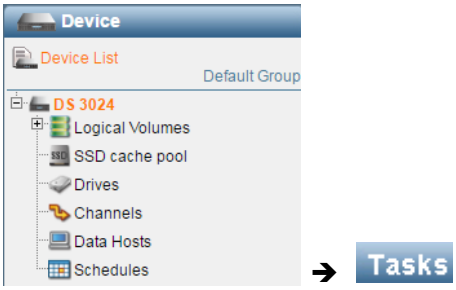
The power-saving option can enhance disk spin-down function for all disks on your subsystem. When there is no host I/O, disk drives may enter two power-saving modes: Level 1 for idle mode and Level 2 in spin-down mode.

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

> You can further tailor power saving settings to your needs by applying different settings to a logical drive, including its local spares. To do so, go to SANWatch Home > Device > Logical Volumes > Logical Volume Name > Logical Drives > Logical Drive Name ➔ Tasks, and then click Power Saving.

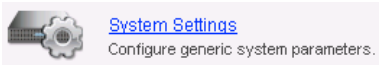
Go to

SANWatch Home > Device sidebar > Device List > device name > Tasks corner



Steps

Click System Settings.



The System Settings screen will appear. Select the Drive-Side tab.

Power saving settings are near the bottom.

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

You may also configure the waiting period for switching to the power saving mode.

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

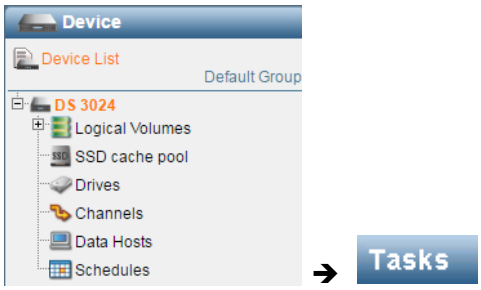
To configure power saving levels for individual logical drives, select the logical drive in the Device sidebar, and click Power Saving in the Tasks corner.

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

Configuring Time Settings

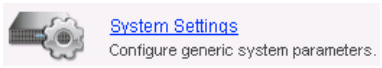
Go to

SANWatch Home > Device sidebar > Device List > device name > Tasks corner



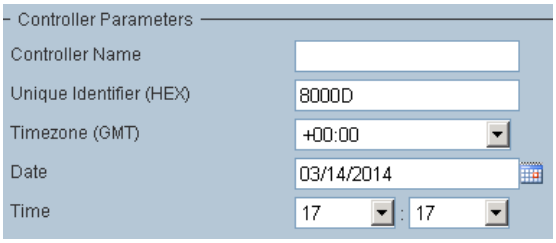
Steps

Click System Settings.

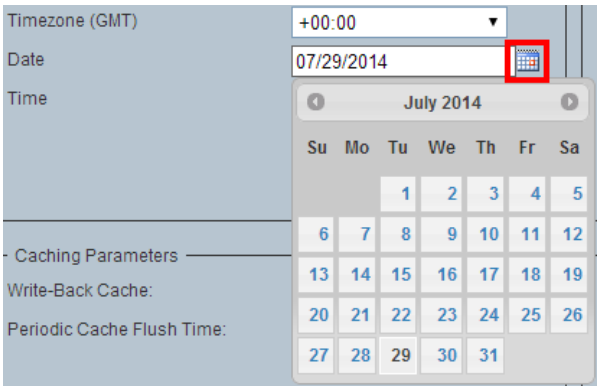


The System Settings screen will appear. Select the Controller tab.

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.



Trunking Host Interfaces to Increase Bandwidth

Increase network bandwidth by combining (trunking) multiple LAN interfaces into one, creating a link aggregation configuration.

Trunking offers the following benefits:

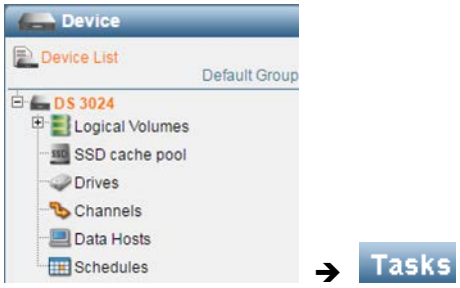
- Increased bandwidth: bandwidths of multiple interfaces will be added up.
- Improved security: Even when one LAN interface fails, the other interface will keep the network connection intact.

Notes

- Multiple LAN ports on your hardware must be connected to the network.
- The network switch must be compatible with trunking.
- The trunking option is available only for iSCSI-host models.

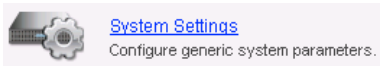
Go to

SANWatch Home > Device sidebar > Device List > device name > Tasks corner

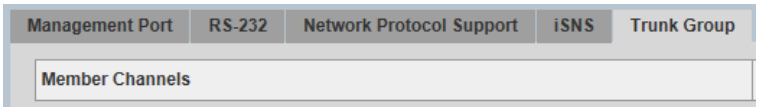


Steps

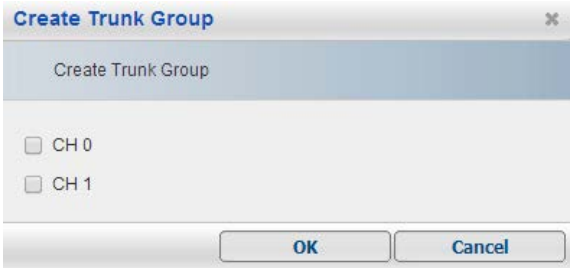
Click System Settings.



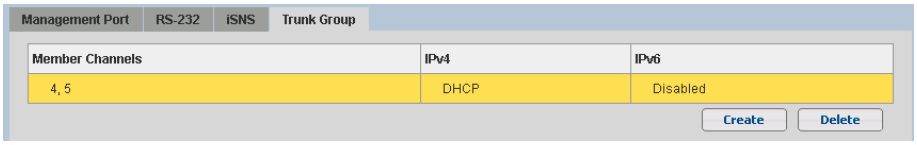
The System Settings screen will appear. Select the Communication tab and select the Trunk Group tab.



Click the Create button. In the popup window, check the LAN interfaces you wish to combine (trunk) and click OK.



The new trunk configuration will appear.



To delete the trunk group, click the Delete button.

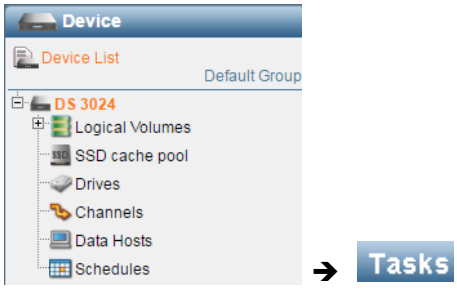
Muting the Beeper Sound

Each RAID system or JBOD expansion enclosure contains hardware beep mechanism to notify users when system errors and hardware failures occur. You may mute the sound on the hardware directly (please refer to the hardware manual for details) or do so remotely through the user interface.

> You can only mute the currently beeping sound: you cannot disable the buzzer setting from the user interface.

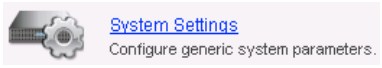
Go to

SANWatch Home > Device sidebar > Device List > device name > Tasks corner

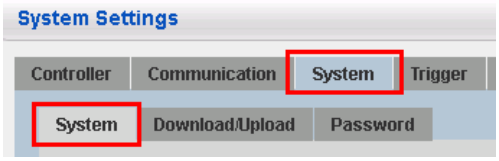


Steps

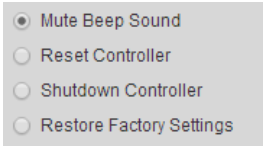
Click System Settings.



The System Settings screen will appear. Select the System > System tab.



Check Mute Beep Sound and click OK.



Exporting/Importing NVRAM

NVRAM (non-volatile memory in storage subsystems) contains system configuration information. You may export it to preserve the current system status or import it to restore system configurations.

When to Export NVRAM

- After firmware upgrade
- Before replacing both controllers
- After mapping logical drives to host LUN or changing system configurations

When to Import NVRAM

- The system has been 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:

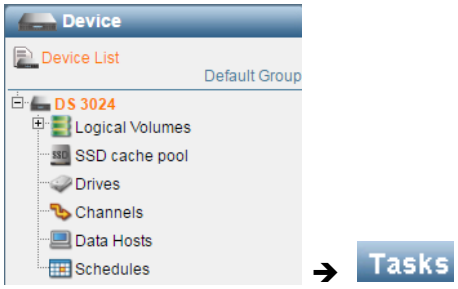
- Disk: Uses the subsystem's internal storage.

> At least one logical drive must exist in the subsystem.

- Host Disk: Uses the host computer's storage.

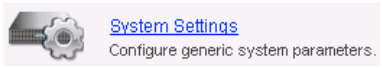
Go to

SANWatch Home > Device sidebar > Device List > device name > Tasks corner

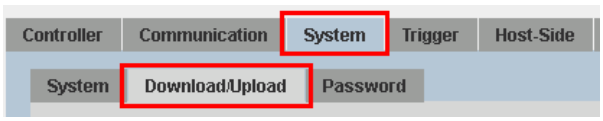


Steps

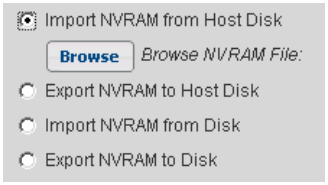
Click System Settings.



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.

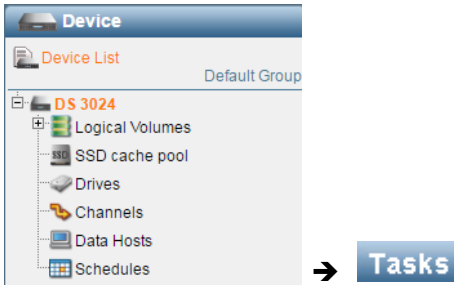

Import NVRAM from Host Disk
Browse
Browse NVRAM File:
Export NVRAM to Host Disk
Import NVRAM from Disk
Export NVRAM to Disk

Removing Isolated Logical Drives

Detect logical drives (or pool elements for ESVA subsystems) that no longer belong to specific logical volumes (or pools for ESVA subsystems) to remove them from the system and subsequently reuse them.

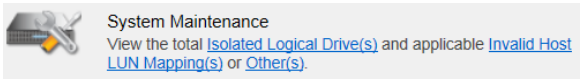
Go to

SANWatch Home > Device sidebar > Device List > device name > Tasks corner

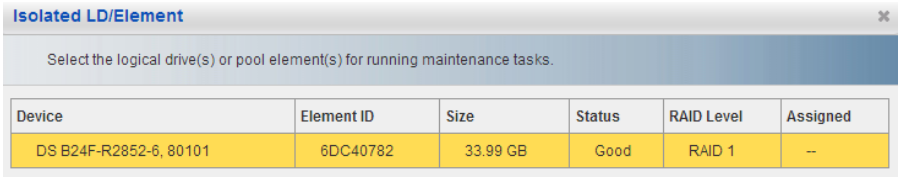


Steps

Click Isolated Logical Drive(s).

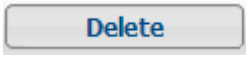


The list of isolated logical drives will appear.



If no isolated elements exist, the window will not appear.

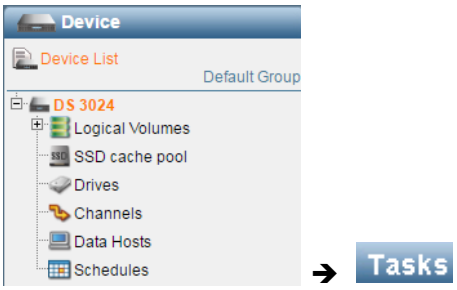
Check the system you wish to remove and click Delete.



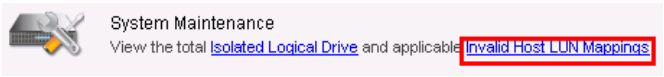
Removing Invalid Host Mappings

Detect invalid host mappings and remove their settings.

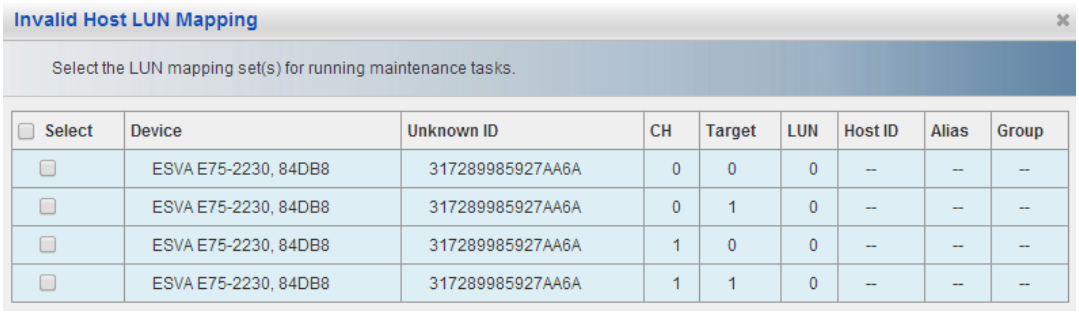
Go to SANWatch Home > Device sidebar > Device List > device name > Tasks corner



Steps Click Invalid Host LUN Mappings.



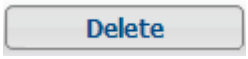
The list of invalid host mappings will appear.



Select	Device	Unknown ID	CH	Target	LUN	Host ID	Alias	Group
☐	ESVA E75-2230, 84DB8	317289985927AA6A	0	0	0	--	--	--
☐	ESVA E75-2230, 84DB8	317289985927AA6A	0	1	0	--	--	--
☐	ESVA E75-2230, 84DB8	317289985927AA6A	1	0	0	--	--	--
☐	ESVA E75-2230, 84DB8	317289985927AA6A	1	1	0	--	--	--

If no invalid mappings exist, the window will not appear.

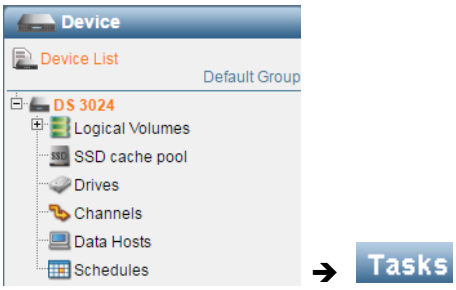
Check the mapping you wish to remove and click Delete.



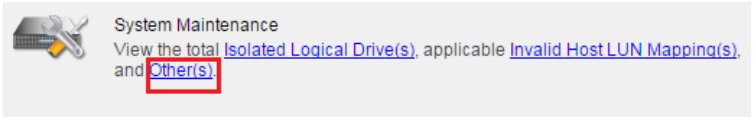
Check Miscellaneous Events

Detect a list of miscellaneous events by the system. The event types, reasons, status will be displayed details on the table, such as problems of partition.

Go to SANWatch Home > Device sidebar > Device List > device name > Tasks corner



Steps Click Other(s) to check if any event being discovered on the list.



The list of other type of error events will appear.

Event Type	Target Unique ID	Status	Cause	Severity	Action
Partition of LV:4E14C315169DB362	403E6BDD1F10A031	Incomplete partition	Partition creation or removal is not completed	Warning	Could be deleted
Partition of LV:4E14C315169DB362	51093C863CD4FA8A	The partition is abnormal but has no immediate risk of danger	The partition size should be multiples of LV's data section size (2MB).	Warning	Contact technical support. Please don't expand the partition on your own.

If no events exist, the window will not appear.

Working with System Events

Events are signals from the storage subsystem that the users (administrators) should know in order to manage the system.

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

- Notifying users in case of system events
- Periodically sending out system log
- Activating user-specified applications in case of system events

Types of Events

Events can be categorized by (1) their scope and (2) their severity. For the detailed list of events and their descriptions, see the Troubleshooting Guide. Contact the Support to obtain it.

Scope of Events

Event Type	Scope
Controller Event	Describes the events related to the storage system controllers.
Drive Event	Describes the events related to the physical disk drives.
Host Event	Describes the events related to the host computer and host ports.
Logical Drive Event	Describes the events related to logical drives and logical volumes.
System Event	Describes the events related to the overall storage subsystem.

Severity of Events

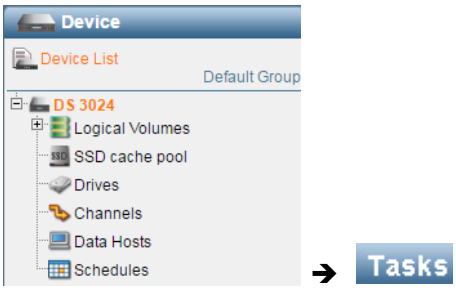
There is a combination of warning, error, and information levels.

Severity	Description
critical error	Describes the events that users should pay immediate attention and perform required actions.
error	Describes the events that users should pay attention and perform required actions.
warning	Describes the events that users should pay attentions.
information	Describes the events that notify users of non-critical changes in system status.

Viewing Event Log

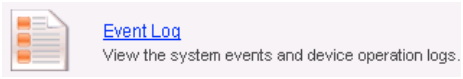
Go To

SANWatch Home > Device sidebar > Device List > device name > Tasks corner

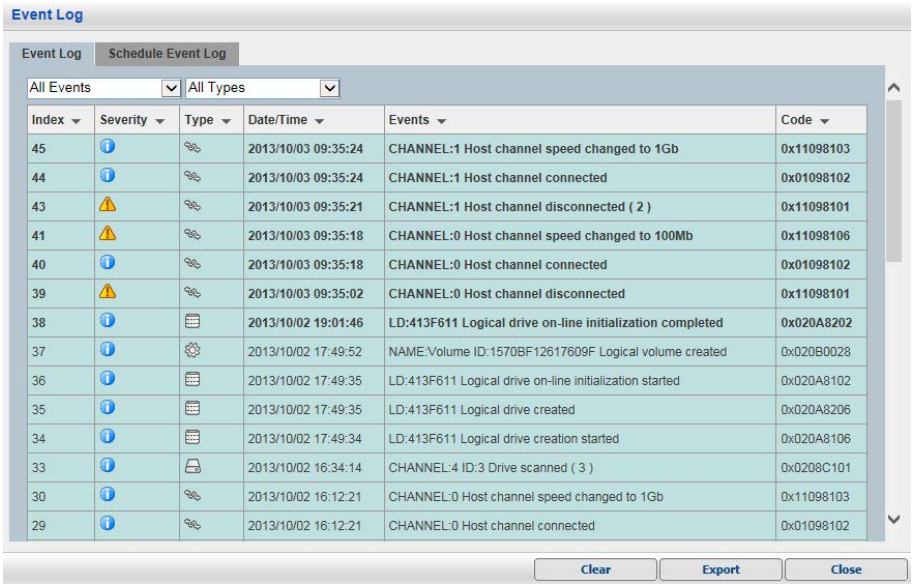


Procedures

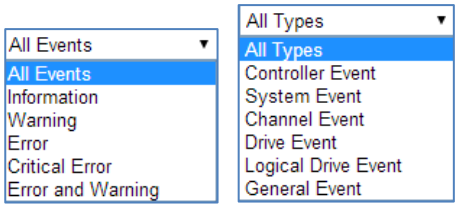
Click the Event Log menu in the Tasks corner.



The list of events will appear.



Select the severity and type of events to filter which events will appear.



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

Parameters

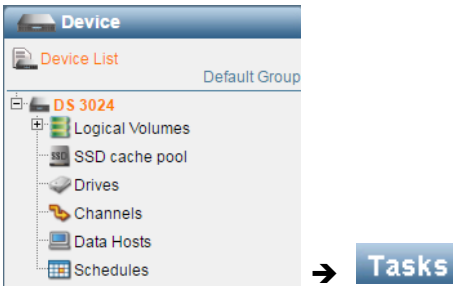
Event Type Selects the types (scopes) of events that will be listed.

Severity	Selects the severity of events that will be listed.

Exporting Event Log

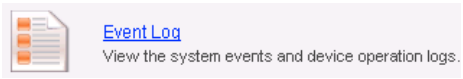
Go To

SANWatch Home > Device sidebar > Device List > device name > Task corner

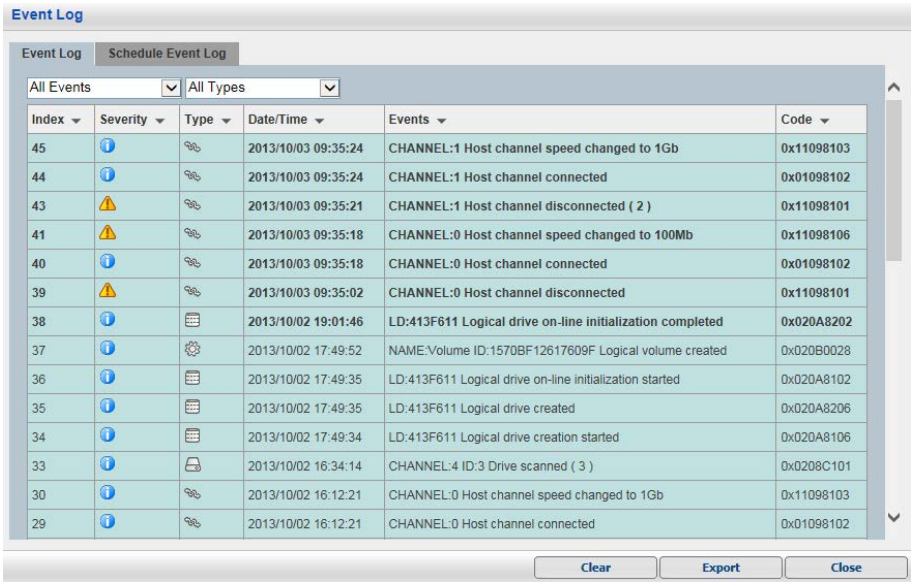


Steps

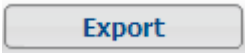
Click the Event Log menu in the Tasks corner.



The list of events will appear.



Click Export. You can save the log into a local file in text format.

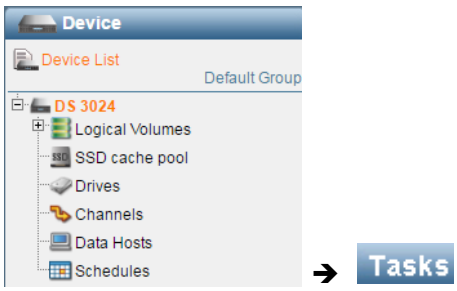


Activating Triggers (Thresholds)

To receive event notifications (especially when the system encounters abnormal status such as high temperature or power supply failure), make sure that the triggering mechanism has been activated.

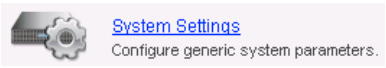
Go To

SANWatch Home > Device sidebar > Device List > device name > Tasks corner



Steps

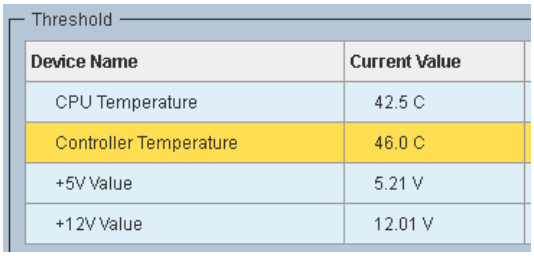
Click System Settings in the Tasks corner.



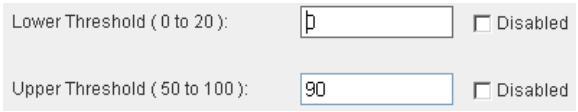
The System Settings screen will appear. Select the Trigger tab.

Configuring the Voltage/Temperature Threshold

Highlight an item in the list.



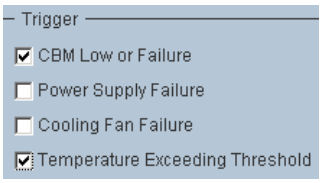
Click Configure. The configuration screen will appear. Enter the threshold value or you may click Disabled if you want to disable the threshold (and notification).



Selecting Triggered Item

You can select which events will be notified to the user.

To receive notifications when the temperature reaches the threshold, make sure that the Temperature Exceeding Threshold checkbox has been enabled.


Trigger
CBM Low or Failure
Power Supply Failure
Cooling Fan Failure
Temperature Exceeding Threshold

Working with Licenses

If you have any license-related issues (local and remote replication) with your subsystem, contact your dealer.

License Types

You will need to apply or download a license key for using the following features in EonStor DS series. The Standard License is provided for free for all users. The Advanced License might need to be purchased beforehand.

Feature/Functionality	License Type
Standard Local Replication	Standard License
Connecting an EonStor DS RAID system with an EonStor JBOD (Applicable when an equivalent EonStor model is available as a compatible JBOD for that particular RAID system)	Standard License
Thin Provisioning	Standard License
Advanced Local Replication	Advanced License
Remote Replication	Advanced License
Automated Storage Tiering	Advanced License
SSD cache pool	Advanced License

Notes

- When your license expires, apply for a license renewal.
- When you have upgraded your features, apply for a license upgrade.
- If you want to try out the advanced license features for 30 days, apply for a Trial License.
- It is required to reset the system for the license to take effect after a license is installed.

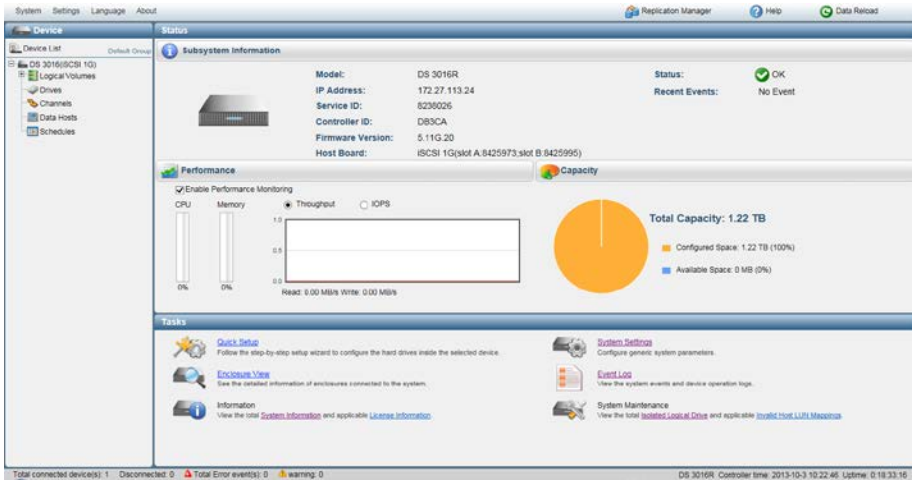
The licensing policy might change without notice. If necessary, check with the customer support for the latest license policy status.

Generating the License Application File

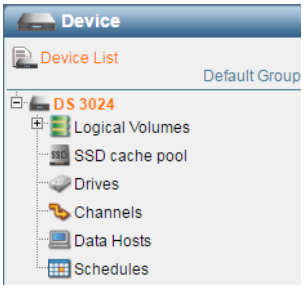
Before starting any EonStor DS license process, please check whether Infortrend's SANWatch management suite, which was shipped together with the EonStor DS storage system, has been properly installed.

Steps

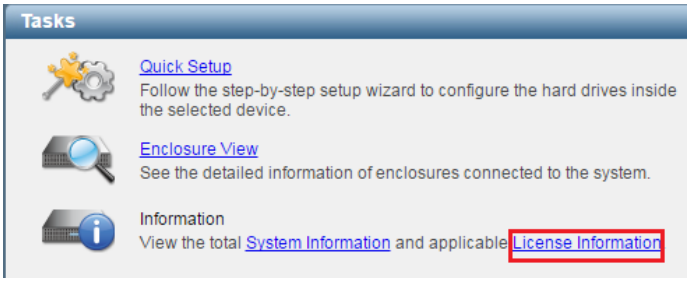
Enter the SANWatch Browser Interface.



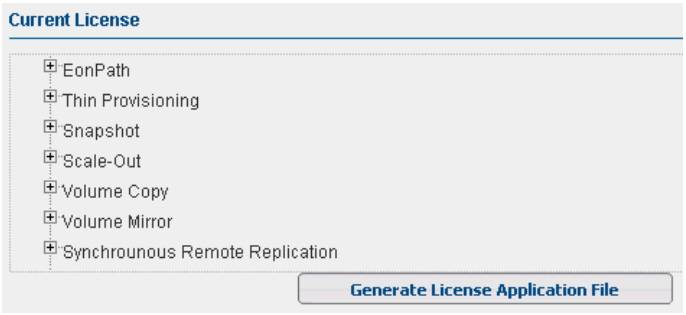
Select (highlight) the subsystem for which you want to apply for a license.



Click **License Information** in the Tasks corner.



In the License Key window, click **Generate License Application File**.



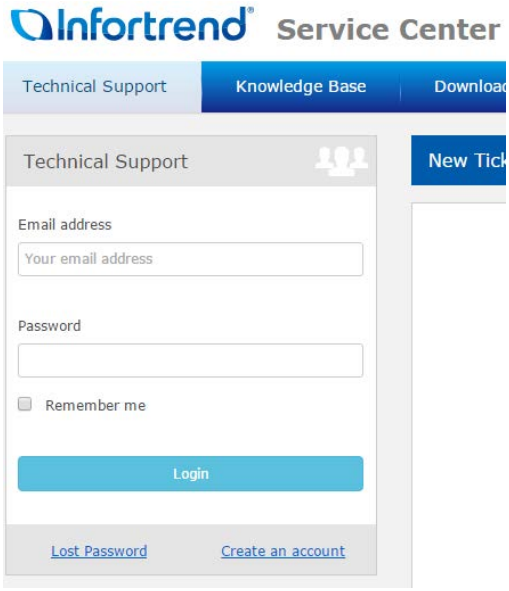
A reminder appears explaining that a License Application File can only be used to generate one license. Click **OK**.

Save the License Application file.

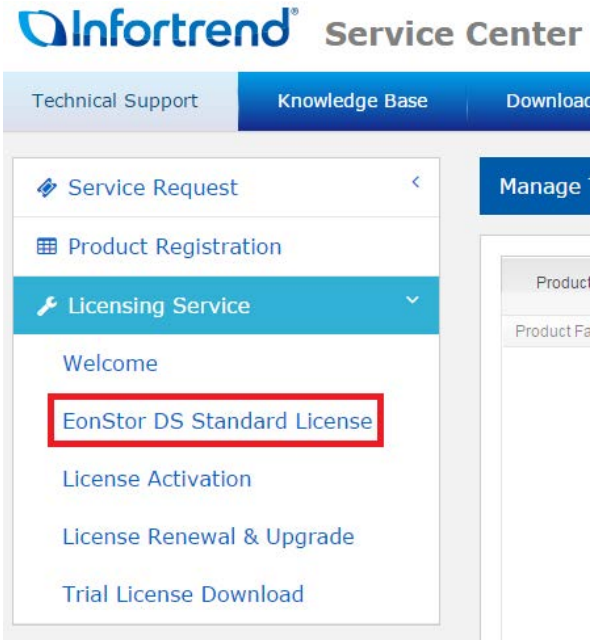
Generating the Standard License Key

Steps

Visit Infortrend's EonStor DS Software License website: http://support.infortrend.com/ and log in. If you don't have an account, please click **Create an account** to register for one.



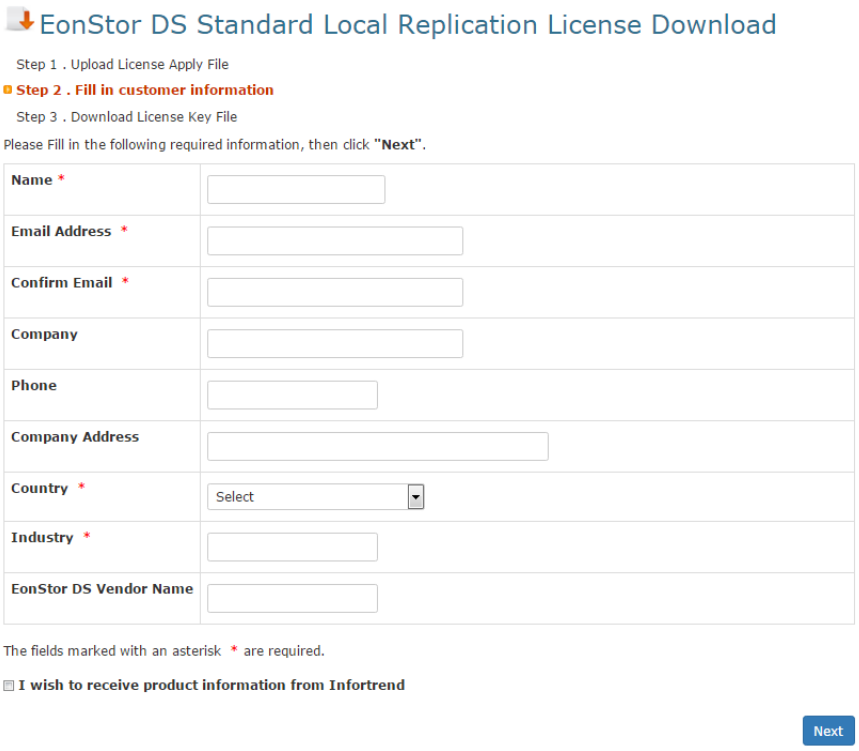
For a Standard License, please select **EonStor DS Standard License**.



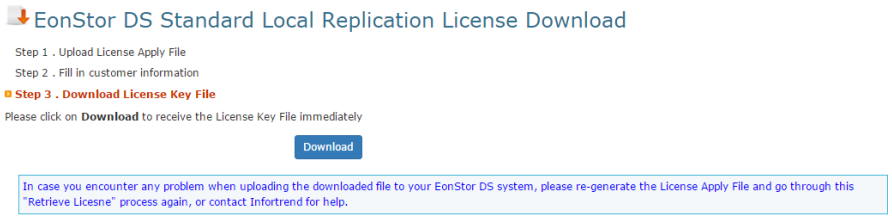
Carefully read the information, click the checkbox, and click **Next**.

Upload the License Application File you obtained through SANWatch, and click **Next**.

Fill in customer information and click **Next**.



Download the License Key File by clicking **Download**.



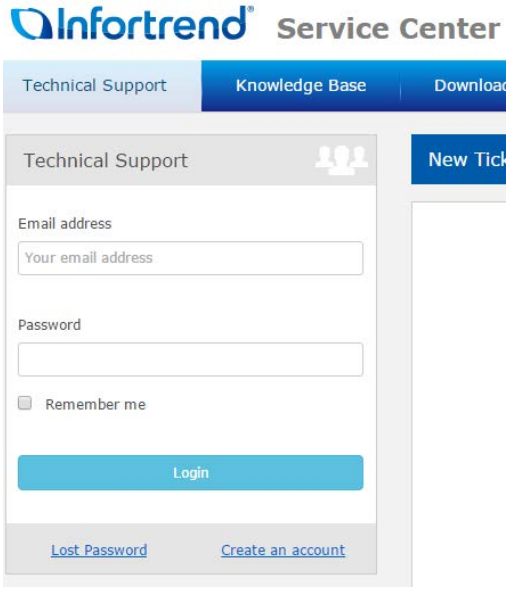
Save the License Key File in a preferred location and upload it to SANWatch.

Generating the Advanced License

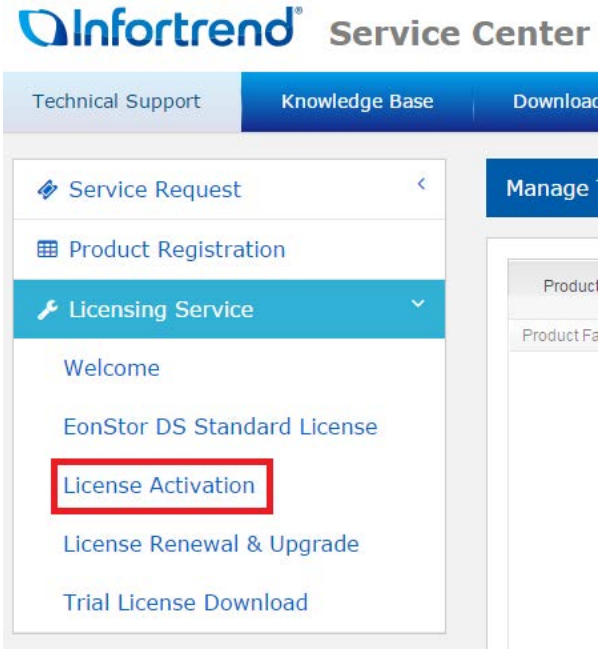
You can try out advanced license features for 30 days using the Trial License before making a purchase decision.

Steps

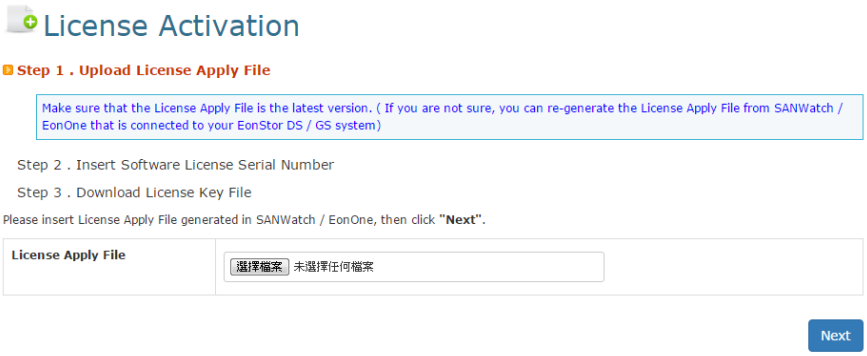
Visit Infortrend's EonStor DS Software License website: http://support.infortrend.com/ and log in. If you don't have an account, please click **Create an account** to register for one.



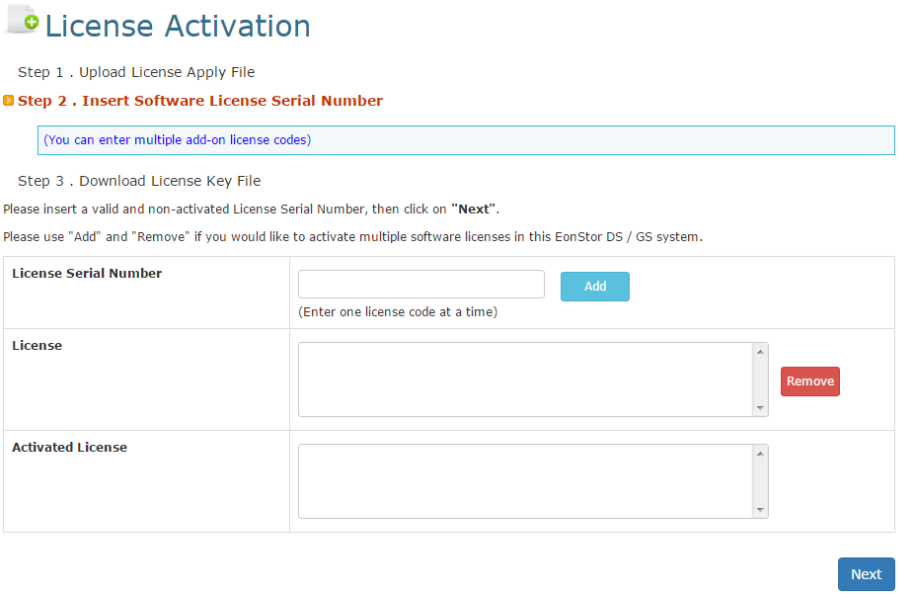
For an Advanced License, please click **License Activation**.



Upload the License Application File you obtained through the SANWatch software and click **Next**.

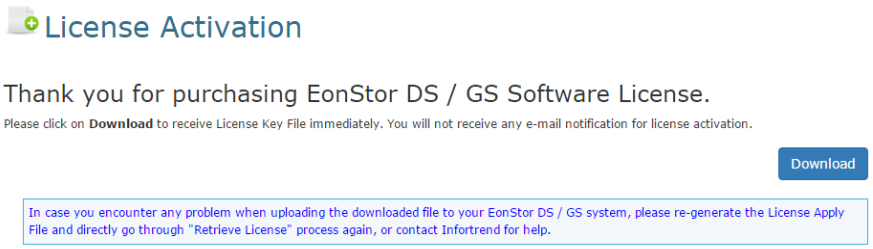


Fill in the License Serial Number you received, and then click **Add**. After adding the License Serial Number, click **Next**.



You can generate multiple licenses in a single activation process. Simply fill in another License Serial Number and click add. The added licenses will be listed in the **License** box.

Click **Download** to receive the License Key File.



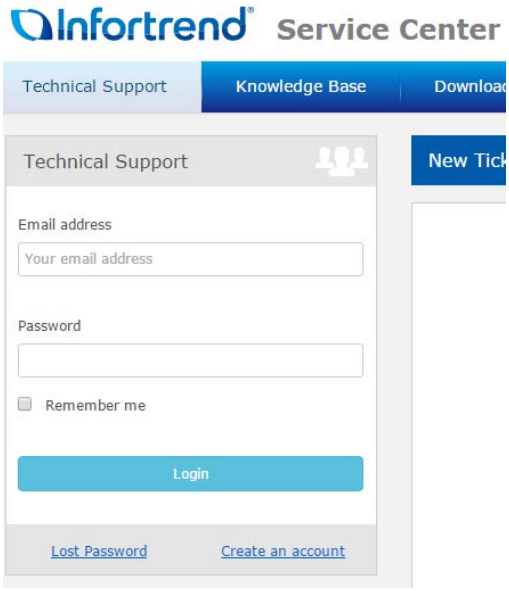
Save the License Key File at a preferred location and upload it to SANWatch.

Upgrading Standard License to Advanced License

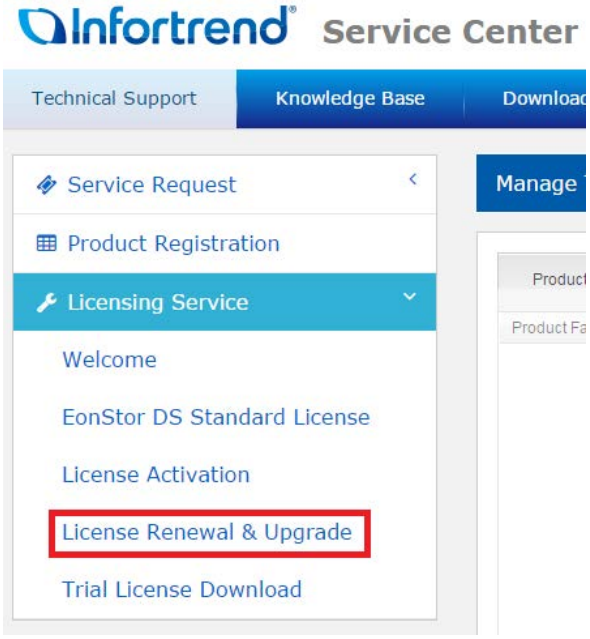
Here we will introduce how to upgrade from a current standard license to a new advanced license.

Steps

Visit Infortrend's EonStor DS Software License website: http://support.infortrend.com/ and log in. If you don't have an account, please click **Create an account** to register for one.

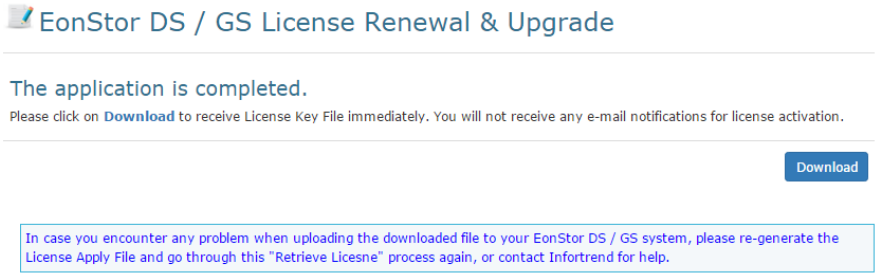


If you have already purchased a standard license and wish to upgrade to advanced license, please click on **License Renewal & Upgrade**.



Upload the License Application File you generated through SANWatch and click **Next**.

Click **Download** to receive the License Key File immediately.



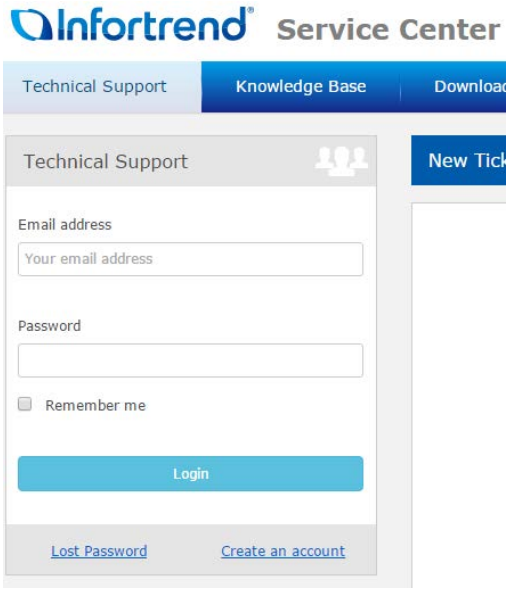
Save the License Key File at a preferred location and upload it to SANWatch.

Renewing the License

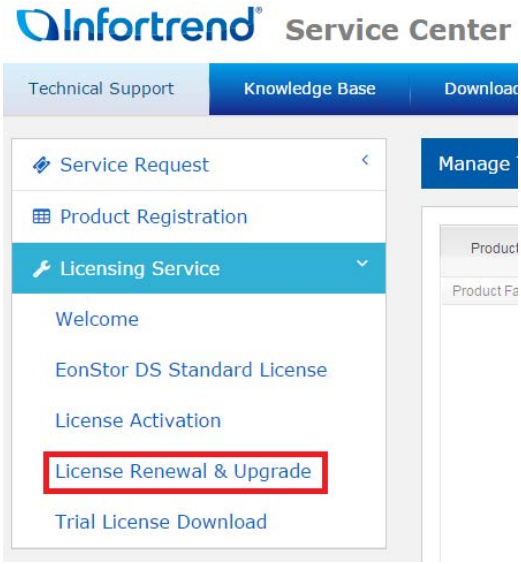
If you have lost a previously generated License Key File, you can re-generate it through the license website.

Steps

Visit Infortrend's EonStor DS Software License website: http://support.infortrend.com/ and log in. If you don't have an account, please click **Create an account** to register for one.

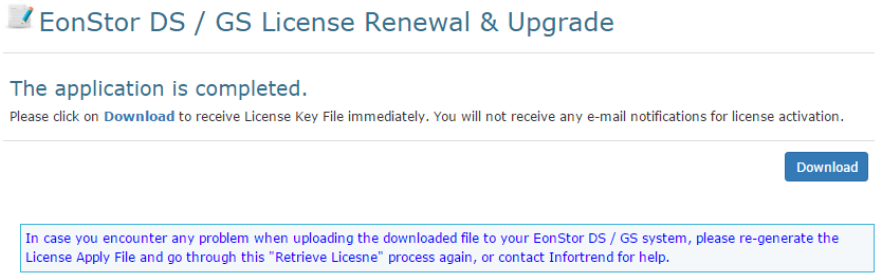


Click **License Renewal & Upgrade**.



Upload the License Application File you have generated through SANWatch and click **Next**.

Click **Download** to receive the License Key File immediately.



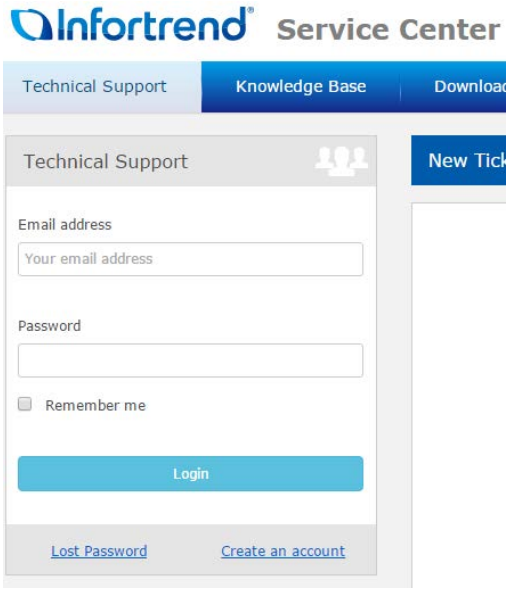
Save the License Key File at a preferred location.

Downloading a Trial License

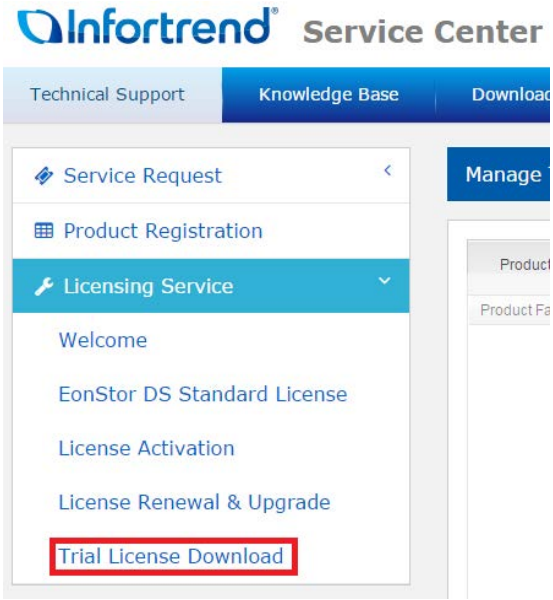
If you want to try out the advanced license features before making a purchase decision, you can use the trial license, which will allow you to use the features for 30 days.

Steps

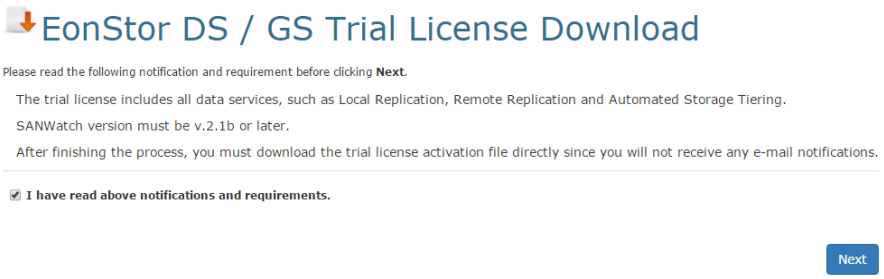
Visit Infortrend's EonStor DS Software License website: http://support.infortrend.com/ and log in. If you don't have an account, please click **Create an account** to register for one.



Click **Trial License Download**.

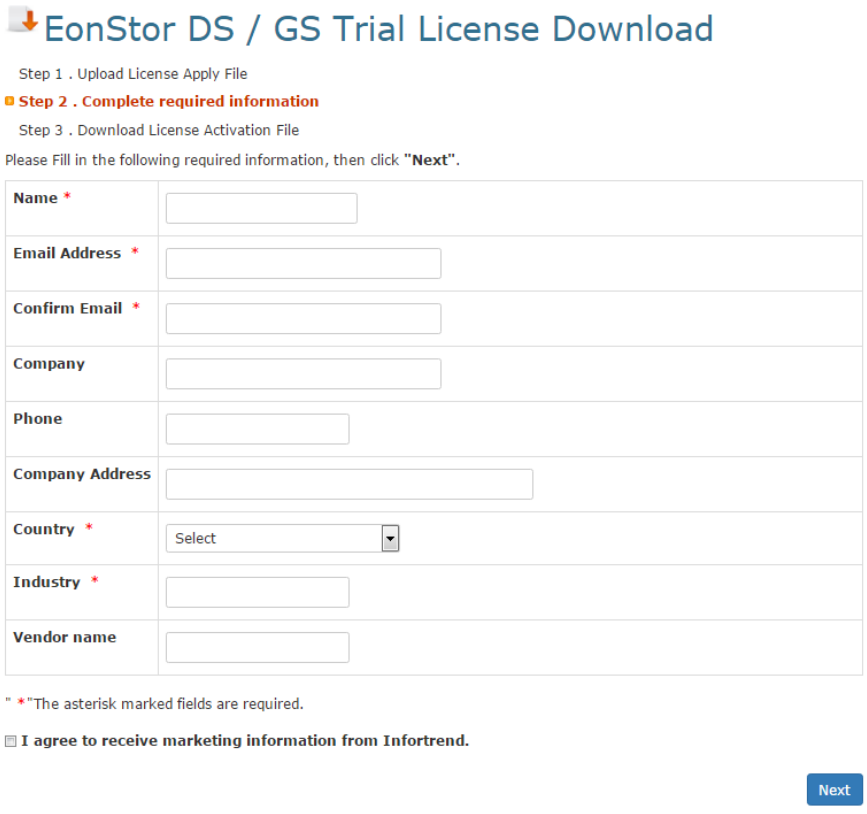


Carefully read the information, select the checkbox, and click **Next**.

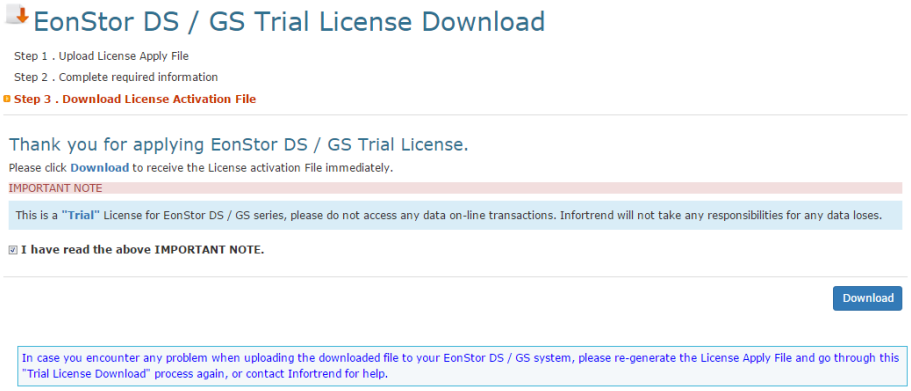


Upload the License Application File you generated through SANWatch and click **Next**.

Fill in customer information and click **Next**.

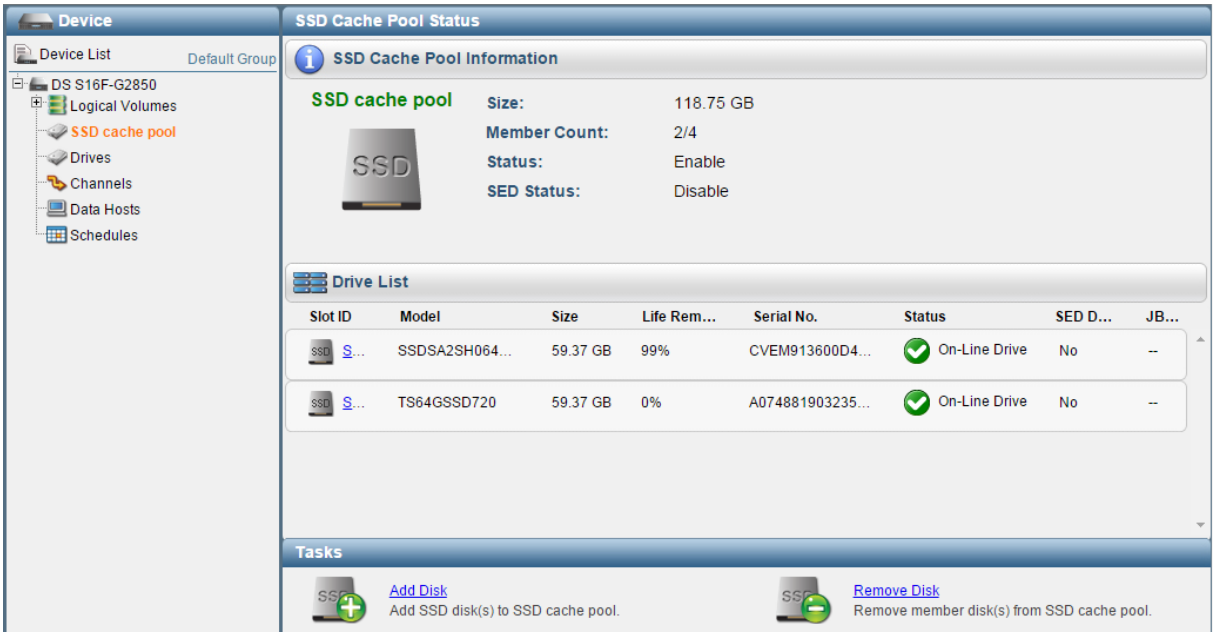


Click **Download** to receive the License Key File immediately.



Save the License Key File at a preferred location and upload it to SANWatch.

Working with SSD Cache Pool (EonStor DS subsystems only)



SSD cache pool is a pool composed of SSD drives, designed to accelerate application workloads by automatically copying the most frequently accessed data (a.k.a. the hot data) to the lower latency SSD drives, so that next time when the same data is requested by a host computer, the subsystem will retrieve it from the SSD cache pool (instead of other drives), thus boosting the data reading performance for the host. SSD cache pool is especially useful for environments with intensive random reading requests, such as OLTP and databases, etc.

Since the SSD cache pool works in ways similar to that of a cache, data stored in it will be removed after the controller is reset or shut down.

To use the SSD cache pool, additional license is required. Go to SANWatch home > Device sidebar > Device List > device name > Tasks corner > License Information (under Information) to apply for it.

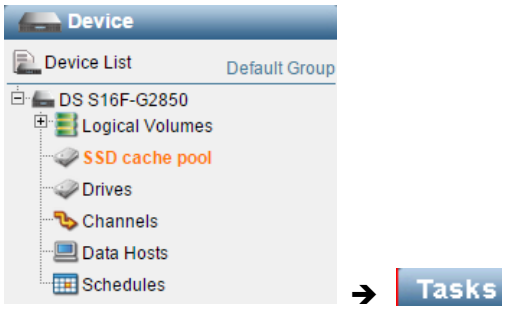
Configuring SSD Cache Pool (EonStor DS subsystems only)

Notes and limitations

- SSD cache pool can only accelerate the reading process for host computers. Writing data from host computers to the SSD cache pool is currently not supported.
- "Sequential read" is not supported by the SSD cache pool, meaning using the SSD cache pool will not enhance the reading performance for sequential data, such as multimedia files. On the other hand, the SSD cache pool can enhance the random reading performance for databases and OLTP.
- After configuring the SSD cache pool for the first time, resetting the controller is required. Resetting the controller will not be required for future configuration.
- Designating drives located in JBOD enclosures as member drives of the SSD cache pool is not allowed.
- One controller can manage up to 4 member drives in the SSD cache pool.
- RAID configuration is not available for member drives in the SSD cache pool.
- Data stored in the SSD cache pool will be removed every time the subsystem reboots.

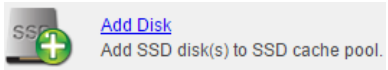
Go to

SANWatch Home > Device sidebar > Device List > device name > SSD Cache pool > Task corner



Activating the SSD cache pool

Click Add Disk in the Tasks corner.



Select any of the available SSD disks from the list.

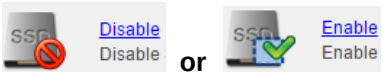
Slot ID	Model	Size	Life ...	Serial No.	Status	SED...	JB...
Slot 1	SSDSA2SH064G1GC	59.37 GB	99%	CVEM913...	Formatted Drive	No	--
Slot 2	TS64GSSD720	59.37 GB	0%	A0748819...	Formatted Drive	No	--

Click OK and then click Close when the process is complete.

If you are enabling the SSD cache pool for the first time, you will be required to reset the controller for the function to take effect. Resetting the controller will not be required for future configuration.

Enabling or disabling the SSD cache pool function

Click Disable or Enable in the Tasks corner.

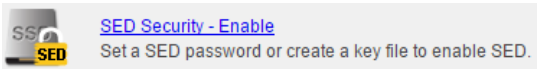


Click Yes and then click Close when the process is complete.

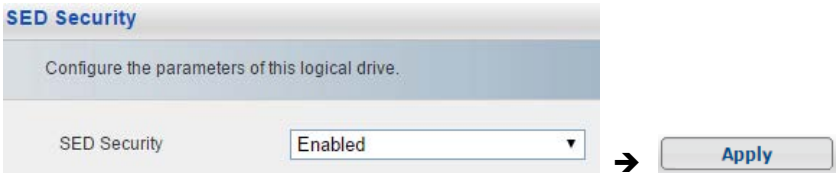
Enabling SED Security

Make sure all member drives support SED before proceeding.

Click SED Security - Enable in the Tasks corner.



In the window that appears, choose an option from the SED security drop-down menu, and then click Apply to enable or disable SED security.

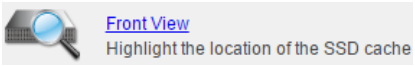


For more information about using a "global" or "local" key to protect drives with SED security, go to SANWatch Home > Device sidebar > Device List > device name, click the Help icon at the top-right corner, and look for the SED related topic.

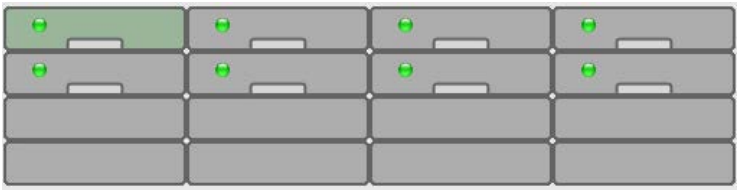
SED security will be enabled when the setting is completed. Click Apply and Close to finish.

Enclosure View

To view the position of member drives, click Front view in the Tasks corner.

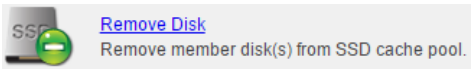


The position of the member drives will be highlighted in the enclosure view.



Removing member drives

Click Remove Disk in the task corner.

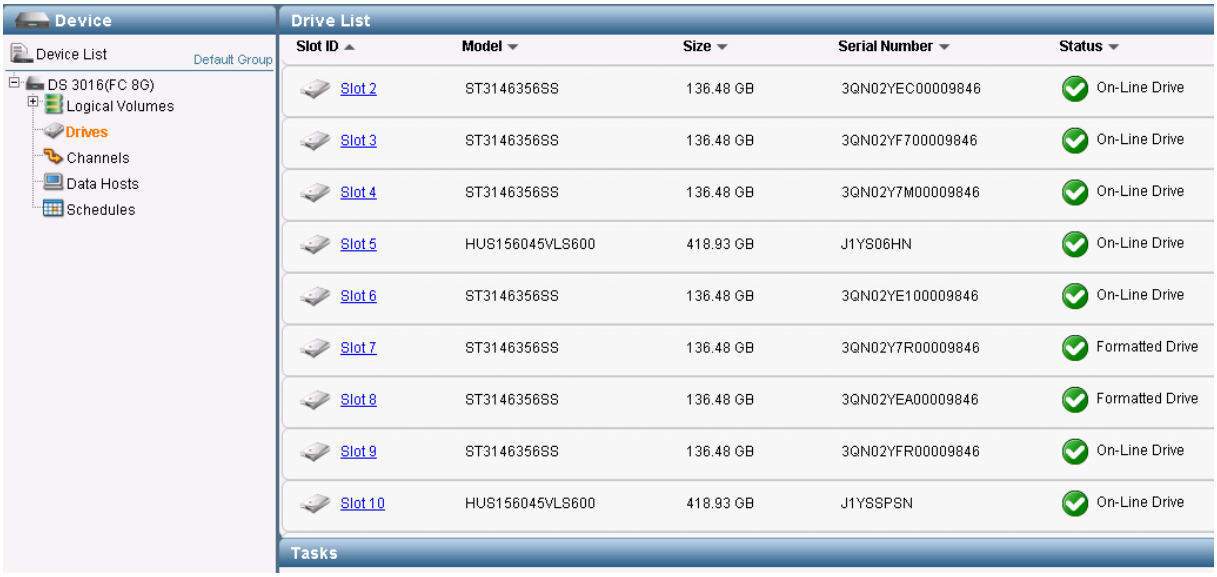


In the window that appears, select the disk(s) you want to remove.

Slot ID	Model	Size	Life ...	Serial No.	Status	SED...	JB...
Slot 1	SSDSA2SH064G1GC	59.37 GB	99%	CVEM913...	Formatted Drive	No	--
Slot 2	TS64GSSD720	59.37 GB	0%	A0748819...	Formatted Drive	No	--

Click OK and Yes to confirm the change.

Working with Drives

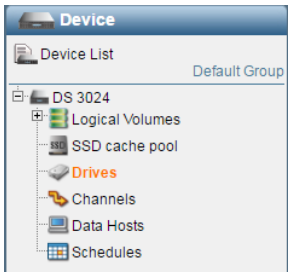


The Drives menu allows you to view the current hard disk drive configurations inside the device (RAID subsystem or JBOD) and monitor the performance, identify the drive with system errors (red system LED), clone (copy) the contents of a drive to another one, and delete the system reserved space inside a drive to save storage capacity.

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.

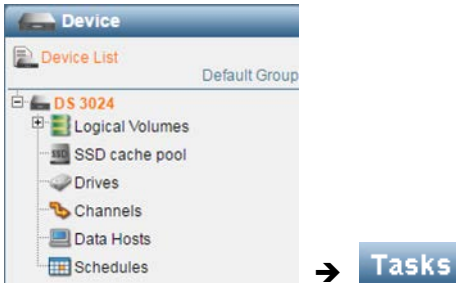
Click the link to see the parameters of the hard drive.

"Life Remaining" is available for SSD drives only.

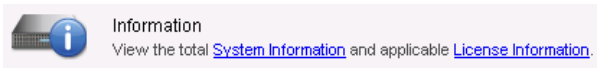
You may click Refresh to update the parameters to the latest status.

Viewing System Hardware Parameters (including drive parameters)

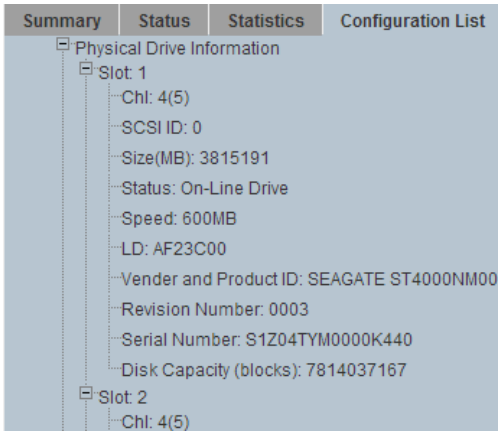
Go to SANWatch Home > Device sidebar > Device List > device name > Tasks corner.



Click the System Information link in the Tasks corner.



Click the Configuration List tab. All system parameters will be listed.

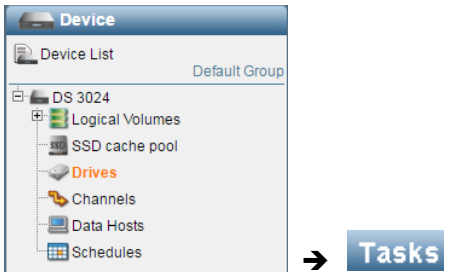


Scanning Drives

To scan a disk drive, it must be an enclosure spare drive or a global spare drive.

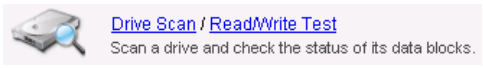
Go to

SANWatch Home > Device sidebar > Device List > device name > Drives > Tasks corner

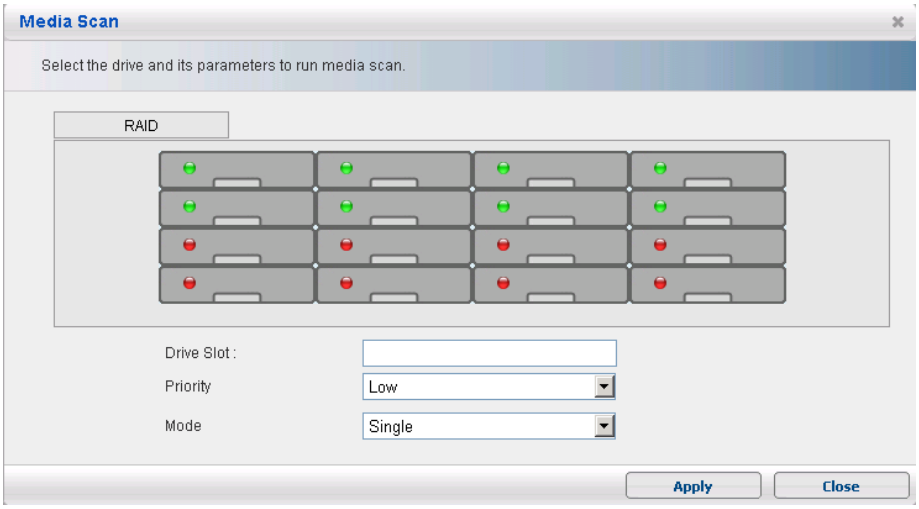


Scheduling Drive Scanning

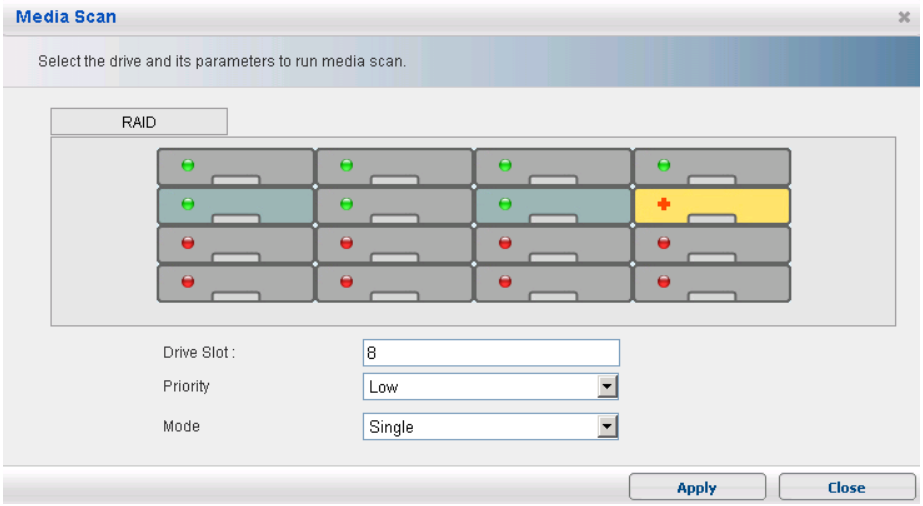
Click Drive Scan in the Tasks corner.



The drive (media) scan window will appear.



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

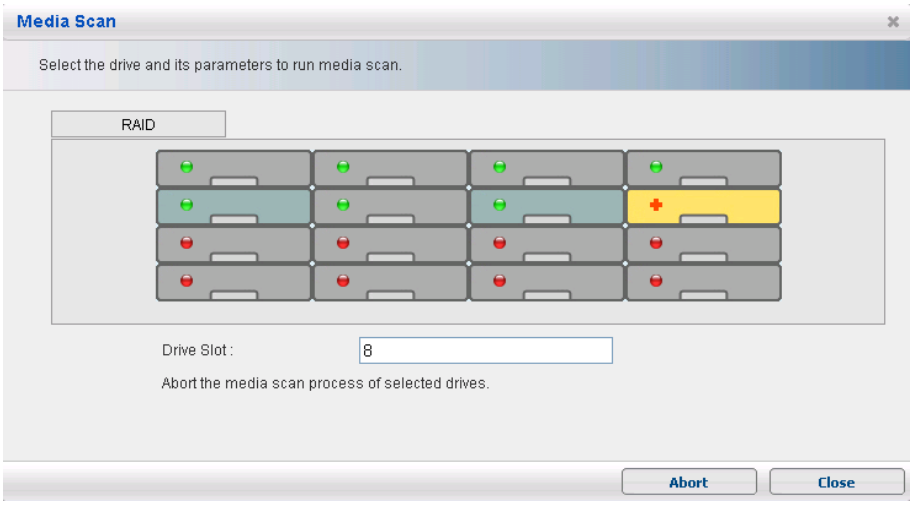


Select the priority and mode, and then click Apply.

The scan will start.

Aborting the Scan

To stop the scan from running, click the drive which is being scanned. The button will turn into “Abort” and you may click it.



Priority	Specifies how much of the system resource be used for scanning. The higher the priority, the faster the scanning but the system performance will decrease.
Mode	Specifies the scanning to be performed once (Execution Once) or continuously.

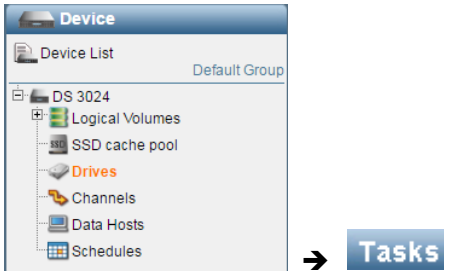
Cloning a Drive

Cloning refers to taking a backup copy of a drive that has been predicted to fail in the near future. You may receive indications of drive failures such as bad sectors through event notifications. When a drive fails, the clone target drive automatically takes place of the failed one to prevent system downtime.

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

Go to

SANWatch Home > Device sidebar > Device List > device name > Drives > Tasks corner

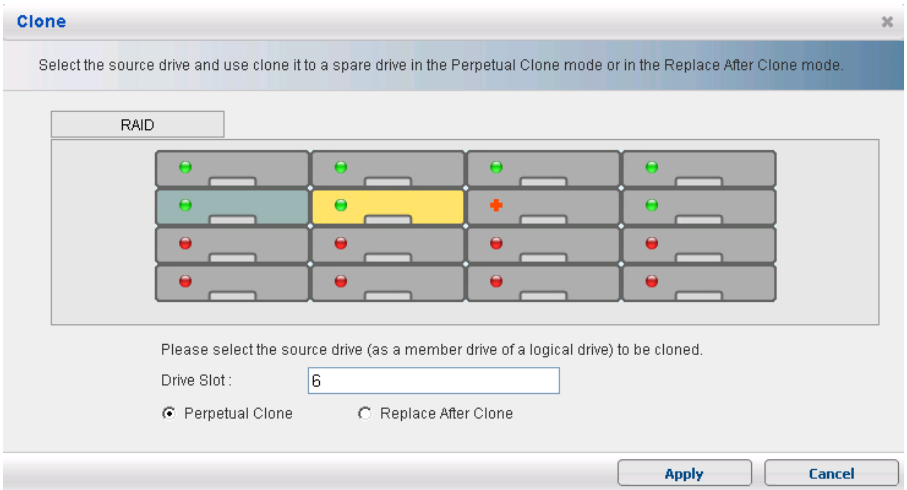


Steps

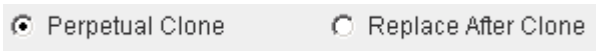
Click the Clone menu in the Tasks corner.

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 cloning 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 place of (replaces) the source drive. The source drive will not be used any more, waiting to be replaced by a new drive.

Click Apply. The target drive (a spare drive) will be chosen automatically and the source drive will be cloned.

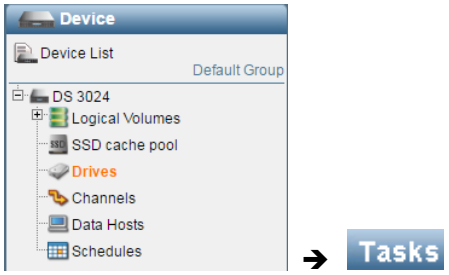
Replacing a Drive

Instead of waiting for a drive to fail (and then be replaced automatically), you may replace a drive that is likely to fail soon with a drive manually.

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

Go to

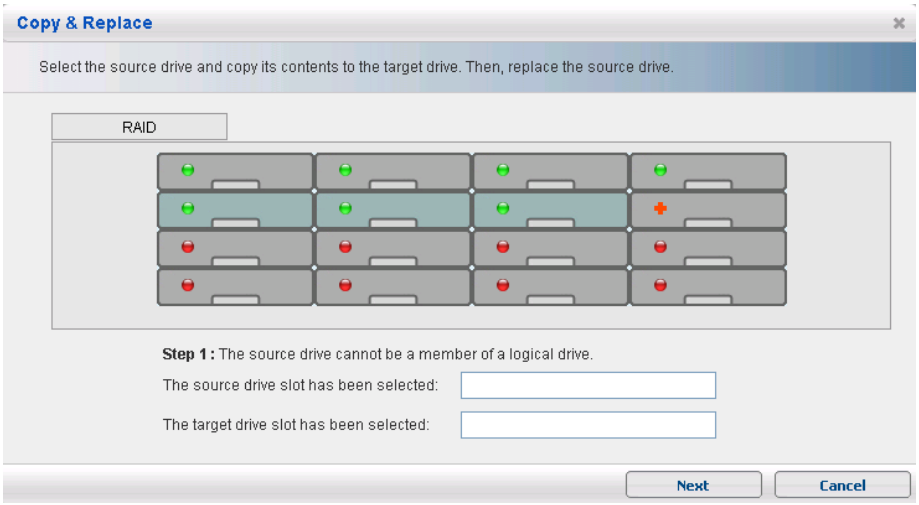
SANWatch Home > Device sidebar > Device List > device name > Drives > Tasks corner



Steps

Click Copy & Replace in the Tasks corner.

The Copy & Replace window will appear.



Click to select the source drive, and click Next

The source drive must be part of a logical drive (or pool element).

Click to select the target drive, and click Apply.

The target drive cannot be a member of a logical drive (or pool element).

The content of the source drive will be copied to the target drive, and then the

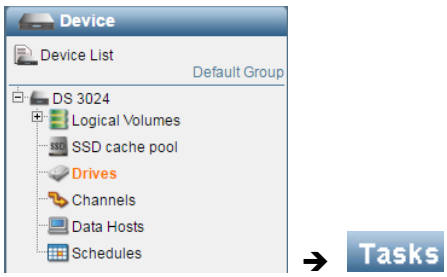
target drive takes place of the source drive.

Identifying a Drive

You may flash the LED on the drive trays to identify the drive hardware-wise on a storage subsystem enclosure.

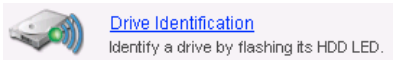
Go to

SANWatch Home > Device sidebar > Device List > device name > Drives > Tasks corner

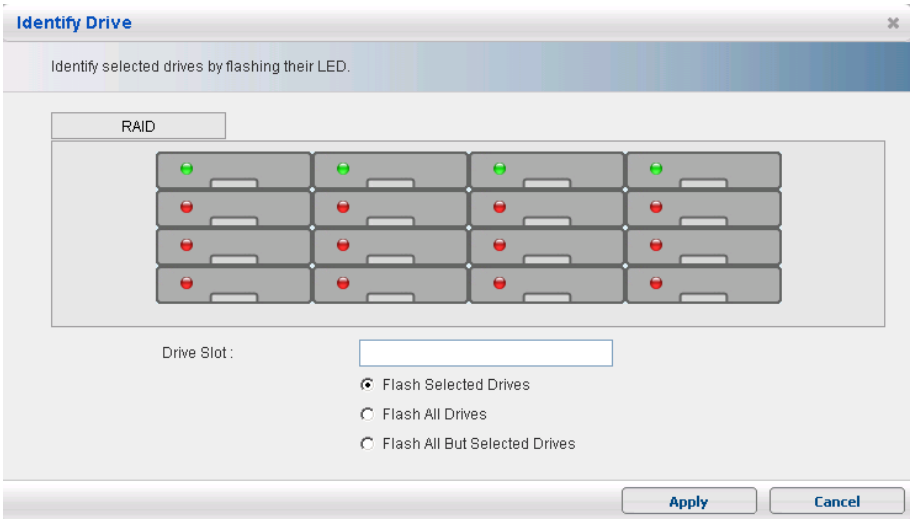


Steps

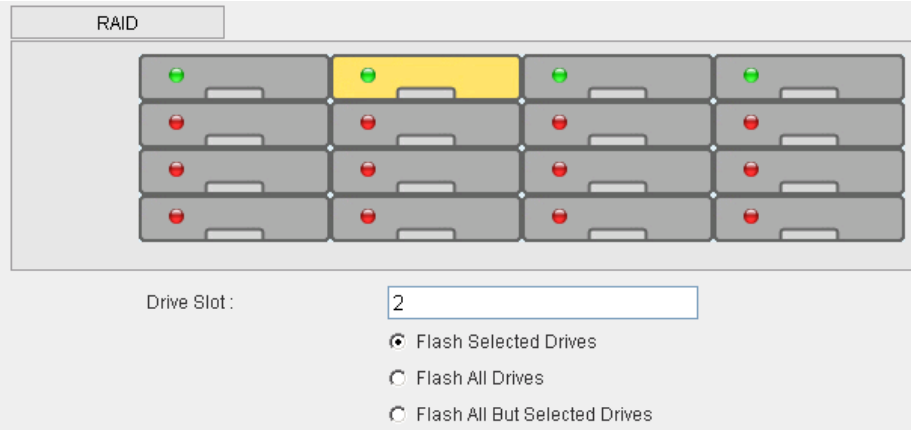
Click Drive Identification.



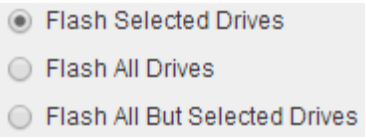
The front view of the drive slots will appear.



Click the drive you would like to identify. The selected 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 five to ten seconds.

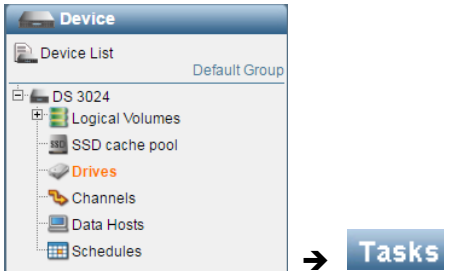
Parameters	**Flash Selected Drive**	Flashes only the LED of the selected drive.
	Flash All Drives	Flashes the LED of all drives in the subsystem enclosure.
	Flash All but Selected Drives	Flashes the LED of all drives in the storage subsystem enclosure but the selected drive.

Configuring the Reserved Space of a Drive

A formatted drive includes a reserved section to be used for event logs and storage virtualization, so that these contents will not be erased upon system reset. You may remove the reserved section (unformatting a drive) to bring the drive status to “new.” This operation is necessary for debugging purposes, especially if you intend to do a read/write test on a drive; otherwise, it is not recommended.

Go to

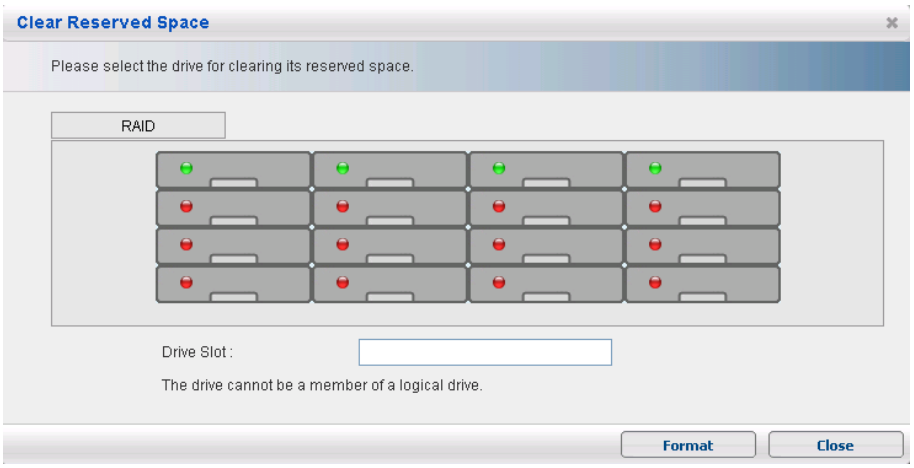
SANWatch Home > Device sidebar > Device List > device name > Drives > Tasks corner



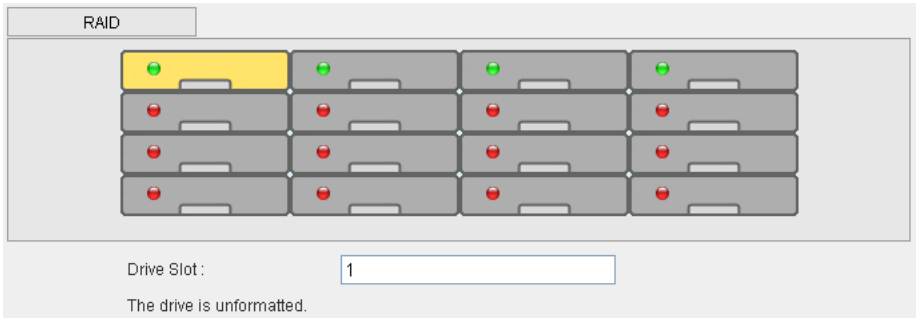
Steps

Click the Reserved Space link in the Tasks corner.

The front view of the drive slots will appear.



Click the drive you would like 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.

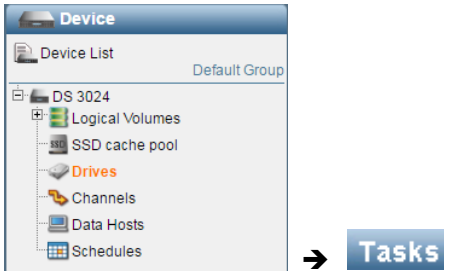
- If the drive has been formatted, click the Reformat button at the bottom to proceed.
- If the drive has been unformatted, click the Format button at the bottom to proceed.

Assigning Spare Drives (EonStor DS subsystems only)

	You need a hard drive that is not part of a logical drive yet. **Warning:** It is HIGHLY RECOMMENDED that you assign a SPARE DRIVE! Without a spare drive, there is an increased risk of data loss!

Go to

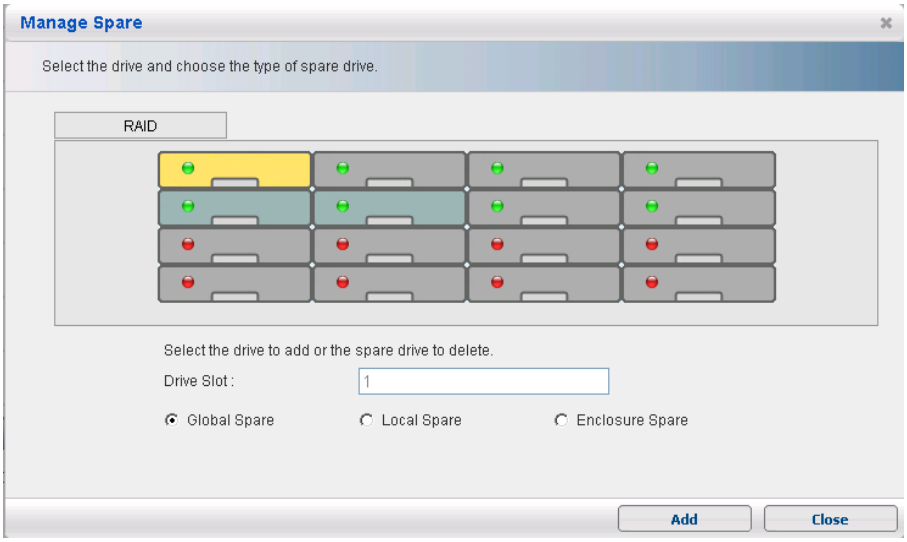
SANWatch Home > Device sidebar > Device List > Device Name > Drives > Tasks corner



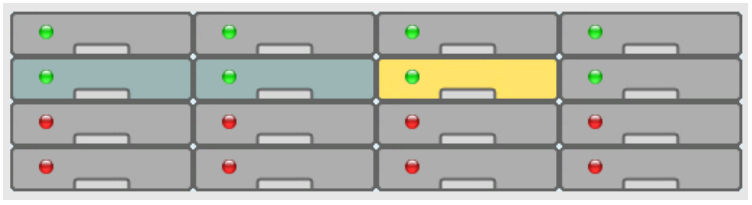
Steps

Click Spare Drive Maintenance in the Tasks corner.

The Spare Drive Management window will appear.



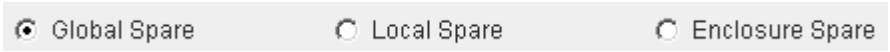
Highlight an available drive.



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

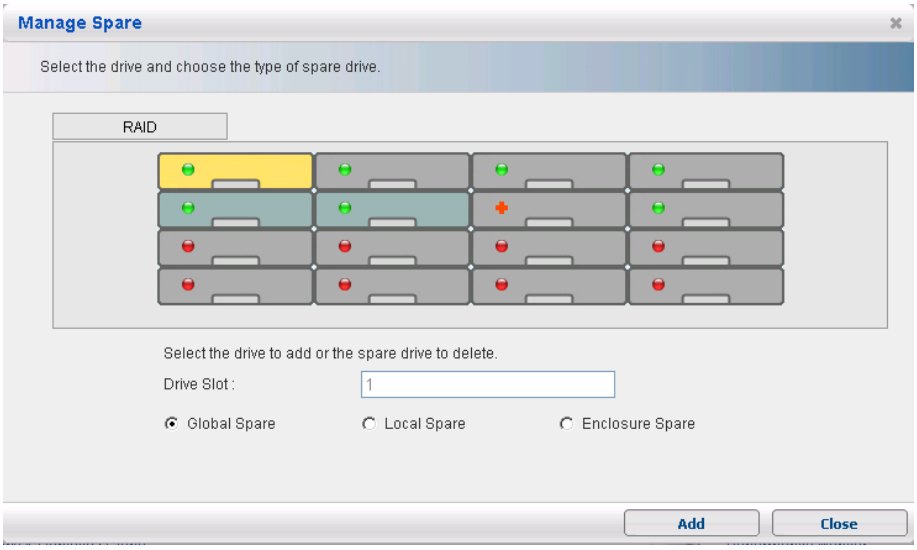
Click Add. The drive will turn into a spare drive.

Deleting Spare Drives

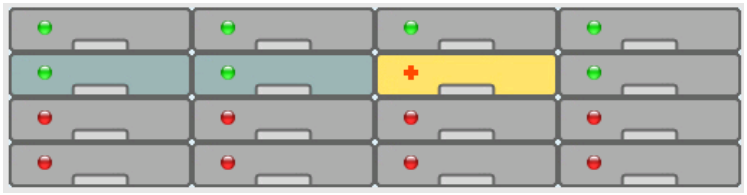
This option is available when one or more spare drives exist.

Click Spare Drive Maintenance in the Tasks corner.

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.

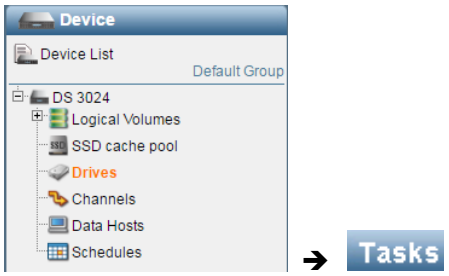
Click Delete to delete the spare drive. The drive will return into a normal (unused) drive.

Monitoring Disk Drive Usage (Performance Monitor)

The Performance Monitor allows you to view the disk drive usage and performance status in real time to help identify where the system performance bottleneck lies.

Go to

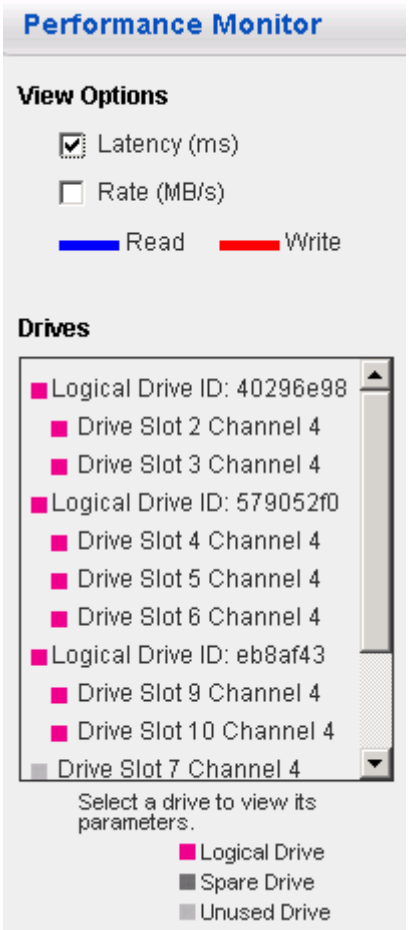
SANWatch Home > Device sidebar > Device List > device name > Drives > Tasks corner



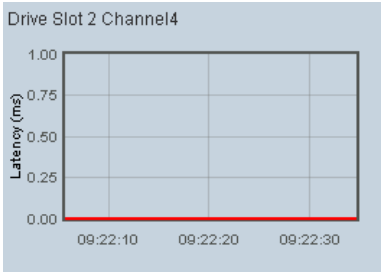
Opening the Performance Monitor

Click the Performance Monitor menu in the Tasks corner.

The Disk Performance Monitor will open updating the disk drive usage in real time.



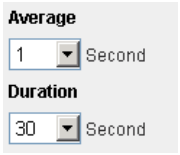
Monitor Graph



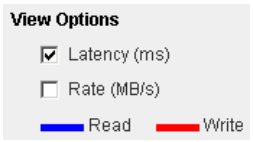
- Title: Specifies the slot location and host channel ID of each drive.
- Vertical axis: Shows the latency. 1.00 millisecond = 100%.
- Horizontal axis: Shows the current time.

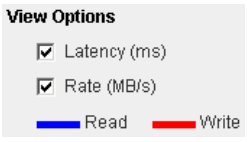
Configuring the Axis

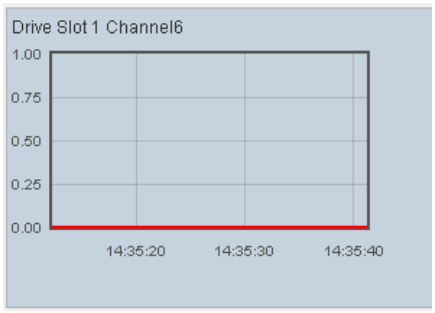
To set the averaging time and duration (x-axis), use the drop-down menu in the sidebar.

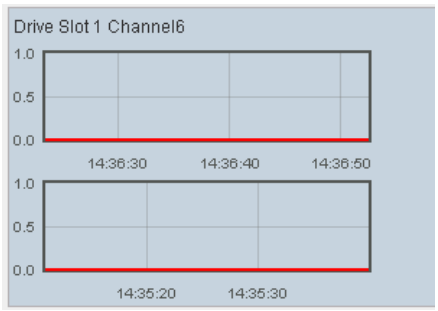


You can select the y-axis item from the sidebar. By default, the y-axis is set to show both latency and data rate. You may replace it with data rate or latency.







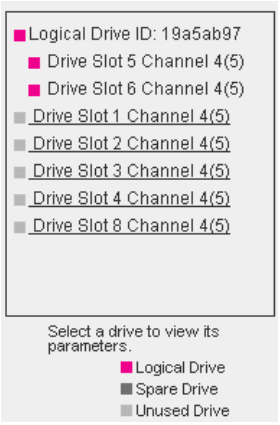


Average	Specifies the data averaging period: 1, 2, 4, and 8 seconds.
Duration	Specifies the time range of the monitor screen: 30, 60, 90, 120, and 160 seconds.

Drive Categories

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

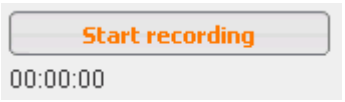
and List



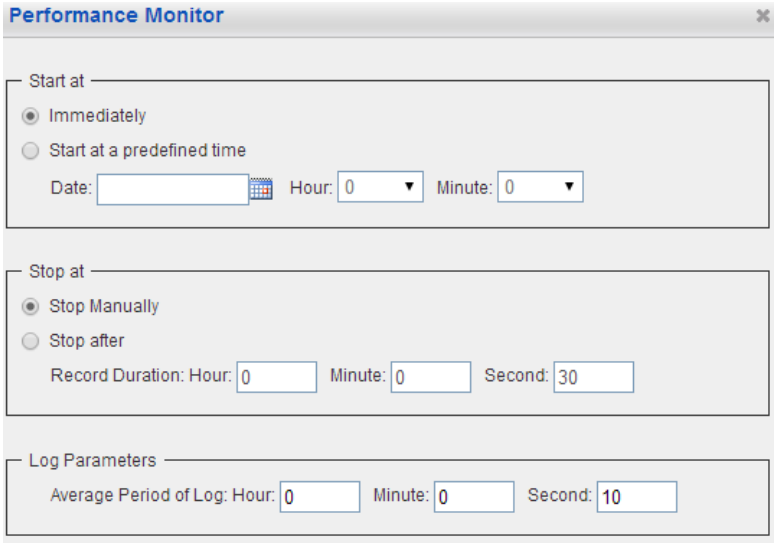
Logical Drive	The hard disk is part of a logical drive.
Spare Drive	The hard disk is part of a local or global spare drive.
Unused Drive	The hard disk does not exist, or is not part of a logical drive.

Recording the Status

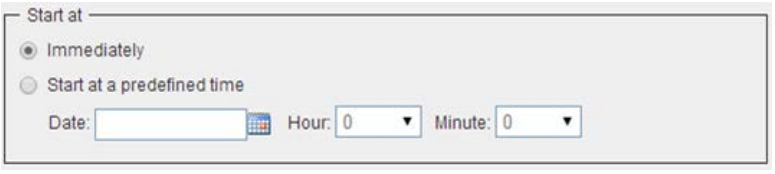
You may record the disk performance data into a log file. Click the Start Recording button.



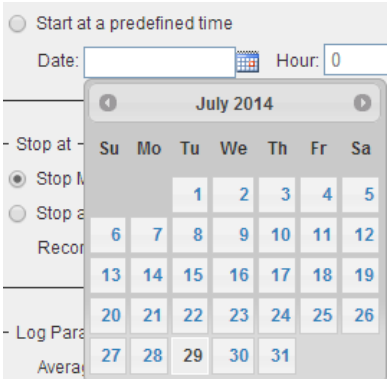
The recording window will appear.



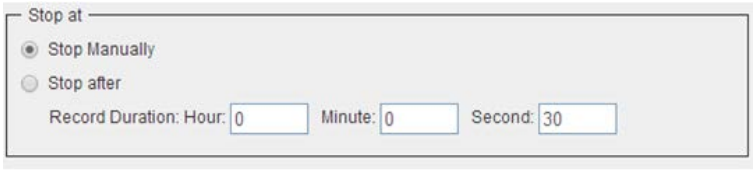
Select the starting time: right now or later.



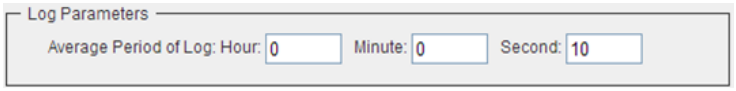
If you click the calendar icon, you can select the starting date.



Select the ending time: manually or after a fixed period.

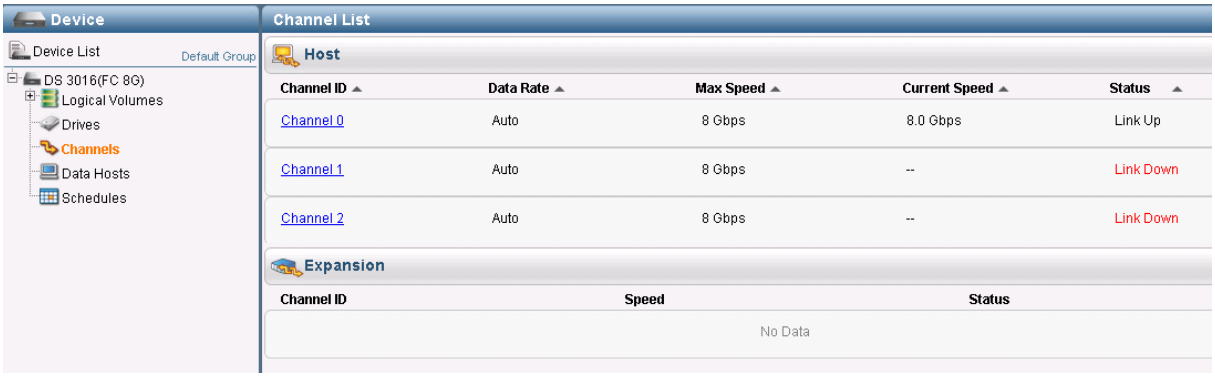


Select how frequently the data will be sampled.



Click OK. The button will turn into Stop Recording and Download Log. You can manually stop the recording and/or download the result into a local file.

Working with Channels (NOT Supported by EonServ)

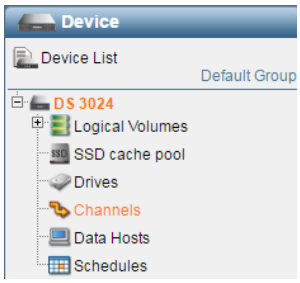


This chapter describes how to view and configure the current host channel configurations, give an alias to a channel, group channels, and check whether the channels are properly connected.

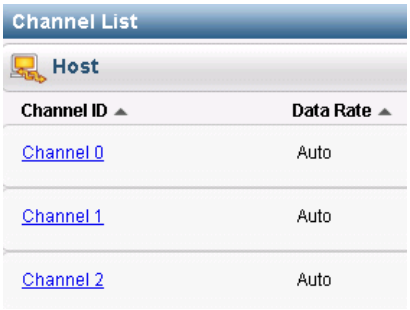
Viewing Channel Configurations

Viewing Channel Parameters

Go to SANWatch Home > Device sidebar > Device List > device name > Channels.

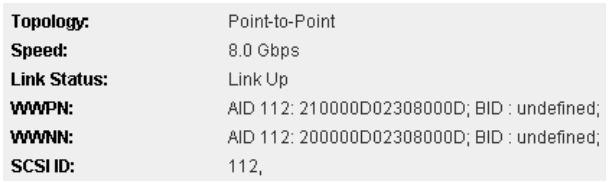


The list of host-device channels will appear.



Click the link to see the parameters of each channel.

This option is available for Fibre channels only.

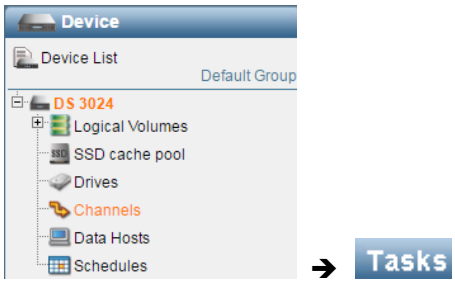


You may click Refresh to update the parameters to the latest status.

Configuring the Host Channel Settings

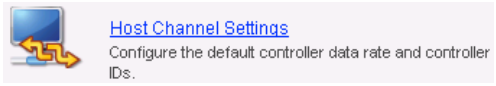
Go to

SANWatch Home > Device sidebar > Device List > device name > Channels > Tasks corner

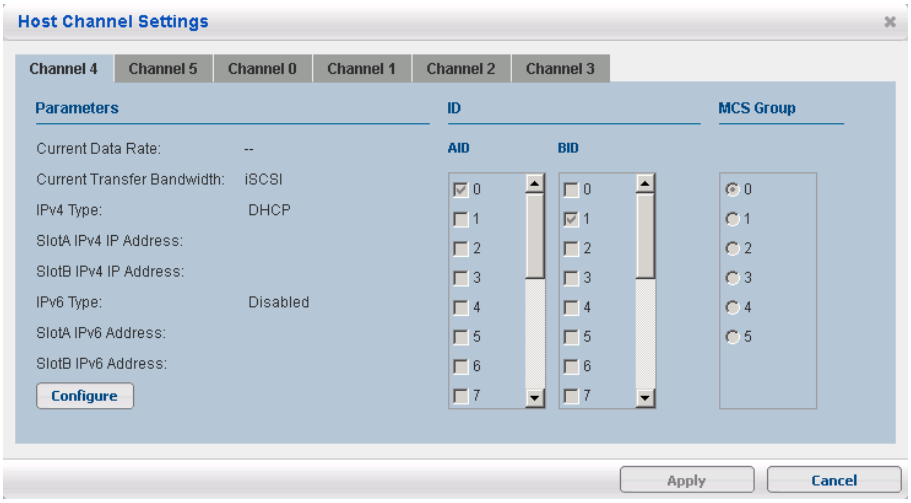


Steps

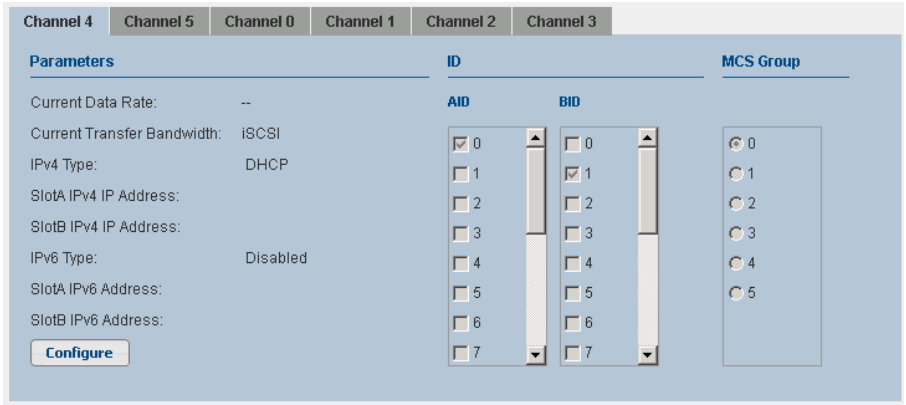
Click Host Channel Settings in the Tasks corner.



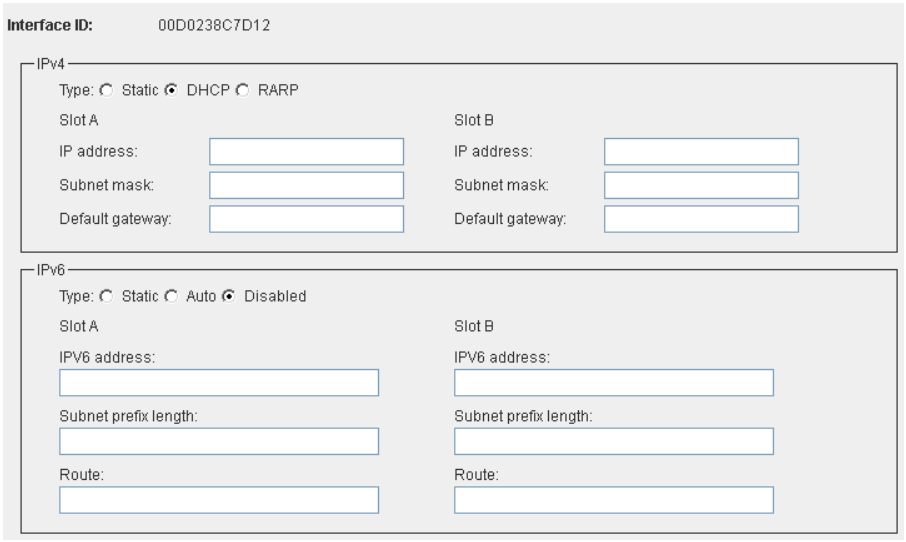
The list of channels and their configurations will appear.



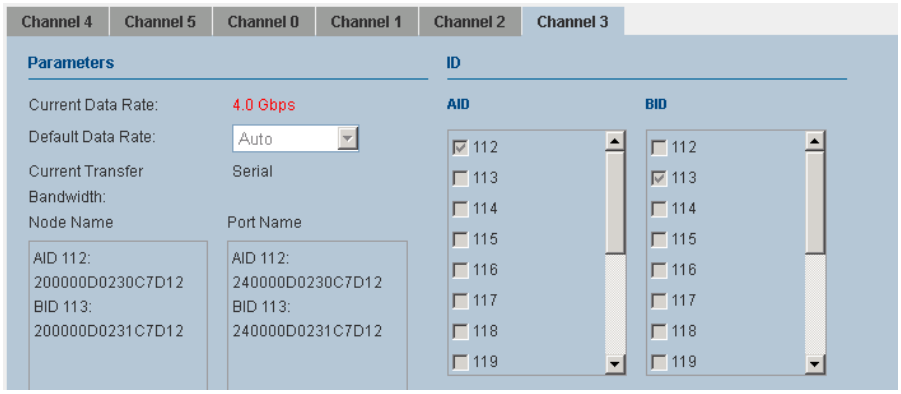
iSCSI Channel Configurations



Click Configure to modify the IP address, subnet, and gateway (route). Note that each slot has its own IP configuration.



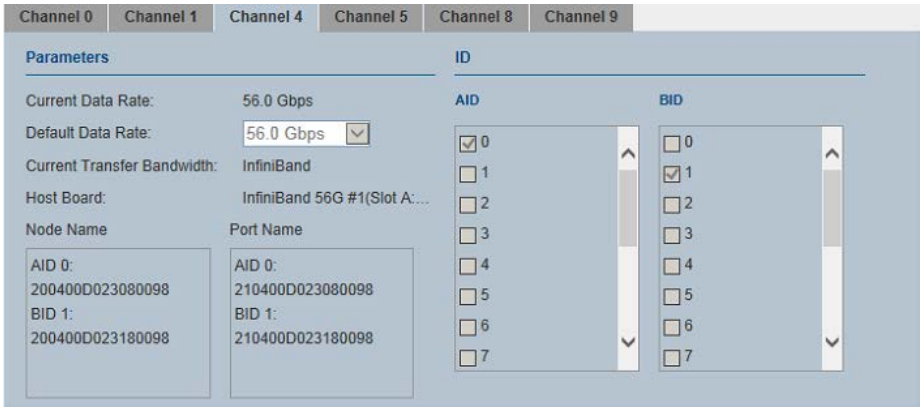
iSCSI Parameters	**Channel ID**	Specifies the LUN mapping ID number.
	MCS Group	MC/S (Multiple Connections per Session) protocol allows combining several channels to improve performance and failover rates.
	Type	(Configurable) ➢ Static: Specifies a fixed IP address. ➢ DHCP (Auto): Allows the router/switch 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 for the subsystem to specify the network subdivision.
Fibre Channel Configurations	There are few configurable parameters for a Fibre Channel port (you may choose 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.

InfiniBand Channel Configurations

There are few configurable parameters for an InfiniBand Channel port.

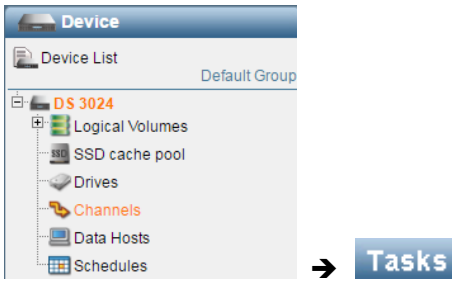


InfiniBand Channel Parameters	**Channel ID**	Specifies the LUN mapping ID number.

Giving Alias / Assigning WWNs to Groups

Go to

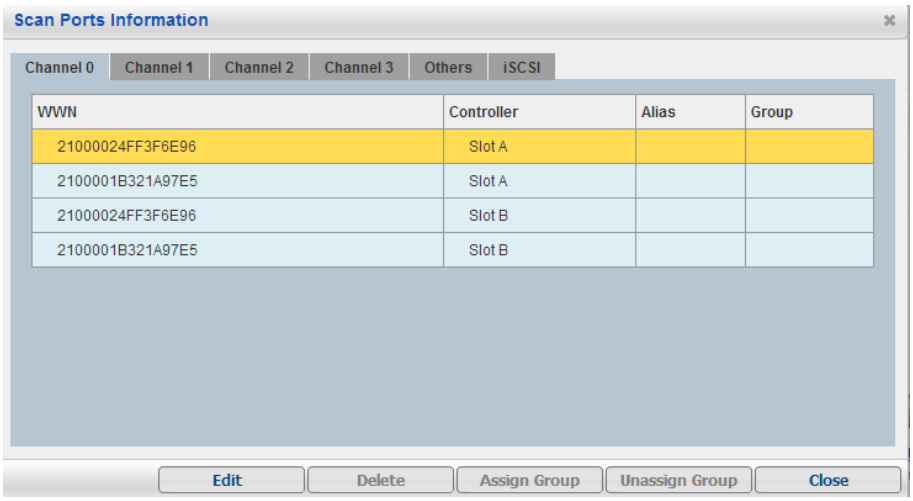
SANWatch Home > Device sidebar > Device List > device name > Channels > Tasks corner



Steps

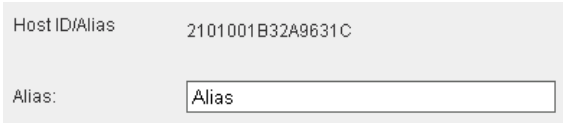
Click Scan Port Information in the Tasks corner.

The list of alias and WWN (World Wide Name) will appear.

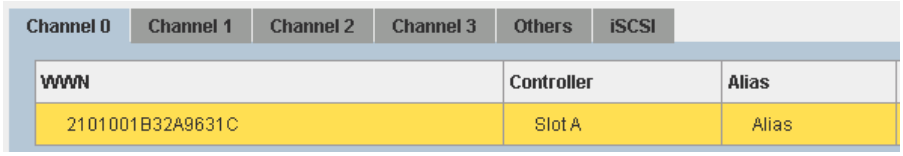


Assigning/Deleting an Alias/WWN

To assign an alias for a WWN, highlight it, click Edit and enter an alias.



The alias will appear in the WWN list.

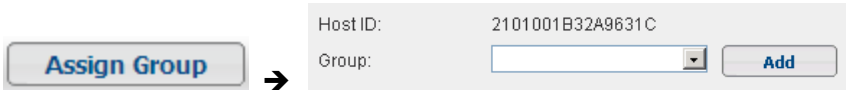


To delete the alias/WWN, click Delete.

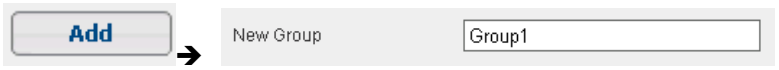
Assigning a WWN to a group

After giving an alias to a WWN, you may bundle it to a group. Click Assign

Group. The Group Assignment window will appear.

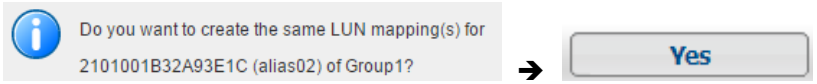


Click Add to name the new group, or choose an existing group from the drop-down menu.



Click OK.

If the group already has LUN mappings, you will be prompted to decide whether you want to add existing LUN mapping(s) already created for the group. Click Yes to include the same LUN mapping(s) for the WWN.

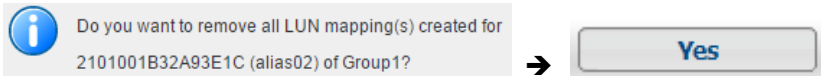


The WWN will be assigned to a group.

Unassigning a WWN from a Group

To unassign a WWN from a group, click Unassign Group, and follow the onscreen instruction to complete the setup.

Depending on the Group's LUN mapping configuration, you might be prompted to decide whether you want to remove existing LUN mapping(s) already created for the group. Click Yes to remove the same LUN mappings for the WWN.



Changing Channel Type for the Converged Host Board

The converged host board allows you to change the channel type for all its four physical ports. When the channel type is changed, all ports on the converged host board will be using the new type after system reboot.

Currently the following channel types are supported by the converged host board includes:

- Fibre Channel 8G
- Fibre Channel 16G
- iSCSI 10G.

Notes and limitations

- System requirement for converged host board: EonStor DS 4000 series.
- LUN mappings should be removed before changing the channel type.
- For FC 16G, its data rate could be optionally set as 16G/8G/4G; For FC 8G, its data rate could be optionally set as 8G/4G.
- If the channel type of the ports on the converged host board is set as Fibre 16G or Fibre 8G, then the storage subsystem could only be connected with other devices through the point-to-point (FC-P2P) topology, meaning Arbitrated Loop (FC-AL) is not supported by the converged host board.
- For Fibre Channel ports on other types of host boards, Arbitrated Loop is supported by Fibre 8G ports, allowing you to change their fibre connection to either loop only or point-to-point only (at System Settings > Host-Side). Arbitrated Loop is not supported by Fibre 16G ports.
- For Fibre Channel ports on other types of host boards, their SCSI ID starts with 112. For the converged host board, its physical ports are all regarded as iSCSI ports even if their type is configured as FC 8G/16G, and their iSCSI IDs are specified according to the following rule:
  Controller A: (accumulated iSCSI channel number) x 16
  Controller B (if available): (accumulated iSCSI channel number) x 16 +1
  Note: The channel number starts from "0", which is also the number of the first physical port.

  The example below demonstrates how to figure out the iSCSI IDs for all available channels on Controller A of a storage subsystem.

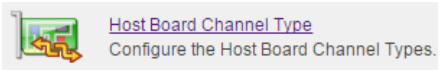
Channel Number	Channel Type	iSCSI ID
0	iSCSI	0 x 16 = 0
1	iSCSI	1 x 16 = 16
2	FC	112
3	FC	112
4	converged host board	2 x 16 = 32
5	converged host board	3 x16 = 48
6	iSCSI	4 x 16 = 64
7	iSCSI	5 x 16 = 80

Go to

SANWatch Home > Device sidebar > Device List > device name > Channels > Tasks corner

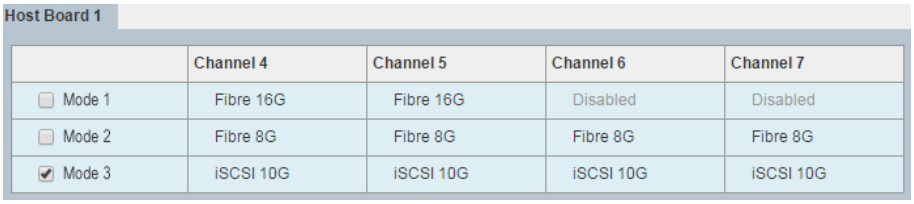
Steps

Click Host Board Channel Type in the Tasks corner.



This option is available only when a converged host board is installed on your controller.

In the window that appears, select one of the checkboxes to change the channel type of all physical ports on the converged host board to the one you specified.



	Channel 4	Channel 5	Channel 6	Channel 7
Mode 1	Fibre 16G	Fibre 16G	Disabled	Disabled
Mode 2	Fibre 8G	Fibre 8G	Fibre 8G	Fibre 8G
Mode 3	iSCSI 10G	iSCSI 10G	iSCSI 10G	iSCSI 10G

Click Apply.

For the change to take effect, restart the storage subsystem.

Parameters

Mode 1	If you select this mode, only the first two ports of the host board will be available for connectivity, with their channel type configured as Fibre 16G.
Mode 2	If you select this mode, all of the 4 ports will be available for connectivity, with their channel type changed to Fibre 8G.
Mode 3	If you select this mode, all of the 4 ports will be available for connectivity, with their channel type changed to iSCSI 10G.

Checking System Health

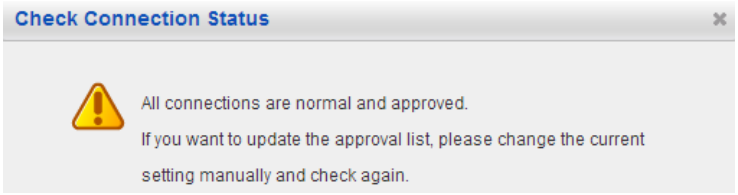
Go to

SANWatch Home > Device sidebar > Device List > device name > Channels > Tasks corner

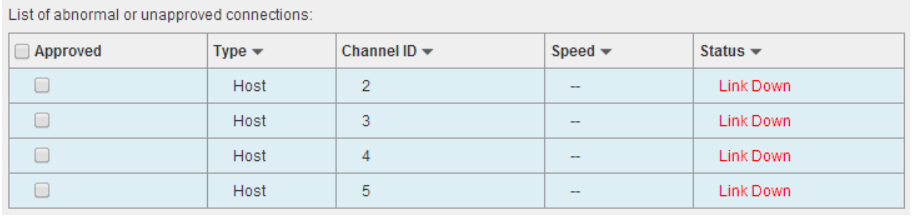
Steps

Click System Health Status Settings in the Tasks corner.

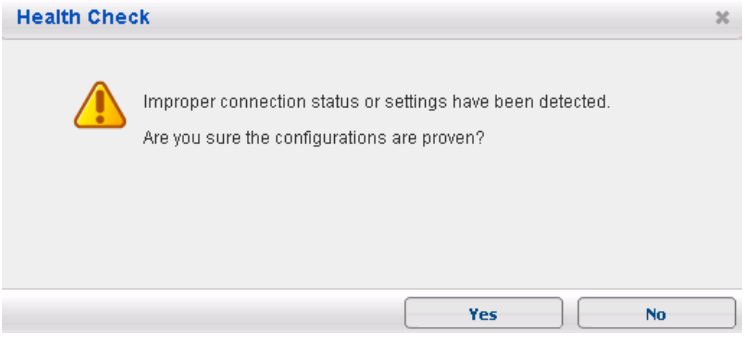
The system will check all channel connections, and display the following message if all connections are normal or approved.



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



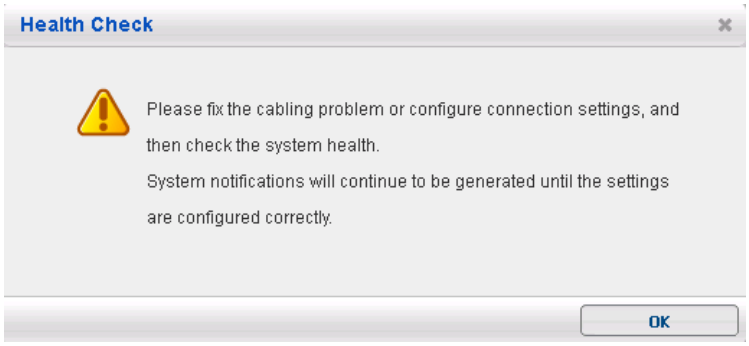
Select the channel(s) whose status you want to approve. If the status to be approved is found to be unhealthy (= contains some network problems), a warning message will appear.



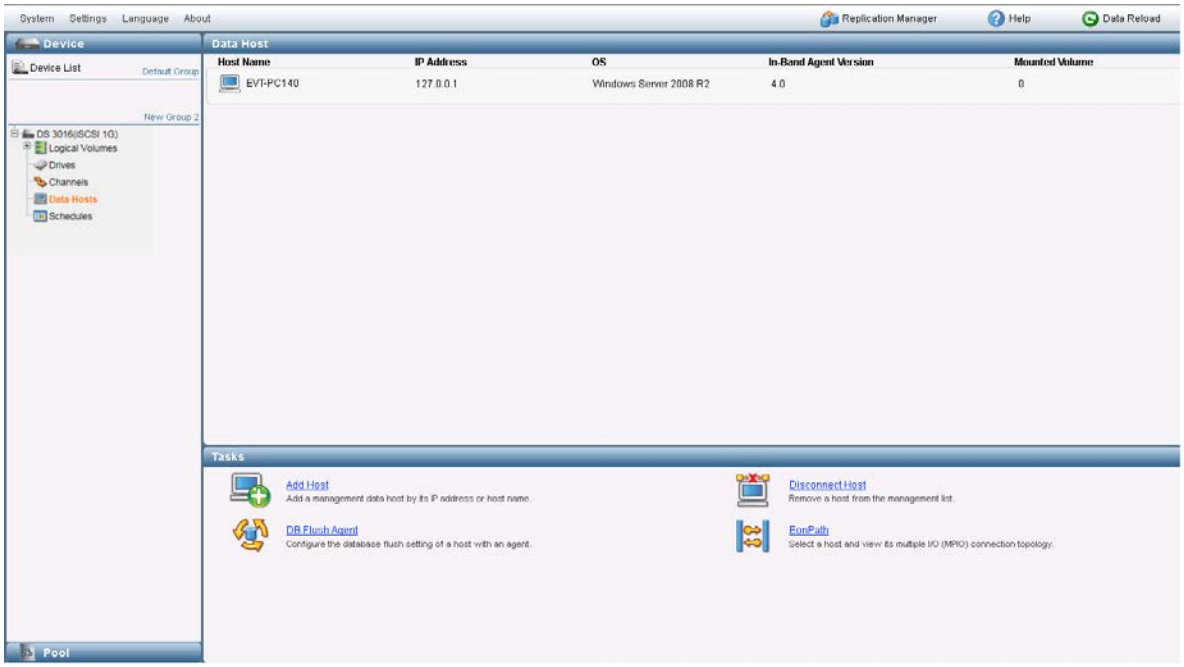
➢ If you click Yes, the message will disappear and the Health Check link will be

disabled (= the connections are normal)

- If you click No, some suggestions on improving the connectivity will appear.

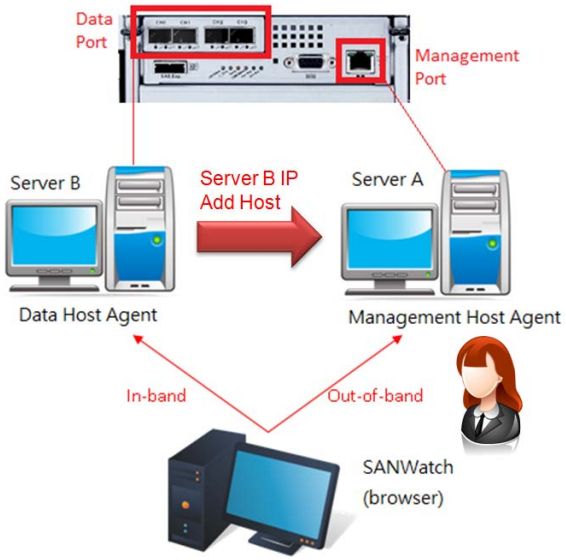


Working with Hosts



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

About Out-of-band & In-band management



(Data Host Agent and Management Host Agent are included in SANWatch)

• Out-of-band	• In-band
Manages the storage through LAN connections.	Manages the storage through host channels.

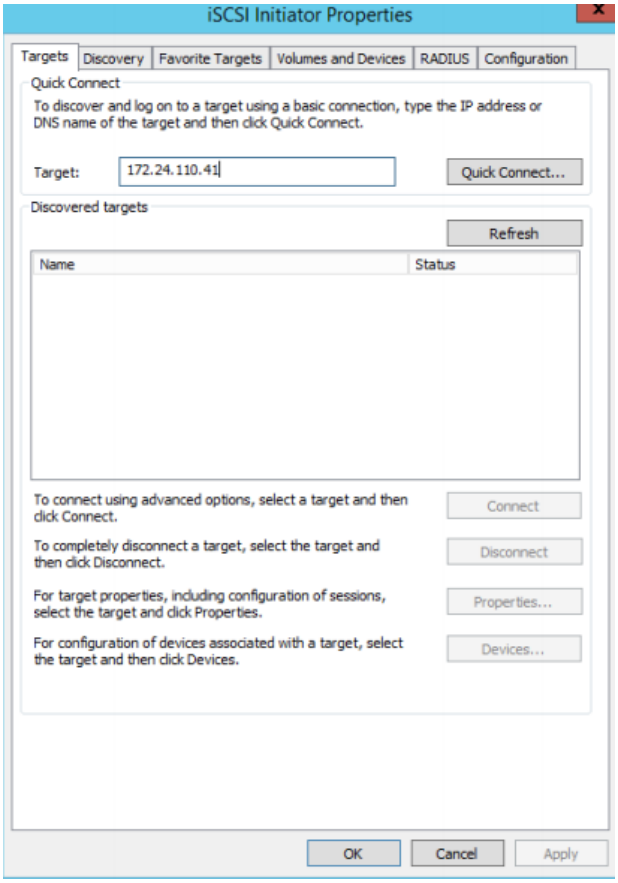
Adding a Host

Before You Start

Go to the host server (for example, Windows Server 2012 R2) > **iSCSI Initiator** > **Targets**.

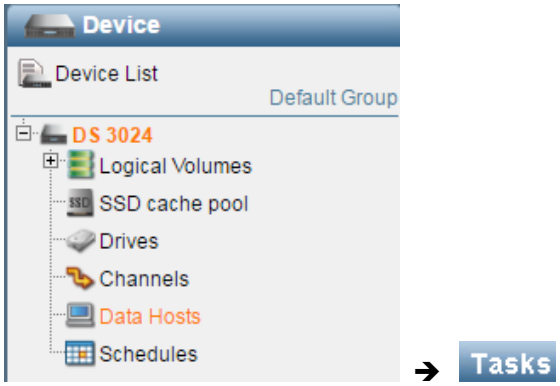
Next, enter a channel IP address of your EonStor DS device in the **Target** field.

Then, click **Quick Connect** to add your device to the **Discovered targets** list. Click **OK** to finish the setting.



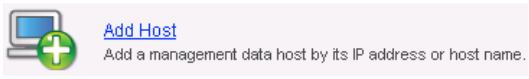
Go to

SANWatch Home > Device sidebar > Device List > device name > Data Hosts > Tasks corner

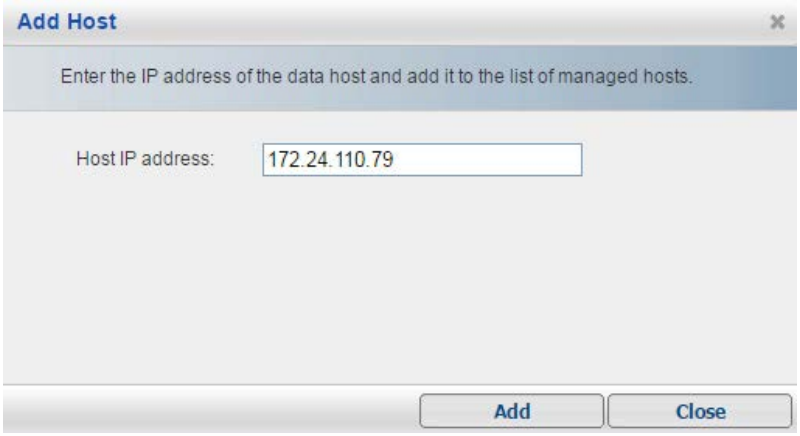


Steps

Click **Add Host**.



Enter the IP address of the new host, then click Add.

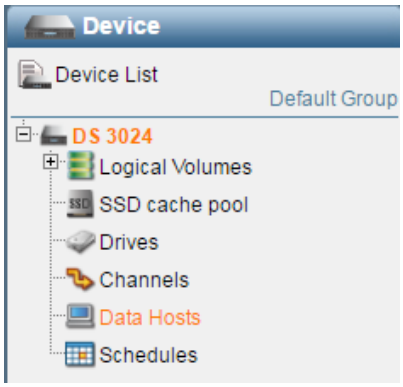


The new host will appear in the Data Host corner.

Removing (Disconnecting) a Host

Go to

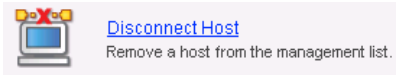
SANWatch Home > Device sidebar > Device List > device name > Data Hosts > Tasks corner



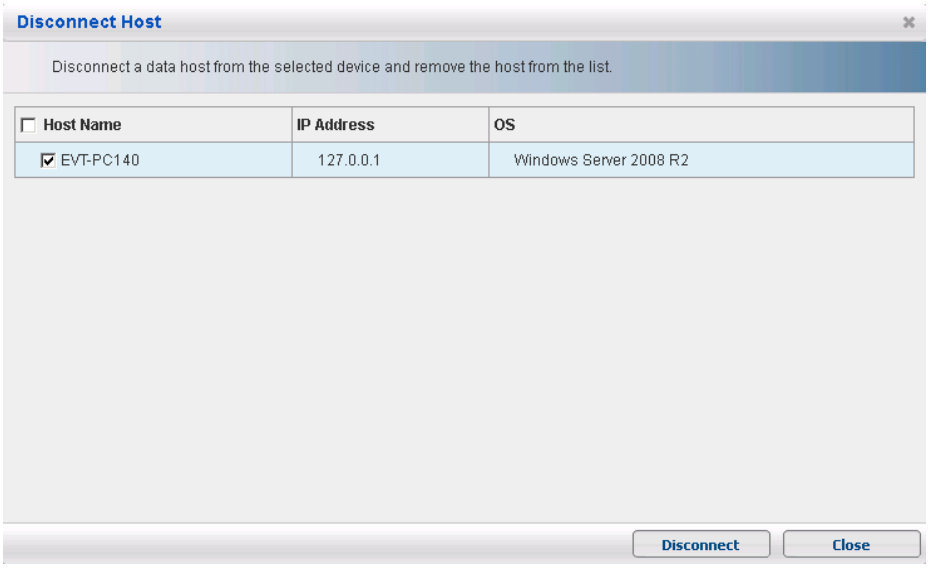
➔ Tasks

Steps

Click Disconnect Host.



Check the host you wish to disconnect from the list and click Disconnect.



The host will be removed from the list.

Disconnecting the host will not affect its configurations. When you reconnect host to the device again, previous configurations will remain intact.

Editing Multipath Devices through EonPath

Only available for Windows 2003 and before.
For Windows 2008 and later, use Microsoft native MPIO settings.

1. Before configuring EonPath setting, you have to install EonPath driver on the host server first (server with Data host agent). For more information about installing EonPath driver, see Working with multipath.
2. You need to add a host (server with Data host agent) to enable in-band management.

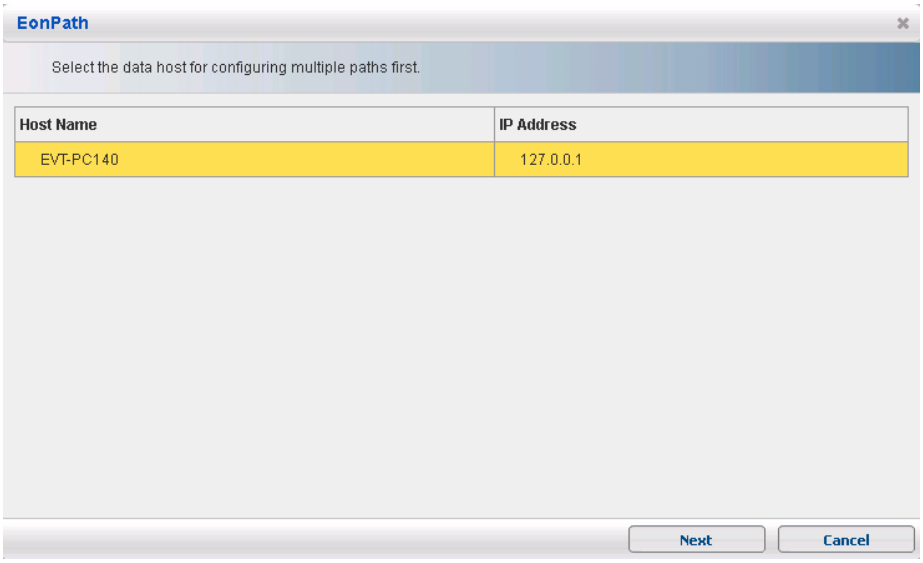
Go to

SANWatch Home > Device sidebar > Device List > device name > Data Hosts > Tasks corner

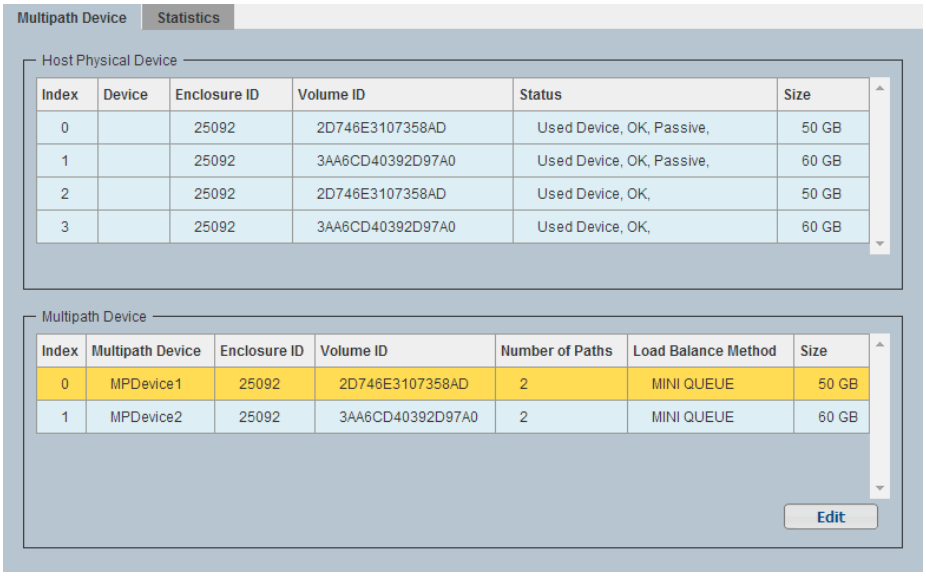
Steps

Click the EonPath menu in the Tasks corner.

The list of current hosts will appear. Highlight the host you would like to configure and click Next.

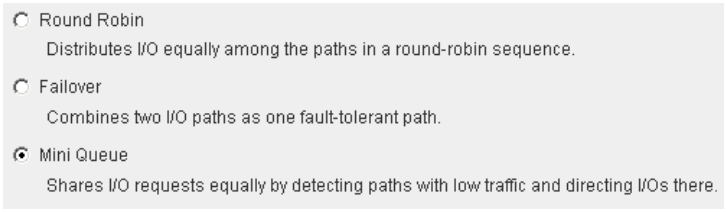


You can view the list of current multipath devices.

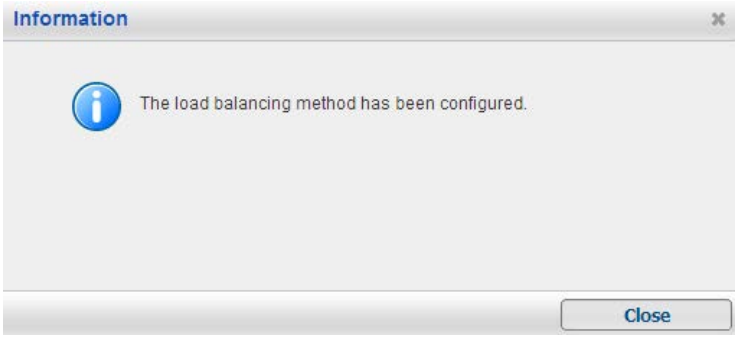


You can edit an existing multipath device.

Select the load balancing policy.
Load balancing applies only to active paths (not applicable to passive paths).



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



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

Parameters	**Failover**	There will be no balancing among multiple paths. One dedicated path will be used for all data transactions, and if the main path fails, the remaining path will take over its role.

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.

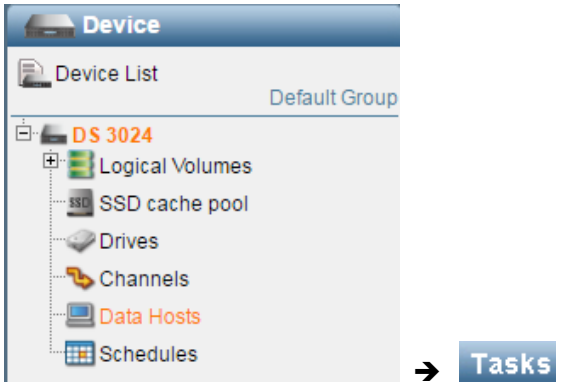
Monitoring Multipath Devices in EonPath

Only available for Windows 2003 and before.

For Windows 2008 and later, use Microsoft native MPIO settings.

Go to

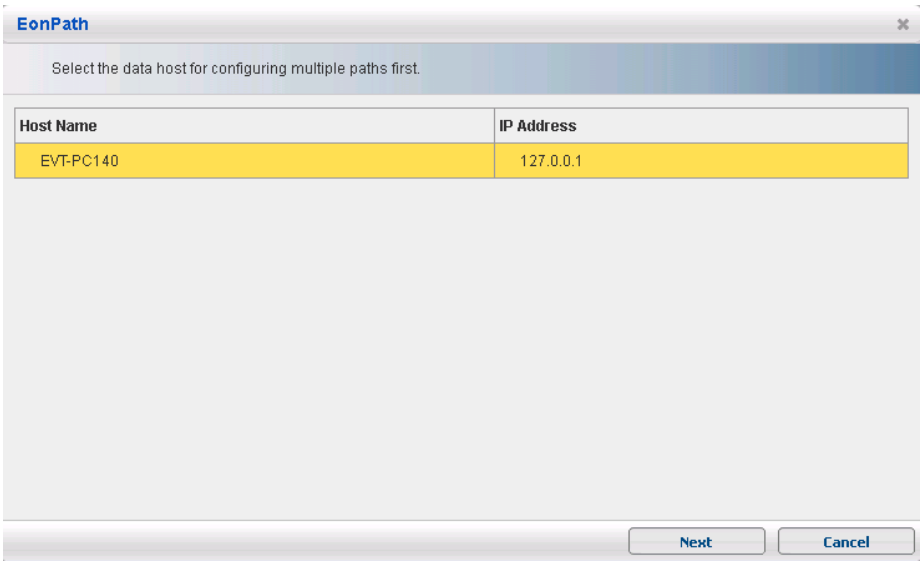
SANWatch Home > Device sidebar > Device List > device name > Data Hosts > Tasks corner



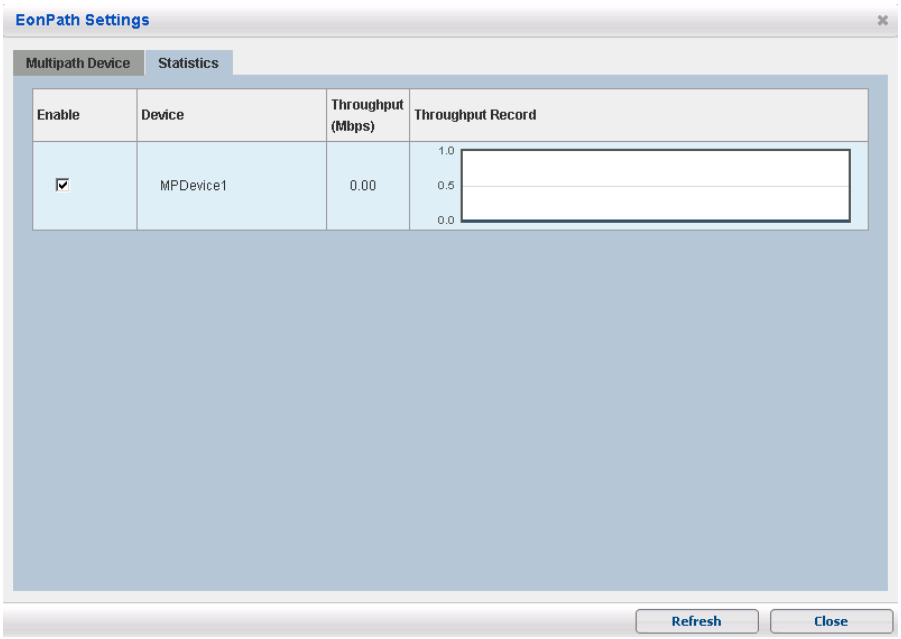
Steps

Click the EonPath menu in the Tasks corner.

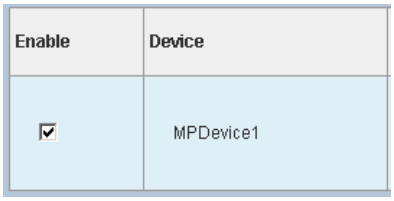
The list of current hosts will appear. Highlight the host you would like to configure and click Next.



Select the Statistics tab. The list of multipath device statistics chart will appear.



Select the checkbox next to the multipath device you want to monitor. The graph will update the I/O statistics in real time.



To refresh the plot, click Refresh.

Flushing Host Cache Memory for Database

When database applications (SQL, Oracle, etc.) are running in the host computer, user data will be temporarily stored inside the host computer's memory (cache memory) before transferred into the RAID subsystem. When you run a replication job (such as snapshot or volume mirror), you must make sure that transferring cache memory content into the RAID subsystem is completed before backing up your data; otherwise, there will be data inconsistency between RAID subsystem and host computer.

The database flush mechanism ensures that any cache data in the host computer will be flushed (transferred) into the RAID system before a replication job is triggered.

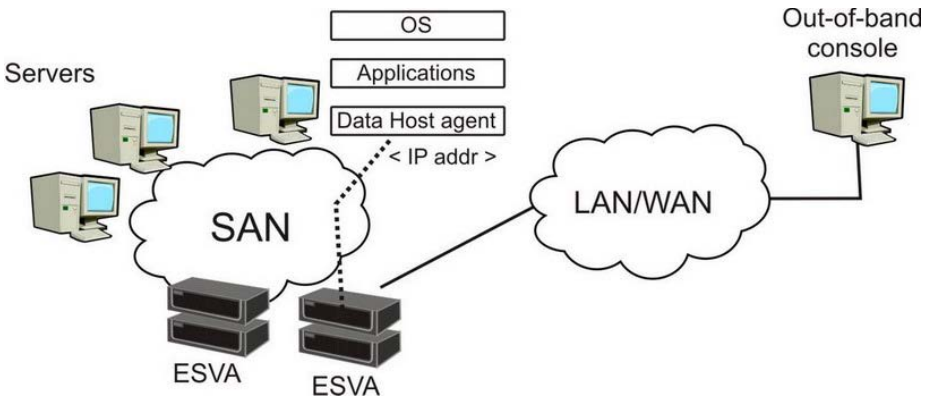
In-Band VS. Out-of-Band

There are two types of cache memory flush, depending on the connection between the host computer and the subsystem.

In-Band Flush

Flushing the cache memory will be triggered by the host computer itself, which is connected to the subsystem through in-band connection. This is the standard flush method when there is only one data host computer or Windows Virtual Machine (VM) is not running in the host computer.

Out-of-Band Flush



Flushing the cache memory will be 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 flush might be in conflict when more than one host computers tries to back up user data at the same time. In this case, out-of-band flush allows multiple servers to perform data flushing in series without conflict.
- Windows Virtual Machine (VM), installed on ESX server, is running in the host computer. VM itself cannot initiate cache data flushing on its own, thus the host computer needs to use the out-of-band connection to initiate flushing indirectly.

Configuring In-Band Flush Using DB Flush Agent

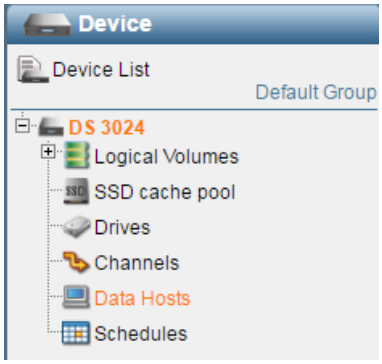
If you are holding data in database forms, you need to flush all data into the storage subsystem before doing a backup job. The DB (database) Flush module in SANWatch allows you to perform it automatically.

DB Flush works for the following databases:

- SQL
- Microsoft Exchange
- Oracle

Go to

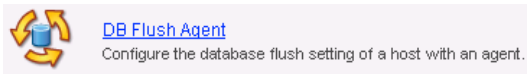
SANWatch Home > Device sidebar > Device List > device name > Data Hosts > Tasks corner



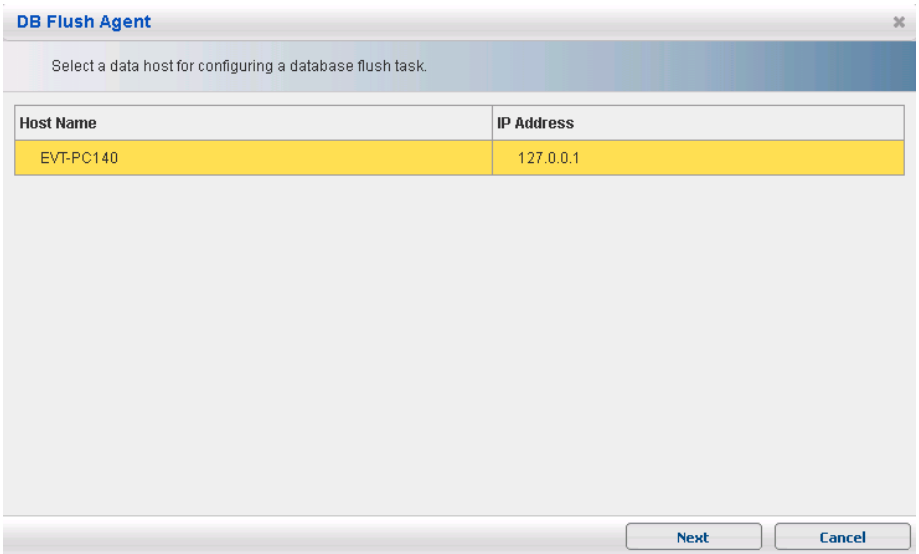
➔ Tasks

Step 1: Activating DB Flush Agent

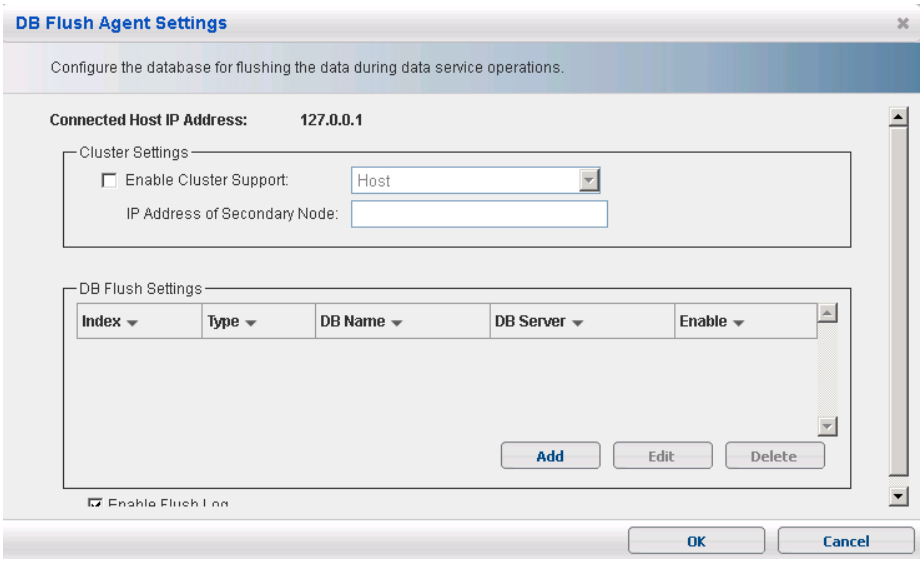
Click DB Flush Agent in the Tasks corner.



The list of current hosts will appear. Highlight the host you would like to configure and click Next.



The DB Flush Agent setting screen will appear.

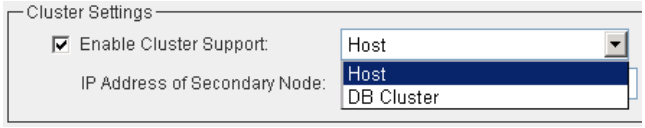


Step 2: Enabling Database Clustering

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

Database clustering refers to storing sequential rows of a database table on a disk. It will boost the database performance for server-centric database systems, since the server can perform database operations by direct access to disk.

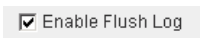
To enable database clustering, check the Enable Cluster Support checkbox and select DB Cluster. If you would like to add another node, select Host and enter the IP address.



Step 3: Enabling Flush Log

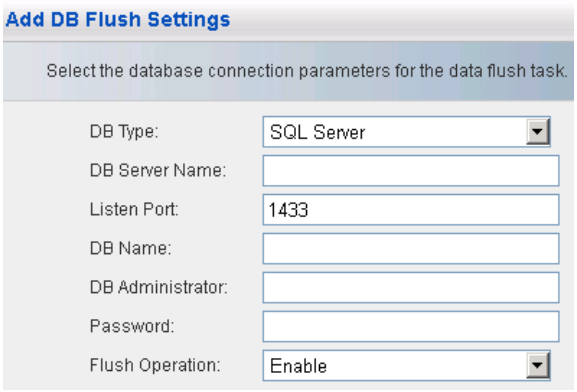
Enable the flush log if you want:

- Event logs for clustered nodes will be kept on this machine.
- Events will 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) which the database listener (a software that manages the 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 you select the security level of your database. By disabling "SA" access, no one will have access to a database system, except logging in as the Windows Administrator. Refer to this section for how to enable an “sa” login.
	DB Password	Specifies the database password.
	Enable DB Flush	Allows flushing database inside cache memory into a local file before taking snapshot images.

Viewing DB Flush Events (Windows)

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

From here you can check on related events.

You can examine event messages from *Windows Computer Management -> System Tools -> Event Viewer -> and 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.

Using DB Flush Agent in Oracle 10g

To ensure the integrity of snapshot copies, before taking a snapshot for a database, users should make sure that all data in the cache memory are flushed to the storage system. For databases a dedicated DB Flush Agent can take over the flushing task automatically. However for other databases, the flushing task has to be done manually.

Note

- The configuration example below assumes that the Oracle database, including its data, log and control files, are all stored in partitions or virtual volumes on the storage system.
- SQL*PLUS is an Oracle command-line utility program.

Step 1. Suspend or Shutdown the Database

Depending on whether you would like to perform snapshot protection online or offline, you can choose to suspend or shutdown the database.

To perform snapshot online, you should suspend the database with the following SQL*PLUS2 commands.

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

To perform snapshot offline, you should shut down the database with 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 for the partitions or virtual volumes storing the database.

> If files of the Oracle database are stored in more than partitions or virtual volumes, to ensure data consistency, please be sure to use the Group Snapshot feature to simultaneously take snapshots for them.

Step 3. Resume or Restart Database Service

If you just suspended the database, resume its service with the following SQL*PLUS commands.

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

If you just shutdown the database, restart its service with the following SQL*PLUS commands.

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

```
SQL>exit
```

Then restart the service on your host server.

When necessary, you can use the snapshots to rollback data or restore files.

Test Script

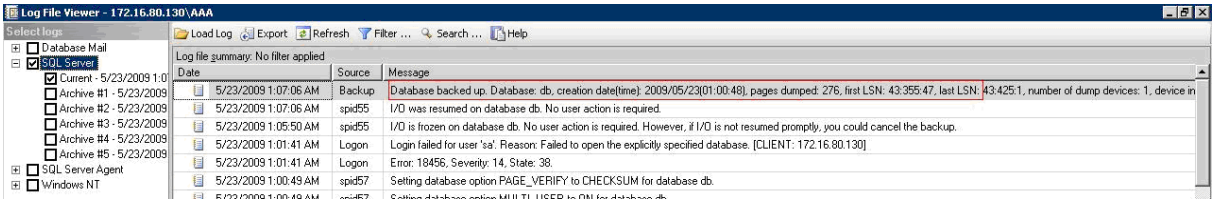
Below is a sample script that runs tests on growing databases in Oracle.

```
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 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.

The backup process can be examined through Oracle Log File Viewer.



Using DB Flush Agent in MS SQL

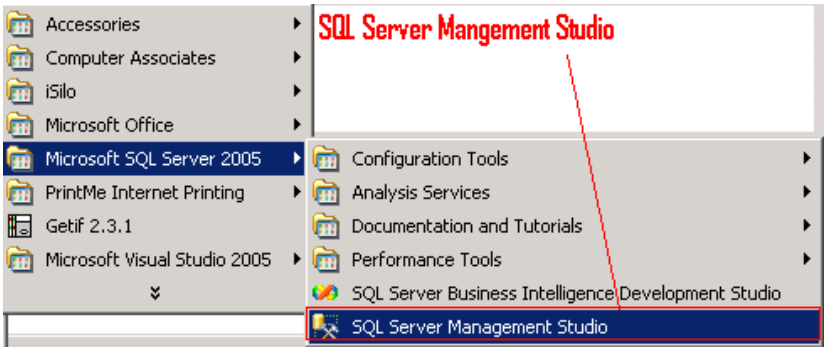
To ensure the integrity of snapshot copies, before taking a snapshot for a database, users should make sure that all data in the cache memory are flushed to the storage system.

Sample Database Configuration Using SQL Server 2005

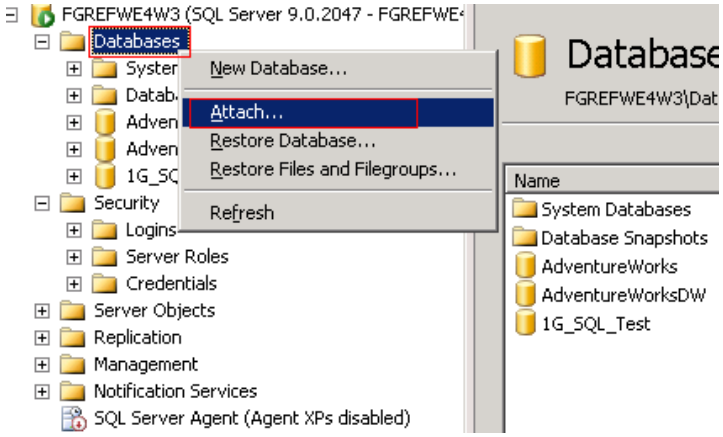
Create volumes. Leave enough unallocated storage space in volumes for performing snapshot backup. Depending on the size of data changes and how frequently they are changed, you normally require 2 to 3 times of a partition or virtual volume capacity for taking snapshot backup.

> When taking snapshots for database applications, such as Oracle, use “Group Snapshot” in the scheduler. Using Group Snapshots ensure consistency between database volumes and log volume. A Group snapshot is taken by selecting multiple source volumes.

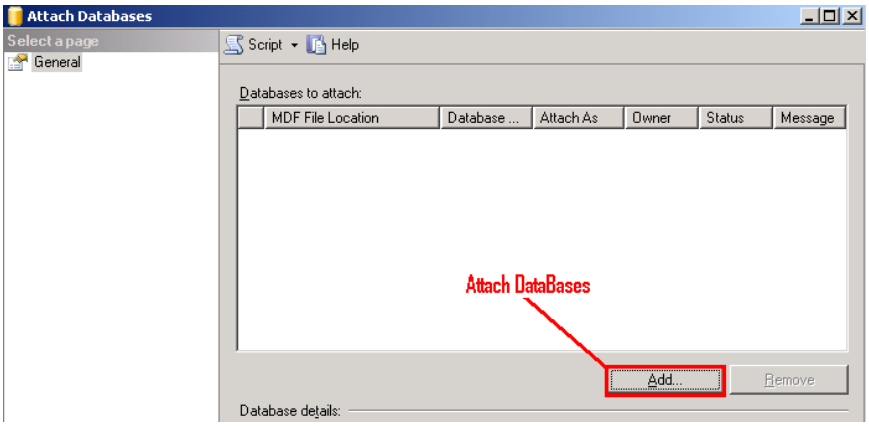
1. Map virtual volumes to hosts.
2. To test backup, copy data files to a virtual volume.
3. Start Microsoft SQL Server 2005.



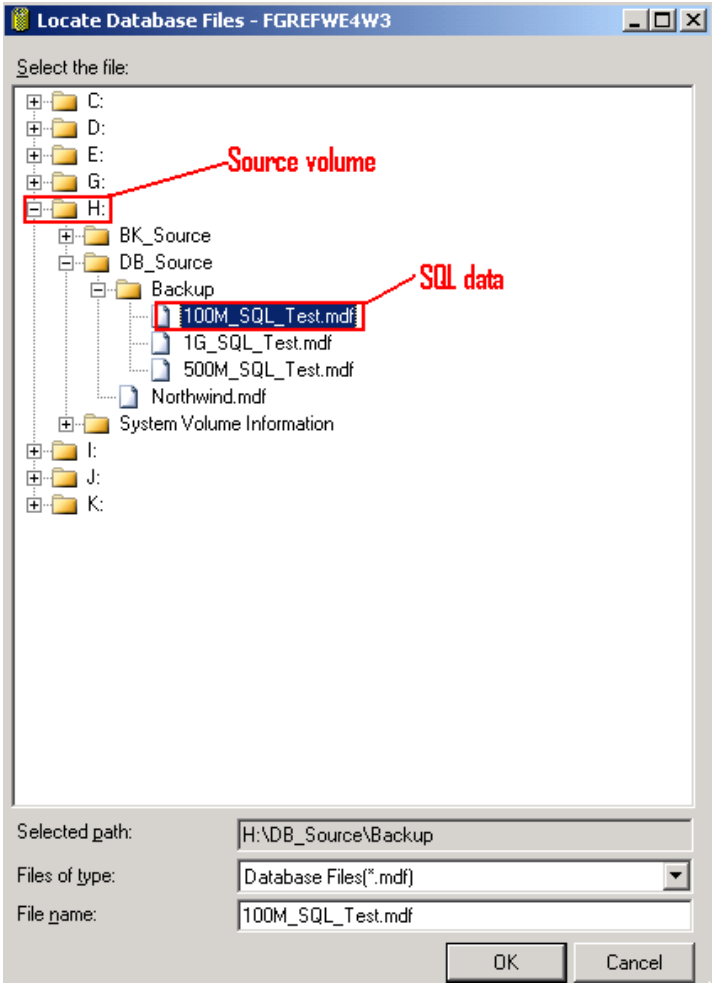
4. Use the Attach function to assign a virtual volume as database location.



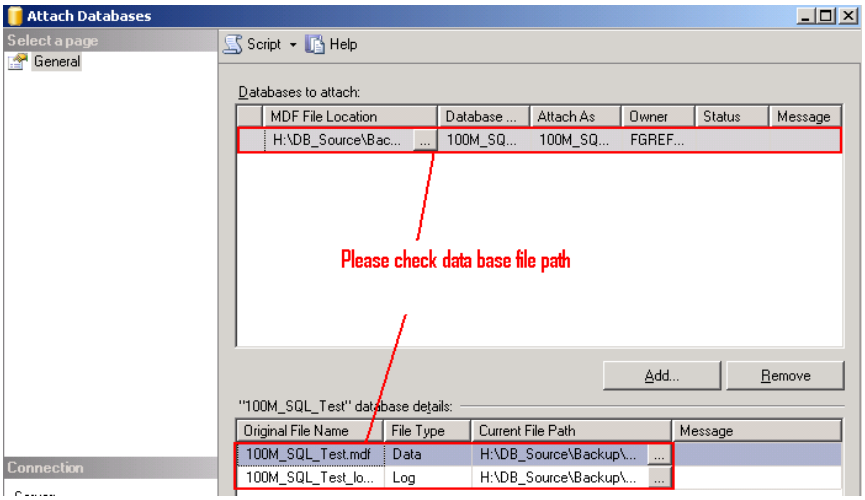
5. On the ensuing screen, click the Add button to attach databases.



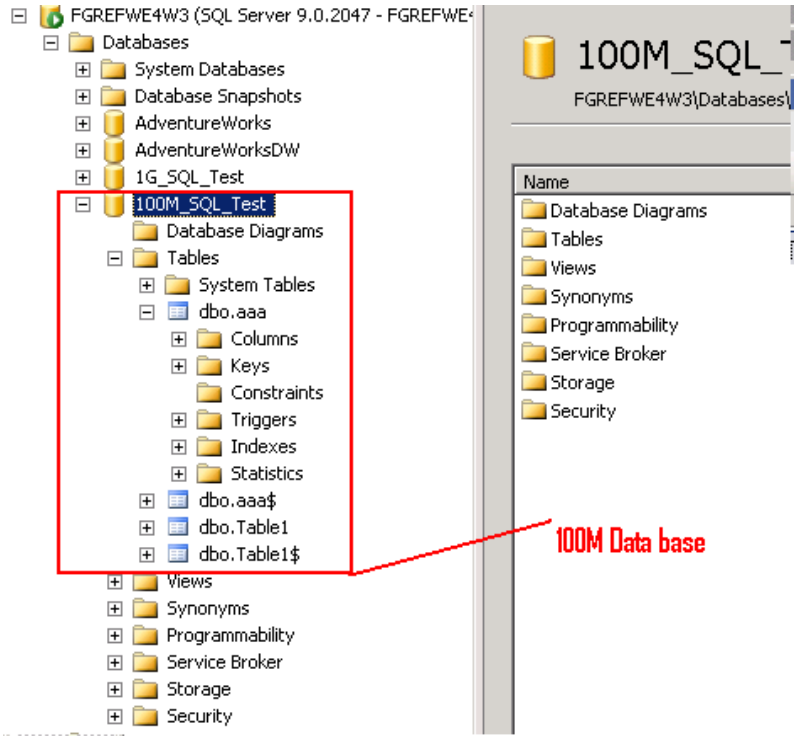
6. Select data base files you previously copied.



7. Verify the correct file paths.



8. Verify the attached data.



Test Script

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

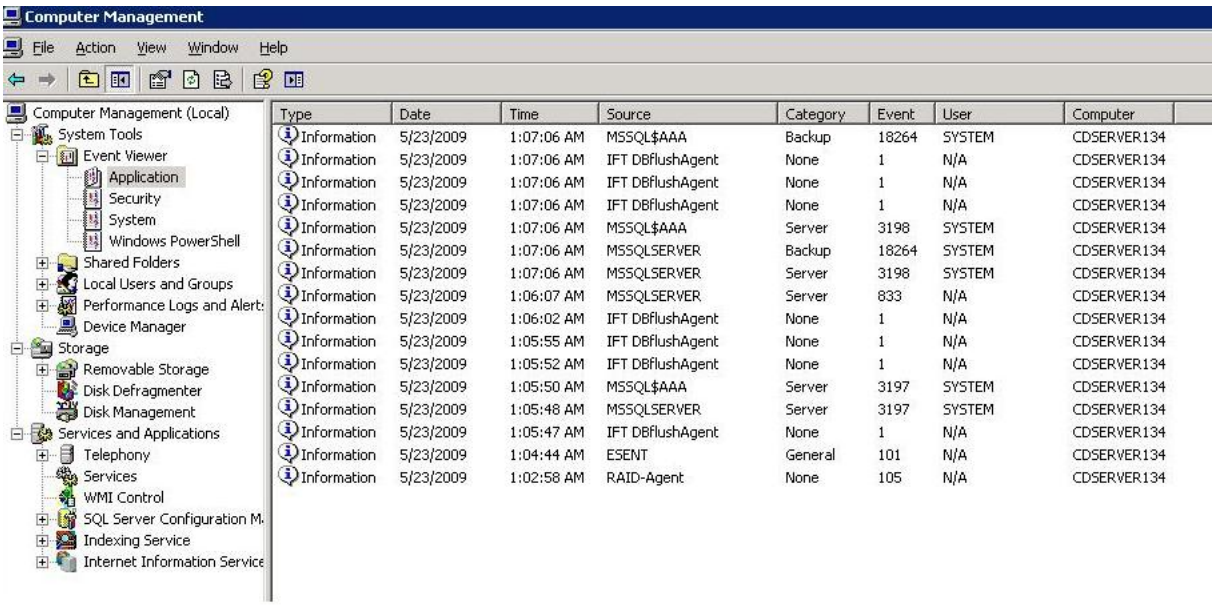
```
create table DBFlush.dbo.DBtest
(ID bigint,
  Rrd_Name char(20),
  Math float,
  English float,
  Chinease float,
  physical float
);

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) values
    (@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 Backup Process

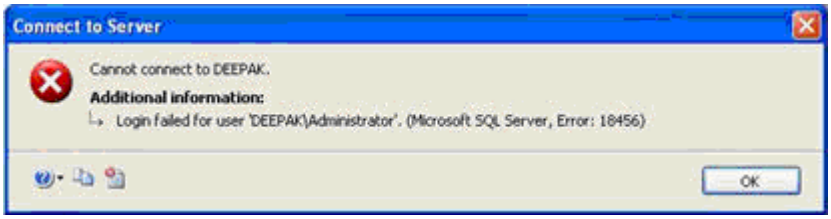
You may perform snapshot backup using schedules that start from an active database and verify correctness of backup by performing the rollback function.

Check *Windows Computer Management -> System Tools -> Event Viewer -> and Application.*

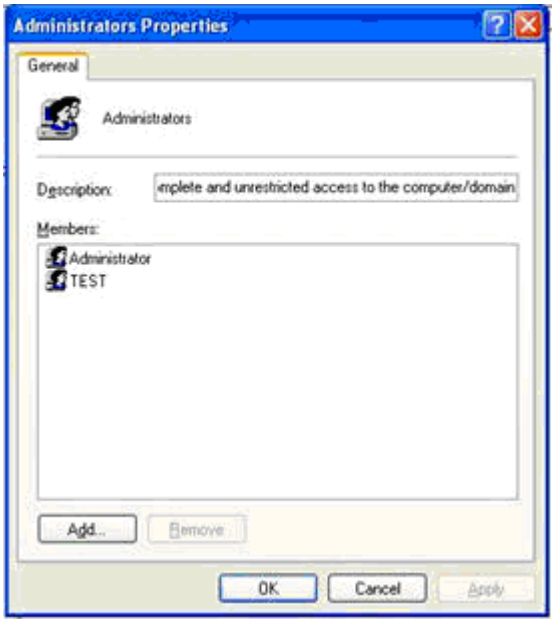


Enabling SA Login in MS SQL

If you disabled sa login or forgot sa login password, the following message will appear.



Refer to the below screenshot that shows the members of the Windows Administrators group.



Note

MSSQLSERVER is for default instance, if you are proceeding in a named instance then use MSSQL$Instancename instead of MSSQLSERVER.

Steps

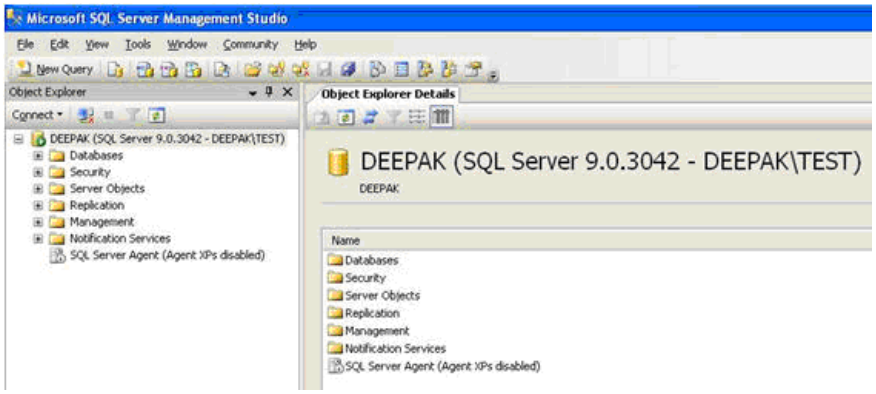
1. Login with the ID Test @OS Level.
2. Stop SQL Server 2005 using this command.

```
NET STOP MSSQLSERVER
```

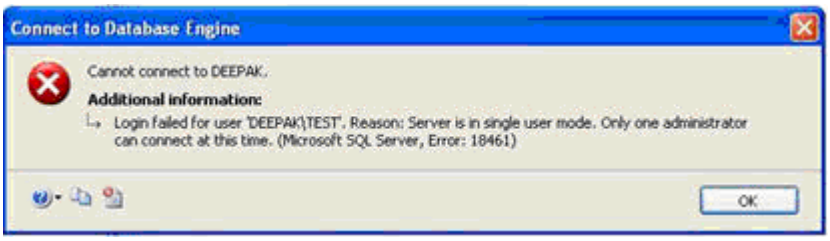
3. Start SQL Server 2005 in Single-User mode using this command.

```
NET START MSSQLSERVER /m
```

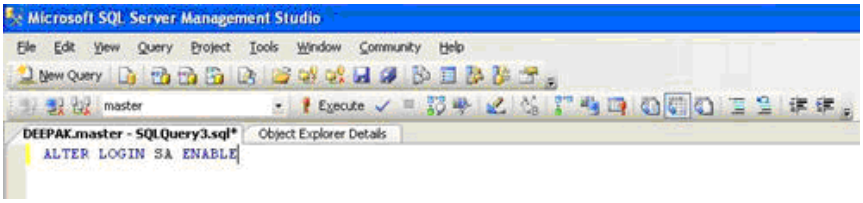
4. Log into SQL Server 2005 using the ID Test as shown in the below screenshot.



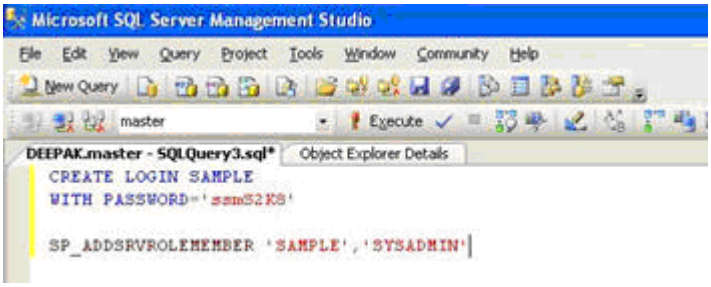
5. Since SQL Server is started in Single-User mode it will allow only one connection and hence you will get the following error if you click the “New Query“



6. Disconnect and close the Object Explorer and then connect using “New Query” you will be able to connect as shown below, and then enable SA login using the command - ALTER Login SA enable.



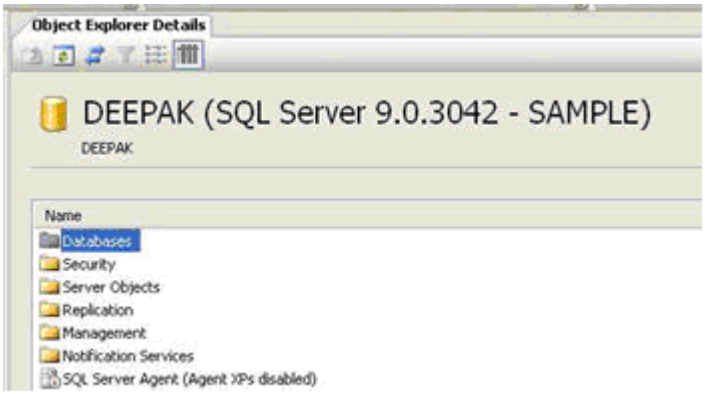
7. If you want to create a new SQL Level login with sysadmin privilege, you can perform as shown in the below screenshot.

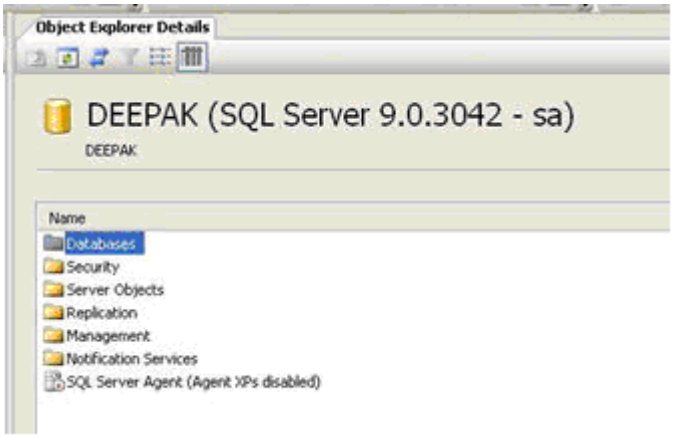


8. Now you need to Stop SQL Server and start it normally using this command.

NET START MSSQLSERVER

9. Connect using SA or the new login you created and proceed as shown below,

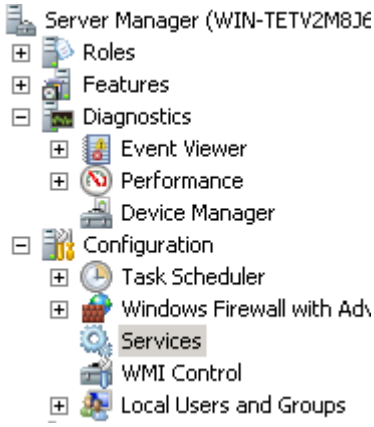

Object Explorer Details
DEEPAK (SQL Server 9.0.3042 - SAMPLE)
DEEPAK
Name
Databases
Security
Server Objects
Replication
Management
Notification Services
SQL Server Agent (Agent XPs disabled)


Object Explorer Details
DEEPAK (SQL Server 9.0.3042 - sa)
DEEPAK
Name
Databases
Security
Server Objects
Replication
Management
Notification Services
SQL Server Agent (Agent XPs disabled)

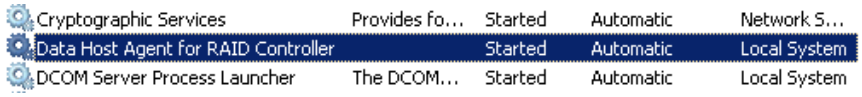
Configuring Out-of-Band Flush

Steps (Windows Environment)

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



2. Make sure Data Host Agent for RAID Controller has started.



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

4. Select the disk in which the volume you want to flush resides. If it is labeled as “Disk 1,” then “1” will become the disk ID for SANWatch flush agent configuration.

5. Refer to "
6. Configuring Out-of-Band Flush Using DB Flush Agent" for SANWatch configuration to complete data flush.

Steps (Linux and Solaris Environment)

1. In Linux, start data host agent.

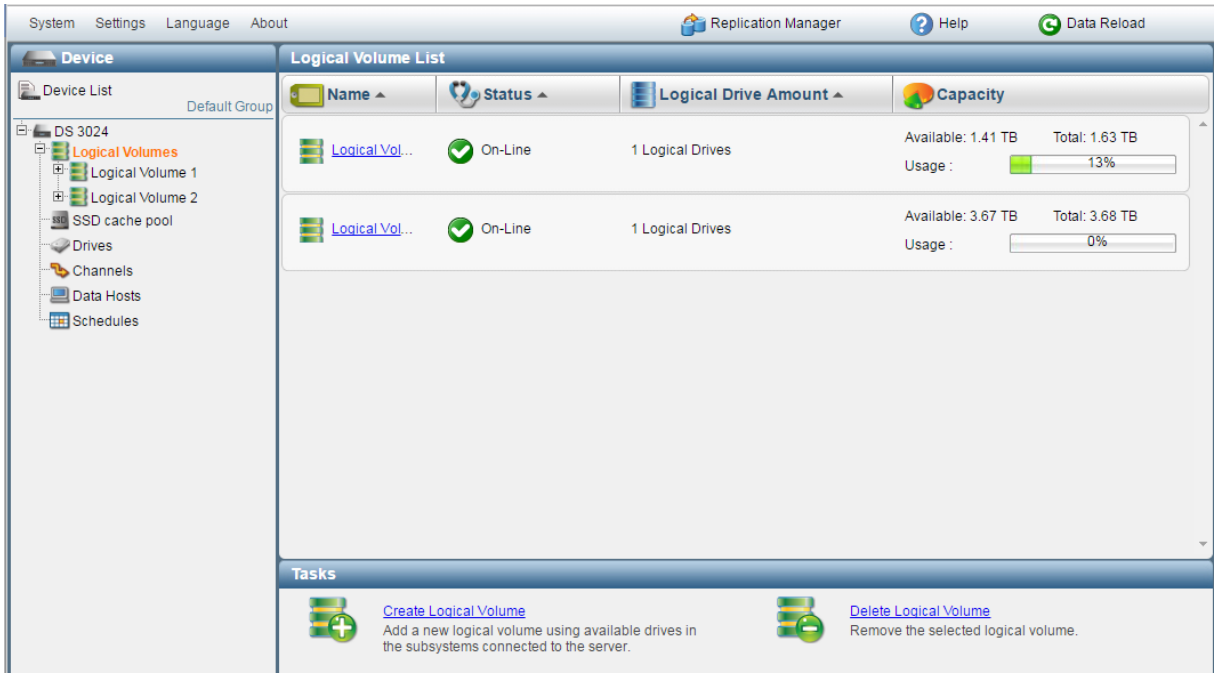
```
[root@tsdRHL55 /]# ps -ef | grep newAgent
root      2675     1  0 09:06 ?        00:00:03 /usr/local/jre1
 -cp newAgent.jar:jconn3.jar:log4j.jar newagent.Agent /usr/loca
root      3707  2927  0 09:36 pts/1    00:00:00 grep newAgent
[root@tsdRHL55 /]#
```

2. Select the device to be flushed. For example, you 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. Open SANWatch with your web browser, locate the partition or virtual volume where the database is located by going to:
   (EonStor DS subsystems) SANWatch Home > Device sidebar > Device List > device name > Logical Volumes > LV name > Partitions > partition name
   (ESVA subsystems) SANWatch Home > Pool sidebar > Pool List > pool name > Virtual Volumes > VV name
4. Click the Help icon at the top-right corner, and look for the "
5. Configuring Out-of-Band Flush Using DB Flush Agent" section for SANWatch configuration to complete data flush.

Working with the Logical Volumes or Pools View



This chapter describes the overall parameters of logical volumes (for EonStor DS subsystems) or pools (for ESVA subsystems) included in a device (for EonStor DS subsystems) or across multiple devices (for ESVA subsystems) and how to create a logical volume or pool.

RAID Levels Available

What is RAID?

The term RAID summarizes technologies that can distribute data to multiple drives, to achieve a high data transfer rate and fail-safe systems. RAID stands for "Redundant Array of Independent Disks". Redundant means that the failure of a single drive will not cause the failure or disruption of the entire system, or even lead to data loss.

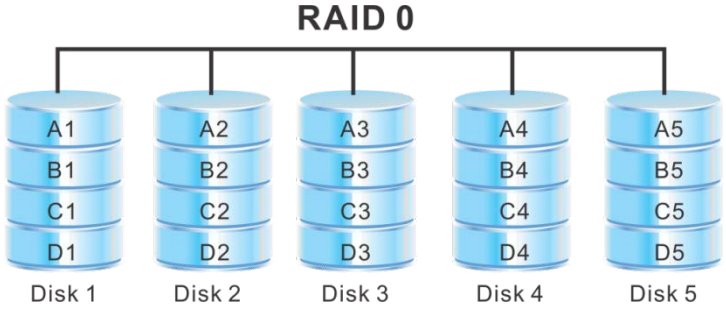
RAID is built on technologies such as mirroring (mirroring two or more drives), duplexing (mirroring with 2 controllers) and striping (Combination of multiple drives to a logical drive and block-wise data distribution to these drives).

There are different ways to distribute data to multiple disks, so that the highest possible data throughput and reliability is achieved. These are referred to as RAID level.

The following sections further describe the configurations of and applications for each RAID level, as well as how to calculate the capacity utilization.

RAID 0

RAID 0 is the fastest RAID mode. In a RAID 0 array, the available capacities of each disk are added together so that one logical volume mounts on the computer. If one physical disk in the array fails, the data of all disks becomes inaccessible because parts of the data have been written to all disks.

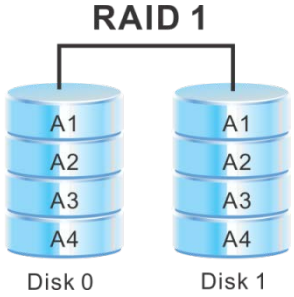


Applications

RAID 0 is ideal for users who need maximum speed and capacity. Video editors working with very large files may use RAID 0 when editing multiple streams of video for optimal playback performance. A RAID 0 array is more suited for actively working with files (editing video, for example) and should not be used as a single storage backup solution or on mission critical systems.

RAID 1

In a RAID 1 array, the data is written again to a second physical disk. This is the so-called mirror disk. If one of the two disks fails, the data is still fully available on the other disk. Use of the disk can continue normally. The disadvantage of RAID 1 is the TCO, because double the capacity than net required has to be calculated and invested.



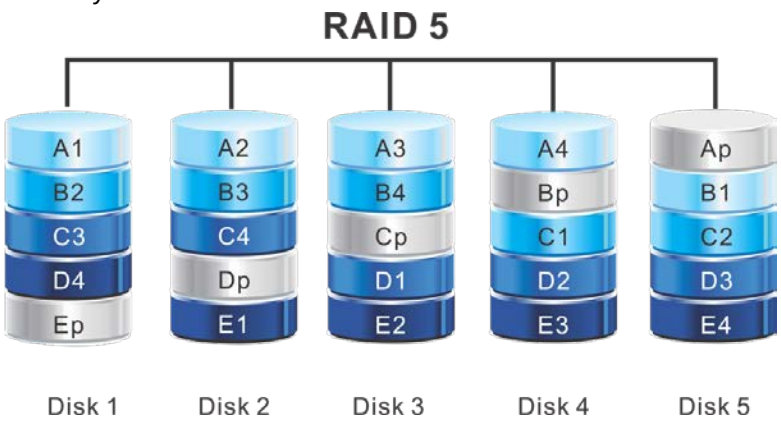
Applications

RAID 1 is ideal for applications requiring high fault tolerance at a low cost, without heavy emphasis on large amounts of storage capacity or top performance. Especially useful in situations where the perception is that having a duplicated set of data is more secure than using parity. For this reason, RAID 1 is popular used in data bases for accounting and other financial data. It is also commonly used for enterprise servers, and for individual users requiring fault tolerance with a minimum of hassle and cost.

RAID 5

In RAID 5, data is striped across all disks (minimum of three) and a parity block for each data block (#p in the diagram) is written on the same stripe. If one physical disk fails, the data from the failed disk can be rebuilt onto a

replacement disk. No data is lost in the case of a single disk failure, but if a second disk fails before data can be rebuilt to a replacement drive, all data in the array will be lost.

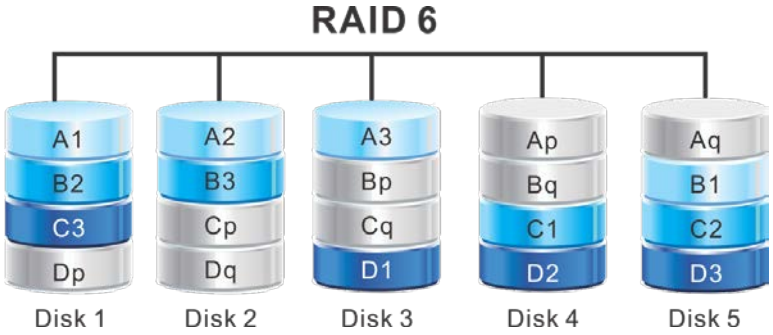


Applications

RAID 5 combines data safety with efficient use of disk space. Disk failure does not result in a service interruption because data is read from parity blocks. RAID 5 is useful for archiving and for people who need performance and constant access to their data, like video editors.

RAID 6

In RAID 6, data is striped across all disks (minimum of four) and a two parity blocks for each data block (p and q in the diagram at right) is written on the same stripe. If one physical disk fails, the data from the failed disk can be rebuilt onto a replacement disk. This Raid mode can support up to two disk failures with no data loss. RAID 6 provides for faster rebuilding of data from a failed disk.



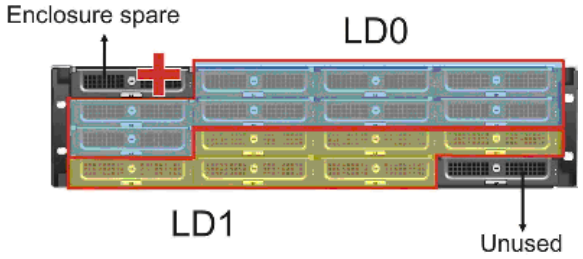
Applications

RAID 6 provides data reliability with the addition of efficient rebuilding in case of a failed drive. RAID 6 is therefore useful for people who need serious security with less of an emphasis on performance.

General Rules for Configuring Virtual Pools (ESVA subsystems only)

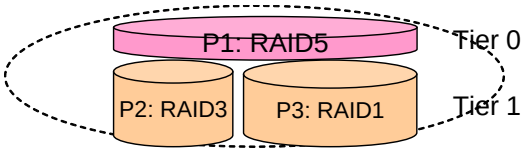
Enclosure Spare

If RAID1 is selected as the RAID level, the first HDD will automatically become an Enclosure Spare. Since RAID1 requires an even number of drives; the last drive in the enclosure will not be utilized. This is applicable to all enclosures within a RAID1 virtual pool.



RAID Levels

A virtual pool can contain multiple RAID levels by using storage tiering. For example, you may use RAID 3 for Tier 0 and RAID 5 for Tier 1. The following diagrams show an example of mixing multiple pool elements in one tier level.



If storage tiering is not enabled, we recommend that a virtual pool use only one RAID level to optimize performance.

Elements

- An element should not span across multiple enclosures.
- If a virtual pool spans across two or more RAIDs, the RAID controller of the first element becomes the master.

Tiering

The maximum level of tiering in a virtual pool is four. Here are the recommended rules for assigning pool elements to tier levels.

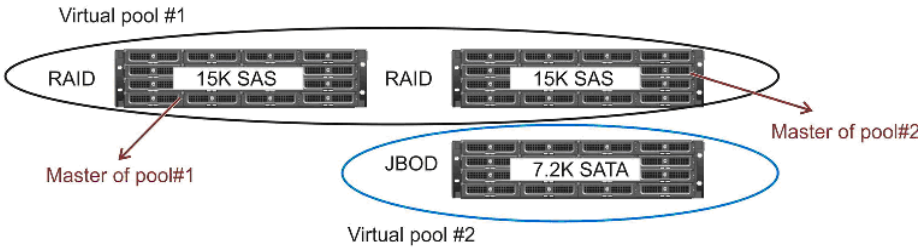
- Tier 0: SSD
- Tier 1: FC/SAS (RAID 1)
- Tier 2: FC/SAS (RAID 0/3/5/6)
- Tier 3: SATA

Max Number

- The maximum number of RAID units in a virtual pool is twelve (not including JBODs).
- The maximum number of virtual pools controlled by a master ESVA unit controller is seven.

Master/Member

A RAID enclosure can be a member of a pool and the master of another pool at the same time.

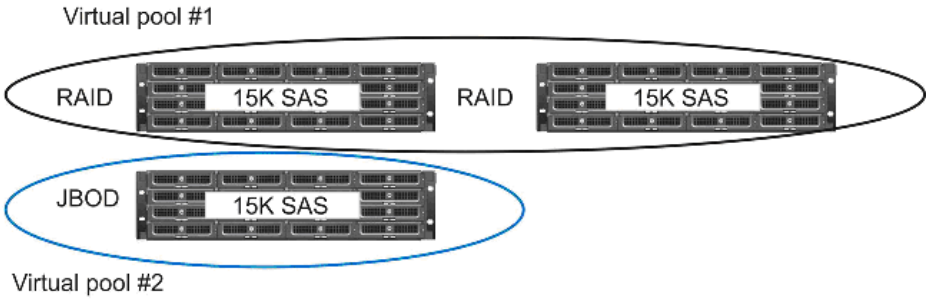


Disk Drives

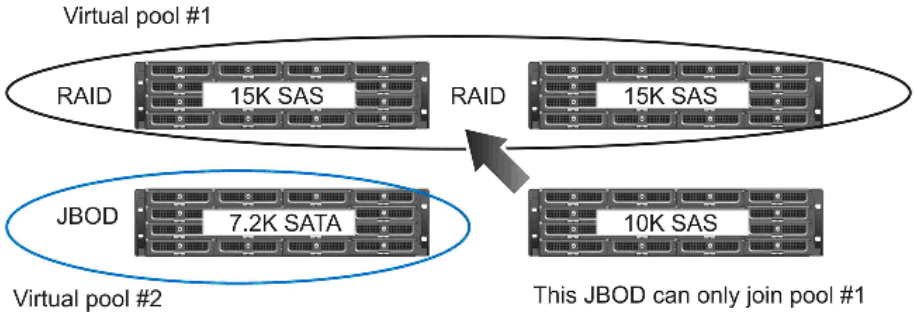
An enclosure should not contain more than one disk types, e.g., SAS and SATA. (As long as the drive interface is the same, drives may have different speeds (RPMs))

Forming a Pool by JBODs

A JBOD itself can create a virtual pool.



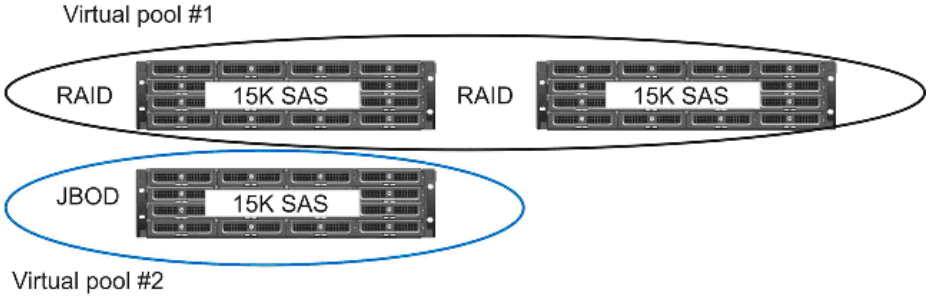
But if a JBOD is added later, it cannot create a new pool. It can only join the pool to which the dominant RAID belongs.



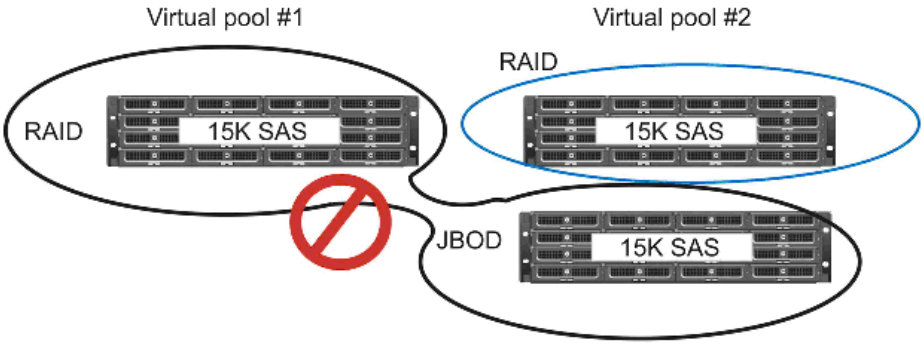
Mixing RAIDs and JBODs

If a virtual pool consists of RAID enclosures and JBODs, the first pool element should be from a RAID.

You may form one Pool across RAID Enclosures and another pool using a JBOD.

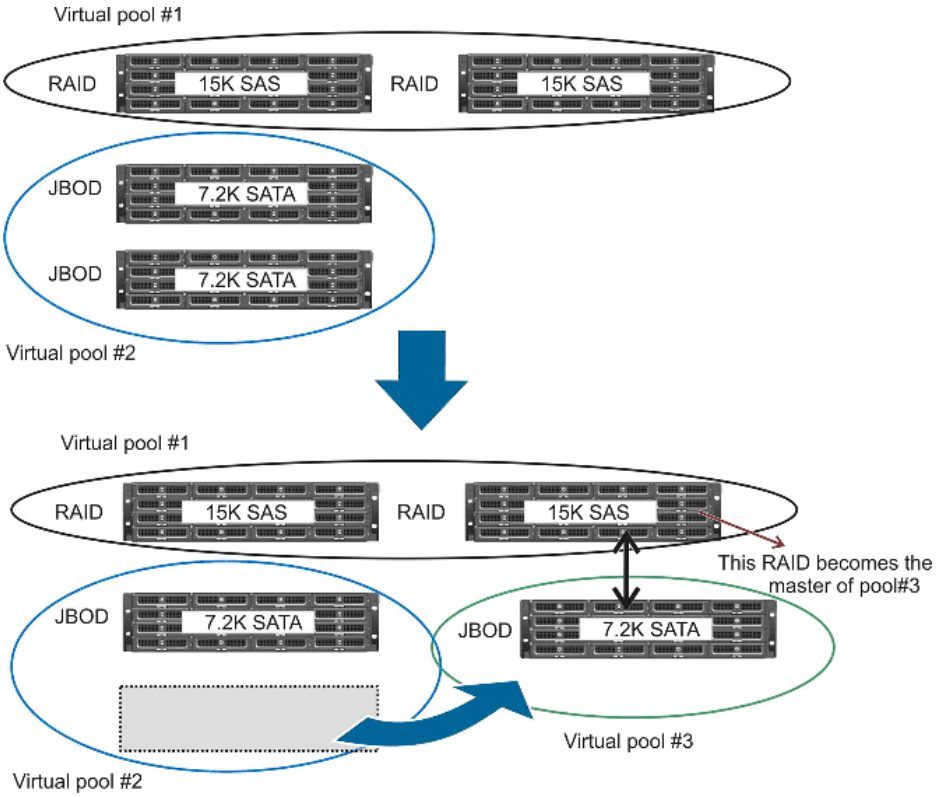


Combining a RAID and a JBOD which is attached to another RAID is not allowed.



Disbanding a JBOD from a Pool

You may balance the load by disbanding a JBOD from the pool and attach it to another RAID.



Disbanding an enclosure from a virtual pool requires re-distributing data, and therefore consumes system resources and time.

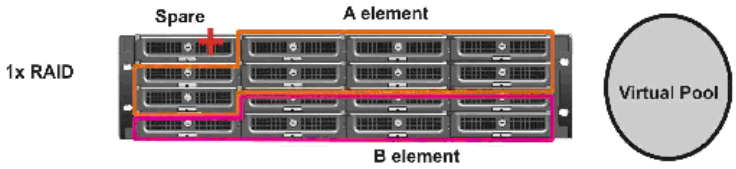
Examples of Combining RAID enclosures and JBODs (ESVA subsystems only)

By default, the SANWatch wizard automatically groups physical disk drives into logical elements which you may manually reconfigure later.

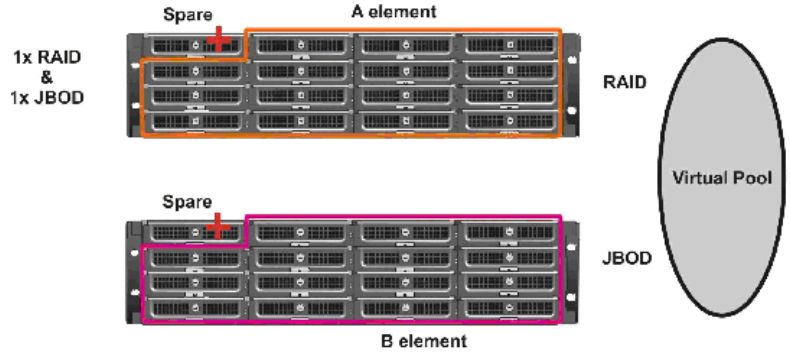
The defaults may use eight or seven drives in a pool element, which theoretically provides best throughput. They are automatically assigned to different RAID controllers to leverage all computing power within an enclosure.

The below samples show elements in RAID5 or RAID6 configuration. The (A) elements and (B) elements indicate ownership by dual-active RAID controllers.

One RAID Enclosure

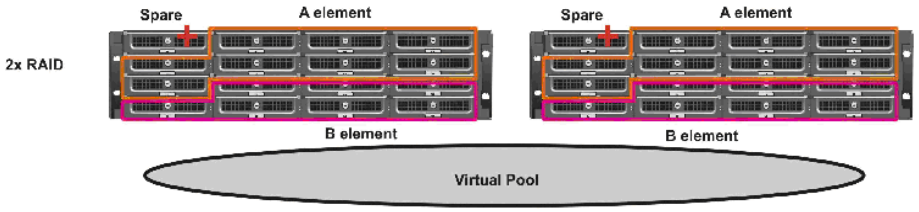


One RAID Enclosure + One JBOD

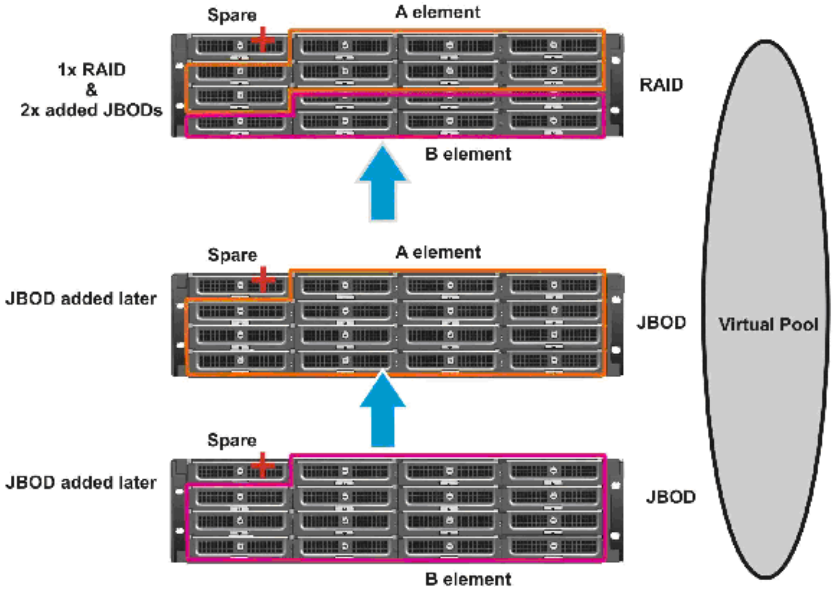


RAID & JBOD are cabled and started together as the initial setup units.

Two RAID Enclosures



Adding JBODs to RAID Enclosures



JBODs were not included in the initial setup and were added into the pool later.

Viewing the List of Logical Volumes or Pools

All volume information can be accessed from the Device sidebar in the user interface.

Go To

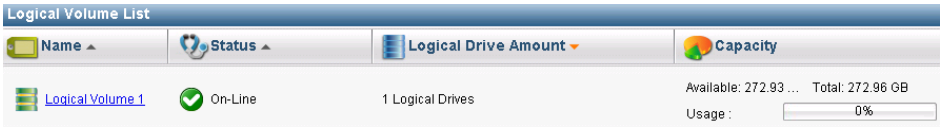
EonStor DS subsystems: SANWatch Home > Device sidebar > Device List > device name > Logical Volumes
ESVA subsystems: SANWatch Home > Pool sidebar > Pool List

or

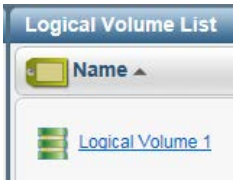
Steps

The list of logical volumes or pools and their logical drives or pool elements will appear.

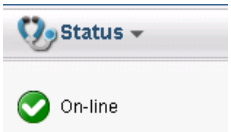
The logical volume or pool status summary will appear to the right, in the main screen.



Clicking the name of each item to see detailed configuration.



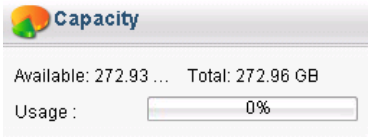
The Status column shows whether this volume is in a healthy (no error) status.



The Logical Drive Amount (EonStor DS subsystems only) column shows the number of its member logical drives .

The System Performance (ESVA subsystems only) column shows the summary of system performance.

The capacity column shows the total and available (free) capacity allocated for this volume/pool.



Creating a Virtual Pool and Virtual Volumes (ESVA subsystems only)

You can create both a virtual pool and its virtual volumes at the same time. You can also manually (and separately) create a virtual volume.

The maximum size of a pool is 2PB.

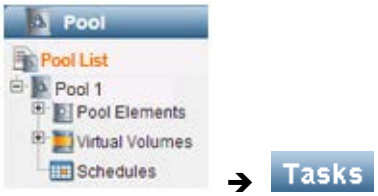
Process

Creating a virtual pool or virtual volumes takes four steps:

1. Selecting pool elements
2. Configuring tiering (if tiering has been enabled)
3. Creating virtual volumes
4. Confirming the result

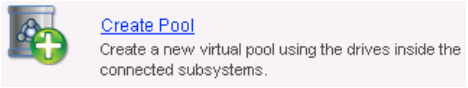
Go To

SANWatch Home > Pool sidebar > Pool List > Tasks corner

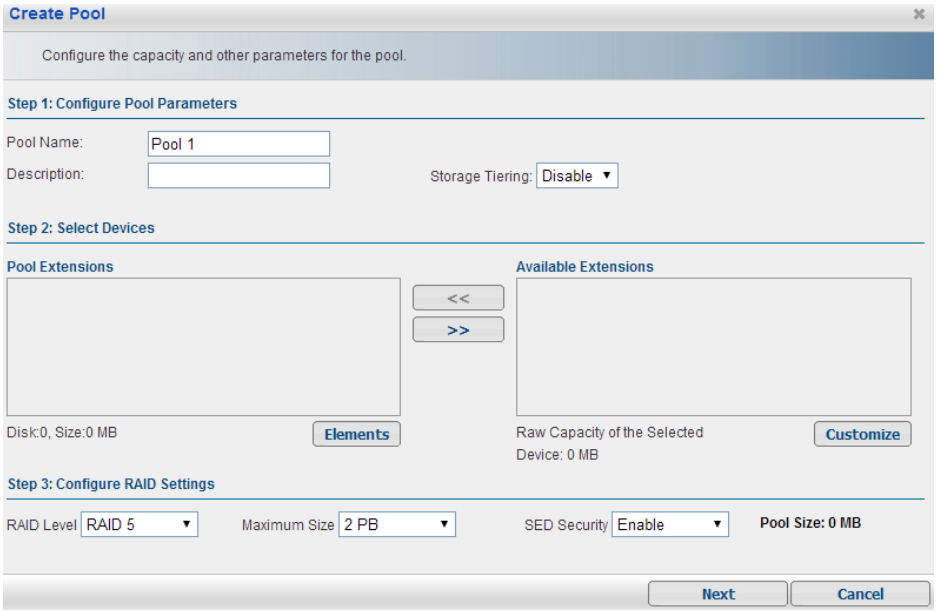


Step1: Selecting Pool Elements

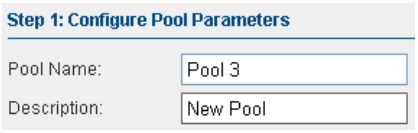
Click Create Pool in the Tasks corner.



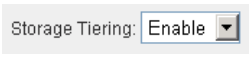
The Pool Configuration screen will appear.



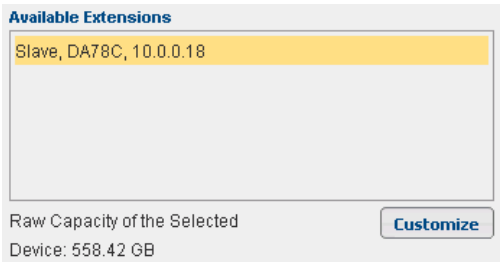
Enter the pool name and description.



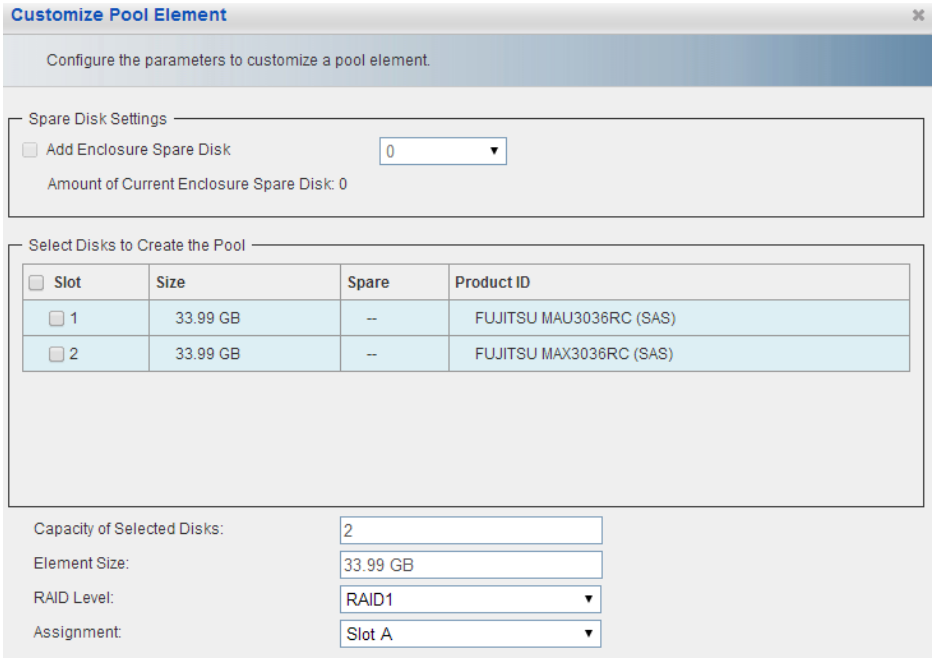
Enable storage tiering (this option will show up when you have the tiering license).



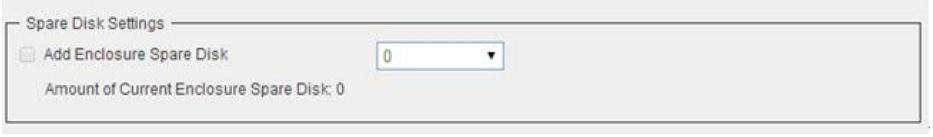
Highlight an ESVA/JBOD in the Available Extensions List and click Customize.



The Customize Pool Element window will appear.

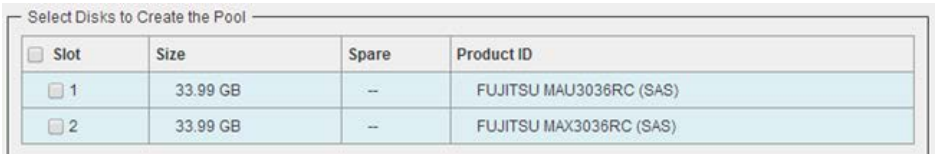


You may add a spare disk to the new pool.



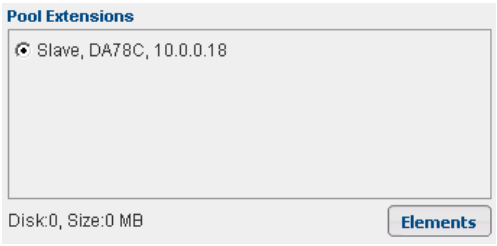
This option will be active only when there are spare drives available. You can create and add a spare drive later.

Select disk drives for the first pool element. If you wish to create multiple pool elements (especially for storage tiering), make sure you do not select all available disk drives.



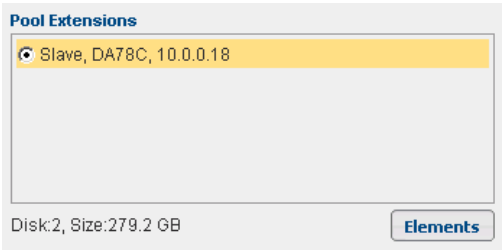
Select the RAID level and the assigned controller. The number and size of disk drives will be updated in the Selected Amount and Element Size corner.

Click Apply. The ESVA system with the new pool element will appear in the Pool Extent List. (The first pool element will become the master element.)

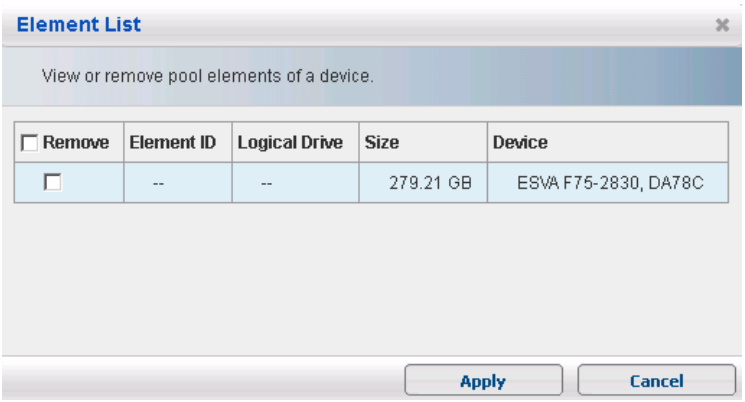


To add more pool elements, repeat above steps.

When all elements have been added, highlight the extension and click Elements to confirm the list of pool elements included in this pool.



You may remove unwanted elements (except for the master element) here.



Select the RAID level and the maximum possible pool size in the Settings corner.

The RAID Level option will be disabled if you have already chosen the RAID level in the Customize dialogue.

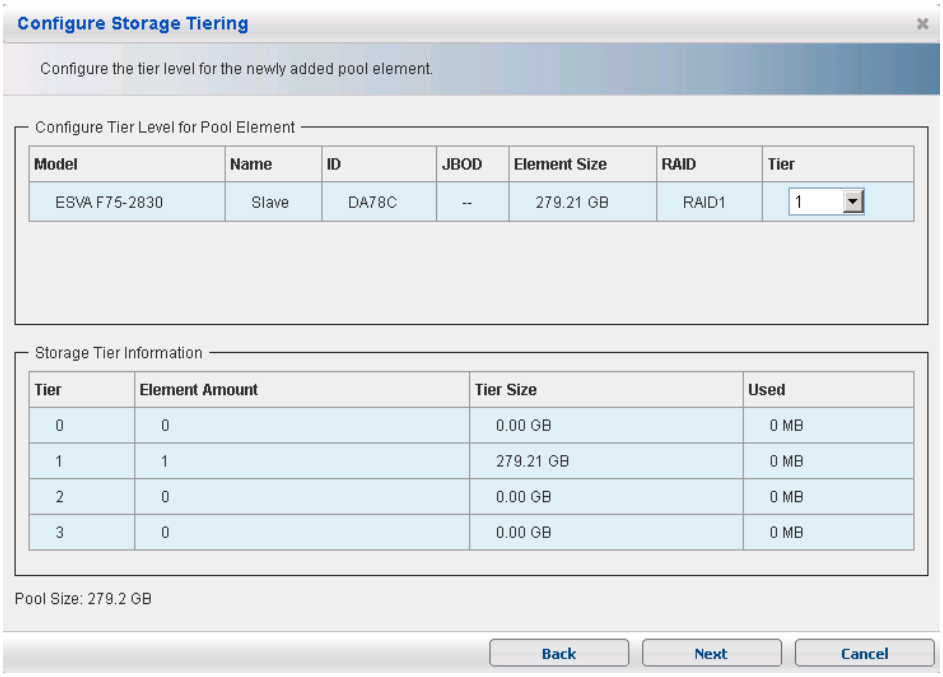
Click Next.

Step 1 Parameters	**Spare Disk**	Creates enclosure spare disk(s) for the virtual pool. You need to have available disks inside the enclosure.
	RAID Level	Specifies the RAID level of the virtual pool: RAID 0, 1, 5, and 6. RAID 5 and RAID 6 offer protection against one and two drive failure, respectively. If you want to take extra caution against data loss (for example, a media error occurs while rebuilding a failed drive), it is recommended to take RAID 6.
	Pool Name	Specifies the virtual pool's name.
	Description	Specifies a short description of the virtual pool.
	Storage Tiering	When enabled, you can configure tiering. See procedures below for details.
	Maximum Size	Specifies the maximum pool size from 64TB up to 2PB. The size also determines the data block section size which ESVA uses to distribute data across pool elements. The larger the Maximum Size, the larger the section size becomes which may not be optimal for random and small I/Os. Use the default size for optimal performance. In order to perform remote mirror, the maximum size of the pool pairs need to match each other.
	SED Security	Protects pool data with SED security.

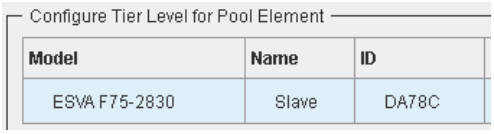
Step 2: Configuring Tiering

If storage tiering has not been enabled, you will see the next step, Configuring Virtual Volumes.

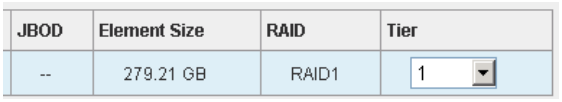
The Storage Tiering Setting appears.



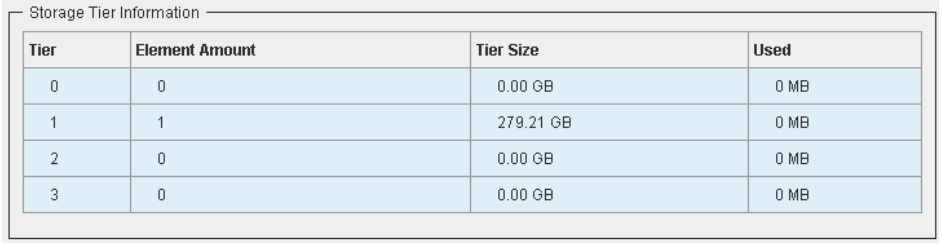
Confirm the list of pool element included in the pool.



Select the tier level of each pool element.



Confirm the summary of pool elements and their tiers in the Storage Tier Information corner.



Click Next.

Step 2 Parameters

Tier Level

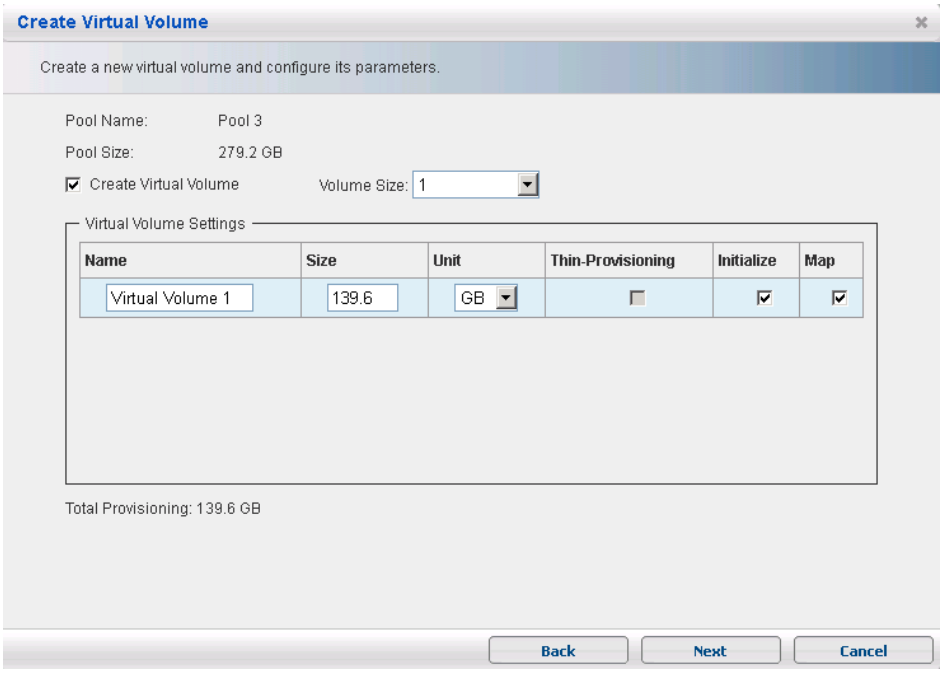
Specifies the tier level of this pool. Four levels exist, with tier 0 having the highest priority. Here are the recommended tier levels for pool element types.

- Tier 0: SSD
- Tier 1: FC/SAS (RAID 1)
- Tier 2: FC/SAS (RAID 0/3/5/6)
- Tier 3: SATA

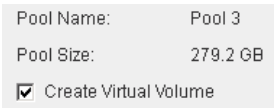
You may select the same or different tier levels for pool elements. Data in the higher tier will be accessed primarily.

Step 3: Configuring Virtual Volume

In the Create Virtual Volume window, check “Create Virtual Volume.”

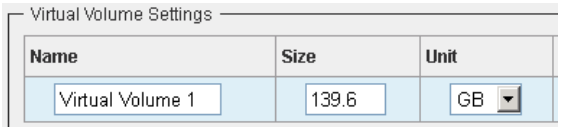


You may also uncheck this box and create virtual volumes later.



Select the number of volumes.

The volumes will then appear in the Virtual Volume Setting corner.



(When multiple storage tiers are available) Select in which tier each volume will reside (Default: All). You may modify this setting later.

Check if you want to enable thin-provisioning/initializing or mapping.

Click Next.

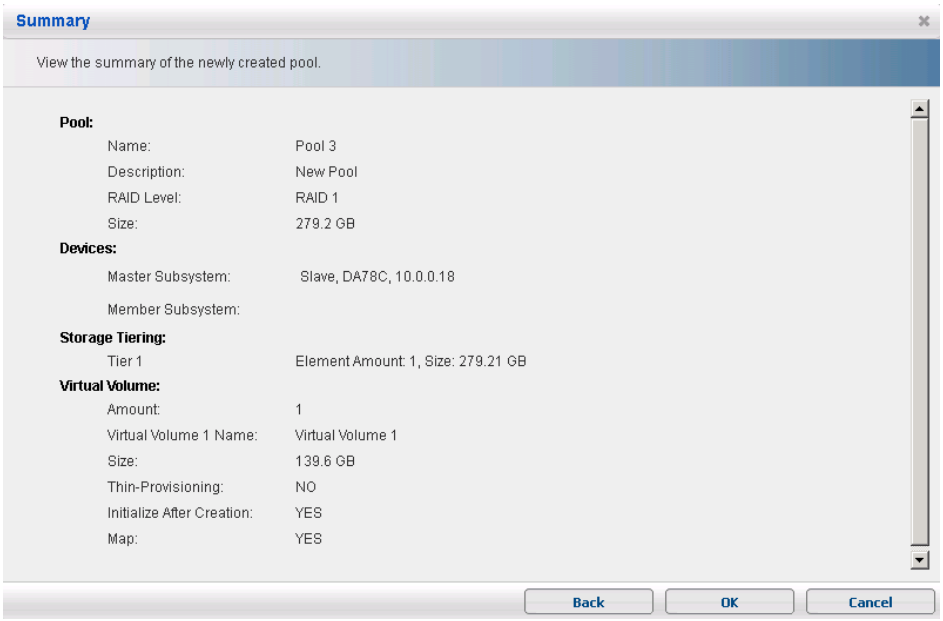
Step 3 Parameters

Volume Size

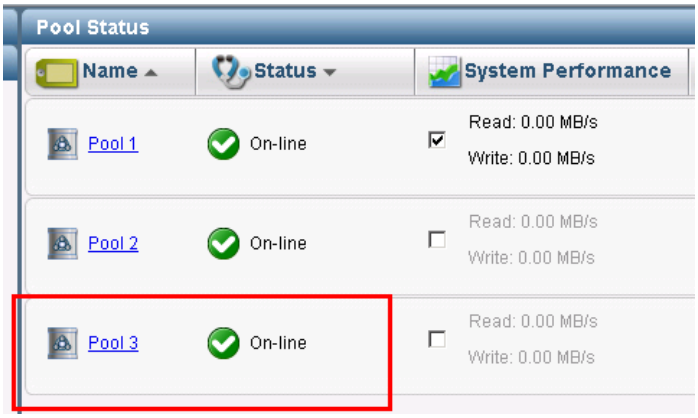
To change the volume size, double-click the number. If Thin Provision is activated, you may enter a volume size

	larger than the pool size.
Unit	Select the unit of volume size: MB, GB, or TB.
Tier Resided	Defines in which storage tier the virtual volume exists. When you select “All,” the virtual volume capacity will be divided equally among the tiers. You may change the ratio manually later.
Thin-Provisioning	➢ When checked, a thin-provisioned volume with no minimum reserved space (0%) will be created. ➢ When unchecked, a full-provisioned volume with initialization will be created. Thin provisioning allows you to allocate a large amount of virtual capacity for a logical volume regardless of the physical capacity actually available. Actual space is used only when data writes occur. By automatically allocating system capacity to applications as needed, thin provisioning technology can significantly increase storage utilization. When the volume is initialized, the virtual volume’s LBA addresses will be allocated consequentially for large and/or sequential I/Os. This is ideal for audio/video application such as media post-editing and video on-demand.
Map	Automatically maps the volume to all host channels, which allows all SAN servers to access the volume. Uncheck this parameter if you intend to create host LUN mapping later.

Step 4: Confirming the New Pool	A summary will appear. Verify configuration details and click OK. If you have chosen not to create virtual volumes or LUN mapping, you may do so later.



The pool will appear in the list.



Creating a Logical Volume (EonStor DS subsystems only)

Note

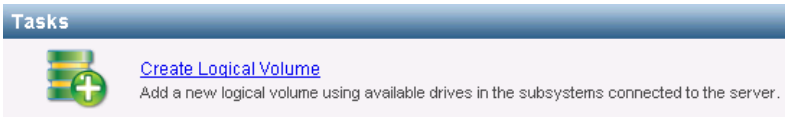
The maximum size of a logical volume is 256TB (before firmware version 3.88) and 512TB (after firmware version 3.88). Make sure that the size of the partition is in line (you cannot make the size of the partition larger than the size of the logical volume). For the latest status, checking with technical support is recommended.

Go To

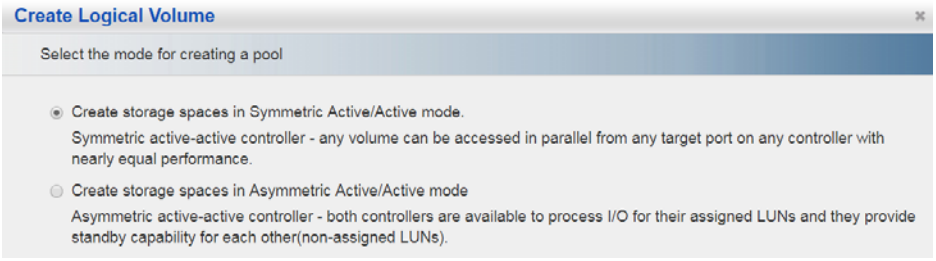
SANWatch Home > Device sidebar > Device List > device name > Logical Volumes > Tasks corner

Steps

Click **Create Logical Volume**, and the configuration window will appear.



1. Select **Create storage spaces in Symmetric Active/Active mode** or **Asymmetric Active/Active mode** under “Select the mode for creating a pool” (Note that this feature will only display/available with two controllers attached on the storage device).

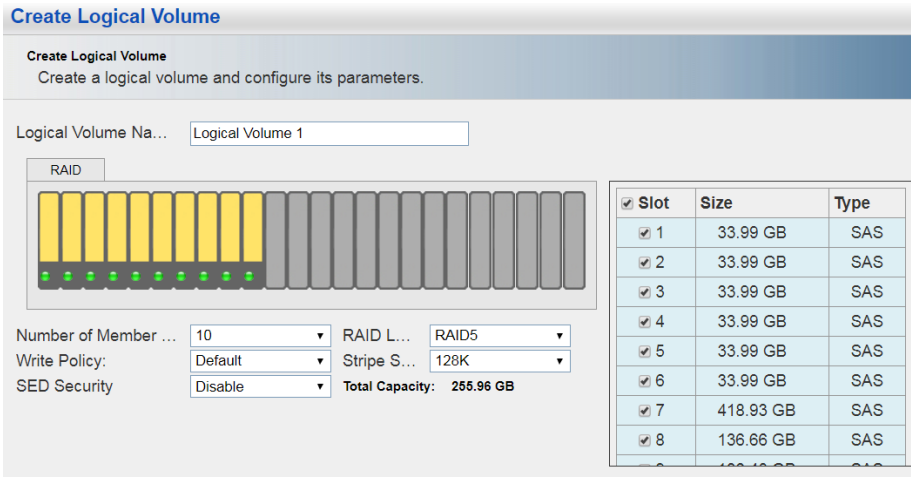


Asymmetric Active/Active mode: read the description carefully, then assign a controller for this pool from the assignment scroll down list (Controller in Slot A / Controller in Slot B).

Symmetric Active/Active mode: read the description carefully. You do not need to assign a controller under this mode. Symmetric Active/Active configuration allows host I/O to come from both controllers. The logical drives of the pool will be evenly distributed to the two controllers. You can create a symmetric pool with multiple logical drives, which will be automatically assigned to controller A or B at creation/boot-up.

2. Select the member drives that will be added to the LV or pool and configure

the parameters.



Parameters

Logical Volume Name

Enter a unique name for the volume.

Storage Tiering / Tier Index

Disable or Enable.

For more information about storage tiering, click a logical volume or pool in the Device sidebar, click the Help icon at the top-right corner, and look for "Storage Tiering."

Number of Member Drives

Select the number of drives you wish to have in the logical volume.

RAID Level

Select the RAID level to protect your data.

> The available RAID level depends on the number of disk drives.

RAID level	Minimum number of drives	Minimum number of drives for Symmetric A/A mode
RAID 0	1	2
RAID 1	2	4
RAID 3	3 (4 if you want to add a spare drive)	6 (7 if you want to add a spare drive)

RAID 5	3 (4 if you want to add a spare drive)	6(7 if you want to add a spare drive)
RAID 6	4 (5 if you want to add a spare drive)	8(9 if you want to add a spare drive)

Write Policy

Specifies the write policy: Default (write policy is determined by the controller's caching mode and event trigger mechanism), Write-Back (writing is considered complete when cache data is overwritten), or Write-Through (writing is considered complete only after the disk data is overwritten). Selecting Write-Through increases security but decreases performance.

Assignment

Specifies to which controller slot the new logical volume will be assigned. This section will be concealed when you configure the logical volume under Symmetric Active/Active mode.

This option is available for R-models only.

Stripe Size

Specifies the array stripe size. Do not change this value unless you are sure the modified value leads to increased performance.

SED Security

Specifies whether you want to protect the member drives with SED (Self Encrypting Drives) security.

Before enabling this option, the following requirements should be met:

- A SED authentication key is created (at SANWatch Home > Device sidebar > Device List > device name > Tasks corner > System Settings > Drive-Side tab > SED Authentication Key).
- All member drives support SED.

Click **Next**, view the summary information, and then click OK to complete the setup.

Creating a Logical Volume with RAID Level 30/50/60

Note

Logical volumes with RAID level 30/50/60 are created by expansion with logical drives.

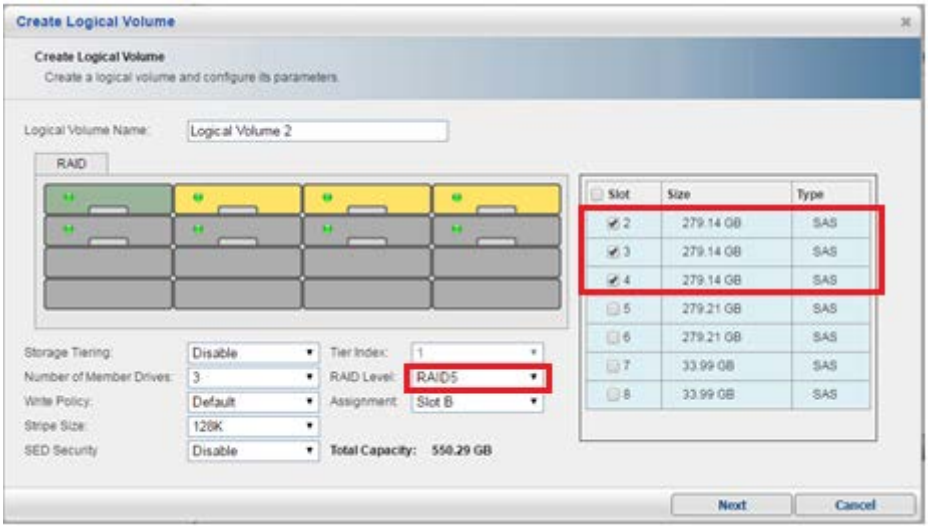
The following explains how to create a RAID 50 logical volume as an example.

Step 1

Create a RAID 5 logical volume.

Refer to Creating a Logical Volume.

Select three drives and set the RAID level as RAID5.

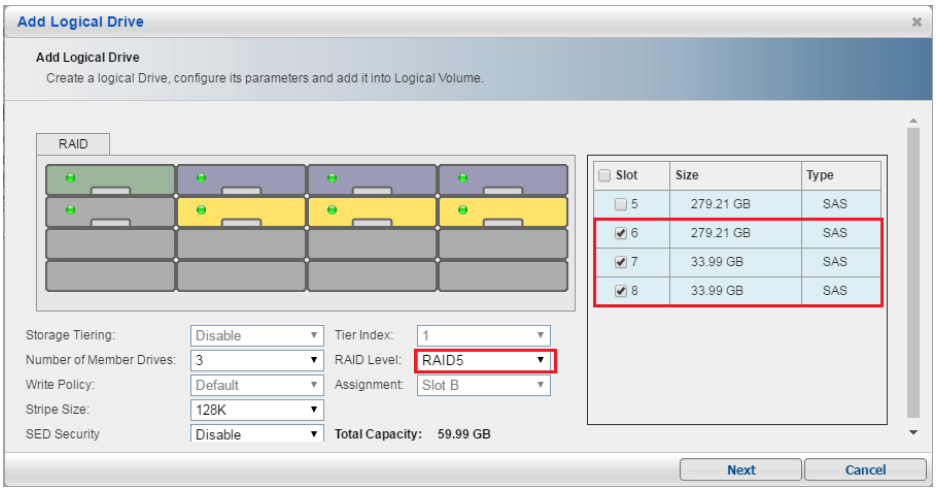


Step 2

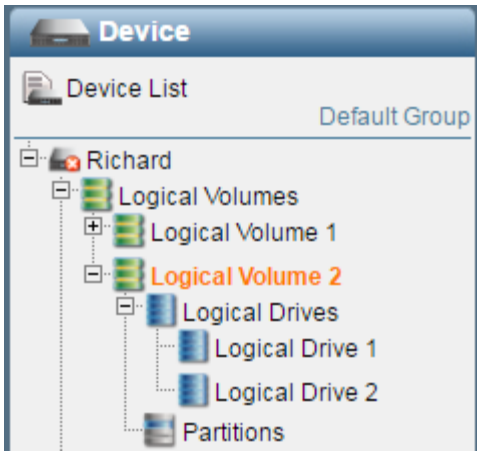
Add a logical drive to the logical volume that was created.

Refer to Adding a Logical Drive to an Existing Logical Volume.

Select three drives and set the RAID level as RAID5.



Then, you can see the logical drive is added to the logical volume.



This step can be repeated to create a RAID 50 logical volume with three logical drives (RAID 5 + RAID 5 + RAID 5).

You can use this method to create a RAID 30/50/60 logical volume. You can also create a logical volume with logical drives of mixed RAID levels, e.g. RAID 5 + RAID 6.

To create a RAID 10 logical volume, if you select 4 or more member drives and set the RAID level to RAID1, it will automatically be a RAID 10 configuration.

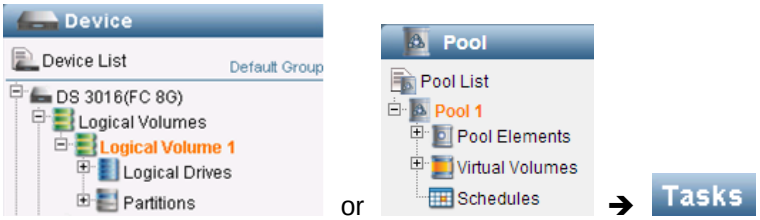
Deleting a Logical Volume or Pool

Deleting a logical volume or pool might lead to loss of data.

Delete the host LUN mapping (if applicable) before you delete the logical volume (for EonStor DS subsystems) or pool (for ESVA subsystems).

Go To

EonStor DS subsystems: SANWatch Home > Device sidebar > Device List > device name > Logical Volumes > LV name > Tasks corner
ESVA subsystems: SANWatch Home > Pool sidebar > Pool List > pool name > Tasks corner

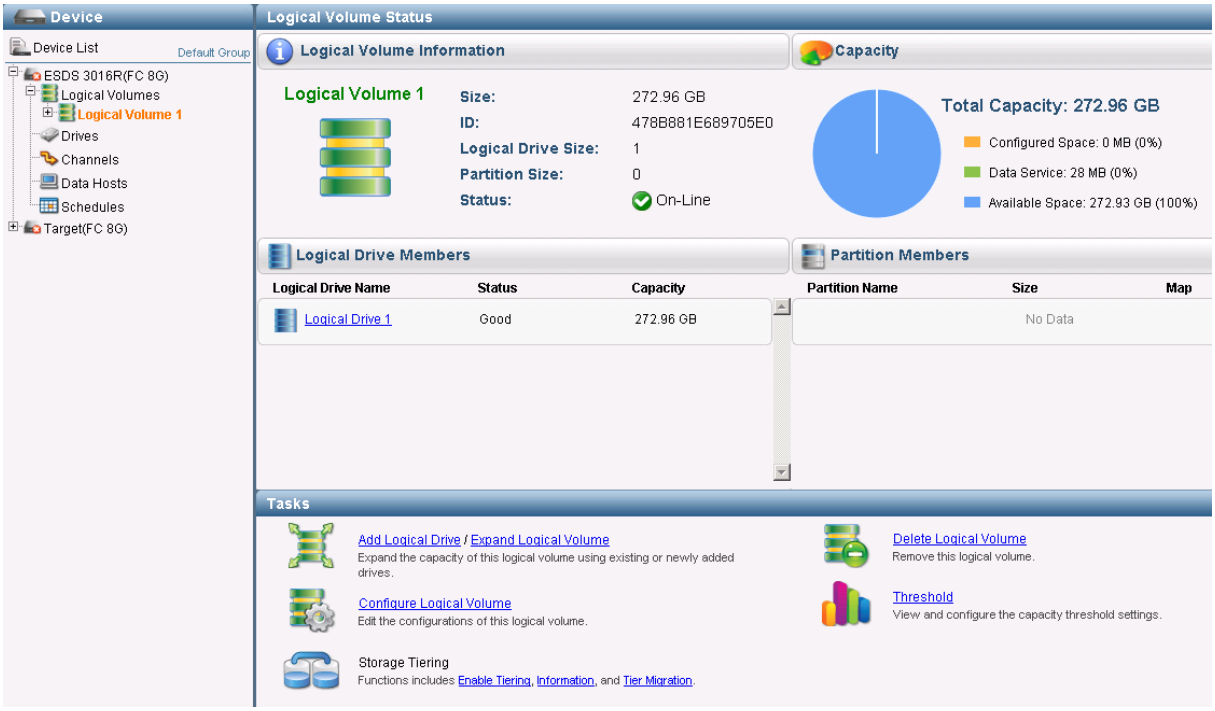


Steps

Click Delete Logical Volume (for EonStor DS subsystems) or Delete Pool (for ESVA subsystems) in the Tasks corner.

Select the virtual volume or pool and click Remove.

Working with Logical Volumes or Pools



This chapter describes the parameters of a logical volume (for EonStor DS subsystems) or a pool (for ESVA subsystems).

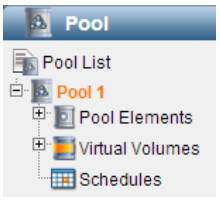
Viewing the Logical Volume or Pool Status

The status of each volume or pool is summarized in the Information page, where you can quickly grasp the configuration, performance, storage capacity.

Go To

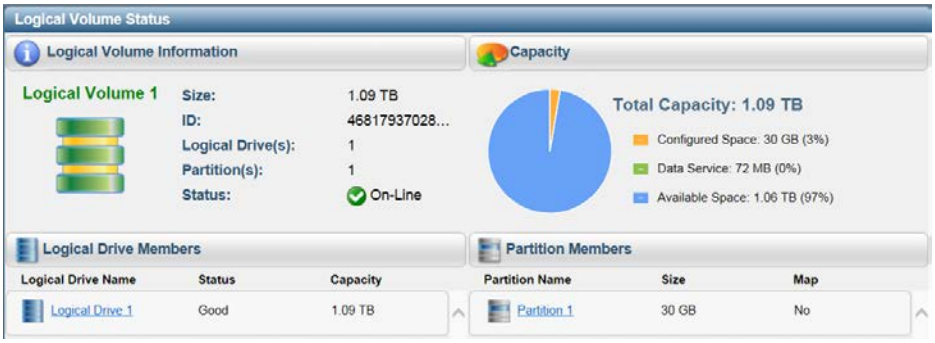
EonStor DS subsystems: SANWatch Home > Device sidebar > Device List > device name > Logical Volumes > LV name
ESVA subsystems: SANWatch Home > Pool sidebar > Pool List > pool name

or



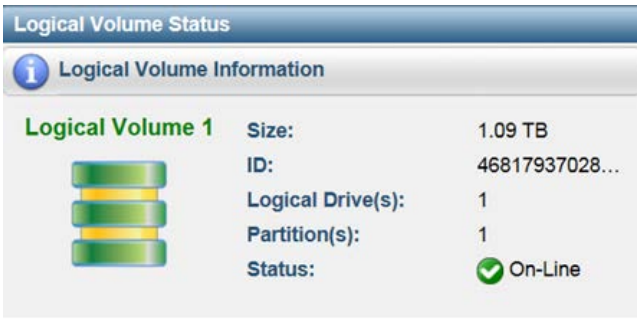
Viewing Volume/Pool Information

The volume/pool status will be summarized in the Status corner.



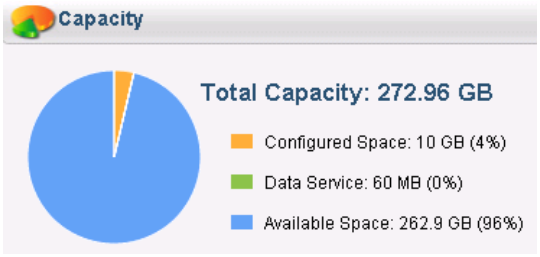
Volume or Pool Configurations

The basic configurations and overall system status will be listed in the Volume Information or Pool Information corner. You can see its size (capacity), ID, status, logical drive information (for EonStor DS subsystems only), or source subsystem(s) (ESVA subsystems only).



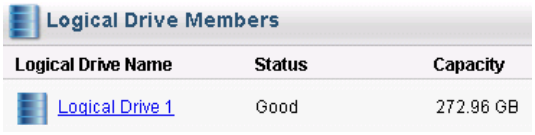
Volume or Pool Capacity

See the amount and ratio of used (configured) capacity and the remaining (available) capacity. You may also view the ratio of capacity used for data service (snapshot, remote replications).



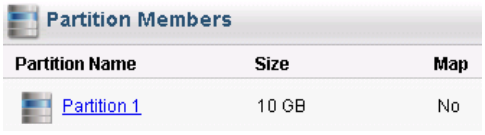
Logical Drive Information (EonStor DS subsystems only)

View the list of member logical drives and their detailed configurations (available when clicking the link).



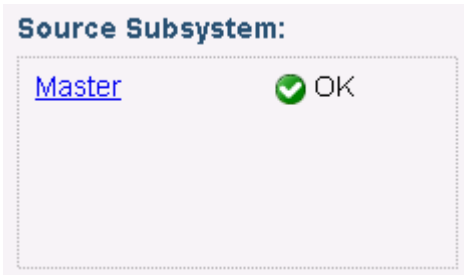
Partition Information (EonStor DS subsystems only)

View the list of LUN mappings and their detailed configurations (available when clicking the link).



Source Subsystem (ESVA subsystems only)

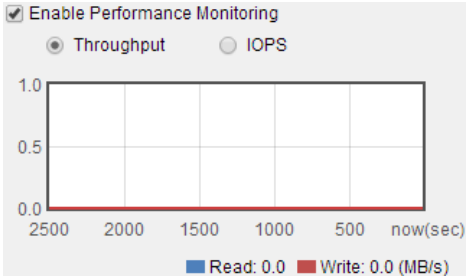
You can see the subsystem in which the main pool element (collection of disk drives) is located. The subsystem status is also displayed to the right, and clicking the link takes you to the device configuration page for the subsystem.



Performance Monitor (ESVA subsystems only)

Check the Enable Performance Monitoring checkbox to see the read/write throughput or IOPS.

The Performance Monitor is disabled by default to save system resources.

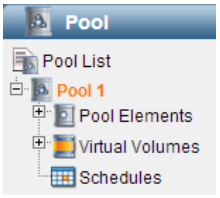

Enable Performance Monitoring
Throughput
IOPS
1.0
0.5
0.0
2500
2000
1500
1000
500
now(sec)
Read: 0.0
Write: 0.0 (MB/s)

Configuring Properties of a Logical Volume or Pool

Go To

EonStor DS subsystems: SANWatch Home > Device sidebar > Device List > device name > Logical Volumes > LV name > Tasks corner
ESVA subsystems: SANWatch Home > Pool sidebar > Pool List > pool name > Tasks corner

or

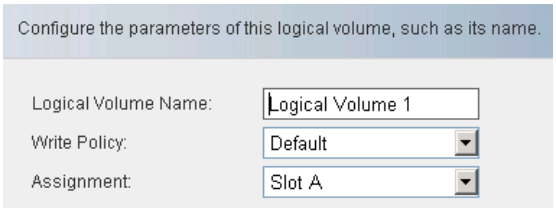


➔ Tasks

Steps

Click Configure Logical Volume or Configure Pool in the Tasks corner.

Change the parameters in the Logical Volume Parameters corner. Click OK to confirm changes.



Parameters

Name

Specifies the logical volume name.

> This option is available only for EonStor DS subsystems.

Write Policy

- When “Write-back” (also Default) is enabled, the write requests from the host will be held in cache memory and distributed to disk drives later. Write-back caching can dramatically improve write performance by caching the unfinished writes in memory and letting them be committed to drives in a more efficient manner. In the event of power failure, a battery backup module can hold cached data for days (usually 72 hours).
- When “Write-back” is disabled (i.e., the Write-through is adopted,) host writes will be directly distributed to individual disk drives. The Write-through mode is safer if your controller is not configured in a redundant pair and there is no battery backup or UPS device to protect cached data.

Assignment

Specifies the controller to which this logical drive or pool element belongs.

> Do not change this setting unless you are ready to switch the controller.

Controller Reassignment Procedure

To re-assign a logical volume or pool to a different controller, we strongly recommend you to follow these steps:

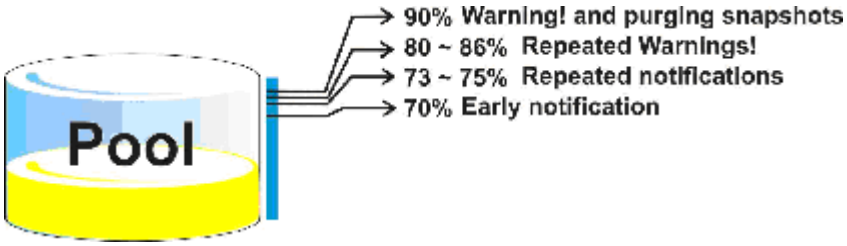
1. List the logical volume (or pool) and all its logical drives (or pool elements).
2. Shutdown the controller.
3. Change the assignment through the command terminal (typically connected through the RS-232 interface) using the **`Set Logical Drive/Volume`** command. For details, refer to the CLI (Command Language Interface) manual.

> Note that a logical volume or pool and all its logical drives or pool elements must be assigned to the same controller. You may not be able to change the assignment partially even when following the procedure mentioned above.

Setting Pool Capacity Thresholds (ESVA subsystems only)

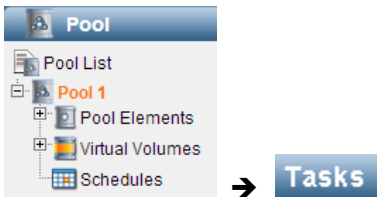
You need to reorganize a virtual pool before applications use up its capacity; otherwise, data loss might occur. You can set up a capacity threshold and receive notification when pool usage surpasses the threshold.

You can configure multiple threshold levels which may trigger notification or purge.



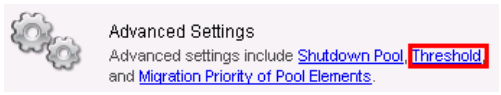
Go To

SANWatch Home > Pool sidebar > Pool List > pool name > Tasks corner



Adding or Editing a Threshold

Click Threshold in the Tasks corner.



The threshold configuration window will appear.

To add a new threshold, click Add. To edit an existing threshold, highlight it and click Modify.

Set the threshold percentage and policy and click OK.

Threshold Policy

Post Notification Events Sends out an event notification.

Post Warning Events	Sends out a warning notification.
Post Critical Events	Sends out a critical notification.
Post Critical Events + Run Purge Operation	Sends out a critical notification and purges (deletes) snapshot images until the used space becomes lower than the threshold.
Post Critical Events + Disassociate Snapshot Images	Sends out a critical notification and marks snapshot images invalid until the amount of healthy (non-invalid) data becomes lower than the threshold.

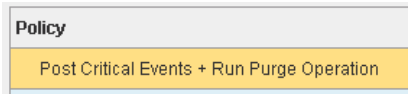
Deleting a Threshold

Highlight a threshold and click Delete.

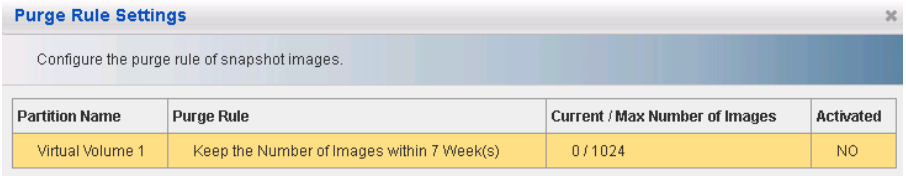
Configuring Purge Policy

This operation is applicable to thresholds with the “Post Critical Events + Run Purge Operation” setting.

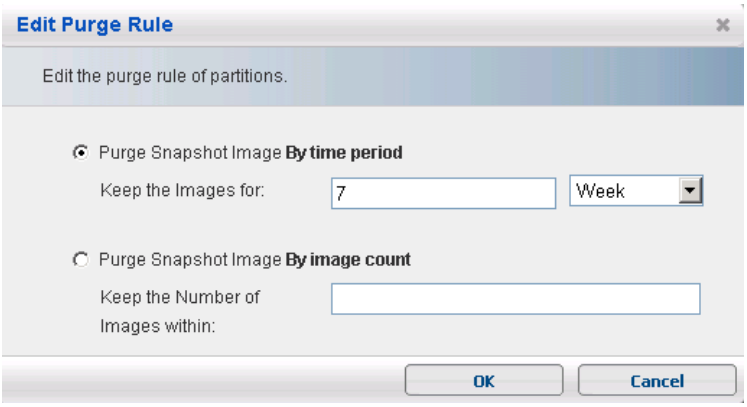
Highlight a threshold and click Purge Rule.



The list of snapshot image purge policy for the threshold’s virtual volume appears. Highlight the policy to edit and click Edit.



Configure the purge policy. First, select if you want to purge snapshot images when an expiration date arrives (by time period) or if the number of images reaches a threshold (by image count).



Purge Parameters	**Purge Threshold**	Specifies the threshold policy: duration (By Time) or the number of snapshot images (By SI Count).
	Value	Specifies the values.

Configuring Notification Thresholds (EonStor DS subsystems only)

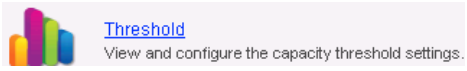
This feature is available only for EonStor DS series.

Go To

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

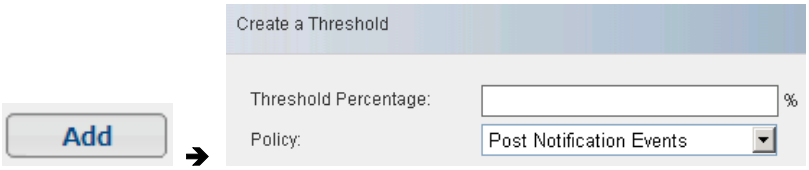
Steps

Click Threshold in the Tasks corner.



The Threshold window will appear.

Click Add, enter the threshold value (% of the logical volume) and the notification type as follows. You may also modify or delete existing thresholds.



Parameters

Post Notification Event	Creates a notification event when the amount of logical volume content reaches the threshold.
Post Warning Event	Creates a warning event when the amount of logical volume content reaches the threshold.
Post Critical Event	Creates a critical event when the amount of logical volume content reaches the threshold.

	Post Critical Event + Run Purge	Creates a critical event and purges all snapshot images when the amount of logical volume content reaches the threshold.
	Post Critical Event + Disassociate Snapshot Images	Creates a critical event and make all snapshot images invalid when the amount of logical volume content reaches the threshold.

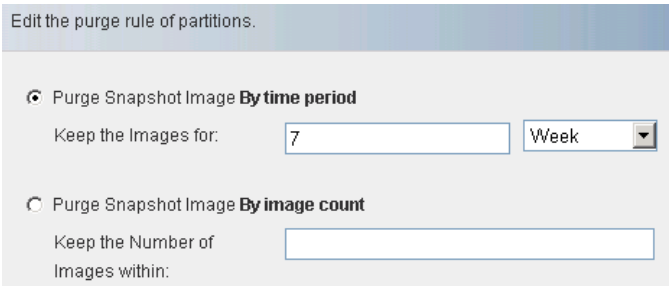
Configuring Purge Rules

This setting is applicable only when there is a policy with the Post Critical Event + Run Purge option.

Purge refers to removing old snapshot images to prevent the storage capacity used up by unused snapshot image files.

Click Purge Rule in the Threshold screen.

Highlight the purge setting and click Edit. The purge rule screen will appear.



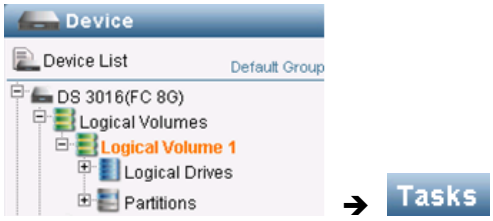
Purge Parameters	**Purge Threshold**	Specifies the threshold policy: duration (By Time) or the number of snapshot images (By SI Count).
	Value	Specifies the values.

Adding a Logical Drive to an Existing Logical Volume (EonStor DS subsystems only)

By default, creating a logical volume (LV) also creates a logical drive (LD) on it. However, you may add a logical drive to an existing logical volume by following the procedures below.

Go To

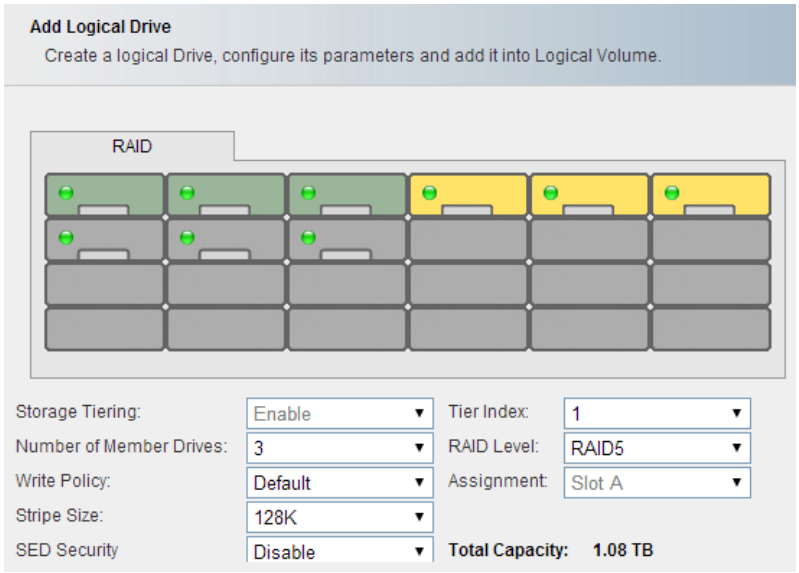
SANWatch Home > Device sidebar > Device List > device name > Logical Volumes > LV name > Tasks corner



Steps

Click Add Logical Drive in the Tasks corner.

The configuration window will appear.



For information about the options on the window, refer to the Steps section of "Creating a Virtual Pool and Virtual Volumes (ESVA subsystems only)

You can create both a virtual pool and its virtual volumes at the same time. You can also manually (and separately) create a virtual volume.

The maximum size of a pool is 2PB.

Process

Creating a virtual pool or virtual volumes takes four steps:

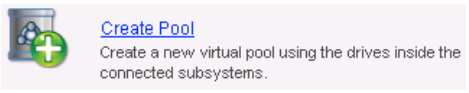
1. Selecting pool elements
2. Configuring tiering (if tiering has been enabled)
3. Creating virtual volumes
4. Confirming the result

Go To

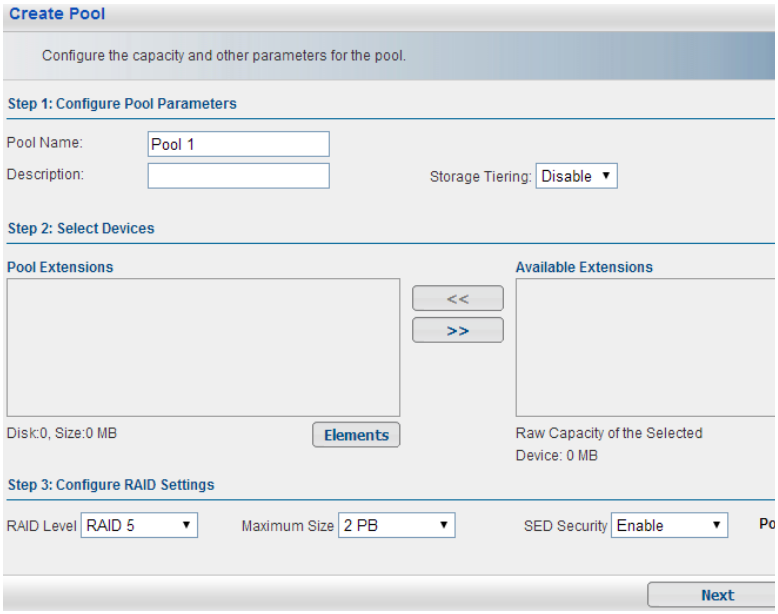
SANWatch Home > Pool sidebar > Pool List > Tasks corner

Step1: Selecting Pool Elements

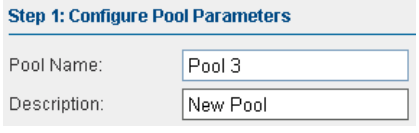
Click Create Pool in the Tasks corner.



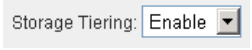
The Pool Configuration screen will appear.



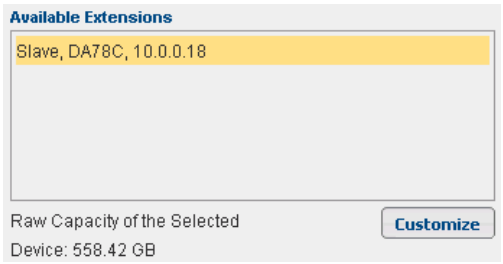
Enter the pool name and description.



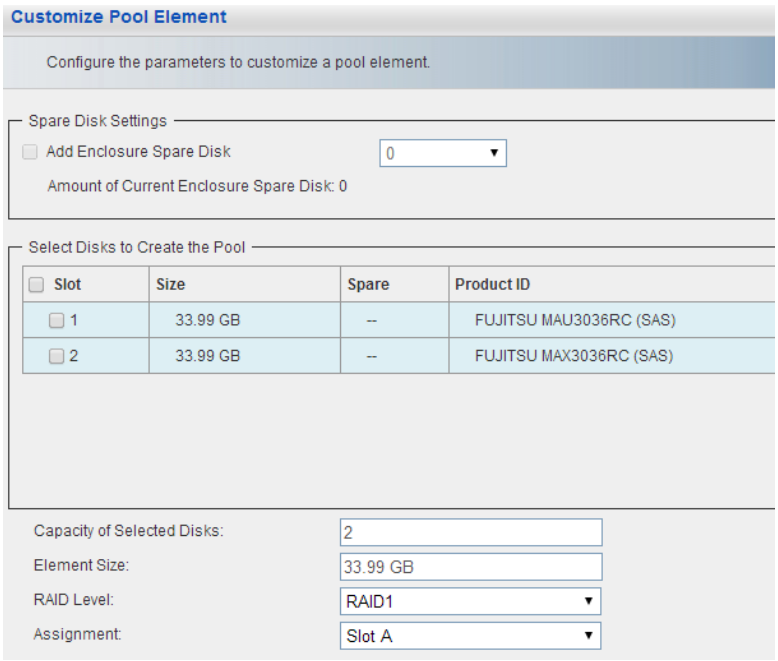
Enable storage tiering (this option will show up when you have the tiering license).



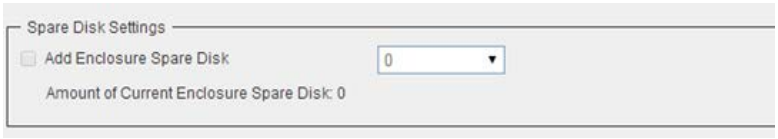
Highlight an ESVA/JBOD in the Available Extensions List and click Customize.



The Customize Pool Element window will appear.

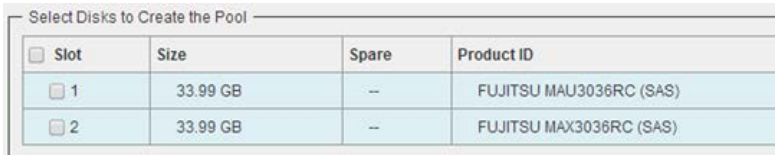


You may add a spare disk to the new pool.



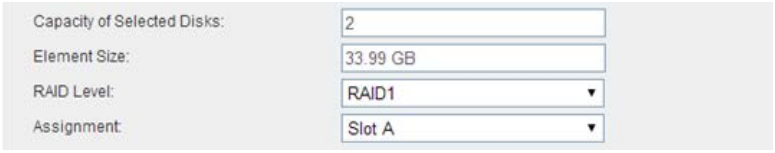
This option will be active only when there are spare drives available. You can create and add a spare drive later.

Select disk drives for the first pool element. If you wish to create multiple pool elements (especially for storage tiering), make sure you do not select all available disk drives.

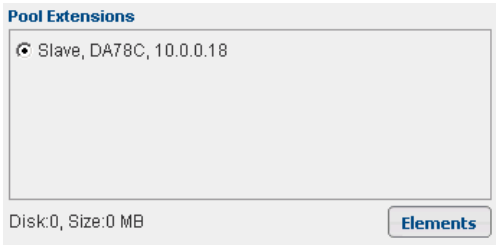


Select the RAID level and the assigned controller. The number and size of disk drives will be updated in the Selected Amount

and Element Size corner.

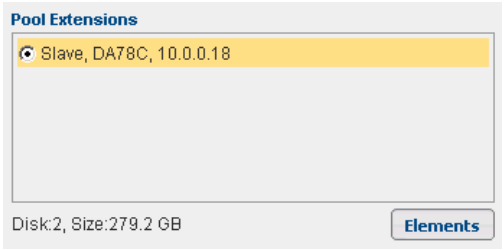


Click Apply. The ESVA system with the new pool element will appear in the Pool Extent List. (The first pool element will become the master element.)

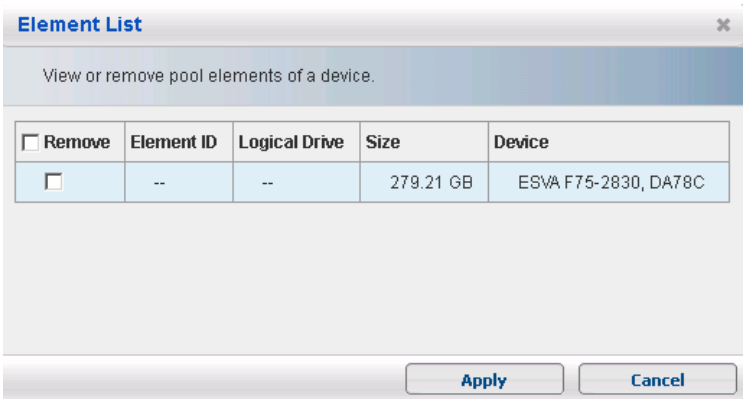


To add more pool elements, repeat above steps.

When all elements have been added, highlight the extension and click Elements to confirm the list of pool elements included in this pool.



You may remove unwanted elements (except for the master element) here.



Select the RAID level and the maximum possible pool size in the Settings corner.

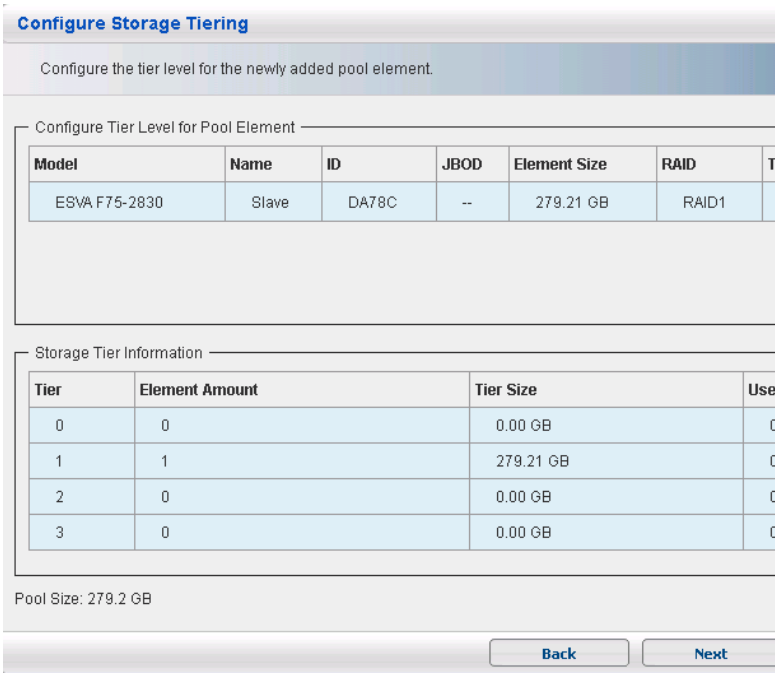
The RAID Level option will be disabled if you have already

chosen the RAID level in the Customize dialogue.

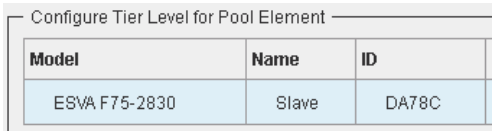
Click Next.

Step 1 Parameters	**Spare Disk**	Creates enclosure spare disk(s) for the virtual pool. You need to have available disks inside the enclosure.
	RAID Level	Specifies the RAID level of the virtual pool: RAID 0, 1, 5, and 6. RAID 5 and RAID 6 offer protection against one and two drive failure, respectively. If you want to take extra caution against data loss (for example, a media error occurs while rebuilding a failed drive), it is recommended to take RAID 6.
	Pool Name	Specifies the virtual pool's name.
	Description	Specifies a short description of the virtual pool.
	Storage Tiering	When enabled, you can configure tiering. See procedures below for details.
	Maximum Size	Specifies the maximum pool size from 64TB up to 2PB. The size also determines the data block section size which ESVA uses to distribute data across pool elements. The larger the Maximum Size, the larger the section size becomes which may not be optimal for random and small I/Os. Use the default size for optimal performance. In order to perform remote mirror, the maximum size of the pool pairs need to match each other.
	SED Security	Protects pool data with SED security.
Step 2: Configuring Tiering	If storage tiering has not been enabled, you will see the next step, Configuring Virtual Volumes.	

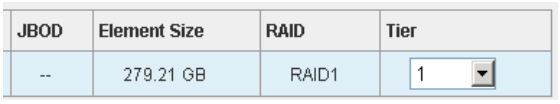
The Storage Tiering Setting appears.



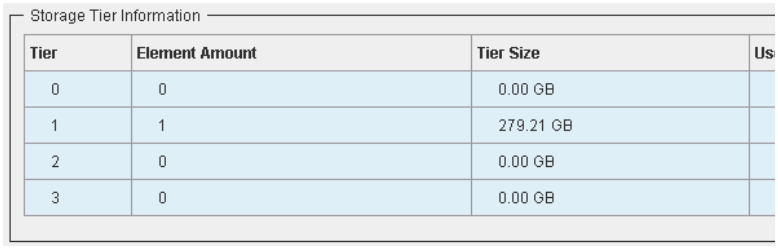
Confirm the list of pool element included in the pool.



Select the tier level of each pool element.



Confirm the summary of pool elements and their tiers in the Storage Tier Information corner.



Click Next.

Step 2 Parameters

Tier Level

Specifies the tier level of this pool. Four levels exist, with tier 0 having the highest priority. Here are the recommended tier levels for pool element types.

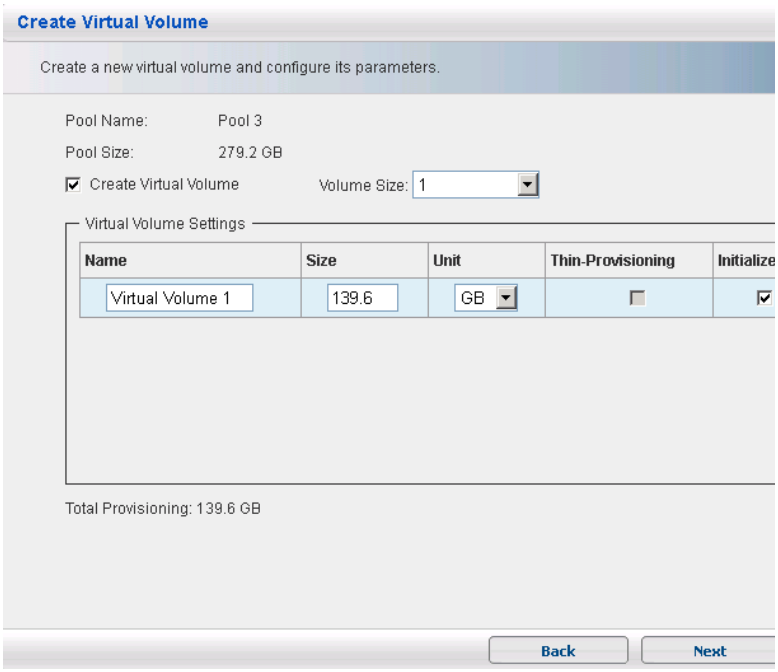
- Tier 0: SSD

- Tier 1: FC/SAS (RAID 1)
- Tier 2: FC/SAS (RAID 0/3/5/6)
- Tier 3: SATA

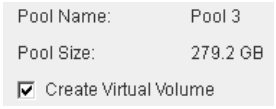
You may select the same or different tier levels for pool elements. Data in the higher tier will be accessed primarily.

Step 3: Configuring Virtual Volume

In the Create Virtual Volume window, check “Create Virtual Volume.”

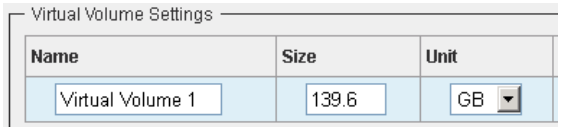


You may also uncheck this box and create virtual volumes later.



Select the number of volumes.

The volumes will then appear in the Virtual Volume Setting corner.



(When multiple storage tiers are available) Select in which tier each volume will reside (Default: All). You may modify this setting later.

Check if you want to enable thin-provisioning/initializing or

mapping.

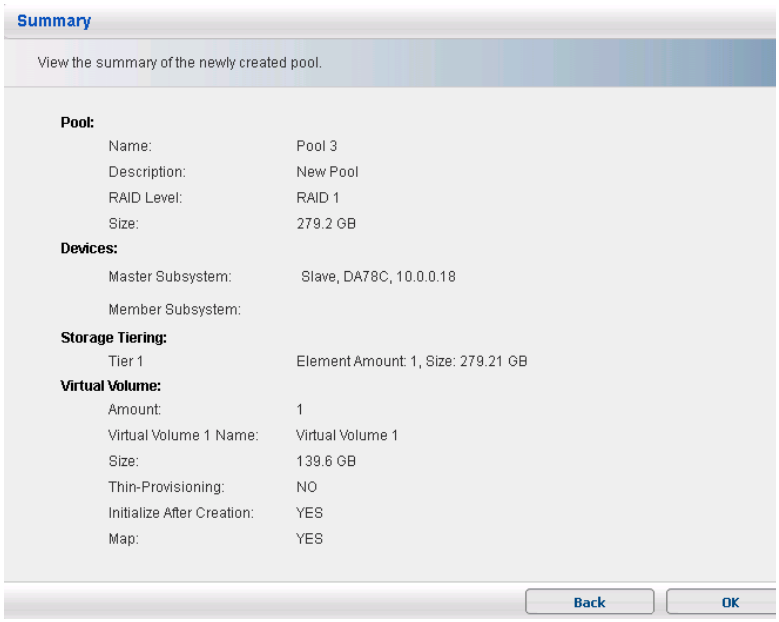
Click Next.

Step 3 Parameters	**Volume Size**	To change the volume size, double-click the number. If Thin Provision is activated, you may enter a volume size larger than the pool size.
	Unit	Select the unit of volume size: MB, GB, or TB.
	Tier Resided	Defines in which storage tier the virtual volume exists. When you select “All,” the virtual volume capacity will be divided equally among the tiers. You may change the ratio manually later.
	Thin-Provisioning	➢ When checked, a thin-provisioned volume with no minimum reserved space (0%) will be created. ➢ When unchecked, a full-provisioned volume with initialization will be created. Thin provisioning allows you to allocate a large amount of virtual capacity for a logical volume regardless of the physical capacity actually available. Actual space is used only when data writes occur. By automatically allocating system capacity to applications as needed, thin provisioning technology can significantly increase storage utilization. When the volume is initialized, the virtual volume’s LBA addresses will be allocated consequentially for large and/or sequential I/Os. This is ideal for audio/video application such as media post-editing and video on-demand.
	Map	Automatically maps the volume to all host channels, which allows all SAN servers to

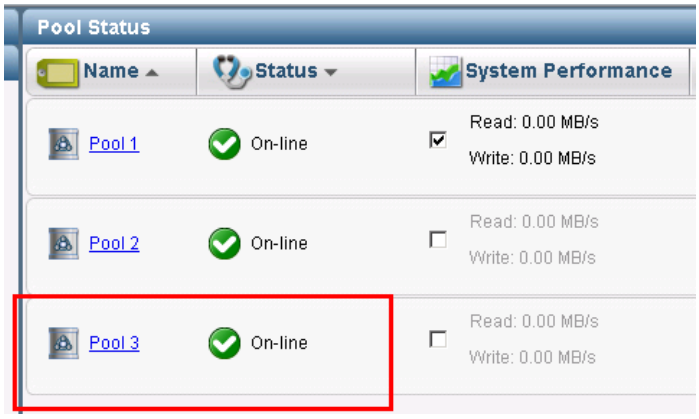
access the volume. Uncheck this parameter if you intend to create host LUN mapping later.

Step 4: Confirming the New Pool

A summary will appear. Verify configuration details and click OK. If you have chosen not to create virtual volumes or LUN mapping, you may do so later.



The pool will appear in the list.



Creating a Logical Volume."

Expanding a Logical Volume (EonStor DS subsystems only)

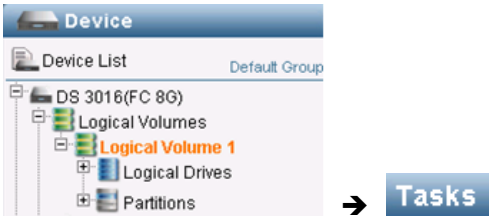
You may expand a logical volume's size in these steps.

Expand the size of its member logical drives. You must expand all logical drives that belong to this logical volume.

Expand the size of the logical volume following the procedures below.

Go To

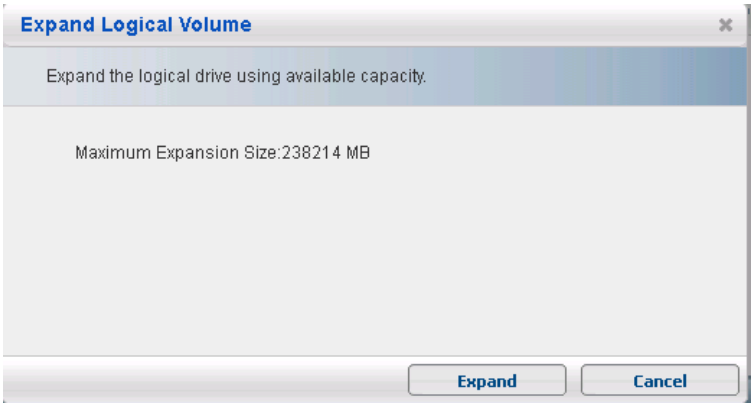
SANWatch Home > Device sidebar > Device List > device name > Logical Volumes > LV name > Tasks corner



Steps

Click Expand Logical Volumes in the Tasks corner.

The expansion screen will appear.



The system will automatically select all available capacity for expansion.

Click Expand to begin the process.

Check the logical volume status in the list to see the expanded size.

Expanding/Shrinking a Virtual Pool (ESVA subsystems only)

Types of Expansion

You may expand a virtual pool in two ways:

- Adding more disk drives/enclosures to the original pool element: In this case, you are going to add disk drives in the same RAID level.
- Adding different pool elements: If you have enabled storage tiering, you can also add pool elements with different RAID levels to an existing pool, by separating their tier level. The data will be written to the tier with the higher level first.

Make sure you have prepared sufficient number of available disk drives corresponding to the RAID level of the element you want to add.

Note

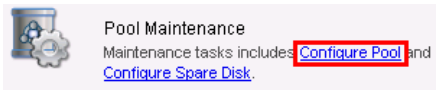
When you try to expand the pool via scale-out mechanism (by adding more ESVA subsystems), we strongly recommend you to build the RAID group as a pool using the same firmware version.

Go To

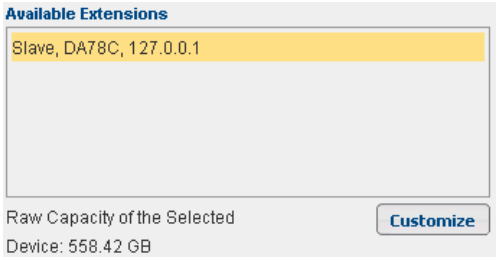
SANWatch Home > Pool sidebar > Pool List > pool name > Tasks corner

Expanding a Virtual Pool (Adding a Pool Element)

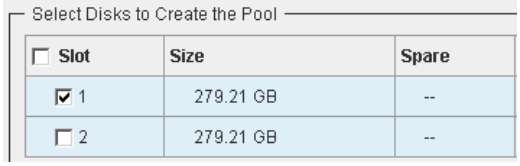
Click Configure Pool in the Tasks corner.



Highlight a ESVA/JBOD in the Pool Extent List and click Customize.

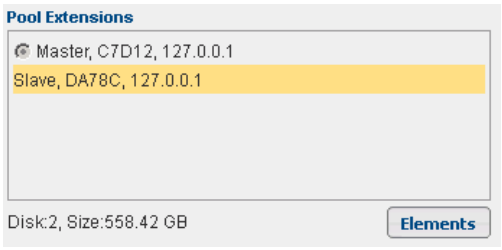


In the Customize window that appears, select the disk drives that will be added.

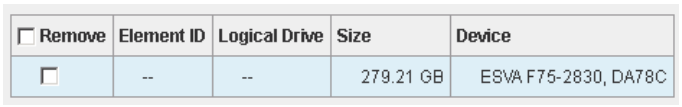


Select the RAID and assigned slot and click OK.

Highlight the pool in the Pool Extension list and click Elements.



Confirm that the newly added pool elements appear in the list.

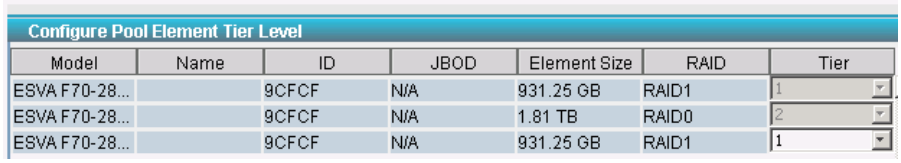


Remove	Element ID	Logical Drive	Size	Device
☐	--	--	279.21 GB	ESVA F75-2830, DA78C

Select the data migration priority in the Settings and click Next.

> The Pause priority is not used until data migration actually starts.

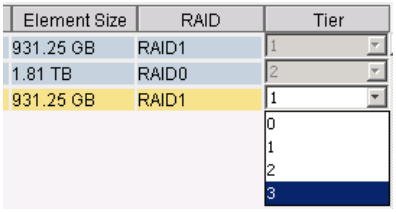
The Storage Tiering Setting (if selected) appears. Confirm that the newly added pool element appears.



Configure Pool Element Tier Level

Model	Name	ID	JBOD	Element Size	RAID	Tier
ESVA F70-28...		9CFCF	N/A	931.25 GB	RAID1	1
ESVA F70-28...		9CFCF	N/A	1.81 TB	RAID0	2
ESVA F70-28...		9CFCF	N/A	931.25 GB	RAID1	1

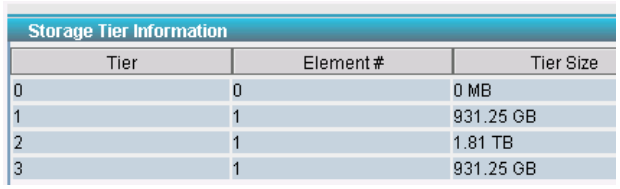
Select the tier level of the newly added element(s). The new element can expand an existing tier or become a new tier for the pool.



Element Size	RAID	Tier
931.25 GB	RAID1	1
1.81 TB	RAID0	2
931.25 GB	RAID1	1

0
1
2
3

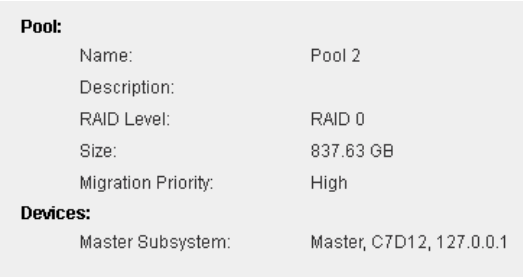
Confirm the summary of pool elements and their tiers in the Storage Tier Information corner.



Storage Tier Information

Tier	Element #	Tier Size
0	0	0 MB
1	1	931.25 GB
2	1	1.81 TB
3	1	931.25 GB

The summary of the updated pool configuration will appear. Click OK.

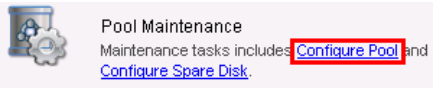


Data migration will begin

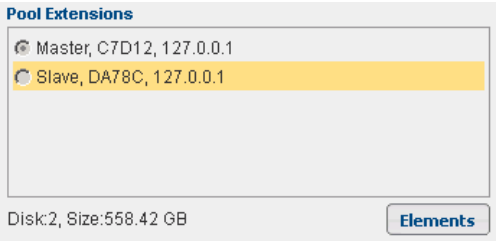
Shrinking a Virtual Pool (Removing a Pool Element)

Make sure you have deleted the virtual volumes that reside in the pool element to be deleted.

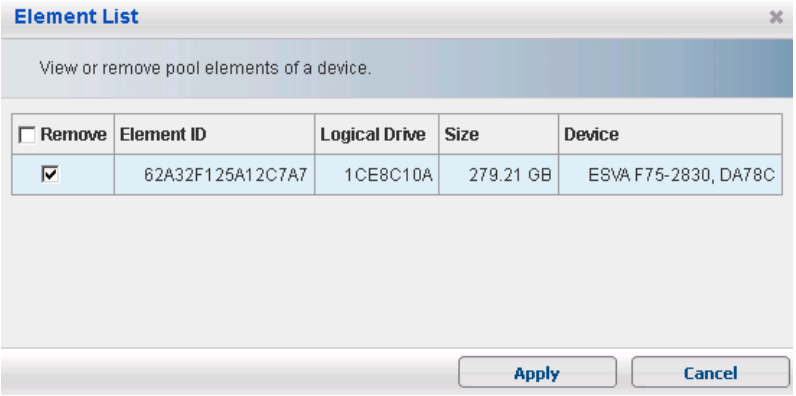
Click Configure Pool in the Tasks corner.



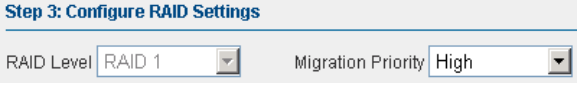
Highlight an ESVA/JBOD in the Pool Extension List and click Elements.



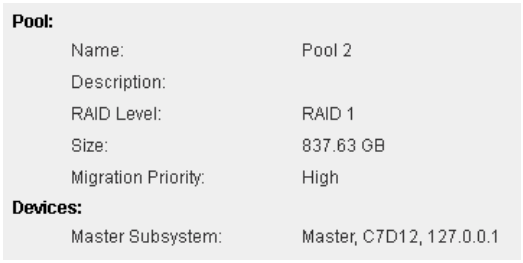
Select the element you want to remove and click Apply.



Select the data migration priority in the Settings and click Next.

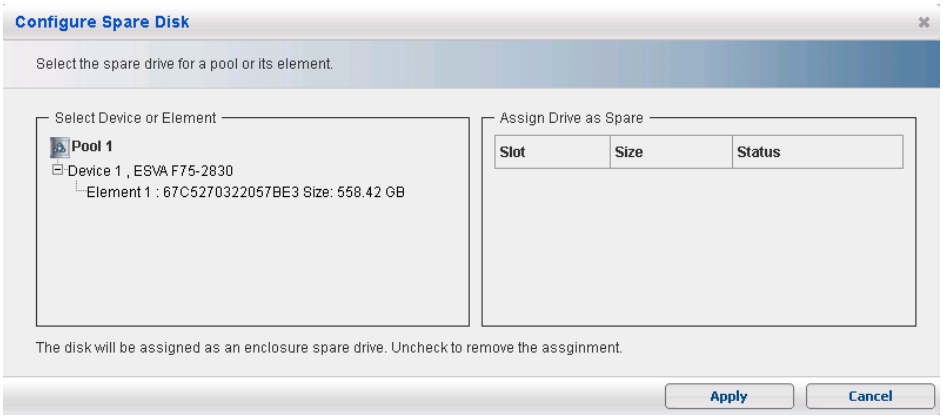
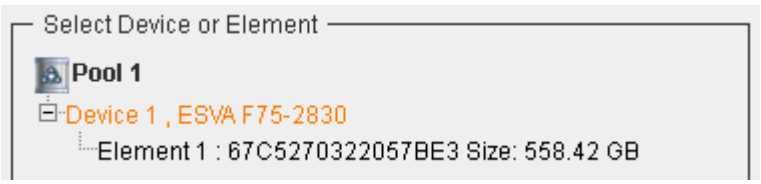


The summary of the updated pool configuration will appear. Click OK.



Data migration will begin.

Assigning a Spare Drive to a Pool (ESVA subsystems only)

	Make sure that an available drive exists (not part of a virtual pool or virtual volume yet).
Enclosure vs. Local Spare Drive	➢ Enclosure spare drives can be access by all pool elements inside the subsystem enclosure. ➢ Local spare drives are exclusive to the pool element the drives are assigned to.
Go To	SANWatch Home > Pool sidebar > Pool List > pool name > Tasks corner 
Steps	Click Configure Spare Disk in the Tasks corner.  The spare drive configuration screen will appear.  Highlight the pool (enclosure spare) or pool element (local spare) to which the spare disk will be assigned. **Pool (Enclosure)** 

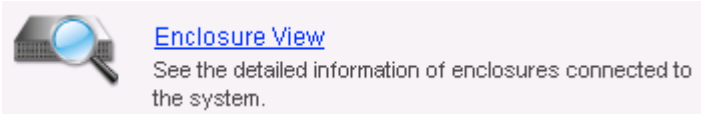
Element (Local)

Check the spare disk on the right-side corner and make sure the status (Enclosure or Local) is correct.

Click the Apply button to assign the spare drive.

Go to Device List > Device > Drives.

Click Enclosure View in the Tasks corner.



The newly assigned spare drive in the front panel figure will show a “+” sign, indicating that it is a spare drive.

Setting Up Thin Provisioning and Host Reclaim

About Thin Provisioning

Thin provisioning allows you to allocate a large amount of virtual capacity for a logical volume or pool regardless of the physical capacity actually available. Actual space is used only when data writes occur. By automatically allocating system capacity to applications as needed, thin provisioning technology can significantly increase storage utilization. Thin provisioning also greatly simplifies capacity planning and management tasks. For more information, see the Infortrend website.

> The thin provisioning / reclaim feature is available in systems with following prerequisites:
>
> EonStor DS G6 systems: FW3.86C or later
> EonStor DS G7 systems: FW3.91B or later
> EonStor DS G7i and 3000 series by default, supports thin provisioning.
>
> Please contact your vendor for more details!
> Dynamically allocating capacity affects the overall performance. If performance is the top priority (such as in AV applications), we recommend you to disable thin provisioning (= use full provisioning).

About Host Reclaim

Thin provisioning keeps increasing the amount of physical storage on demand whenever new files are added. This works perfectly as long as all of the original files remain intact, but in reality some files will be deleted by host computers in the long run. As a result, available LV or pool capacity of your subsystem often appears less than its real available size. In order to make the most use of storage area, the size of deleted files/blocks should be checked occasionally to adjust the size of the logical volume.

The host reclaim function calculates the size of the deleted files in partitions or virtual volumes, and “shrink” the logical volume or pool size so that it reflects the currently used area. Host reclaim should be used in conjunction with thin provisioning, and is especially useful for data replication such as snapshot and volume copy/mirror, allowing for shortened replication time and reduced target area.

> Host Reclaim only works when the host computer is running on Windows or Linux.

Prerequisites

The subsystem needs to meet the following conditions.

License

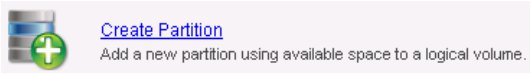
Thin Provisioning available

To view the license information, go to SANWatch Home > Device sidebar > Device List > device name > Tasks

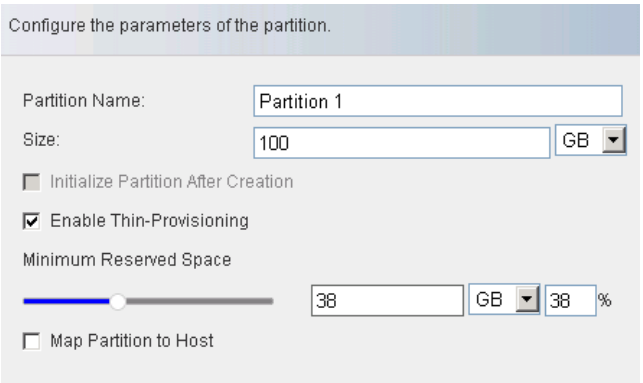
	corner > License Information
Firmware	To view the firmware version, open SANWatch Home > Device sidebar > Device List > device name > Status corner > Firmware Version
SANWatch	To view the SANWatch version, go to SANWatch Home > About.
Thin-Provisioned Partition or Virtual Volume Size	**Maximum 256TB or 512TB** The maximum size of a single partition or virtual volume is 256TB (before firmware version 3.88) or 512TB (after firmware version 3.88). Make sure that the size of the logical volume or pool is in line (you cannot make the size of the partition or virtual volume larger than the size of the logical volume or pool). For the latest status, checking with technical support is recommended. Although we allow you to “over-provision” (the size of the thin-provisioned partition or virtual volume can be larger than the actual logical volume size), the partition or virtual volume size cannot exceed the size limit for the EonStor DS series.

Thin Provisioning Settings

1. Thin provisioning is configured during creating a partition (for EonStor DS subsystems) or virtual volume (for ESVA subsystems).



2. In the partition or VV creation screen, thin provisioning options will appear in the lower half.



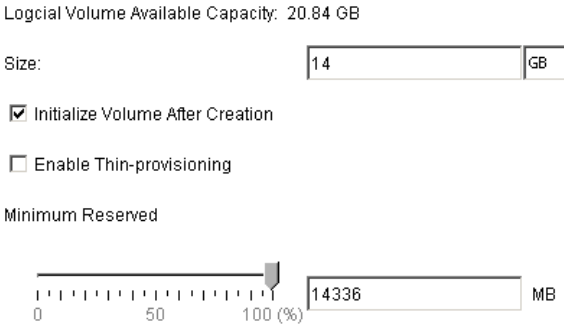
3. After the new partition or virtual cool has been created, create one or more notification thresholds to make sure that the administrator receives warning/critical messages before all of the logical volume space or pool will be used up, and to give him or her ample time for expanding the size of the

logical volume.

> We recommend you to create multiple thresholds to stay on the safe side. (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 you uncheck “Enable Thin-provisioning,” thin provisioning will be disabled and all of the configured logical volume size or pool size (in the below diagram’s case, 14GB) will be taken from the capacity actually available. The partition or virtual volume will be created as a continuous physical space reserved only for the target application, and then will be initialized if the “Initialize Volume After Creation” box is checked (you may uncheck this option if you prefer).



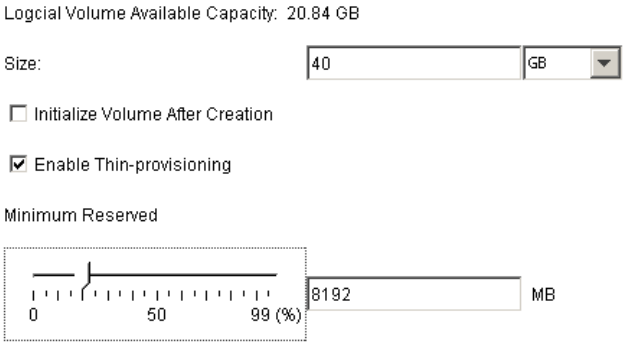
Full provisioning is suitable for mission-critical applications with large amount of uninterrupted data, such as audio/video streams. Dynamically allocating space and expanding usable area slows the I/O performance down, therefore allocating a large physical capacity from the beginning optimizes the performance.

Case 2: Thin Provisioning

To enable thin provisioning, check the “Enable Thin-provisioning” box and select the Minimum Reserved space using the slider.

When the application use up the minimum reserved area, additional space will be taken from the rest of the logical volume (or virtual pool) space and will be added to the partition or virtual volume dynamically.

In this example, The actual logical volume size or pool is 20GB but the partition or virtual volume is set at 40GB, larger than the available size. This is fine as long as the minimum reserved space (the actual physically allocated space) is smaller than the logical volume size or pool size: 8GB in this case.



The reserved space cannot exceed the actual available capacity.

Storage Tiering

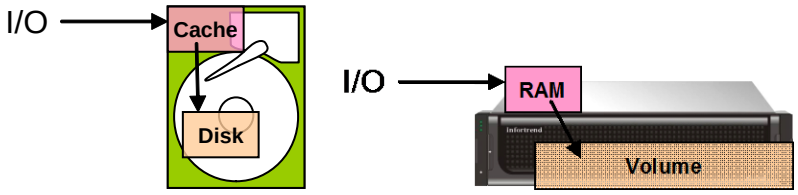
This section is applicable when storage tiering has been enabled.

What is Storage Tiering?

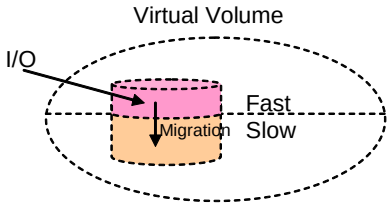
What Tiering is about

Tiering creates vertical layers inside a virtual pool (or logical volume for EonStor DS subsystems) to improve data I/O performance compared to the traditional, monolithic pool.

Tiering is a simulation of cache mechanism deployed in a disk drive or a RAID subsystem, where data transaction takes place in fast cache memory without waiting for slower physical drives to respond.



To simulate cache system inside a pool, a tier system separates the pool elements (or logical drives for EonStor DS subsystems) into layers called tiers. I/O transaction will primarily occur between the higher tier, where pool elements or logical drives with faster access (such as a LD composed of SSDs) will be assigned. The data will then be migrated into the lower tier, where slower but more economically feasible pool elements or logical drives (such as a pool element composed of SATA drives) are assigned.



Benefits of Tiering

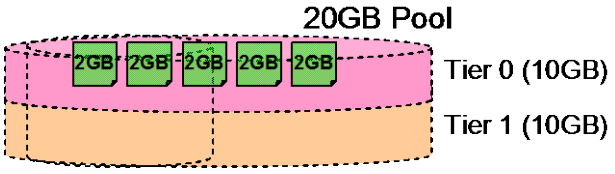
- Fast data transaction: Data will always be written to the top tier first, then will be migrated into lower tiers. By assigning a pool element or logical drive to fast drives (such as SSDs) to the top tier, you can achieve higher data throughput.
- Flexible pool configuration: You can mix different RAID levels and drive types (SSD / SAS, NL-SAS, etc.) inside a virtual pool; you are no longer restricted to build it from a single hardware type.
- Economic pool creation: You can assign fast but expensive hardware to the top tier, and construct lower tiers with slower but more economic hardware.

Tiered Migration

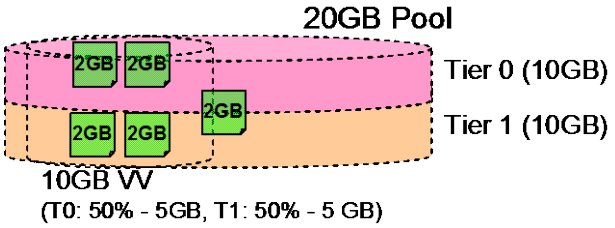
By default, the host always writes to the highest priority tier (usually Tier 0). In order not to use up all capacity of the top tier, you will need to migrate

unimportant data into lower tiers, either manually or automatically by schedule.

Before: All data is written to the top tier, or tier 0.



After: Some data will be migrated to the lower tier, or tier 1.



"Hotness" of Data

The system determines the priority of data by two factors:

- Residing time: the newer, the higher priority
- Access frequency: the more heavily accessed, the higher priority

Data with higher priority is marked as "hot" and will likely reside in higher tiers after migration.

Tiering Rules

Tier Levels

ESVA and EonStor DS system may have four tier levels to choose from, with tier 0 the fastest. Here are the recommended tier levels for RAID and drive types.

- Tier 0: SSD
- Tier 1: SAS
- Tier 2: Nearline SAS
- Tier 3: SATA

SSD and SAS drives have fast I/Os but are expensive, suited for performance-oriented usage. NL-SATA drives are slower but are inexpensive, suited for capacity-oriented usage.

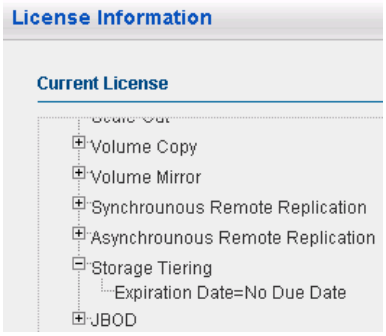
Host I/O Priority

- The host always writes to the highest tier in a given pool or logical volume.
- Data service (snapshot, volume copy, volume mirror) will occur at the lowest tier.

License

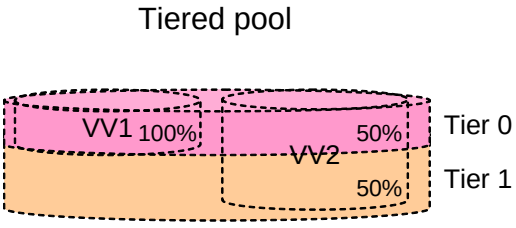
To use storage tiering, you need to apply for a tiering license. Go to Device > Information > License Information.

Click License information.



Virtual Volumes

A virtual volume (for ESVA subsystems) or partition (for EonStor DS subsystems) can exist either entirely inside one tier or among multiple tiers. In case of the latter, you will need to specify the ratio of the virtual volume assigned to each tier.



Reserve Ratio

Tier reserve ratio defines the capacity in higher tiers that will not be used up by

tiered pools/volumes. Because the highest tier will be accessed preferentially, there is a risk of data filling up all capacity of the higher tiers. Setting the reserve ratio secures free space for the higher tiers.

You cannot set a reserve ratio for the lowest tier. (= If there is only one tier level, you cannot configure the reserve ratio.)

Limitations on Provisioning and Tiering

Here are the limitations regarding creating a thin/full provisioned partition (for EonStor DS subsystems) or virtual volume (for ESVA subsystems) on a tiering-enabled logical volume:

- If you check Initialize Partition after Creation or Initialize Virtual Volume after Creation to create a full provisioned partition or VV, data stored on the partition or VV could only reside on one tier. Only data stored on thin provisioned partition could be migrated between another tier.
- If you check Enable Thin-Provisioning to create a thin provisioned partition, or VV you are not allowed to set minimum reserved space for it.

Existing Elements after Obtaining Tiering License

The logical volumes / drives (or pools / pool elements for ESVA subsystems) that were created before obtaining Tiering license will be summarized as follows.

Logical volumes or pools:

- Existing LVs or pools could be tiered but with only one tier.
- The default tier index belongs to the first volume element.

Logical drives or pool elements:

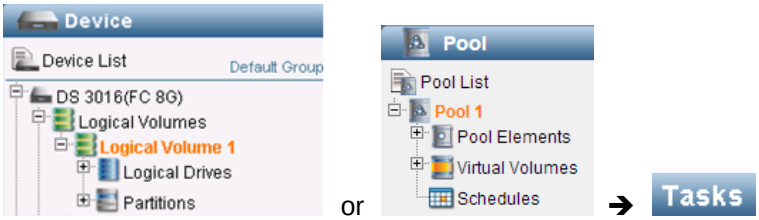
- All logical drives or pool elements will reside in their logical volume's or pool's tier if the LV or pool has been transformed into a tiered one.

Activating Storage Tiering for Legacy Logical Volumes or Pools

You may enable tiering for pools or logical volumes that were created without enabling tiering.

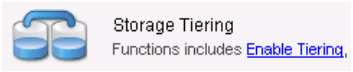
Go to

EonStor DS subsystems: SANWatch Home > Device sidebar > Device List > device name > Logical Volumes > LV name > Tasks corner
ESVA subsystems: SANWatch Home > Pool sidebar > Pool List > pool name > Tasks corner

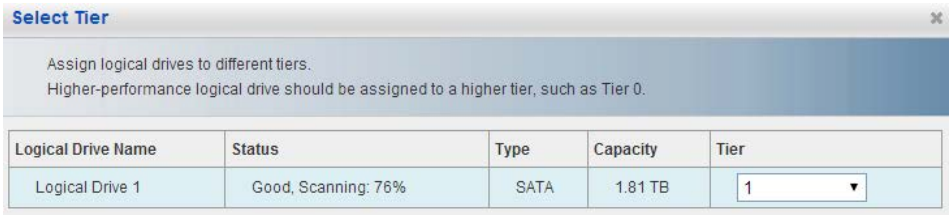


Enabling Storage Tiering

Click Enable Tiering in the Tasks corner.

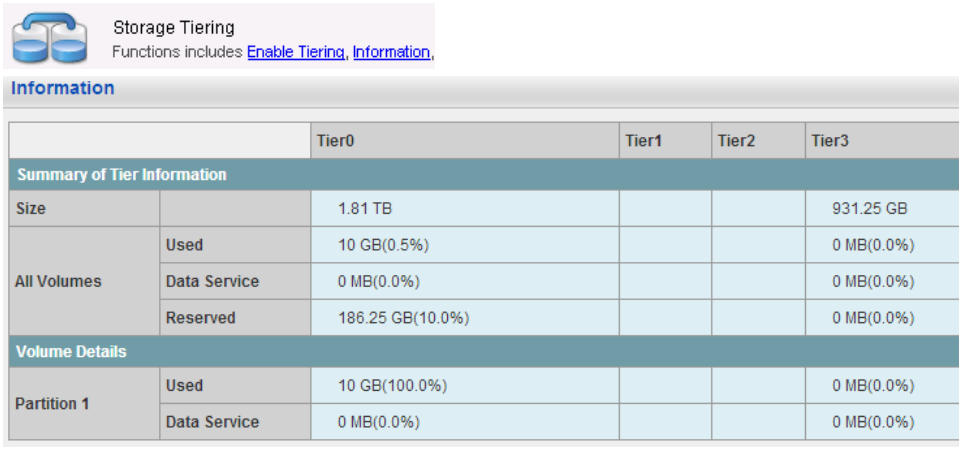


Select the tiering level and click OK.



All pool elements (or logical drives) of the pool (or logical volume) will be transferred to one tier.

Users may click Information to view the pool's (or logical volume's) tiering information.

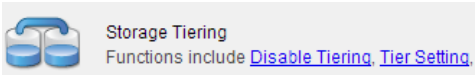


You can click Tier Migration to perform tier migration for optimized data allocation.

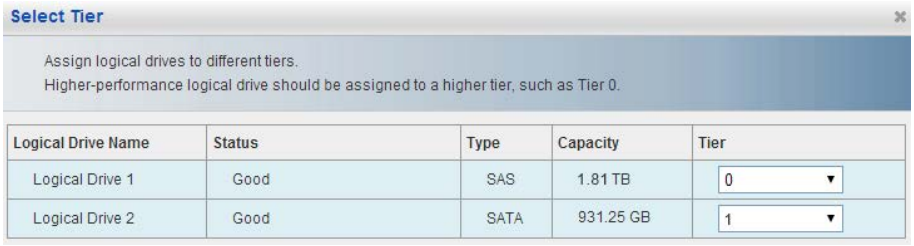
Or you can perform tier migration by schedule, go to SANWatch Home > Device sidebar > Device List > device name > Schedules, click the Help icon at the top-right corner, and then search for "Creating Tiered Data Migration by Schedule" for more information.

Changing Residing Tiers for Elements or LDs

Click Tier Setting in the Tasks corner.

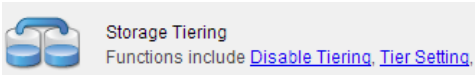


Select tier levels for elements or LDs, and then click OK.



Disabling Storage Tiering

Click Disable Tiering in the Tasks corner, and then click Yes in the dialog that appears.



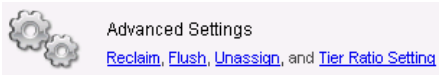
Configuring Tier Reserve Ratio for VV of the / Pool (only available for ESVA subsystems)

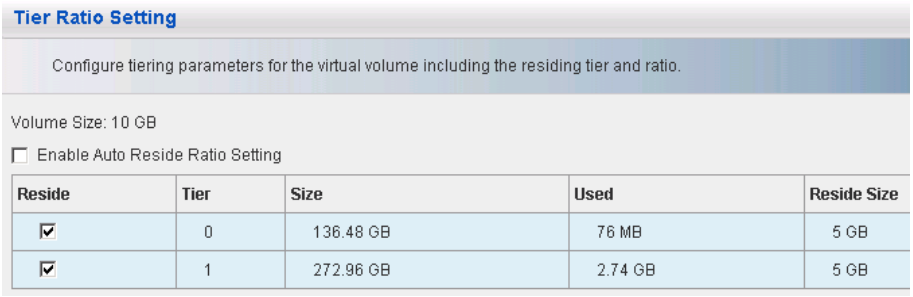
Tier reserve ratio defines the capacity in higher tiers that will not be used up by tiered pools. Because the highest tier will be accessed preferentially, there is a risk of data filling up all capacity of the higher tiers. Setting the reserve ratio secures free space for the higher tiers.

VV must be thin-provisioned to set tier ratio. You cannot set a reserve ratio for the lowest tier. (= If there is only one tier level, you cannot configure the reserve ratio.)

Configuring Tier Reserve Ratio

Under Advanced Settings in the Tasks corner, click Tier Ratio Setting.





"Enable Auto Reside Ration Setting" is available for ESVA subsystems only.

Using the above screenshot as an example, user can allocate 100% of the reserve ratio to either tier or split it 50 / 50 amongst the two tiers.

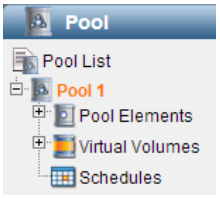
Configure the ratio and click OK.

Viewing Tiering Information

Go to

EonStor DS subsystems: SANWatch Home > Device sidebar > Device List > device name > Logical Volumes > LV name > Tasks corner
ESVA subsystems: SANWatch Home > Pool sidebar > Pool List > pool name > Tasks corner

or

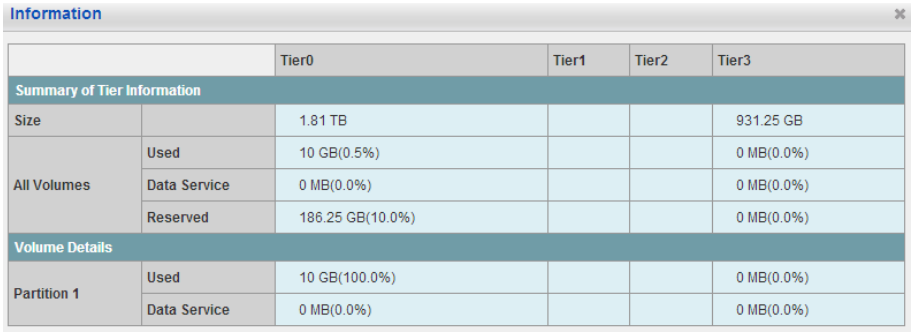


➔ Tasks

Steps

Click Information under Storage Tiering in the Tasks corner.

Existing tiering information will appear.



		Tier0	Tier1	Tier2	Tier3
Summary of Tier Information					
Size		1.81 TB			931.25 GB
All Volumes	Used	10 GB(0.5%)			0 MB(0.0%)
	Data Service	0 MB(0.0%)			0 MB(0.0%)
	Reserved	186.25 GB(10.0%)			0 MB(0.0%)
Volume Details					
Partition 1	Used	10 GB(100.0%)			0 MB(0.0%)
	Data Service	0 MB(0.0%)			0 MB(0.0%)

Parameters

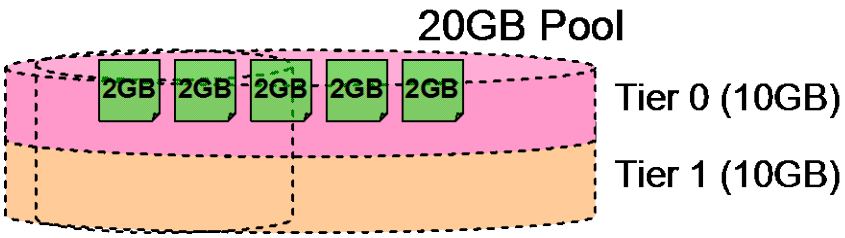
Used	Shows the size and ratio of used data capacity in each tier level.
Data Service	Shows the size and ratio of capacity used for data replication (snapshot, volume copy, volume mirror).
Reserved	Shows the tier reserve ratio of the volume.

Configuring Tiered Data Migration

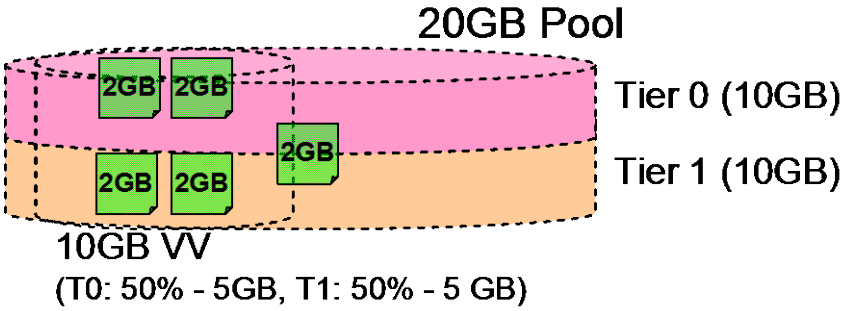
About Tiered Migration

By default, the host always writes to the highest priority tier (usually Tier 0) as long as there is available space. In order not to use up all capacity of the top tier, you will need to migrate unimportant data to lower tiers, either manually or automatically by schedule.

Before: All data is written to the top tier, or tier 0.



After: Some data will be migrated to the lower tier, tier 1.

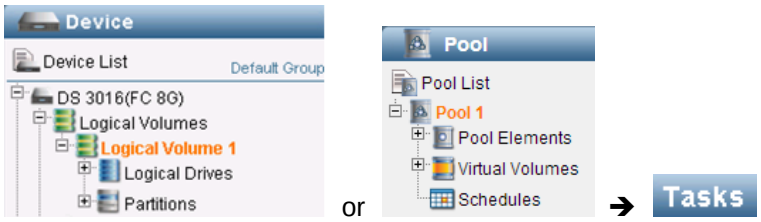


Limitations

Tier migration together with the performance gain it brings are NOT available for full-provisioned partition.

Go to

EonStor DS subsystems: SANWatch Home > Device sidebar > Device List > device name > Logical Volumes > LV name > Tasks corner
ESVA subsystems: SANWatch Home > Pool sidebar > Pool List > pool name > Tasks corner

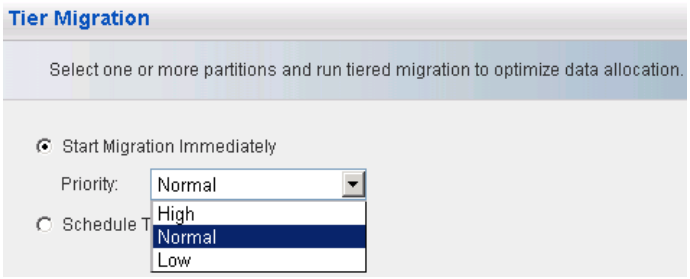


Steps

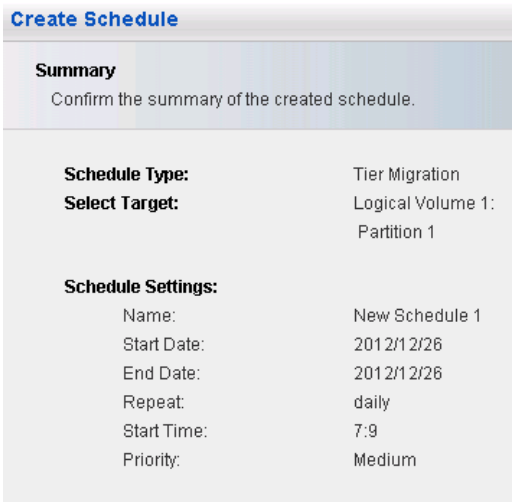
Tiered migration is available only when there are more than one tiers.

Click Tier Migration under Storage Tiering.

the migration timing: immediate or scheduled.



Priority options are: High / Normal / Low

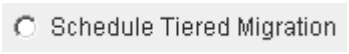


For scheduled migration, see below.

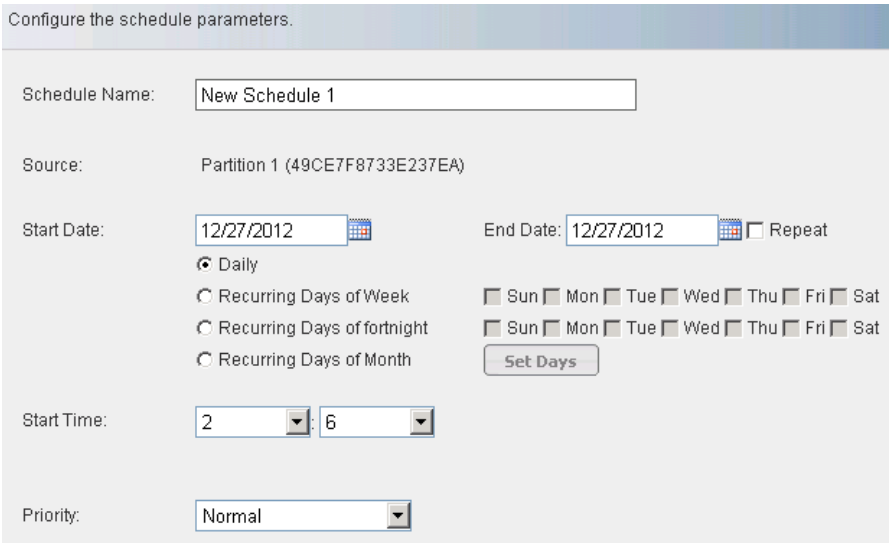
Scheduled Tiered Migration

To run a scheduled tiered migration, the subsystem must be connected to SANWatch Manager through in-band connection.

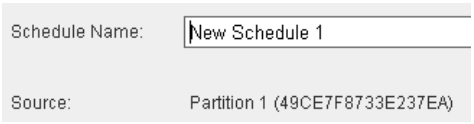
Select scheduled migration and click on Next.



The schedule setting window will appear



Name the schedule. The source information (virtual pool) appears below the name.

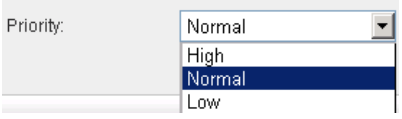


Set the start date and end date of this migration. To make it a repeated process with no end date, check the Repeat box.

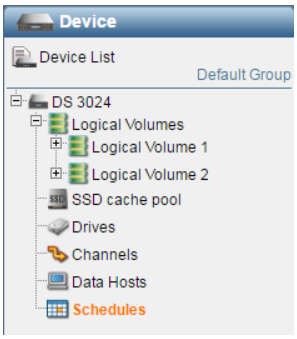
Set the date.

Set the starting time.

Choose a priority level.



Click OK. Migration will start at the specified date.
To check the schedule, go to SANWatch Home > Device sidebar > Device List > device name > Schedules.



If another migration is already ongoing at the scheduled start time, the ongoing migration will be cancelled and the scheduled migration will begin.

Tier Migration Policies

Migration Priorities

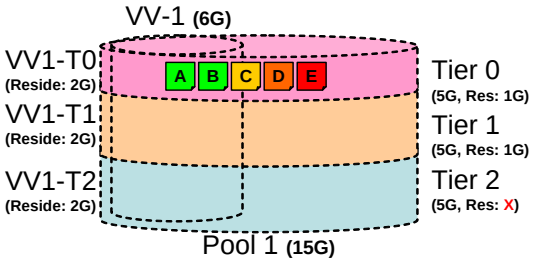
Tier migration has the following priorities:

- High
- Medium
- Low

Case 1: Single Virtual Volume or Partition

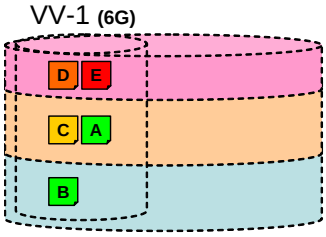
Before migration

The virtual pool (or logical volume for EonStor DS subsystems) Pool 1 is comprised of a single virtual volume (or partition for EonStor DS subsystems) VV-1 which has three tiers, T0, T1, and T2. The data blocks, A to E, are written into the top tier, T0.



After migration

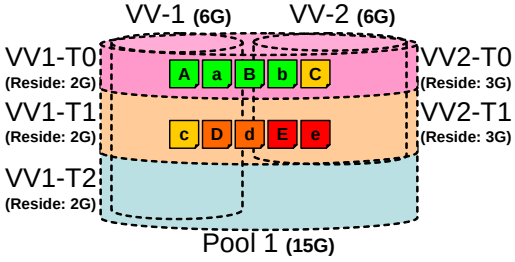
Data blocks are migrated to lower tiers, according to their volume tier ratios.



Case 2: Multiple Virtual Volumes

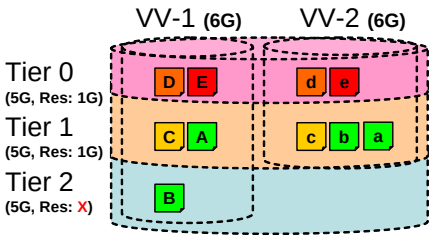
Before migration

The virtual pool (or logical volume for EonStor DS subsystems) Pool 1 is comprised of two virtual volumes (or partitions for EonStor DS subsystems) VV-1 with tiers T0-T2 and VV-2 with tiers T0 and T1. The data blocks, Aa to Ee, are written to the top two tiers, T0 and T1.



After migration

Data blocks are migrated to lower tiers, according to their tier settings and pool tier reserves.

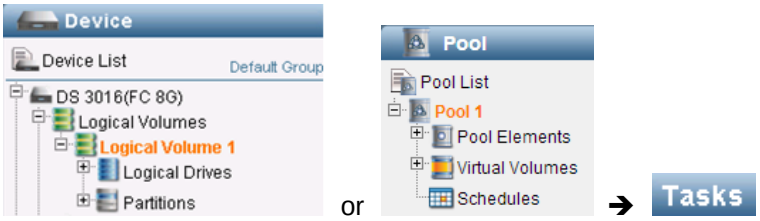


Viewing Tier Migration Information

This feature is available when tiered data migration has been enabled.
Viewing tier information is available when more than one tiers are available.

Go to

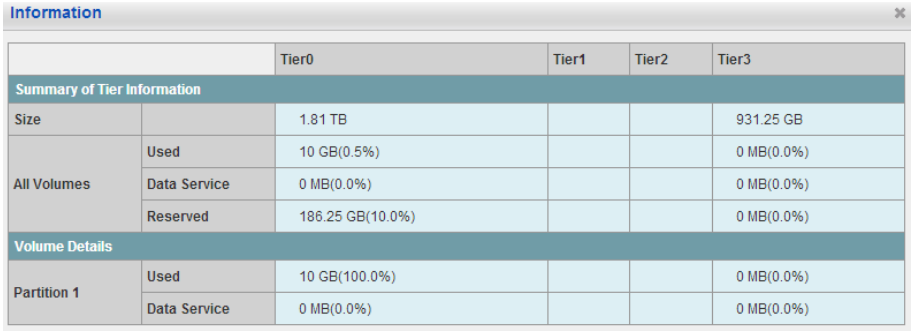
EonStor DS subsystems: SANWatch Home > Device sidebar > Device List > device name > Logical Volumes > LV name > Tasks corner
ESVA subsystems: SANWatch Home > Pool sidebar > Pool List > pool name > Tasks corner



Steps

Click Information under Storage Tiering in the Tasks corner.

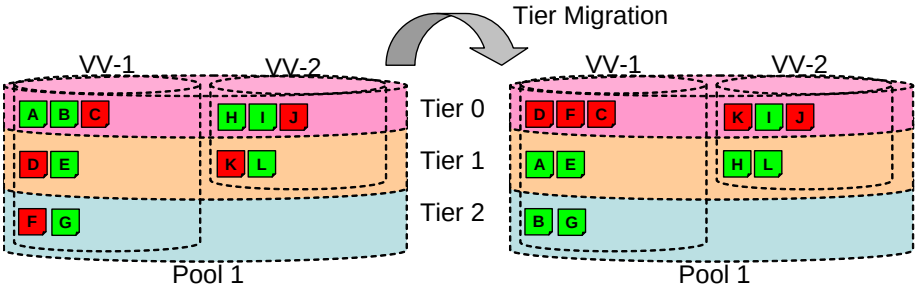
The migration status of tiers and volumes in the pool (or logical volume) will appear.



		Tier0	Tier1	Tier2	Tier3
Summary of Tier Information					
Size		1.81 TB			931.25 GB
All Volumes	Used	10 GB(0.5%)			0 MB(0.0%)
	Data Service	0 MB(0.0%)			0 MB(0.0%)
	Reserved	186.25 GB(10.0%)			0 MB(0.0%)
Volume Details					
Partition 1	Used	10 GB(100.0%)			0 MB(0.0%)
	Data Service	0 MB(0.0%)			0 MB(0.0%)

Migration Statistics Parameters

The diagram below shows an example of tier migration.



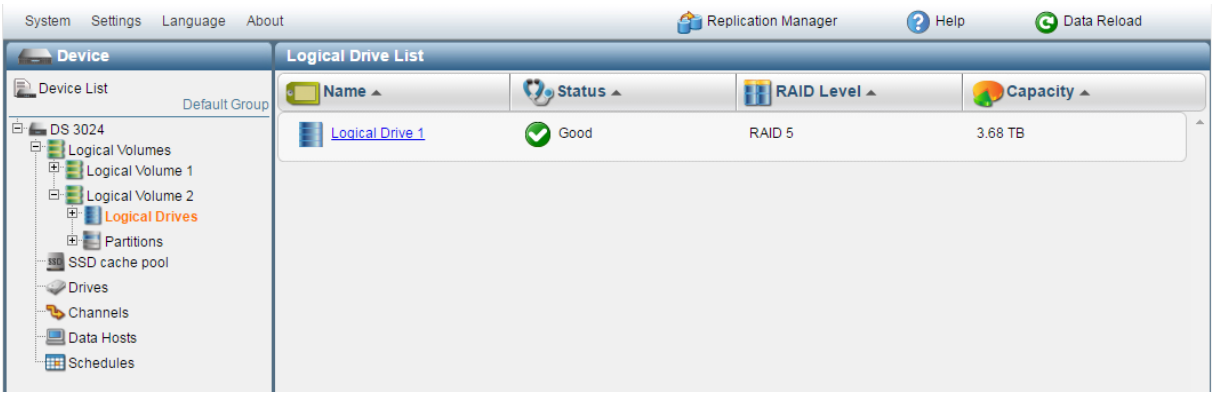
Here is the migration result of virtual volume (or partition for EonStor DS subsystems) VV-1.

Promoted	Demoted	Migrate-In
X	2 (A,B)	2 (D,F)
1 (D)	0	1 (A)
1 (F)	X	1 (B)

Here is the migration result of virtual pool (or logical volume) Pool1.

Promoted	Demoted	Migrate-In
X	3 (A,B,H)	3 (D,F,K)
2 (D,K)	0	2 (A,H)
1 (F)	X	1 (B)

Working with the Logical Drives or Pool Elements View

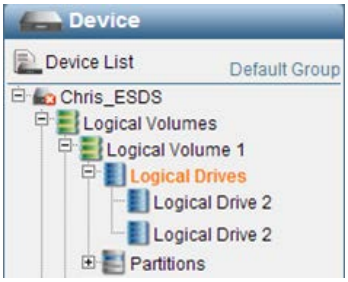


A logical drive (for EonStor DS subsystems) or pool element (for ESVA subsystems) is a collection of disk drives that serves as a virtual storage element that constitutes a logical volume (for EonStor DS subsystems) or virtual pool (for ESVA subsystems). You may create and configure logical drives or pool elements when you create a virtual pool or logical volume. This chapter describes how to view the status of all elements in a logical volume or pool: logical drive or pool element configuration, capacity, hardware device, and task progress (if available).

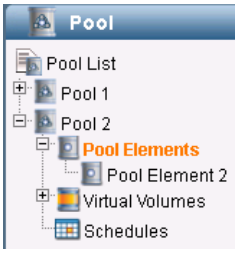
Viewing the List of Logical Drives

Go To

EonStor DS subsystems: SANWatch Home > Device sidebar > Device List > device name > Logical Volumes > LV name > Logical Drives
ESVA subsystems: SANWatch Home > Pool sidebar > Pool List > pool name > Pool Elements

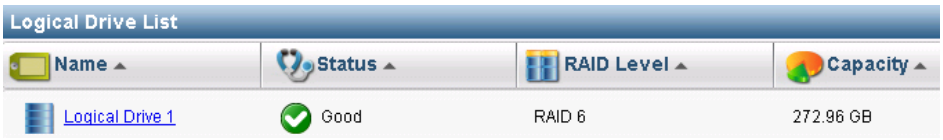


or



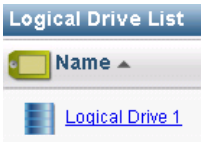
Steps

The list of logical drives or pool elements recognized by the system will appear. The logical drive or pool element status summary will appear to the right, in the main screen.



Logical Drive or Pool Element

Click the link to view detailed configurations of each logical drive or pool element that is included in the logical volume or pool.



The Status corner shows whether this logical drive is in a healthy (no error) status.

RAID Level

The RAID level corner shows the RAID configuration used for this logical drive.

Capacity

The capacity of each logical drive appears. To view the total capacity of volumes or devices, go to the respective menus.

To refresh the status (in case you want to make sure that the logical volume or pool status has been updated), click the *Data Reload* menu at the top bar.

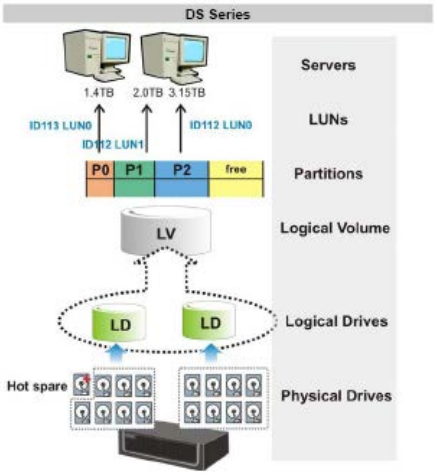
Note If the Help screen does not appear, you might need to enable pop-up windows from the browser's configuration options.

Working with Logical Drives or Pool Elements

This chapter describes how to view and change parameters of a logical drive (for EonStor DS subsystems) or pool element (for ESVA subsystems), configure power saving setting, and add a logical drive or pool element to a remote hardware device. If a logical drive or pool element has been offline or locked, you may restart it manually.

From Physical Drive to Logical Drive (or Pool Element) to Logical Volume (or Pool)

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



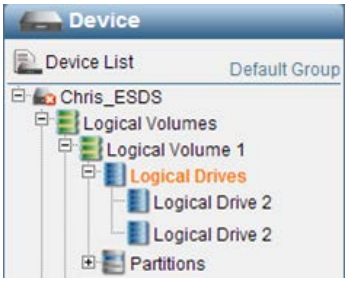
- A collection of physical drives creates a logical drive (for EonStor DS subsystems) or pool element (for ESVA subsystems).
- A collection of logical drives or pool elements creates a logical volume (for EonStor DS subsystems) or pool (for ESVA subsystems).
- A logical volume or pool can be separated into partitions (for EonStor DS subsystems) or virtual volumes (for ESVA subsystems).
- Each partition or virtual volume is assigned with a LUN (logical unit number) from the host computer.

Viewing the Logical Drive Status

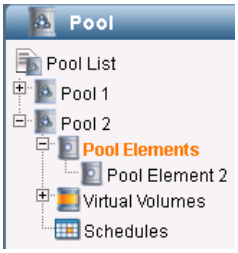
The status of each logical drive is summarized in the Logical Drive Information page, where you can quickly grasp the element configuration and locations of member hard disk drives.

Go To

EonStor DS subsystems: SANWatch Home > Device sidebar > Device List > device name > Logical Volumes > LV name > Logical Drives
ESVA subsystems: SANWatch Home > Pool sidebar > Pool List > pool name > Pool Elements

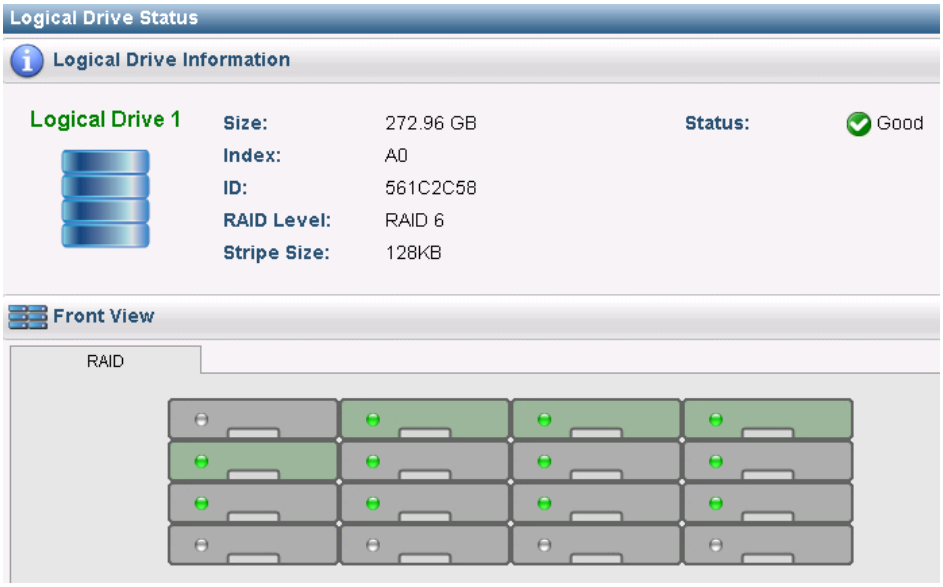


or



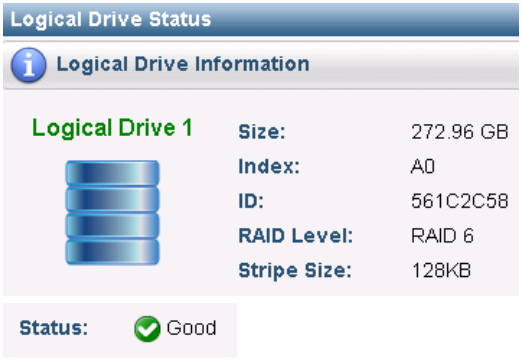
Viewing the Logical Drive or Pool Element Information

The logical drive or pool element status will be summarized in the Status corner.



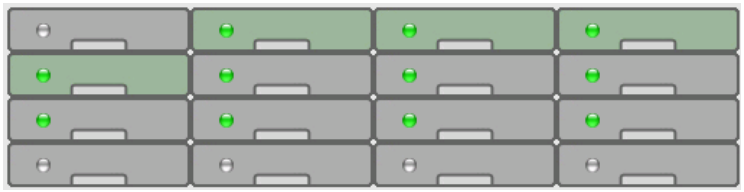
Logical Drive or Pool Element Configurations

The basic system configurations and overall system status will be listed in the Logical Drive Information corner. You can see the size (capacity), logical drive or element ID, RAID level, and the controller module location.



Hard Drive Locations

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



Green status LED shows that the hard drive is online.

The location of logical drive or pool element is highlighted in different colors.

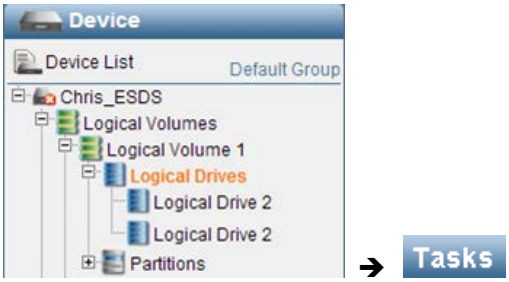
Adding Disk Drives to a Logical Drive (EonStor DS subsystems only)

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

> Before you attempt to expand a logical drive, make sure there are available (unused) disk drives inserted to the enclosure.
> **Warning:** It is HIGHLY RECOMMENDED that you assign a SPARE DRIVE! Without a spare drive, there is an increased risk of data loss!

Go To

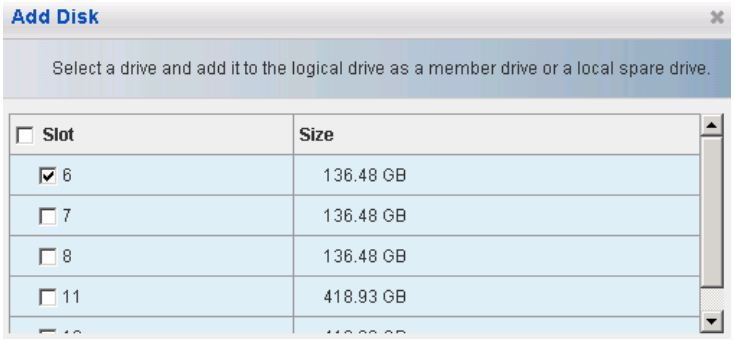
SANWatch Home > Device sidebar > Device List > device name > Logical Volumes > LV name > Logical Drives > Tasks corner



Steps

Click Add Disk in the Tasks corner.

Check the drive you want to add from the list.



Select if you want to add it as a spare drive or as part of the logical drive.

If a local spare drive has been added

The spare drive will be marked in the front view.

If member drives have been added

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

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

Expanding the Size of a Logical Drive (EonStor DS subsystems only)

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

When All Disk Capacity Has Been Used

You cannot expand a logical drive if all disk drive capacity has been used up for the logical drive. In that case, there are two options:

- You may add more disk drives.
- You may copy and replace member disk drives with larger capacity drives, and then use the additional capacity to expand the logical drive following steps in this section.

You must replace all member drives.

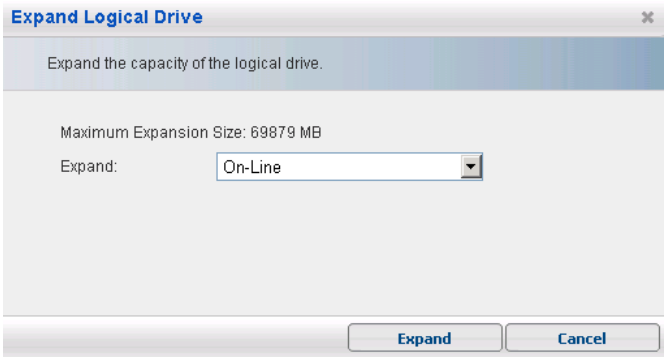
Go To

EonStor DS subsystems: SANWatch Home > Device sidebar > Device List > device name > Logical Volumes > LV name > Logical Drives > Tasks corner

Steps

Click Expand Logical Drive in the Tasks corner.

The Expansion screen will appear.



Select the initialization mode and click Expand.

Expand Size The available size is automatically calculated by (Total capacity) – (Current logical drive capacity).

Execute Specifies whether accessing the logical drive is available

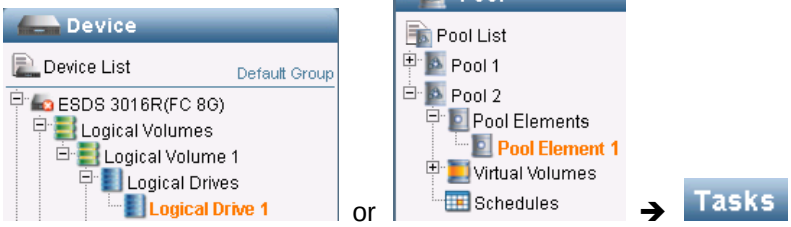
Expand (Initialization)	during initialization (On-Line) or not available (Off-Line). Note that in On-Line initialization, read/write performance to the logical drive will decrease because of the background initialization process.

Configuring Logical Drives or Pool Elements

Go To

EonStor DS subsystems: SANWatch Home > Device sidebar > Device List > device name > Logical Volumes > LV name > Logical Drives > LD name > Tasks corner

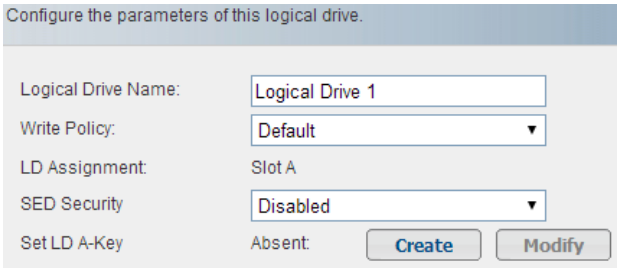
ESVA subsystems: SANWatch Home > Pool sidebar > Pool List > pool name > Pool Elements > PE name > Tasks corner



Configuring Properties

Click Configure Logical Drive (for EonStor DS subsystems) or Configure Pool Element (for ESVA subsystems) in the Tasks corner.

Change the parameters in the screen.



Logical Drive Name or Pool Element Name (EonStor DS subsystems only)	Specifies the name for this logical drive.
Write Policy (EonStor DS subsystems only)	Changes the write policy: Write-back (default) or Write-through. For detailed descriptions, see below.
LD Assignment (EonStor DS subsystems only)	The option cannot be modified because LD and its LV should be managed by the same controller. To change the LV's controller, select it in the Device sidebar, and click Configure Logical Volume in the Tasks corner.
SED Security (EonStor DS subsystems only)	Enhances data security with SED for all logical drives on your subsystem. Once enabled, all LDs will be SED-protected, therefore this mechanism is

called "global key."

Before enabling this option, first create a SED authentication key at SANWatch Home > Device sidebar > Device List > device name > Tasks corner > System Settings > Drive-Side tab.

Set LD A-Key (EonStor DS subsystems only)

Creating a global key (at SANWatch Home > Device sidebar > Device List > device name > Tasks corner > System Settings > Drive-Side tab > SED Authentication Key) will disable and hide this option here.

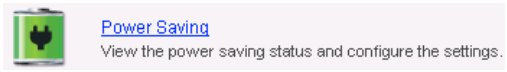
Enhances data security with SED using a "local key" for this logical drive. SED security will be enabled whenever a "local key" is created and imported. SED security using local keys will become ineffective after system reboots; Enabling it requires you to import the key file or password every time the subsystem reboots.

Write Back vs. Write Through

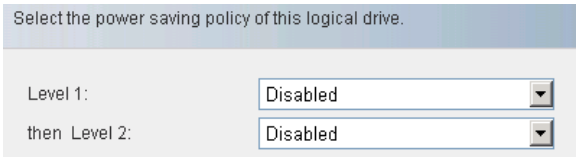
- When “Write-back” is “Enabled,” the write requests from the host will be held in cache memory and distributed to disk drives later. Write-back caching can dramatically improve write performance by caching the unfinished writes in memory and letting them be committed to drives in a more efficient manner. In the event of power failure, a battery backup module can hold cached data for days (usually 72 hours).
- When “Write-back” is “Disabled” (i.e., the Write-through is adopted,) host writes will be directly distributed to individual disk drives. The Write-through mode is safer if your controller is not configured in a redundant pair and there is no battery backup or UPS device to protect cached data.

Configuring Power Savings

Click Power Saving in the Tasks corner.



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

You may also configure the waiting period for switching to the power saving mode.

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

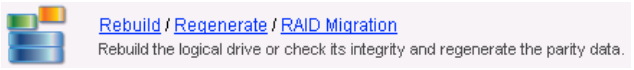
If you want to configure the power saving levels for the entire device, go to SANWatch Home > Device sidebar > Device List > device name > Tasks corner > System Settings > Drive-Side tab > Power Saving

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 applies to RAID level 1 or above and checks if data inconsistency or error has occurred with data parity.

Click Regenerate in the Tasks corner.



The parity data will be regenerated.

Scanning Logical Drives or Pool Elements

Go To

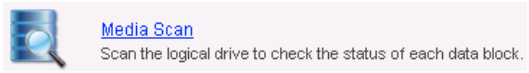
EonStor DS subsystems: SANWatch Home > Device sidebar > Device List > device name > Logical Volumes > LV name > Logical Drives > LD name > Tasks corner

ESVA subsystems: SANWatch Home > Pool sidebar > Pool List > pool name > Pool Elements > PE name > Tasks corner

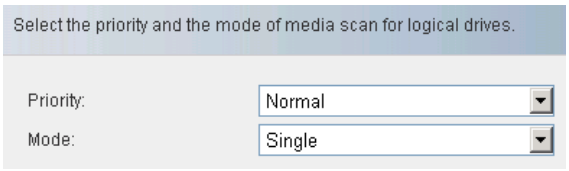
or

Steps

Click Media Scan in the Tasks corner.



The scan configuration window will appear.



Parameters

Priority	The higher the priority, the faster the scanning but the system performance will decrease.
Mode	Scans once (Execution Once) or continuously.

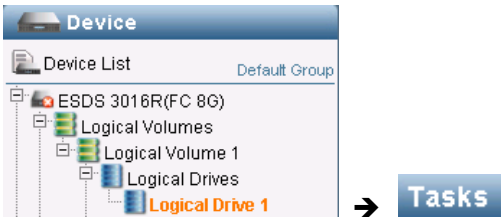
Migrating Logical Drive between RAID 5 and RAID 6 (EonStor DS subsystems only)

Migration allows you to change the RAID level of a logical drive to another. You may need to add or delete member drives due to the minimum required number of drives for a RAID level.

> Migrating works only for logical drives with RAID 5 or RAID 6 level.
> You cannot migrate a logical drive if it is already part of a logical volume.
> In order to migrate from RAID 5 to RAID 6, you need at least one available drive.

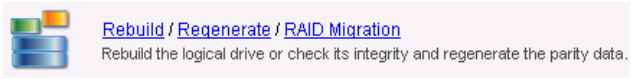
Go To

SANWatch Home > Device sidebar > Device List > device name > Logical Volumes > LV name > Logical Drives > LD name > Tasks corner

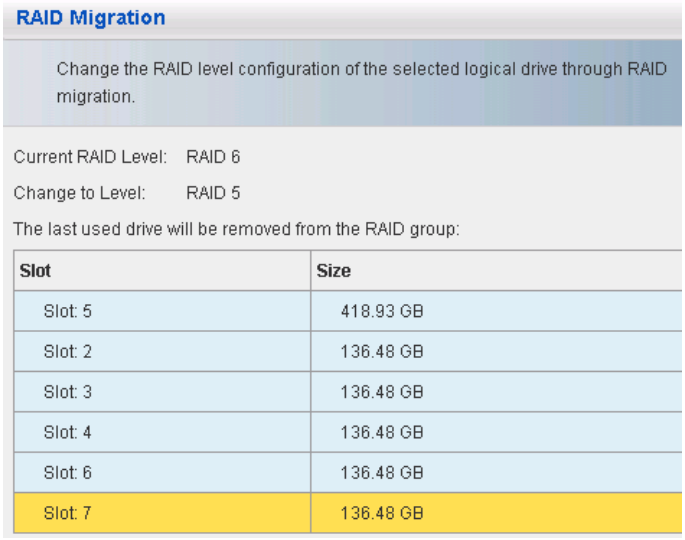


Steps

Click on RAID Migration

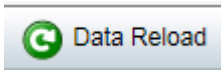


Current RAID level will show.



4. Click on the Migrate button.

5. Click on Data Reload to refresh drive statuses


Data Reload

Rebuilding a Logical Drive or Pool Element

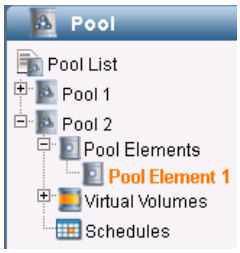
> The Rebuild menu is available only when a logical drive or pool element is in a Degraded state due to drive failure(s).

Go To

EonStor DS subsystems: SANWatch Home > Device sidebar > Device List > device name > Logical Volumes > LV name > Logical Drives > LD name > Tasks corner

ESVA subsystems: SANWatch Home > Pool sidebar > Pool List > pool name > Pool Elements > PE name > Tasks corner

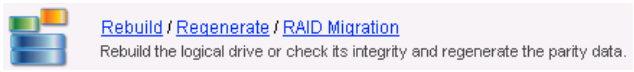
or



➔ Tasks

Steps

Click Rebuild in the Tasks corner.



Select the logical drive or pool element that is in a degraded state and click Rebuild.

If the logical drive or pool element does not go back to healthy state after rebuilding, remove it and create a new one.

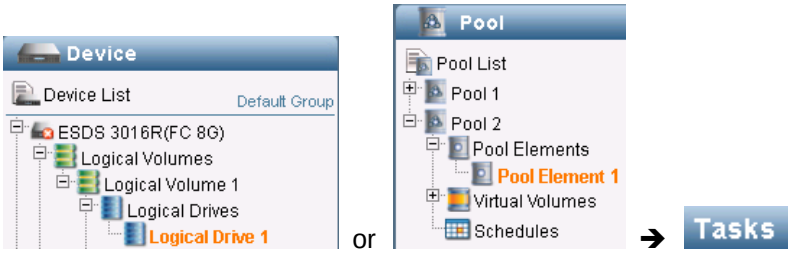
Restarting a Logical Drive or Pool Element

If you need to shut down a logical drive before moving it (all member drives) into another enclosure, or if a pool element has gone offline or has been locked, you might need to restart it.

Go To

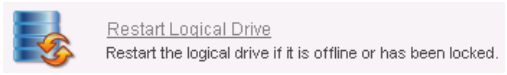
EonStor DS subsystems: SANWatch Home > Device sidebar > Device List > device name > Logical Volumes > LV name > Logical Drives > LD name > Tasks corner

ESVA subsystems: SANWatch Home > Pool sidebar > Pool List > pool name > Pool Elements > PE name > Tasks corner



Steps

Click Restart Logical Drive or Restart Pool Element in the Tasks corner.



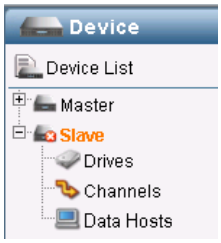
Configuring Remote Pool Element (ESVA subsystems only)

You may assign a pool element to another hardware device so that the remote device can extend its capacity and use the pool element as part of its own pool.

Note To use this feature, the hardware device must be connected and online.

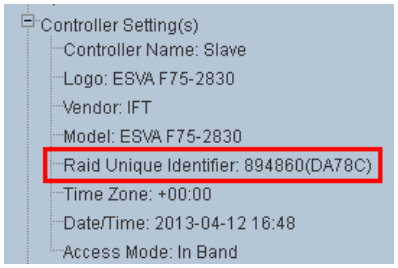
Step 1: Obtaining the Device ID and Channel IP Address

In the Device sidebar of SANWatch, click the target device to which the pool will be assigned remotely.



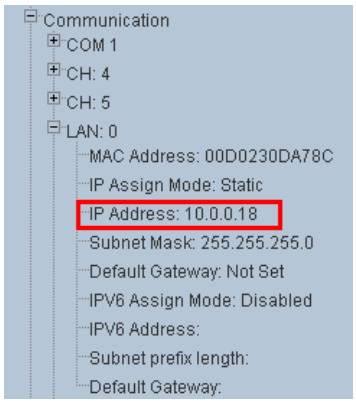
Click System Information in the Tasks corner.

Select the Configuration List tab and go to Controller Setting(s) > RAID Unique Identifier.



Copy the first half of the Identifier (for example, 894860).

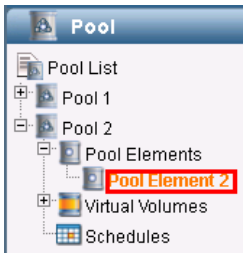
Go to the Communication > LAN > IP Address and copy the IP address.



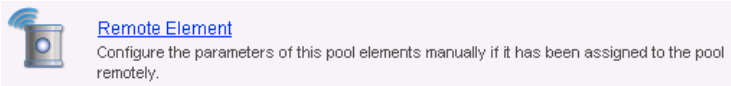
Step 2: Configuring Remote Pool

Go to SANWatch Home > Sidebar, locate the pool element you want.

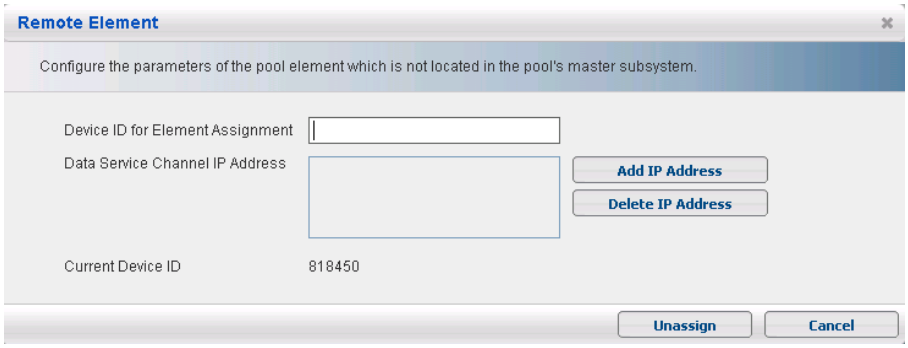
Element



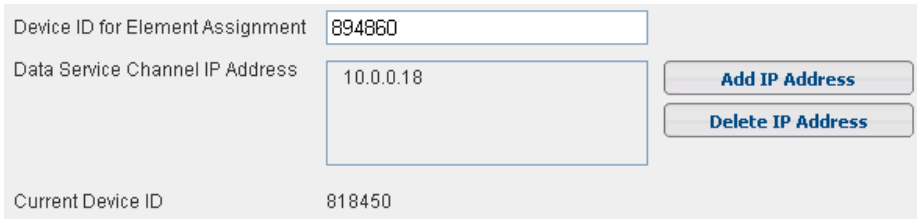
Click Remote Element in the Tasks corner.



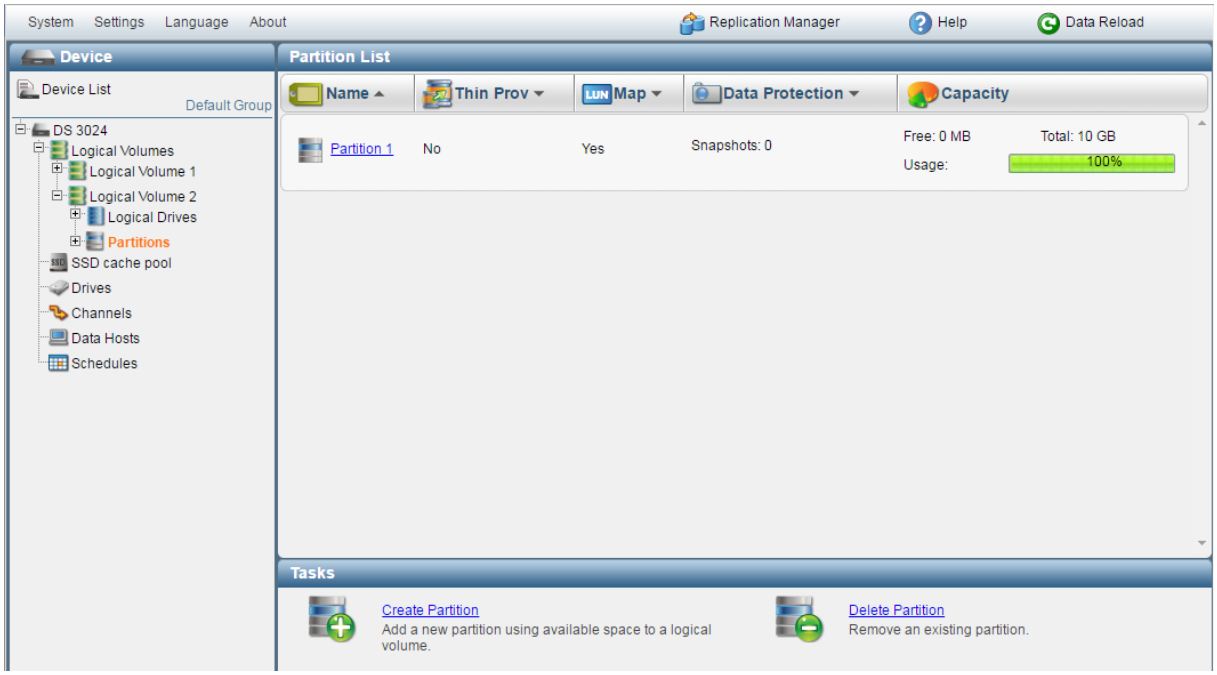
The Remote Element window will appear.



Enter the remote device ID and add the IP address you just copied.



Working with the Partitions or Virtual Volumes View



This chapter describes the overall parameters of partitions (for EonStor DS subsystems) or virtual volumes (for ESVA subsystems) included in a logical volume (for EonStor DS subsystems) or pool (for ESVA subsystems).

General Rules

Maximum Number

The maximum number of partitions or virtual volumes are:

- Per RAID: 80
- Per JBOD: 40

Note on Over-Provisioning

Over-provisioning is a situation that may occur inside a thin-provisioned storage system. It means that the available physical capacity is actually LESS than the logical capacity allocated for applications. Over-provisioning has the advantage of maximizing capacity utilization, but also has the risk of I/O failure when the actual usage reaches the physical limitation, which might crash the application or even the host.

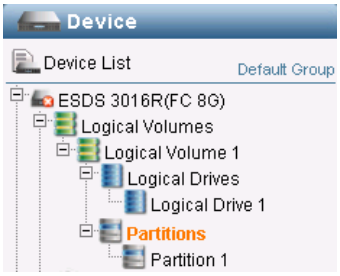
Over-provisioning is allowed but not recommended. If there is any possibility for allocating or wasting out all the spaces (over-provisioning), a warning message will be generated but you may still be able to create partitions (for EonStor DS subsystems) or virtual volumes (for ESVA subsystems).

Viewing the List of Partitions or Virtual Volumes

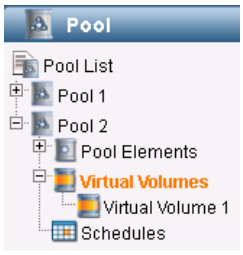
All partition or virtual volume information can be accessed from the sidebar in the user interface.

Go To

EonStor DS subsystems: SANWatch Home > Device sidebar > Device List > device name > Logical Volumes > LV name > Partitions
ESVA subsystems: SANWatch Home > Pool sidebar > Pool List > pool name > Virtual Volumes



or



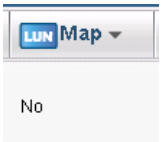
Steps

When you click the Partitions or Virtual Volumes tab in the left sidebar, the list of partitions or VVs and their parameters recognized by the system will appear.

Clicking the name of each partition or virtual volume will lead to detailed configuration page for the volume.

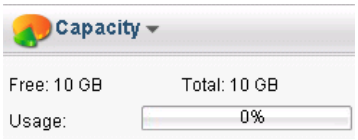
The Thin Prov tab (EonStor DS subsystems only) show whether thin provisioning was enabled on this partition.

The LUN Mapping tab shows whether this partition or virtual volume has been mapped to the host.



The Data Protection corner shows the number of snapshot images taken for this partition or virtual volume.

The capacity corner shows the total and available (free) capacity allocated for this partition or virtual volume.



To refresh the status (in case you want to make sure the status has been updated), click the *Data Reload* menu at the top bar.

Note If the Help screen does not appear, you might need to enable pop-up windows from the browser's configuration options.

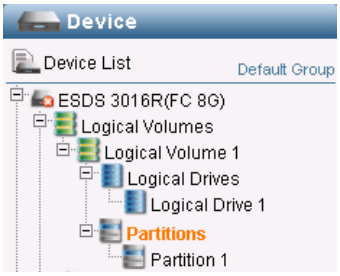
Creating a Partition or Virtual Volume

Note

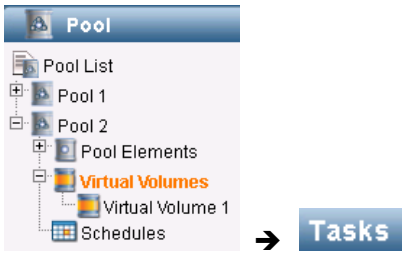
The maximum size of a single partition or virtual volume is 256TB (before firmware version 3.88) and 512TB (after firmware version 3.88). Make sure that the size of the logical volume or pool is in line (you cannot make the size of the partition or virtual volume larger than the size of the logical volume or pool). For the latest status, checking with technical support is recommended.

Go To

EonStor DS subsystems: SANWatch Home > Device sidebar > Device List > device name > Logical Volumes > LV name > Partitions > Tasks corner
ESVA subsystems: SANWatch Home > Pool sidebar > Pool List > pool name > Virtual Volumes > Tasks corner

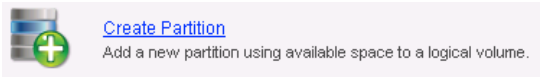


or

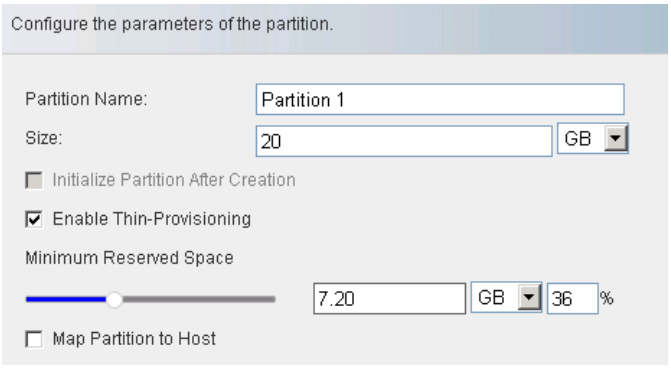


Steps

Click Create Partition (for EonStor DS subsystems) or Create Virtual Volume (for ESVA subsystems) in the Tasks corner.



The configuration window will appear.



Enter the name of the partition or virtual volume.

Enter the size and select the unit.

The size of a partition or virtual volume must be the multiples of 2MB.

Enable Initialization or Thin-Provisioning (mutually exclusive).

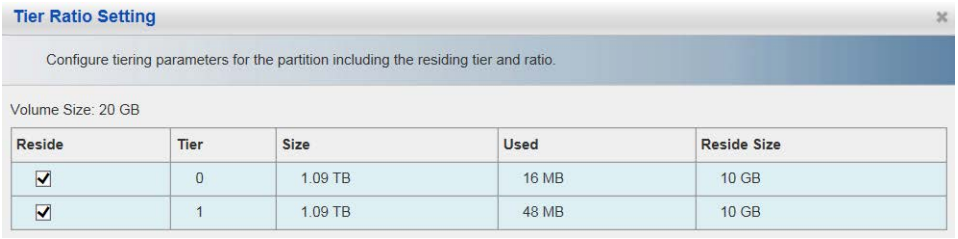
For more detailed description on thin provisioning, refer to the next section.

Set the minimum reserved amount.

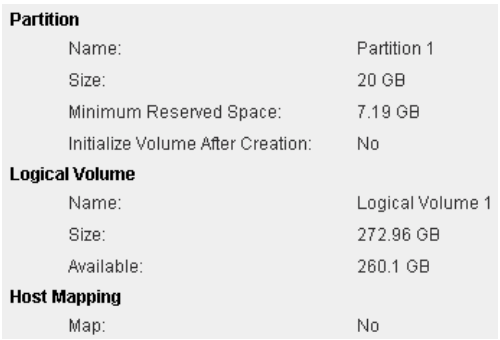
You may map the partition or virtual volume to the host here or do it later.

For details of mapping, refer to the instructions that follow.

Click Next. If you are creating a partition or VV on a tiered logical volume or pool, decide the residing tier and ratio.



Click Next. The summary will appear.



The partition or virtual volume will appear in the list.

Size

Specifies the size and unit of the partition or virtual volume. If Thin Provisioning is enabled, the total size of partitions or virtual volumes can exceed the size of the logical volume or pool.

The minimum size of a partition or virtual volume is 10GB.

Initialize Partition (or Virtual Volume) After Creation

When this option is enabled, the partition or VV's LBA addresses will be allocated consequentially for large and/or sequential I/Os. This is ideal for audio/video application such as media post-editing and video on-demand.

Thin Provisioning	Enables thin provisioning. Move the slide bar to set the percentage of the partition or VV capacity that will be physically allocated as a safe reserve. If the reserve reaches 100%, the partition or VV becomes fully-provisioned (all space is allocated from the virtual pool). For more information, refer to the next sections.
Map Partition (or Virtual Volume) to Host	Maps the partition or virtual volume to all host ports. If you want to select the host port, you may map it manually later. For more information, refer to the next sections.

About Thin Provisioning

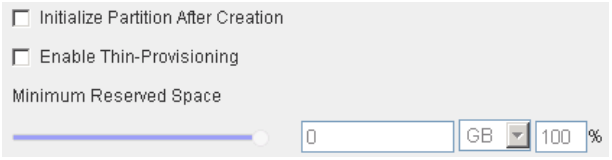
Thin provisioning allows you to allocate a large amount of virtual capacity for a logical volume or pool regardless of the physical capacity actually available. Actual space is used only when data writes occur. By automatically allocating system capacity to applications as needed, thin provisioning technology can significantly increase storage utilization. Thin provisioning also greatly simplifies capacity planning and management tasks. For more information, see the Infortrend website.

> Dynamically allocating capacity affects the overall performance. If performance is the top priority (such as in AV applications), we recommend you to disable thin provisioning (= use full provisioning).

Thin Provisioning Settings

Thin provisioning is configured during partition or VV creation in a logical volume or pool.

In the creation screen, thin provisioning options will appear in the lower half.

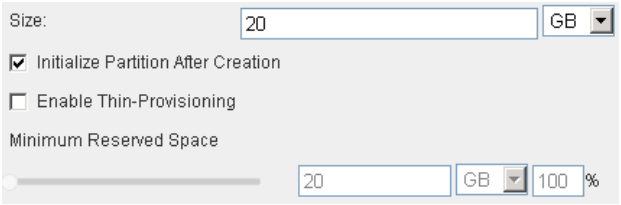


After the new partition or virtual volume has been created, create one or more notification thresholds to make sure that the administrator receives warning/critical messages before all of the logical volume or pool space will be used, and to give him or her ample time for expanding the size of the logical volume or pool.

> We recommend you to create multiple thresholds to stay on the safe side. (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 you uncheck “Enable Thin-provisioning,” thin provisioning will be disabled and all of the configured logical volume or pool size (in the below diagram’s case, 14GB) will be taken from the capacity actually available. The partition or VV will be created as a continuous physical space reserved only for the target application, and then will be initialized if the “Initialize Partition (or Virtual Volume) After Creation” box is checked (you may uncheck this option if you prefer).



Full provisioning is suitable for mission-critical applications with large amount of uninterrupted data, such as audio/video streams. Dynamically allocating space

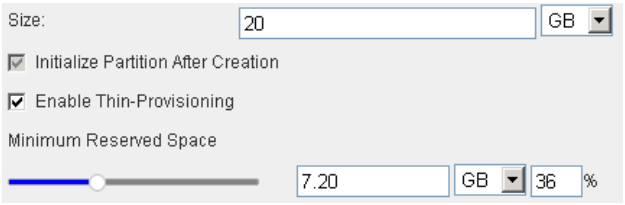
and expanding usable area slows the I/O performance down, therefore allocating a large physical capacity from the beginning optimizes the performance.

Case 2: Thin Provisioning

To enable thin provisioning, check the “Enable Thin-Provisioning” box and select the Minimum Reserved space using the slider.

When the application uses up the minimum reserved area, additional space will be taken from the rest of the logical volume or pool space and will be added to the partition or VV dynamically.

In this example, the actual logical volume size is 10GB but the partition is set at 20GB, larger than the available size. This is fine as long as the minimum reserved space (the actual physically allocated space) is smaller than the logical volume size: 7.20GB in this case.



The reserved space cannot exceed the actual available capacity.

Provisioning and Reserved Space

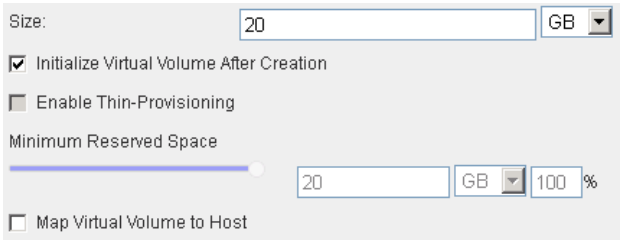
Here are the three patterns of provisioning/initialization combinations.

Options

- Initialize Partition (or Virtual Volume) After Creation: Initializes the partition or virtual volume content. This option becomes available only when Thin Provision is disabled (= Full Provision is enabled), because a partition or virtual volume must have its full capacity in physical storage space to be initialized.
- Enable Thin-Provisioning: When checked, thin-provisioning (physical partition or virtual volume capacity will be provided as required) will be enabled. When unchecked, full-provisioning (all of the partition or virtual volume capacity will be provided physically).
- Minimal reserve: The minimal physical capacity that will always be allocated to the partition or virtual volume. If the minimal reserve is set at 0%, the partition or VV does not have any real capacity allocated by default. If the minimal reserve is set at 100%, the real capacity of the partition or VV always matches the theoretical maximum (= becomes the same as full provisioning).

Full Provisioning with Initialization

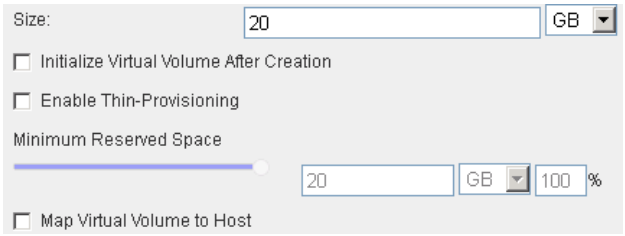
- Initialization + 100% minimal reserve



This configuration can reside in only one storage tier.

Full Provisioning without Initialization

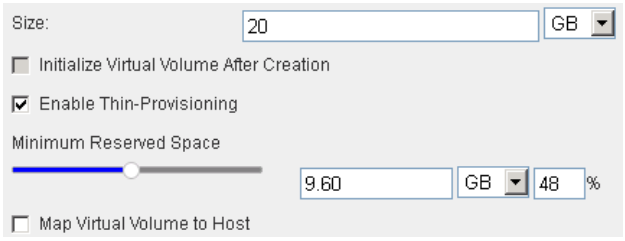
- Thin provisioning + 100% minimal reserve



This configuration is not allowed in multi-tiered LVs or pools.

Thin Provisioning with Minimal Reserve Space

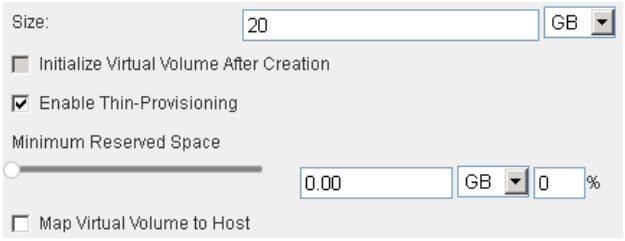
- Thin provisioning + 1-99% minimal reserve



This configuration is not allowed in multi-tiered LVs or pools.

Thin-Provisioning without Minimal Reserve Space

- Thin provisioning + 0% minimal reserve



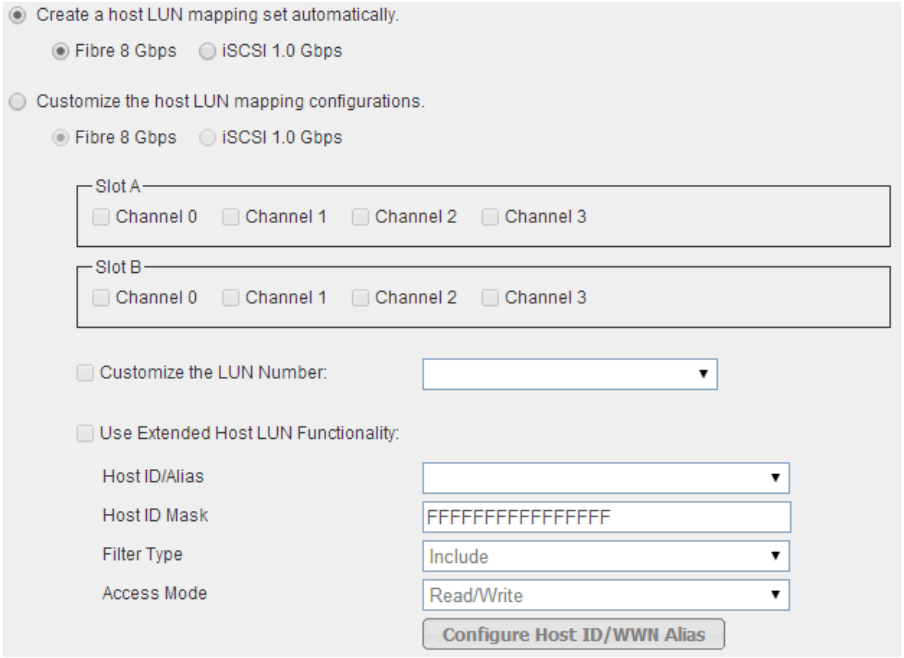
Mapping/Unmapping Partitions or Virtual Volumes to Host

Host LUN mapping is also a part of creating partitions (for EonStor DS subsystems) or virtual volumes (for ESVA subsystems).

Mapping Host LUN

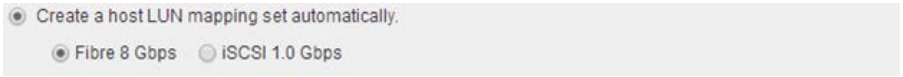
The Host Mapping Configuration Window

The diagram below shows the prompt for Fibre-channel models. For hybrid (Fibre and iSCSI) host models, you need to configure both settings. (Example: Hybrid models)



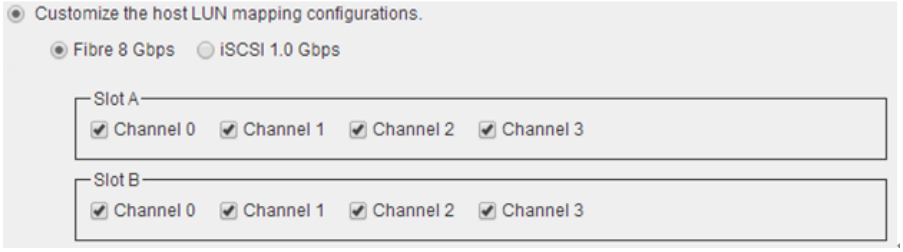
Automatic Configuration

If you let the system create LUN mapping automatically, check it. For hybrid models, you need to select the host type.

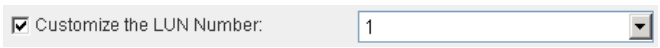


Manual Configuration

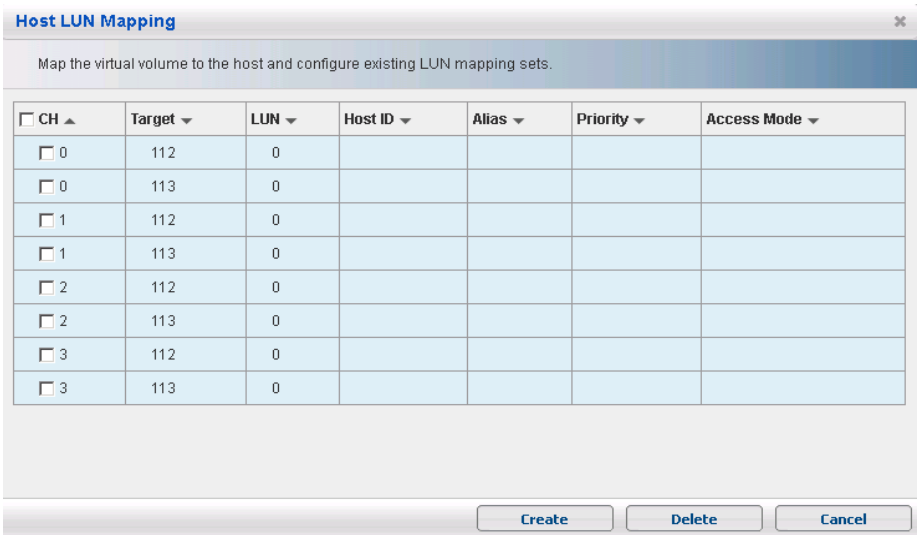
If you manually configure the LUN mapping, check the Customize option and select the Channels.



Select the LUN number from the drop-down list.



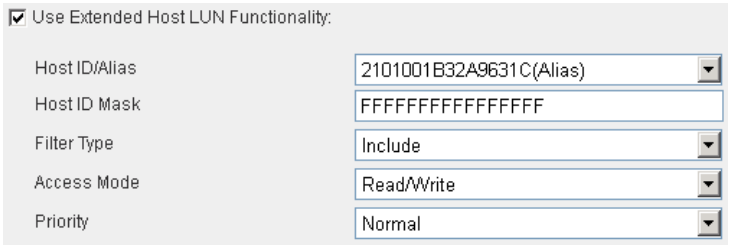
Click OK. The list of Host LUN Mapping configurations will appear in the window.



Using Extended LUN Mapping (Fibre Channel)

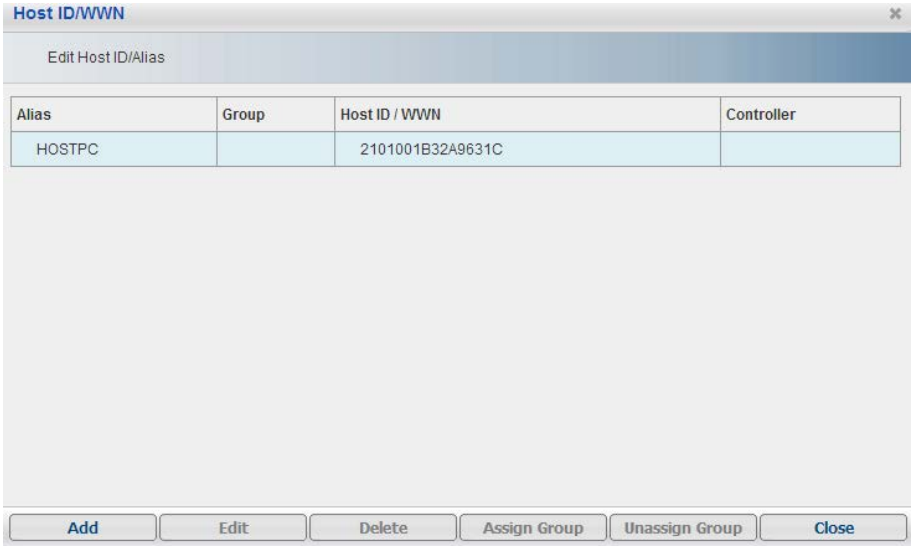
Extended LUN Mapping is available only for manual configuration.

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

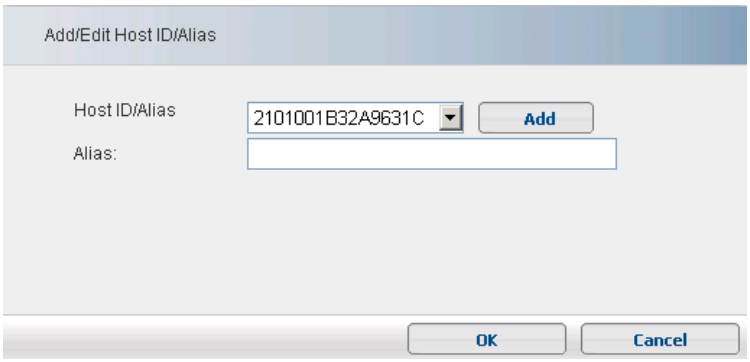


- Host ID/Alias: Specifies the host ID, referring to WWPN port name. You can also see OUI (Organizationally Unique Identifier) of a system: “00:D0:23” oui. Note: Avoid checking the OUI while mapping host LUN.
- Host ID Mask: Works as a prefix mask in hexadecimal format.
- Filter Type: Specifies whether to allow (include) WWNs or to forbid (exclude) them from accessing after filtering.
- Access Mode: Specifies the access right of LUN mapping for the host: read-only or read-write.
- Priority: Specifies access priority. For example, high priority can be assigned to volumes serving applications and lower priority to volumes storing archives or user data.

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.

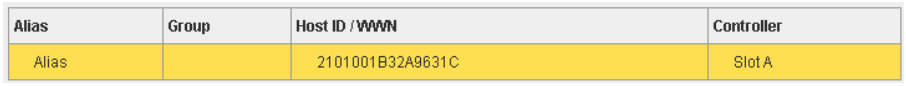


Click OK. Repeat the above process to create more LUN mappings especially if you have multiple HBA ports accessing the same virtual volume (e.g., in high-availability application).

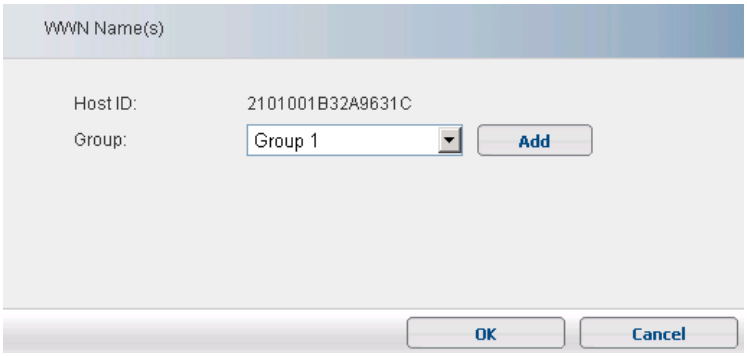
Assigning a WWN to a Group

A WWN group allows multiple hosts to be accessed in a single mask, which becomes useful in a clustered storage server environment.

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

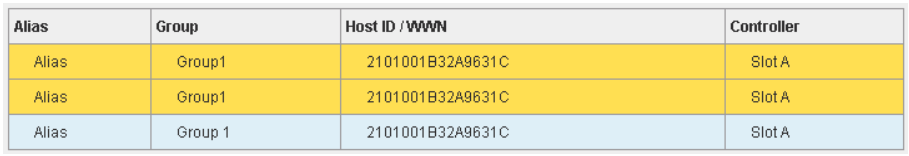


Click Assign Group and select the group from the drop-down menu.



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

The group name will appear in the list.



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

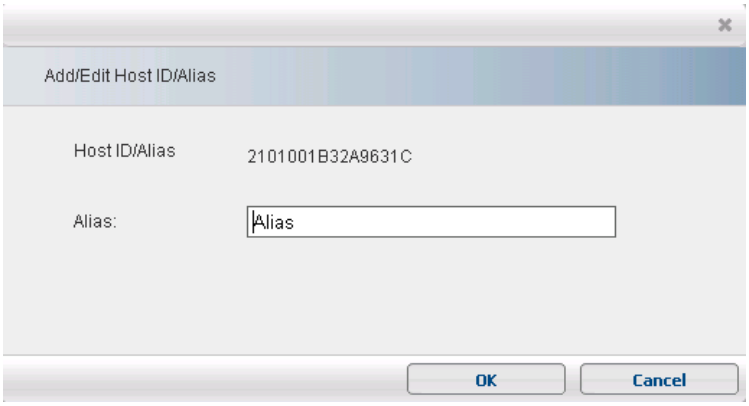
To unassign a WWN from a group, click Unassign Group.

Deleting a WWN Name from the List

Highlight a WWN in the list and click Delete.

Changing the Alias name

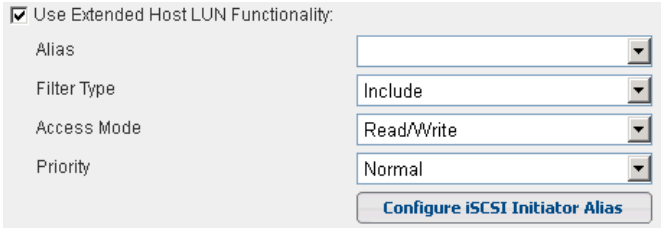
To edit the alias name of the WWN, click Edit and enter the new name.



Using Extended LUN Mapping (iSCSI Channel)

Extended LUN Mapping is available only for manual configuration.

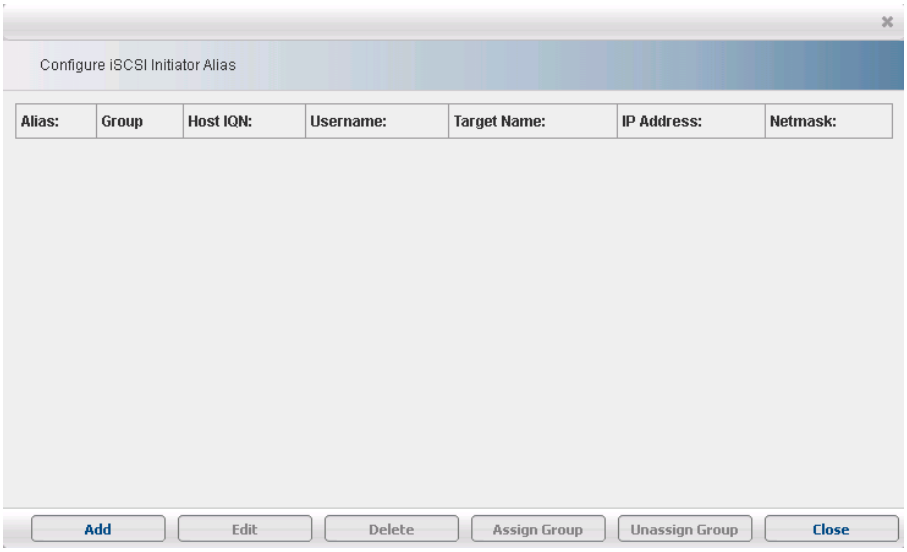
Click Use Extended LUN Functionality and enter the parameters.



- Alias: Specifies a pre-configured iSCSI initiator instance. To create a new initiator alias, click the Configure iSCSI Initiator Alias button.
- Filter Type: Specifies whether to allow (include) initiators or to forbid (exclude) them from accessing after filtering.
- Access Mode: Specifies the access right of LUN mapping for the host: read-only or read-write.
- Priority: Specifies access priority. For example, high priority can be assigned to partitions or virtual volumes serving applications and lower priority to partitions or virtual volumes storing 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: Infortrend's storage IQN is composed of the system serial number and 3 more digits in the following format:
  iqn.2002-10.com.infortrend:raid.snXXXXXX.XXX
  6 digits of serial number follows "sn."
  The next 3 digits are: channel number, host ID, LD ownership.
  The LD ownership digit is either "1" or "2" where "1" indicates Controller A and"2" indicates Controller B. The IQN is in accordance with how you map your 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 easy to remember name for the iSCSI initiator.
- 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 setting. The User Password (One-way, from initiator) has to 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) has to 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 sometimes share the same IQN.

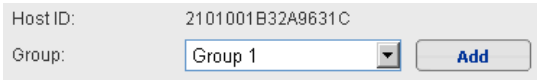
Click OK. Repeat the above process to create more LUN mappings especially if you have multiple HBA ports accessing the same virtual volume (e.g., in high-availability application).

Assigning an Initiator to a Group

A group allows multiple host LUNs to be accessed in a single mask, which becomes 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

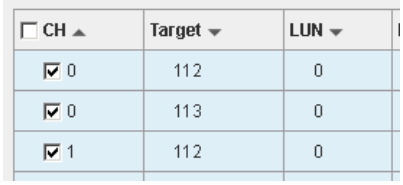
Highlight an initiator in the list and click Delete.

Editing the Initiator

To edit the configuration of an initiator, click Edit.

Unmapping Host LUN

Select the host LUN you want to unmap.



Click Delete.

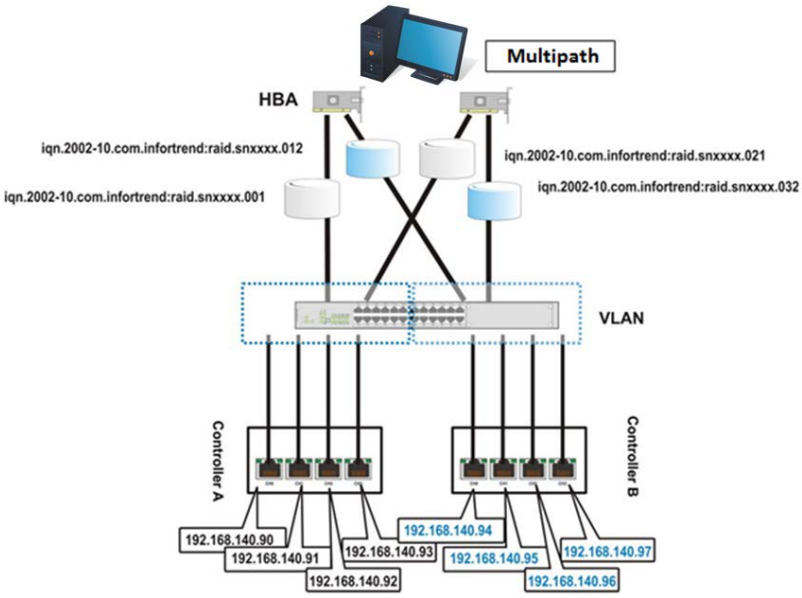
Managing LUN Mapping on the Host Side	Select the partition or virtual volume whose LUN mappings you want to manage, click the Help icon at the top-right corner, and then search for " Managing LUN Mapping on the Host Side" for detailed instruction.

Notes

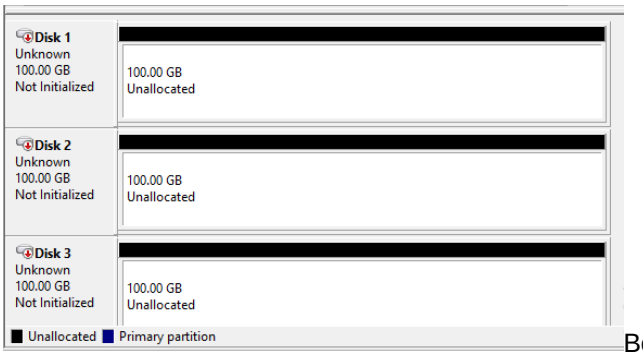
- By mapping a partition or virtual volume to multiple ports on multiple HBAs, you acquire path redundancy. To manage fault-tolerant paths to a single volume, you should have EonPath driver installed on Windows servers, Device Mapper on Linux, and Solaris MPXIO on Solaris platforms (Sparc machines).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

Working with Multipath

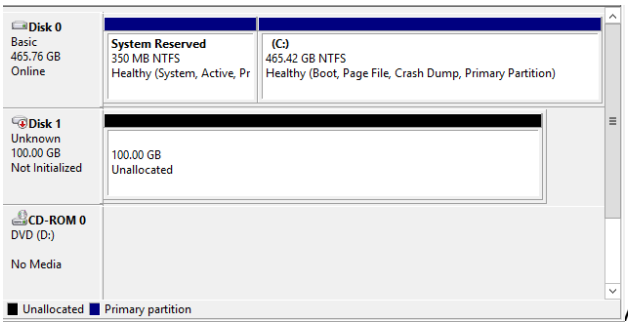
Multi-path I/O functionality can recognize and manage redundant data paths to an individual volume. It ensures greater reliability through the path failover mechanism in the event of cabling component failures.



Before and After enabling MPIO on Windows server



Before



After

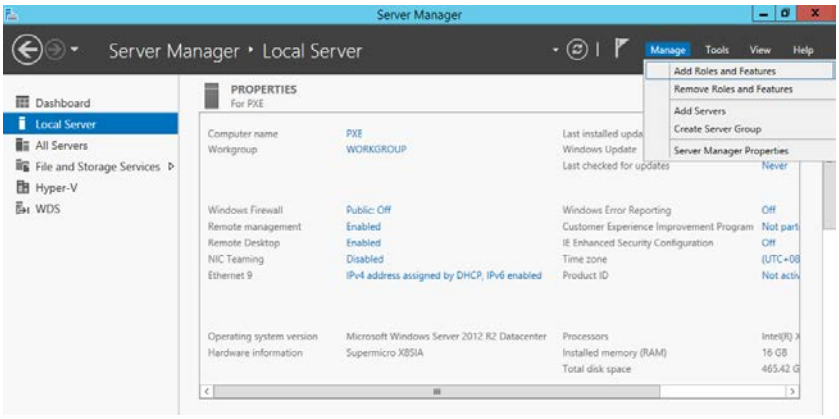
For Linux OS

On Linux/Unix platforms, it is recommended using the native MPIO driver. For detailed configurations, refer to the application note.

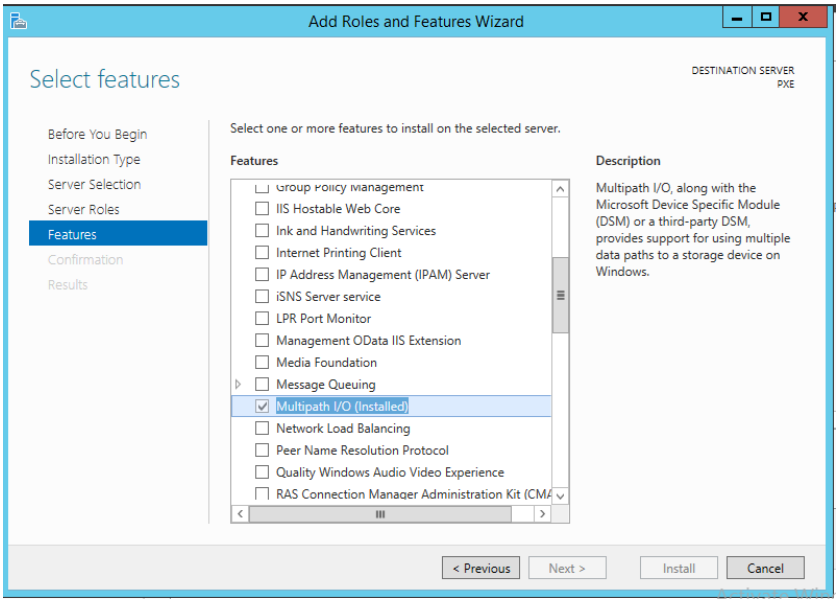
Enabling Linux Device Mapper Multipath on EonStor®

Enabling the MPIO on Windows server 2012 R2

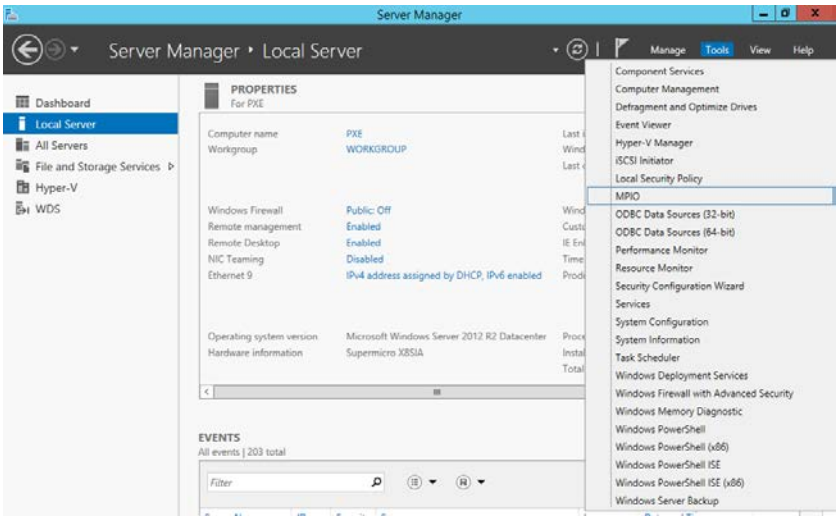
1. Server Manager → Manage → Add Roles and Features



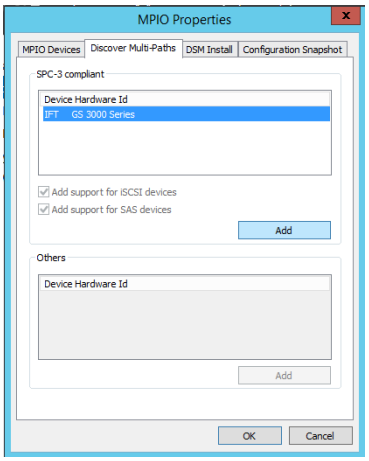
2. Click Next until the Features step and check the Multipath I/O. We have already installed the features so it shows (installed).



3. Server Manager → Tools → MPIO

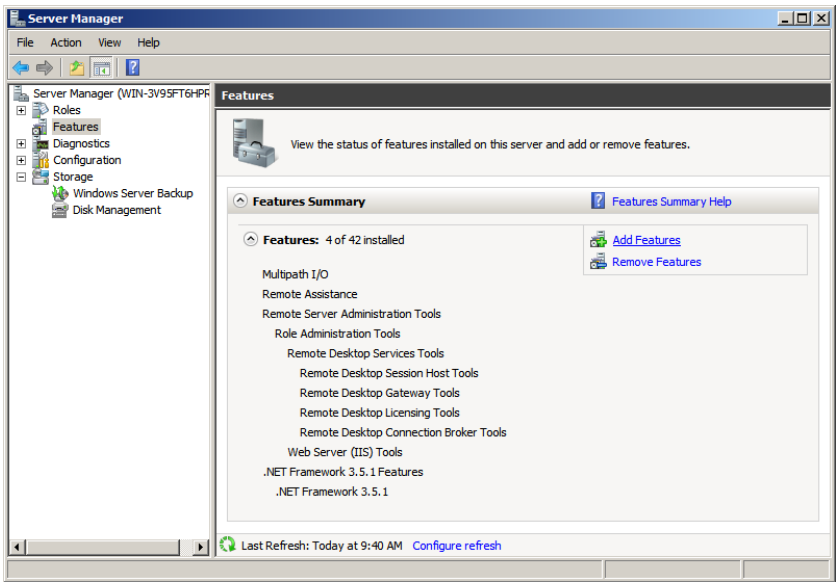


4. You will find the storage device shows in the Discover Multi-Paths tab. Click Add and reboot the server to enable MPIO.

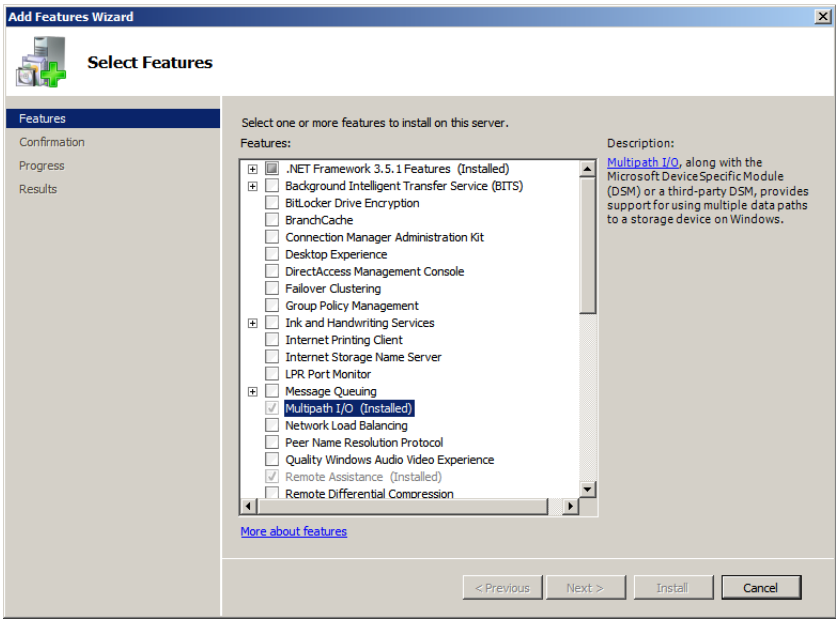


Enabling the MPIO on Windows server 2008 R2

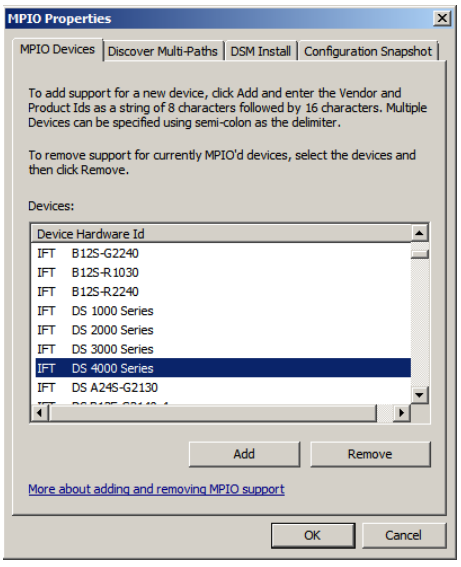
1. Server Manager → Features → Add Features



2. Check the Multipath I/O. We have already installed the features so it shows (installed).



3. Click Start and type “MPIO” to launch the MPIO Properties panel. Click on the Discover Multi-Paths tab and check the box for “Add support for iSCSI devices”. Click Add and reboot the system.

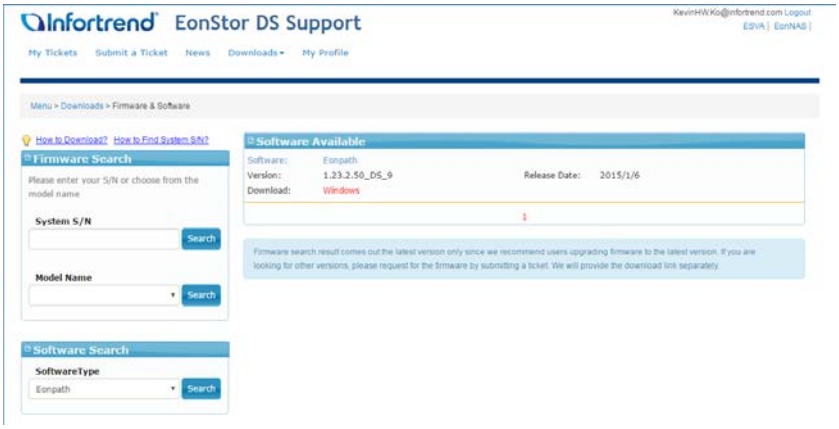


Installing EonPath (Multipathing) Driver (only for Windows 2003 and before)

1. Download EonPath from the support site

   http://support.infortrend.com/

   Download → Firmware & Software



2. Execute the Setup file to install. Restart the computer when the installation is complete.

3. You can configure the setting of EonPath via SANWatch.

   SANWatch Home > Device sidebar > Device List > device name > Data Hosts > Tasks corner > EonPath

   For more information about EonPath see Working with Hosts.

Deleting Partitions or Virtual Volumes

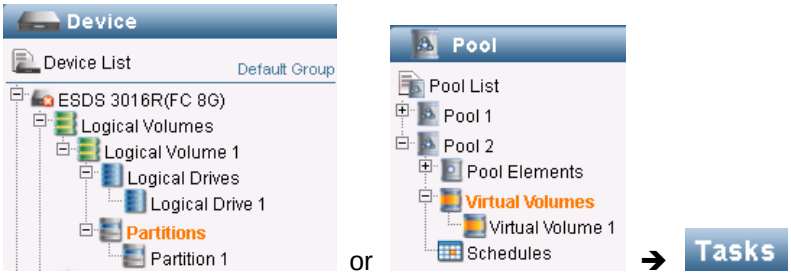
To delete a partition or virtual volume, you need to delete the following features if they have been applied.

- Delete Snapshot images
- Delete Partition Pair or Volume Pair relationships
- Delete LUN mappings

Deleting a partition or virtual volume will also delete all of its data.

Go To

EonStor DS subsystems: SANWatch Home > Device sidebar > Device List > device name > Logical Volumes > LV name > Partitions > Tasks corner
ESVA subsystems: SANWatch Home > Pool sidebar > Pool List > pool name > Virtual Volumes > Tasks corner



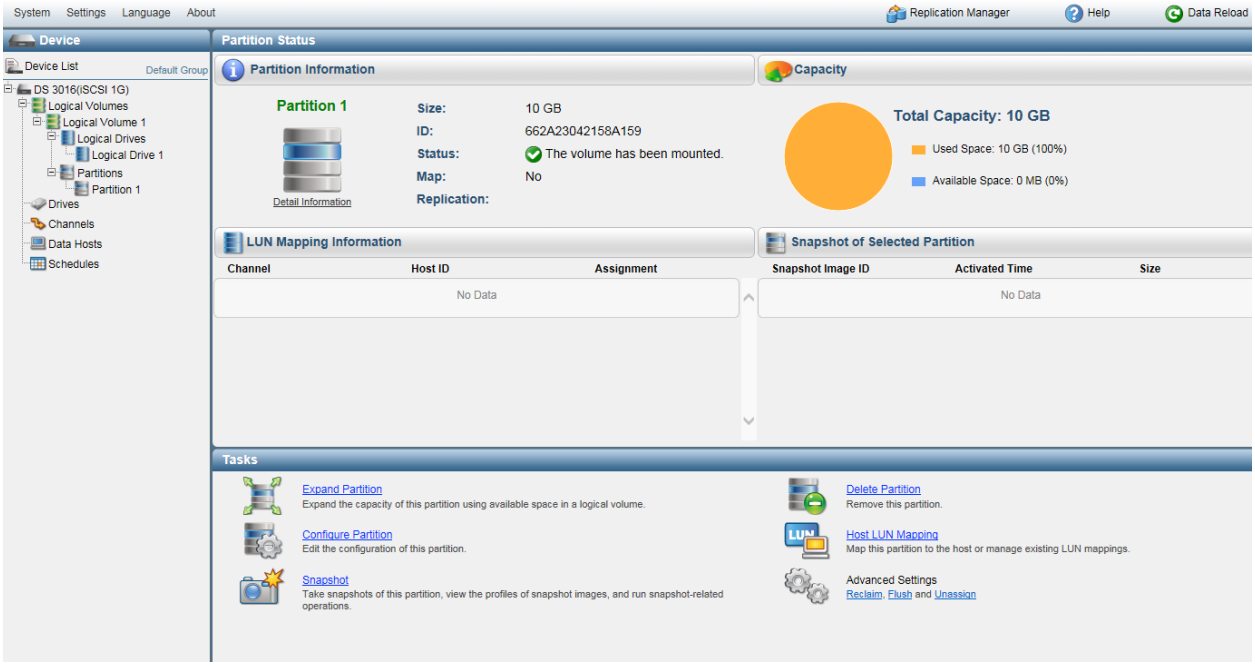
Steps

Click Delete Partition or Delete Virtual Volume in the Tasks corner.

Select the partition or virtual volume and click Delete.

A warning message will appear. Click Yes to proceed.

Working with Partitions or Virtual Volumes



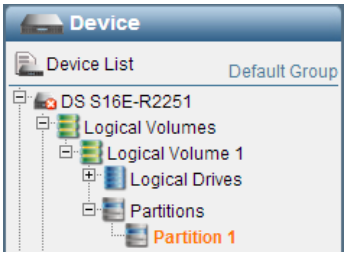
This chapter describes how to view status and parameters of a partition (for EonStor DS subsystems) or virtual volume (for ESVA subsystems), expand or shrink its size, configure host LUN, take snapshot images, and configure advanced settings such as database flush and reclaiming unused space.

Viewing Partition or VV Status

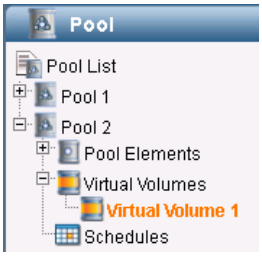
The status of each partition or virtual volume is summarized in the Partition Information or Virtual Volume Information page, where you can quickly grasp the configuration, performance, storage capacity.

Go To

EonStor DS subsystems: SANWatch Home > Device sidebar > Device List > device name > Logical Volumes > LV name > Partitions > partition name
ESVA subsystems: SANWatch Home > Pool sidebar > Pool List > pool name > Virtual Volumes > VV name

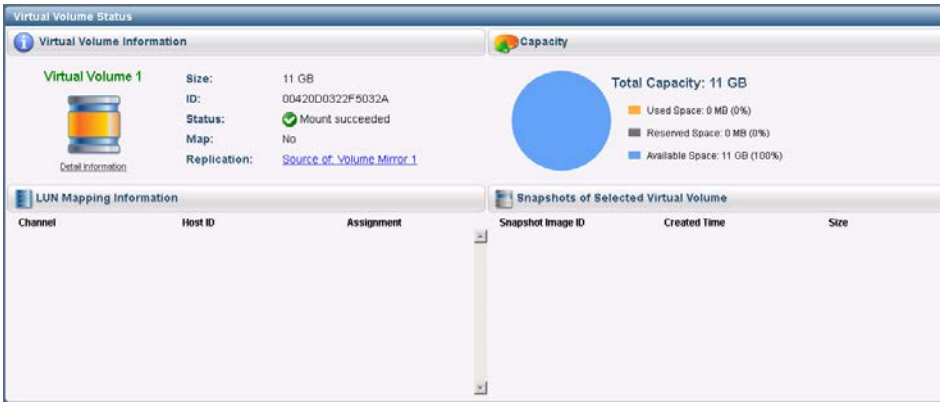


or



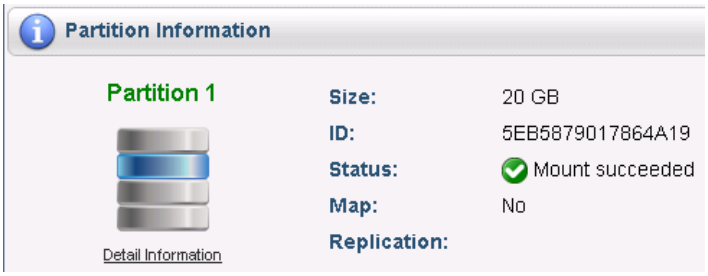
Viewing the Partition or VV Information

The partition or VV status will be summarized in the Status corner.



Partition or VV Configurations

The basic partition or virtual volume configurations and overall system status will be listed in the Partition Information or Virtual Volume Information corner. You can see the size (capacity), partition ID, status, mapping information, and replication information (if you click the link, the Replication Manager will open up to show you detailed configurations of data replication services).

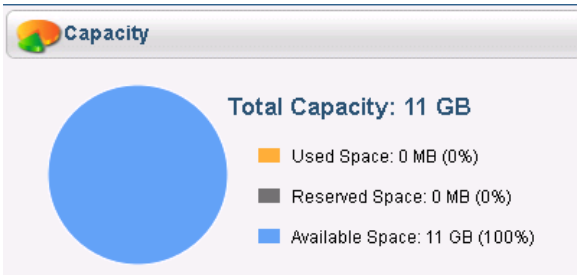


Click the Detail Information link below the partition or virtual volume icon to view more parameters, such as created time and current tasks in progress and

storage tiering status. Click Refresh to update the status.

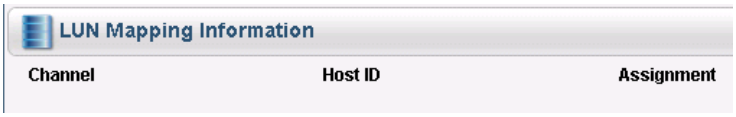
Capacity

See the amount and ratio of used (configured) capacity and the remaining (available) capacity. You may also view the ratio of capacity used for data service (snapshot, remote replications).



LUN Mapping Information

Shows the current LUN mapping status (if available). You can create or configure host LUN mapping from the Tasks corner, Host LUN Mapping icon.



Snapshot Information

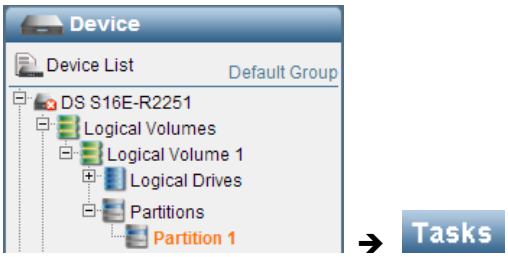
Shows the current list of snapshot images for the partition or virtual volume. You can create a new snapshot image from the Tasks corner, Snapshot icon.

Expanding Partitions (EonStor DS subsystems only)

Expanding the capacity of a partition is available only when its partition or volume has available capacity.

Go To

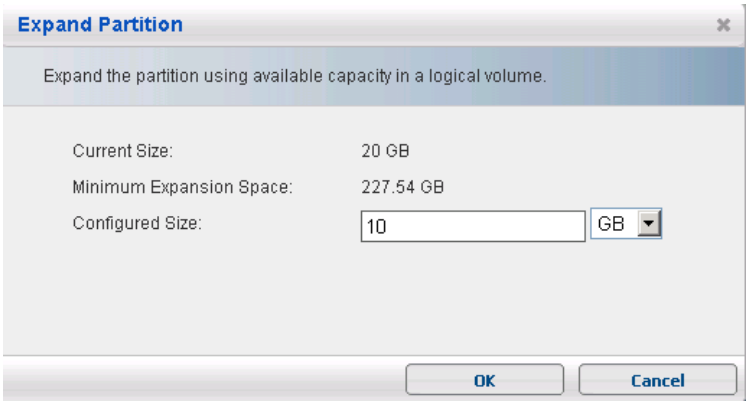
SANWatch Home > Device sidebar > Device List > device name > Logical Volumes > LV name > Partitions > partition name > Tasks corner



Steps

Click Expand Partition in the Tasks corner.

The expansion setting window will appear. Specify the capacity you want to expand.



Expansion will begin. When it is completed, check that the size of the partition has increased by the specified amount.

Reclaiming Unused Partition Space (EonStor DS subsystems only)

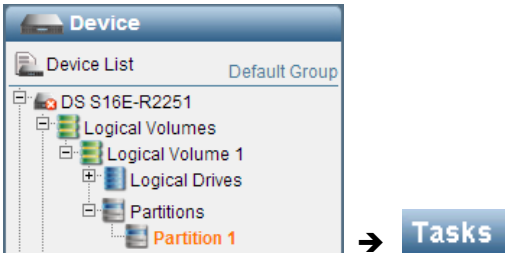
In thin-provisioned partitions, you cannot reuse the space of deleted data unless you reclaim it manually. The storage subsystem is aware of the actual space usage in the host and will optimize data allocation in the subsystem.

Note

- To reclaim unused space, the partition or virtual volume has to be mapped to the host.
- The Partition Space Reclaim function is only supported in Microsoft Windows or Linux environments.

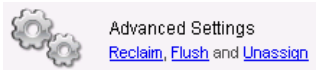
Go To

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

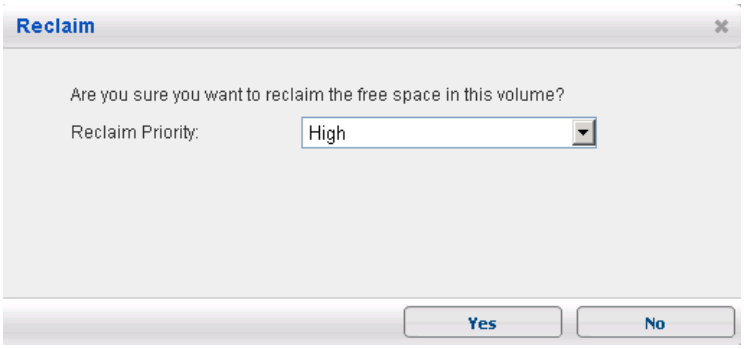


Steps

Click *Reclaim* in the Advanced Settings in the Tasks corner.



The Reclaim window will appear. Select the priority and click OK.



- High Priority: Reclaim will be processed efficiently but might affect the system performance.
- Normal Priority: Follows the original reclaim setting that might be processed slowly but has less chance of affecting the system performance.

If a reclaim process is already ongoing, you need to wait until it is completed or stop the existing process and restart it.

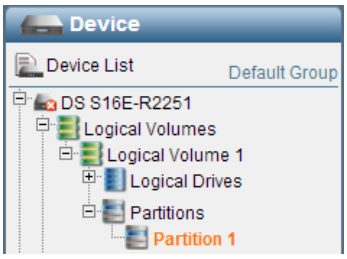
Configure Host LUN Mappings

Host LUN mapping is also a part of creating partitions or virtual volumes.

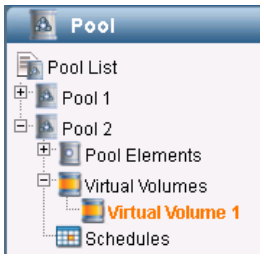
Go To

EonStor DS subsystems: SANWatch Home > Device sidebar > Device List > device name > Logical Volumes > LV name > Partitions > partition name > Tasks corner

ESVA subsystems: SANWatch Home > Pool sidebar > Pool List > pool name > Virtual Volumes > VV name > Tasks corner



or



➔ Tasks

Mapping/Unmapping Host LUN

Before configuring LUN mapping, go to:

EonStor DS subsystems: SANWatch Home > Device sidebar > Device List > device name > Logical Volumes > LV name > Partitions

ESVA subsystems: SANWatch Home > Pool sidebar > Pool List > pool name > Virtual Volumes

Click the Help icon at the top-right corner, and search for the "Mapping/Unmapping Partitions or Virtual Volumes to Host " section for detailed instructions on LUN mapping configurations.

Managing LUN Mapping on the Host Side

In this section, an example of configuring LUNs on the host side is shown for Windows, Linux, and Solaris environment.

Notes

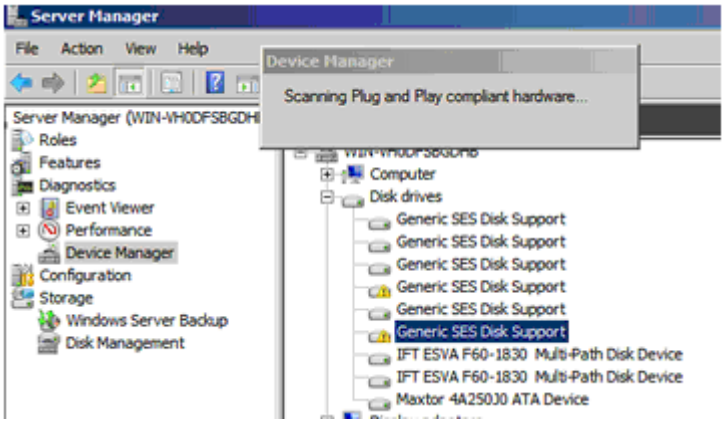
If you are unable to find any LUN from the host side, try to change the type of SES device by doing the following:

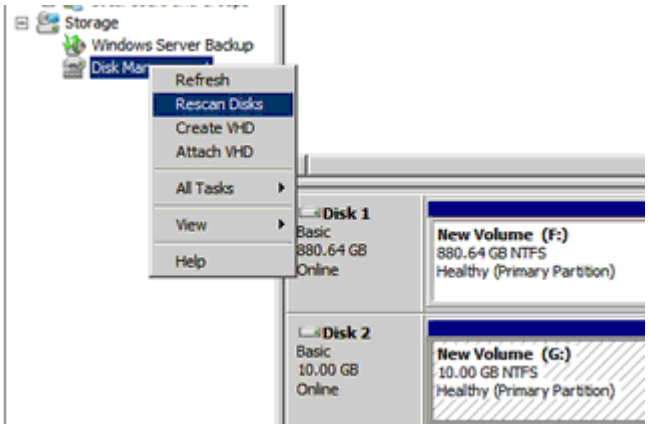
Go to SANWatch Home > Device sidebar > Device List > device name > Tasks corner > System Settings > Host-side tab, and then choose "No Device Present (Type=0x7F)" from the Peripheral Device Type drop-down menu.

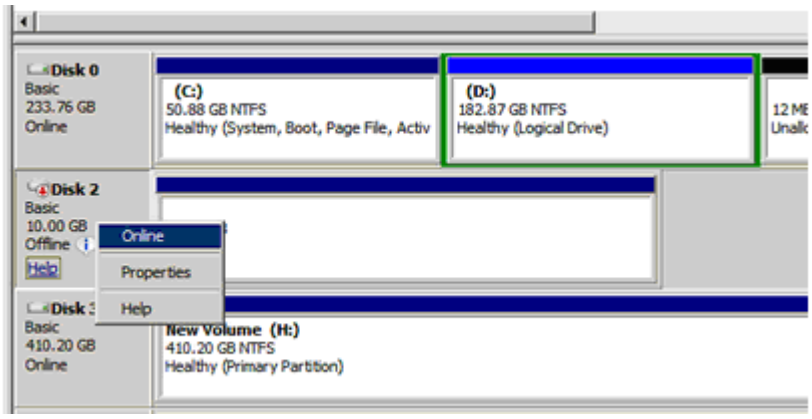
Restart your subsystem for the change to take effect.

Managing LUNs on Windows Server

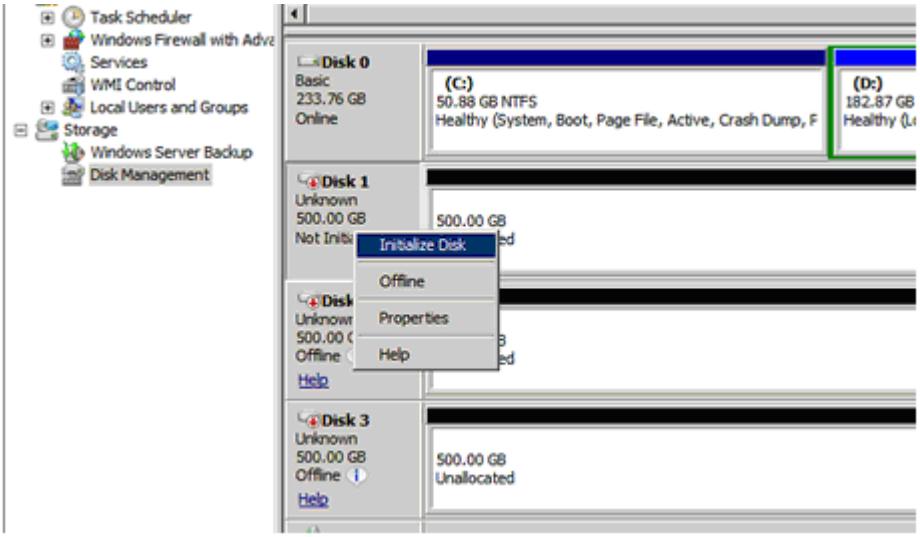
The below process shows screens captured from Windows Server 2008 R2, Server Manager. With mapped partitions, you can scan, initialize, and format these partitions.



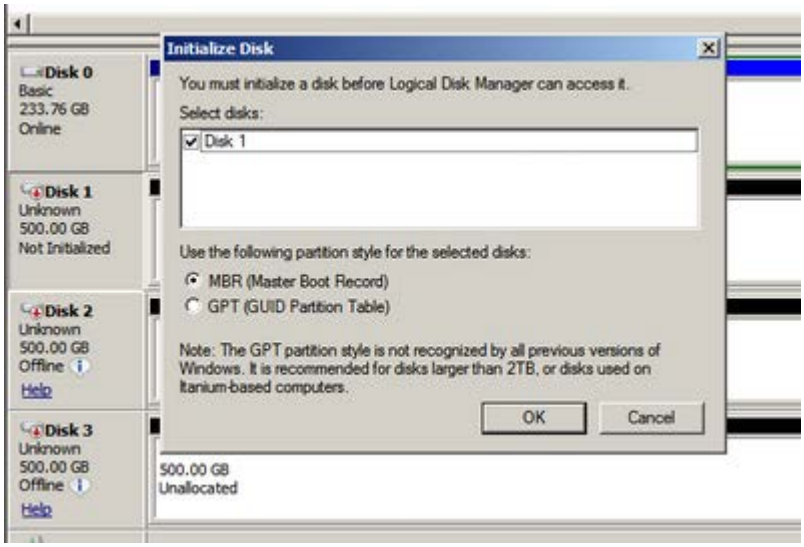




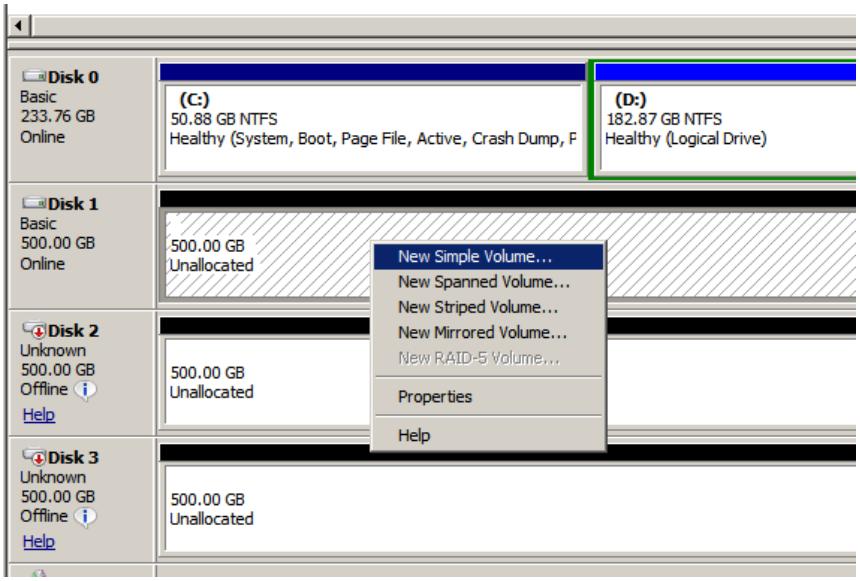
Left-click to select a Disk and then right-click to display the Online command.



When done, right-click to display and execute the Initialize Disk command.

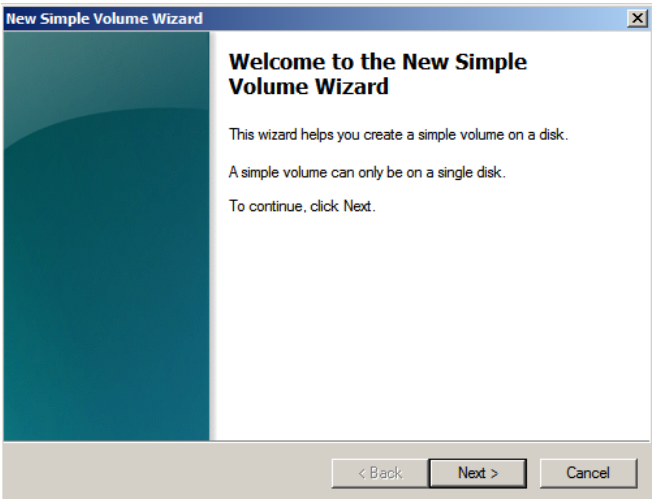


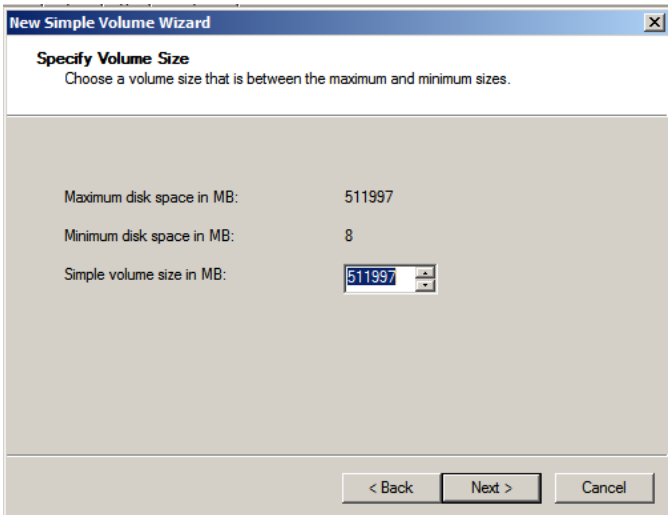
Proceed with the rest of the procedure following the onscreen instructions.

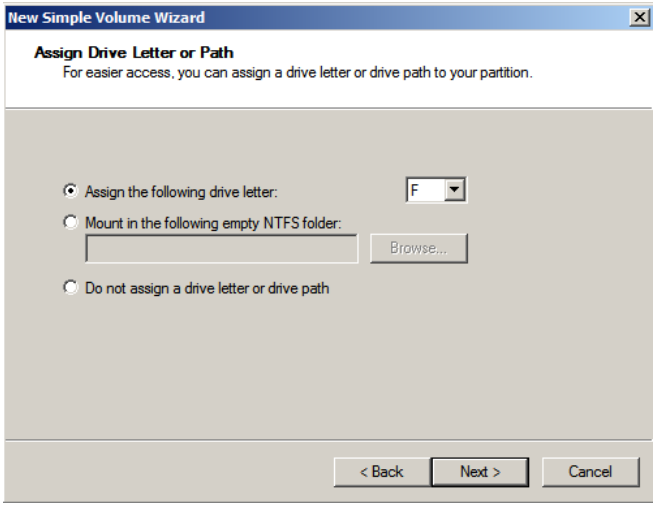


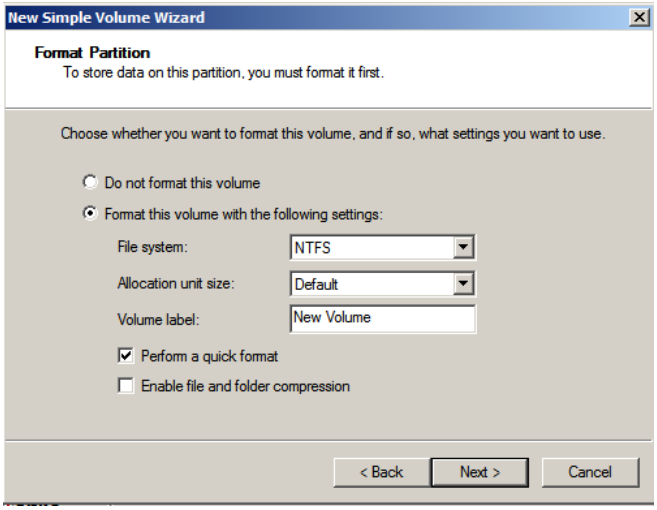
Right-click on an Unallocated partition to create a New Simple Partition.

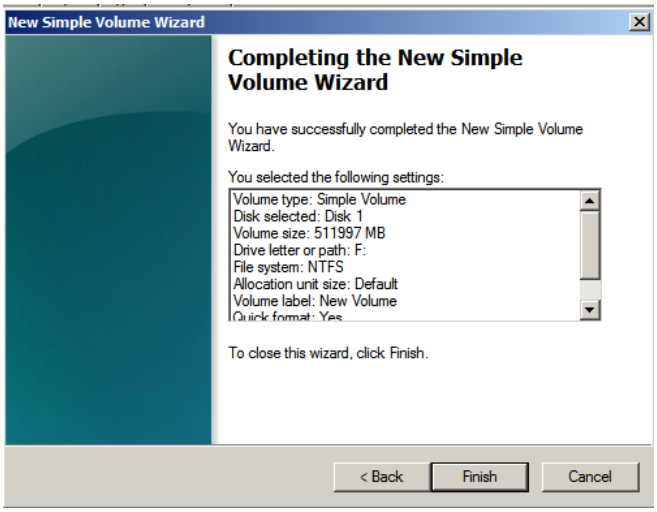
Follow the instructions on the Partition Wizard to complete the rest of the procedure.











Managing LUNs on Linux

Shell commands are shown below as how to manage LUNs on Linux.

```
[root@rh53-admin ~]# /etc/init.d/multipathd restart
Stopping multipathd daemon:
[FAILED]
Starting multipathd daemon:
[  OK  ]
```

```
[root@rh53-admin ~]# cd /proc
[root@rh53-admin proc]# /etc/init.d/multipathd restart
Stopping multipathd daemon:
[  OK  ]
Starting multipathd daemon:
[  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 Infortrend and is provided "AS IS"
and
   Infortrend cautions users to determine for themselves the
suitability of
   the version of this software.
2. Infortrend  disclaims any  express or implied warranty, relating to
sale
   and/or use  of Infortrend  products, including, liability or
warranties
   relating to  fitness for  a particular purpose, merchantability or
inf-
   ringement of any patent, copyright or other intellectual property
right.
3. Infortrend  assumes  no  responsibility  for  loss of  use, loss
of data,
```

```
    malfunction or damages to  your equipment  arising from the
installation
    or use of  this software  and  shall in no event be liable for any
loss
    of profit or any other commercial damages including, but not
limited to,
    indirect, special, incidental, consequential or other damages.
4. Infortrend reserves the right to make  changes  to  the software
at any
    time, without notice.

* Brands, product names and website addresses herein are
trademarks or
  registered trademarks of their respective owners.
* If you have problems with this software, please visit our website at
  www.infortrend.com.tw or contact our technical support team at
  http://www.infortrend.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/kernel/drivers/virtual/virtual.ko
version:            1.4
author:             Infortrend 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   virtual.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)

- **Solaris iSCSI Software and Hardware Requirements**

  - 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 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:
- Configure the device dynamically discovered (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 statically discovered.

  - # 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 using one of the following:

  - If you have configured a dynamically discovered (SendTargets) device, enable the Send Targets discovery method.
  # iscsiadm modify discovery --sendtargets enable
  - If you have configured static targets, enable the static target discovery method.
  # iscsiadm modify discovery --static enable

- Create the iSCSI device links for the local system.

  - # devfsadm –i iscsi

Configuring Out-of-Band Flush Using DB Flush Agent

If you are holding data in database forms, you need to flush all data into the storage subsystem before doing a backup job. The DB (database) Flush module in SANWatch allows you to perform it automatically.

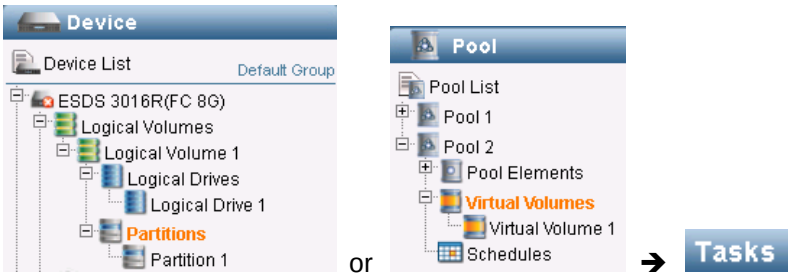
DB Flush works for the following databases:

- SQL
- Microsoft Exchange
- Oracle

For more information about configuring out-of-band flush on the host side, refer to "Configuring Out-of-Band Flush."

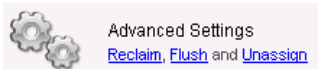
Go to

EonStor DS subsystems: SANWatch Home > Device sidebar > Device List > device name > Logical Volumes > LV name > Partitions > Tasks corner
ESVA subsystems: SANWatch Home > Pool sidebar > Pool List > pool name > Virtual Volumes > Tasks corner

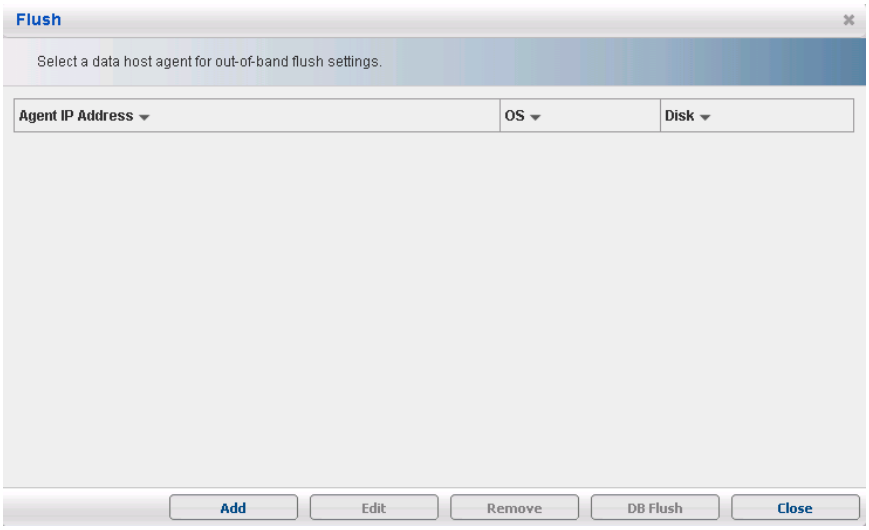


Step 1: Activating DBFlush Agent

Click Flush in the Tasks corner.



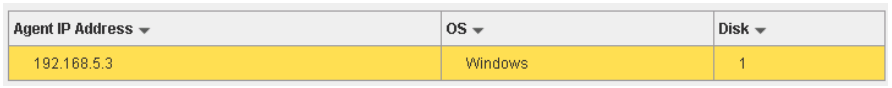
The Flush Settings window will appear.



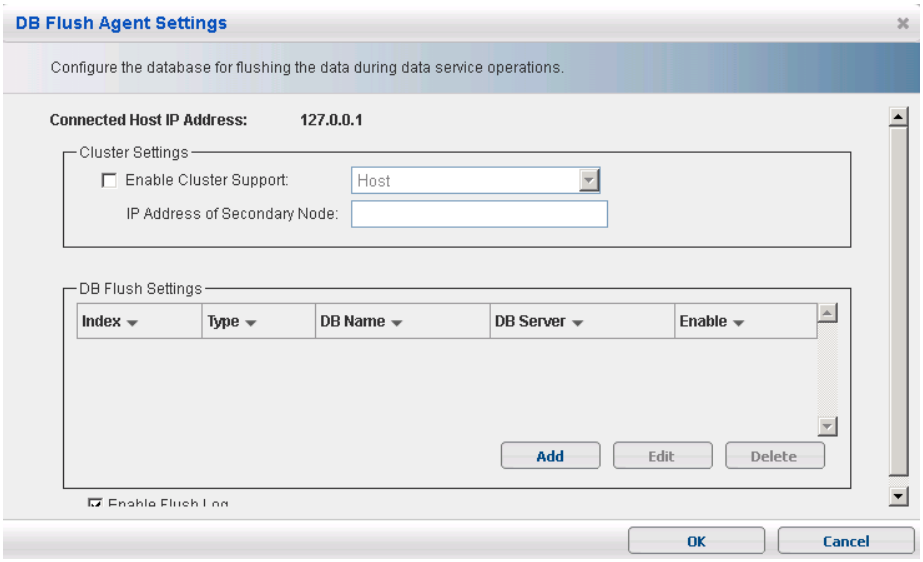
Click Add to add a setting. In the Flush Agent Setting, enter the host agent IP

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)

You will see the Flush Agent list, select the item for which you want to perform out-of-band flush.



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

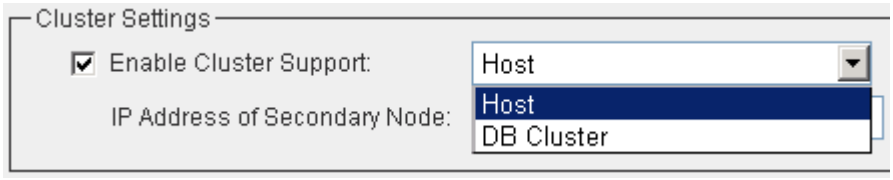


Step 2: Enabling Database Clustering

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

Database clustering refers to storing sequential rows of a database table on a disk. It will boost the database performance for server-centric database systems, since the server can perform database operations by direct access to disk.

To enable database clustering, check the Enable Cluster Support checkbox and select DB Cluster. If you would like to add another node, select Host and enter the IP address.



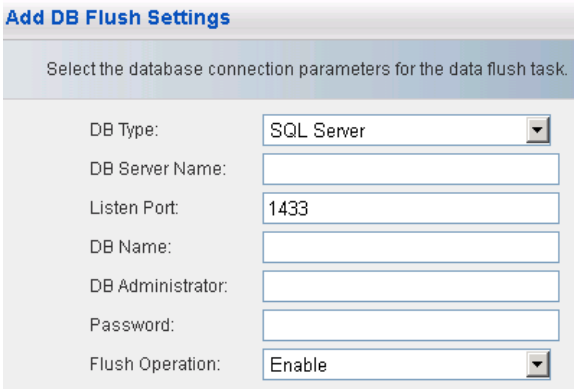
Step 3: Enabling Flush Log

Enable the flush log if you want:

- Event logs for clustered nodes will be kept on this machine.
- Events will 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) which the database listener (a software that manages the 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 you select the security level of your database. By disabling "SA" access, no one will have access to a database system, except logging in as the Windows Administrator. Refer to this section for how to enable an “sa” login.
DB Password	Specifies the database password.
Enable DB Flush	Allows flushing database inside cache memory into a local file before taking snapshot images.

Working with Snapshots

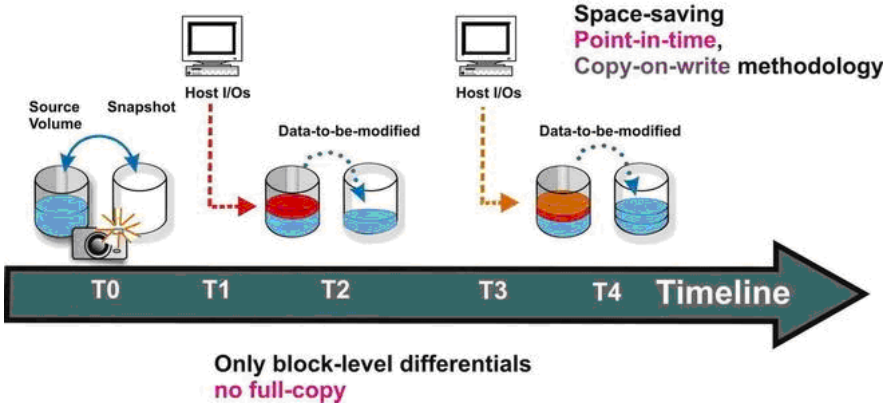
General Snapshot Rules

Number of Snapshots

- The maximum number of snapshot images in a partition or virtual volume is 1024.
- The maximum number of snapshot images in a logical volume or pool is: 16000.
- The maximum number of online snapshot images (snapshots mapped to hosts) is 1024.

Space Concerns

- The storage space required for storing snapshot images is automatically allocated from the logical volume or pool.
- When you create a logical volume or pool in SANWatch, 30% of free space will be marked, and if you use more than 70% of its space, you will be notified. Make sure you always have enough space.
- The space required for taking snapshots is determined by how frequently your data change.



- Use the prune rule option in the snapshot scheduler window to put a cap on the maximum number and lifespan of snapshots.

Database Concerns

When taking snapshots for database applications such as Oracle, use “Group Snapshot” in the scheduler. You can select multiple source partitions or virtual volumes when creating a snapshot schedule. Using Group Snapshots ensure integrity of backup data between database and log partitions or virtual volumes.

What to Evaluate when Planning

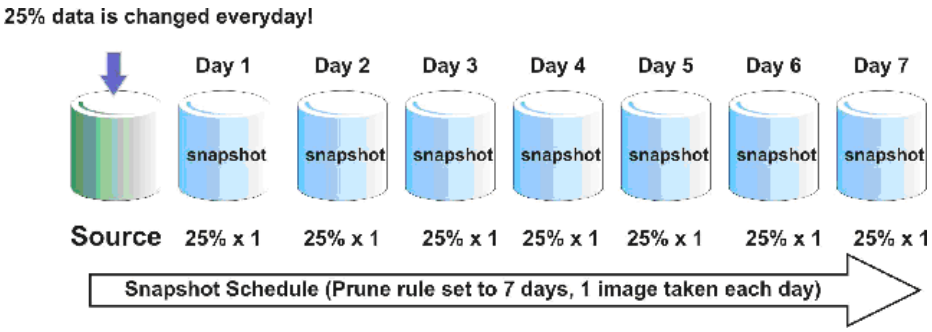
When planning snapshots, evaluate the following concerns:

- How many data changes will occur within a time frame?
- How many snapshots might you need to recover?
- How long can you tolerate loss of data (= how frequently do you need to take snapshots)?

Case Study: Calculating the Required Space

Here we calculate required data space based on these assumptions.

- 25% of data is expected to change every day.
- A snapshot is taken every day.
- You need 7 snapshots to preserve data protection.
- The lifespan of a snapshot is 7 days.



The storage space required from a logical partition will be: (25% x 1) + (25% x 1) + (25% x 1) + (25% x 1) + (25% x 1) + (25% x 1) + (25% x 1) = 1.75 times of the source partition size.

Pruning vs. Purging Snapshot Images

To use the storage space efficiently, there are two mechanisms, pruning and purging, that allows you to automatically remove older snapshot images.

Pruning

Pruning refers to removing older snapshot images once it reaches the threshold size or passes the retention period. 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 older snapshot images when the used storage space hits the threshold (= available space becomes insufficient). Purging will continue until the used storage space becomes lower than 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 as a critical issue for the overall system. When purging occurs, you may take either of the following actions:

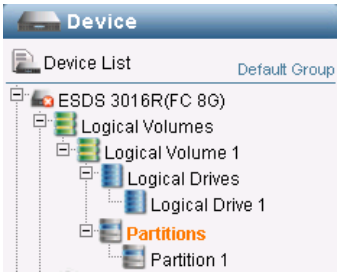
- Increase the size of the logical volume or pool to expand the available storage space
- Remove unnecessary data from existing LVs or pools or reconfigure them to use storage space more efficiently
- Increase the pruning threshold (least recommended)

If a snapshot image is marked as invalid during purging, that image can no longer be used and needs to be deleted immediately.

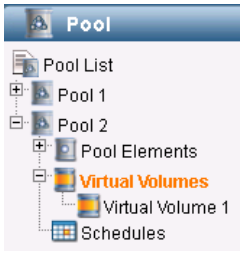
Taking Snapshots

Go to

EonStor DS subsystems: SANWatch Home > Device sidebar > Device List > device name > Logical Volumes > LV name > Partitions > Tasks corner
ESVA subsystems: SANWatch Home > Pool sidebar > Pool List > pool name > Virtual Volumes > Tasks corner



or

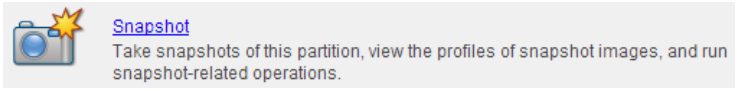


➔ Tasks

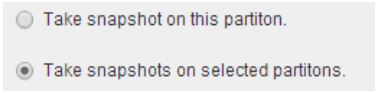
You can also take snapshots by schedule. For more information, go to the following location and click the Help icon at the top-right corner:
EonStor DS subsystems: SANWatch Home > Device sidebar > Device List > device name > Schedules
ESVA subsystems: SANWatch Home > Pool sidebar > Pool List > pool name > Schedules

Steps

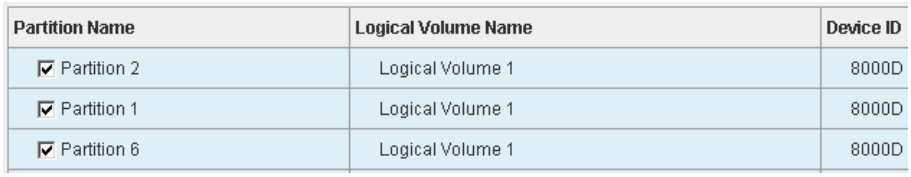
Click Snapshot in the Tasks corner.



Select the partition or virtual volume you wish to take snapshots of.



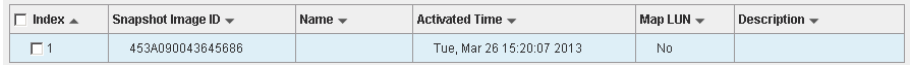
If you choose to select other partitions or VVs, select Take snapshots on selected partitions (or virtual volumes), and select the partition(s) or VVs you wish to take snapshot images of.



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.

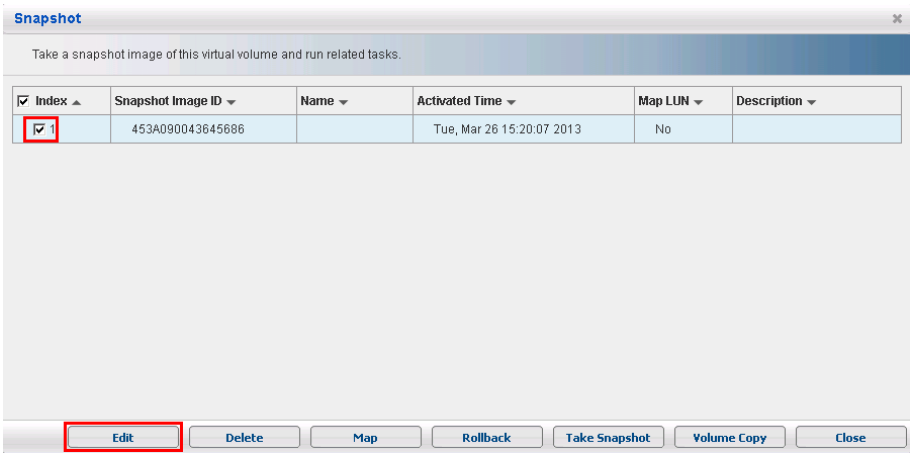


Index	Snapshot Image ID	Name	Activated Time	Map LUN	Description
1	453A090043645686		Tue, Mar 26 15:20:07 2013	No	

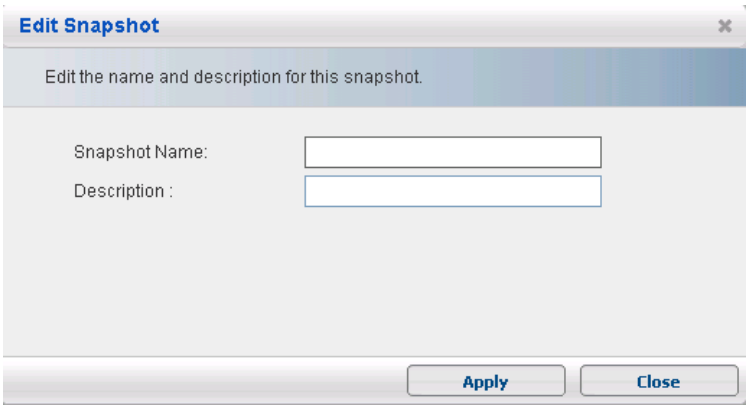
Configuring

Select a snapshot image and click Edit.

Snapshots

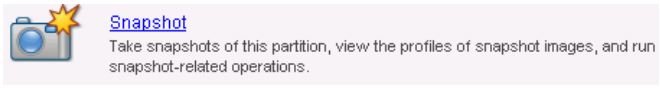


You may change the name and description of the snapshot.



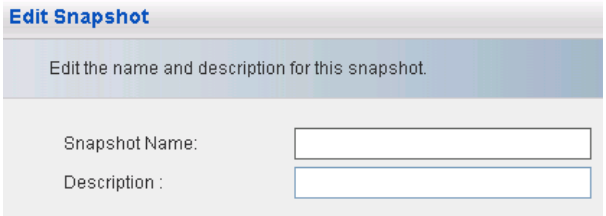
Configuring Snapshots

Navigate to the partition or virtual volume whose snapshots you want to modify, and click Snapshot in the Tasks corner.



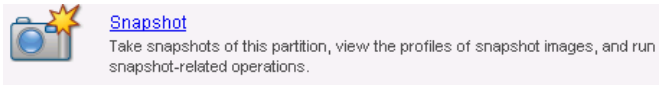
Click Next, check the box next to the snapshot image ID, and click Edit.

Edit the name and description for the snapshot image, and click OK to finish.



Deleting Snapshots

Select the partition or virtual volume whose snapshots you want to modify, and click Snapshot in the Tasks corner.



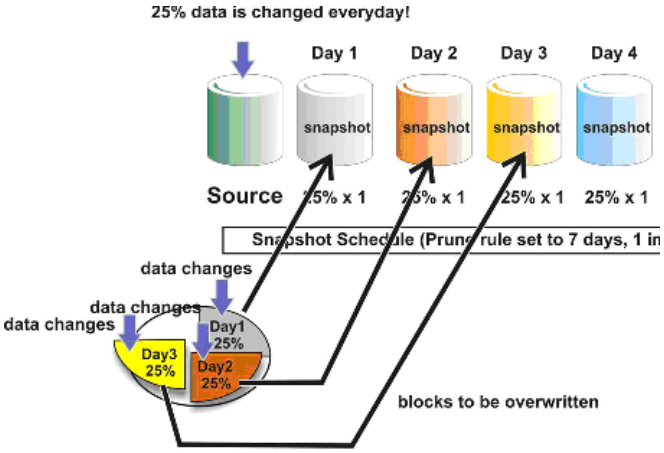
Click Next, check the box next to the snapshot image ID, and click Edit.

Click Delete and then click Yes.

Note Taking multiple snapshots at once is useful for database applications that require coherent and simultaneous backup of multiple partitions or virtual volumes.

Recovering Source Partition or Virtual Volume from a Snapshot (Rollback)

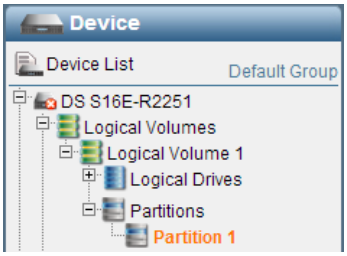
If you rollback a source partition (for EonStor DS subsystems) or virtual volume (for ESVA subsystems) back to a specific state, all images must remain intact because data is consequentially stored in different snapshot images. The below example shows a source partition or VV with 3 daily snapshots. If you want to rollback to day 1, all 3 images must be intact, ready to be referred to in order for past data to be pieced together.



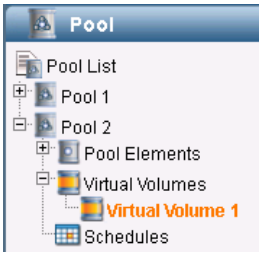
Go to

EonStor DS subsystems: SANWatch Home > Device sidebar > Device List > device name > Logical Volumes > LV name > Partitions > partition name > Tasks corner

ESVA subsystems: SANWatch Home > Pool sidebar > Pool List > pool name > Virtual Volumes > VV name > Tasks corner



or

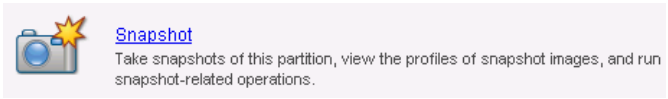


➔ Tasks

Steps

> If the partition or virtual volume has been mapped, you must unmap the partition or VV first in order to rollback a snapshot image into the partition or virtual volume.

Click Snapshot in the Tasks corner.



Click Next and select the snapshot image you want to rollback.

Click Rollback, and then click Yes in the confirmation dialog.

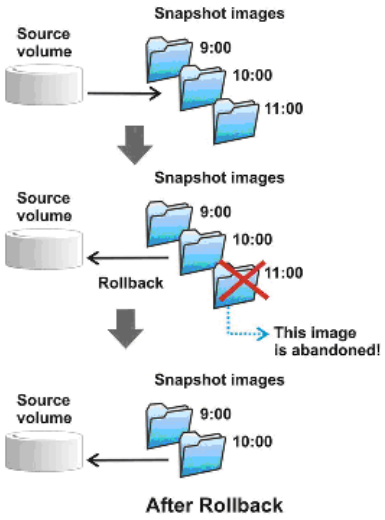
The source virtual volume or partition will be rolled back.

The process can take up to several minutes depending on the size of source virtual volume or partition.

You may re-establish host LUN mappings for the source virtual volume or partition.

Note on Rollback Timing

If a snapshot image rolls a source partition or virtual volume back, snapshot images taken after that image will be erased. In the example below, the snapshot image taken at 11:00 will be lost because the original source partition or virtual volume it was referring to was replaced by the image taken at 10:00.

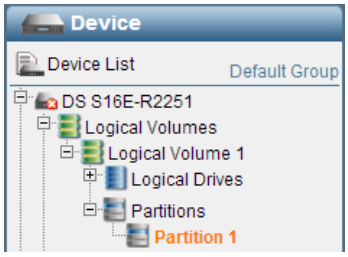


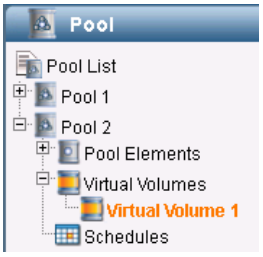
Mapping a Snapshot Image to the Host

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

Go to

EonStor DS subsystems: SANWatch Home > Device sidebar > Device List > device name > Logical Volumes > LV name > Partitions > partition name > Tasks corner
ESVA subsystems: SANWatch Home > Pool sidebar > Pool List > pool name > Virtual Volumes > VV name > Tasks corner

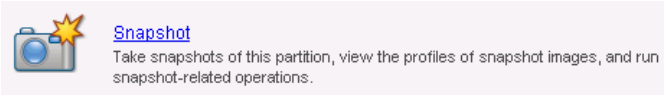


or


➔ Tasks

Steps

Click Snapshot in the Tasks corner.



Click Next and check the box next to the snapshot image ID.

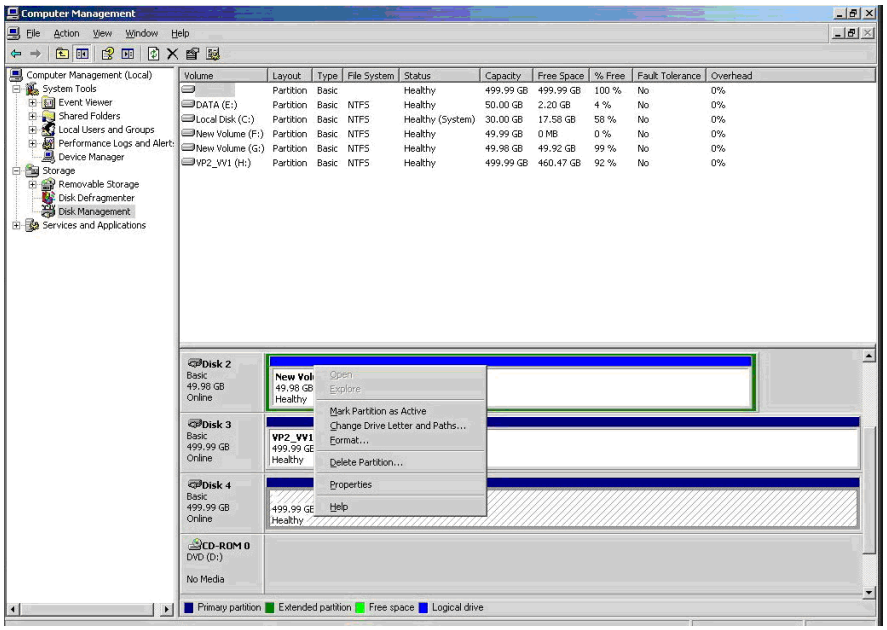
Click Map.
The Host LUN Mapping window will appear. The rest of the steps to take are the same as mapping a partition or virtual volume to a host. For detailed instruction, go to:

- EonStor DS subsystems: SANWatch Home > Device sidebar > Device List > device name > Logical Volumes > LV name > Partitions
  ESVA subsystems: SANWatch Home > Pool sidebar > Pool List > pool name > Virtual Volumes
- Click the Help icon at the top-right corner, and search for "Mapping/Unmapping Partitions or Virtual Volumes to Host."

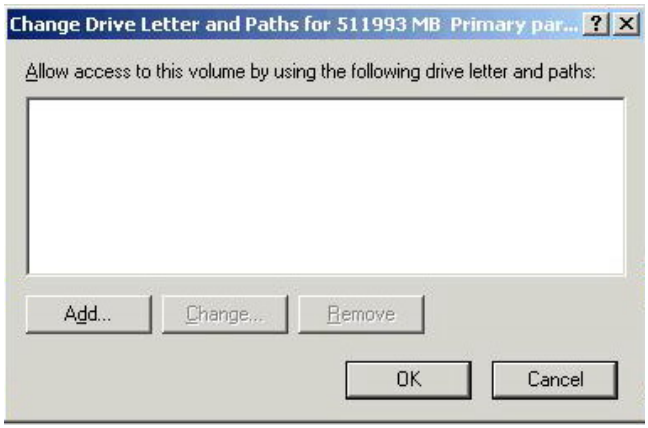
Assigning a Drive Letter to the Snapshot

Before accessing data in the snapshot, you need to assign a drive letter to it. Here are the procedures for Windows Server environment.

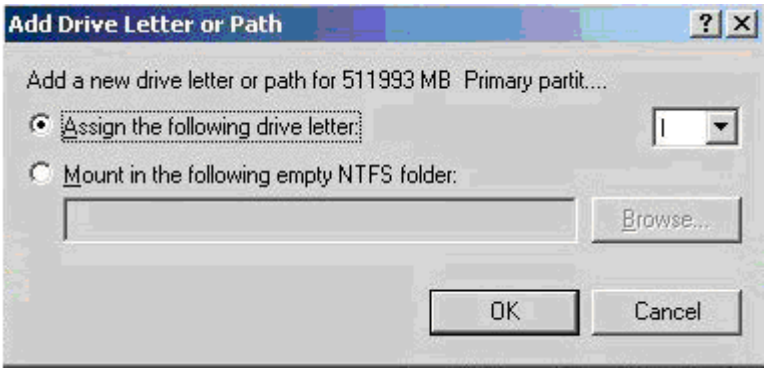
1. When an image is mapped, it will appear as a new drive to the computer.



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



4. Select the drive letter and click OK.

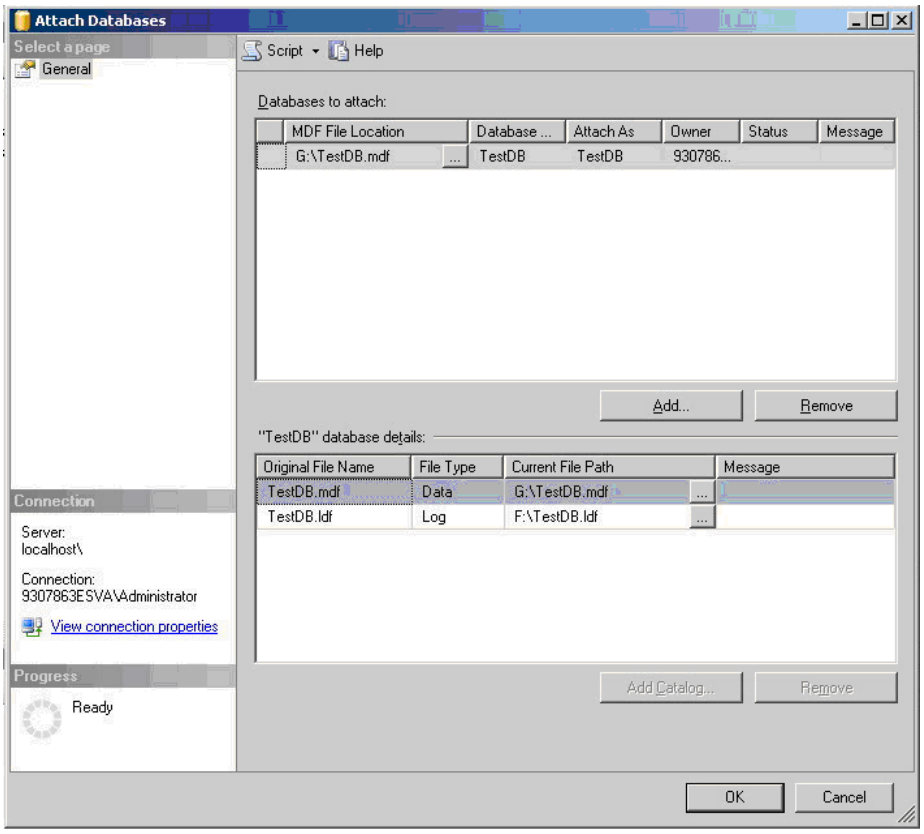


5. You should be able to access the data in the snapshot.

Recovering Database Volume from Grouped Snapshots

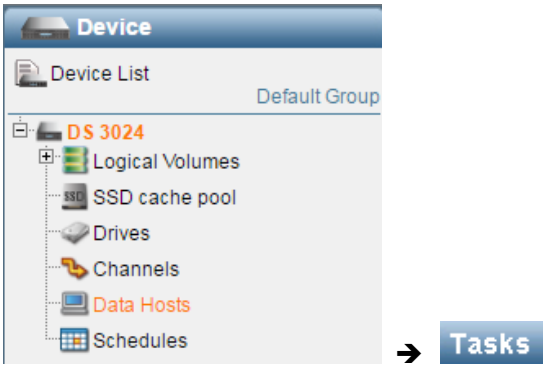
Background

The procedure below is based on a simple configuration: two virtual volumes presented to the host, one as Data volume and the other as Log volume for SQL Server.

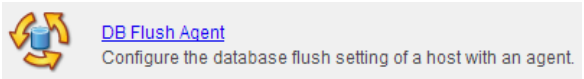


Step 1: Configuring SANWatch

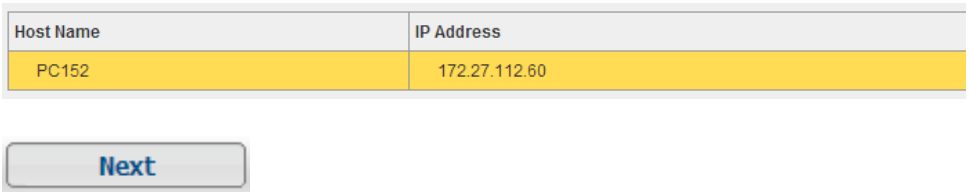
Go to SANWatch Home > Device sidebar > Device List > device name > Data Hosts > Tasks corner.



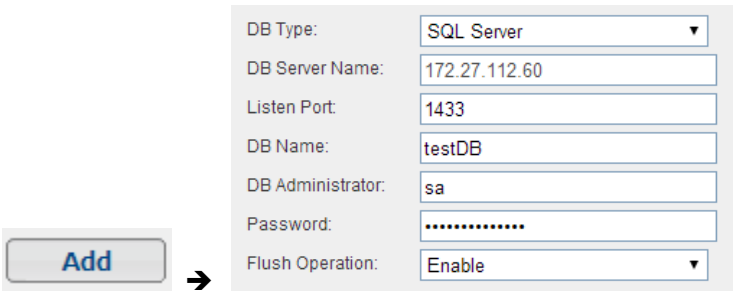
Click DB Flush Agent.



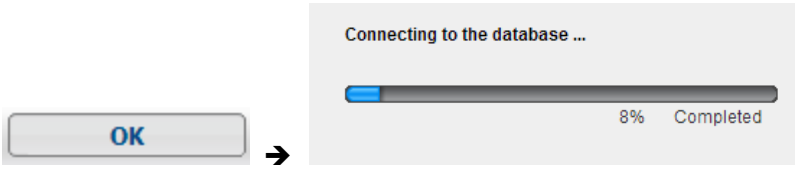
Select a data host for configuring database flush, and click Next.



Click Add. A configuration prompt will appear.



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



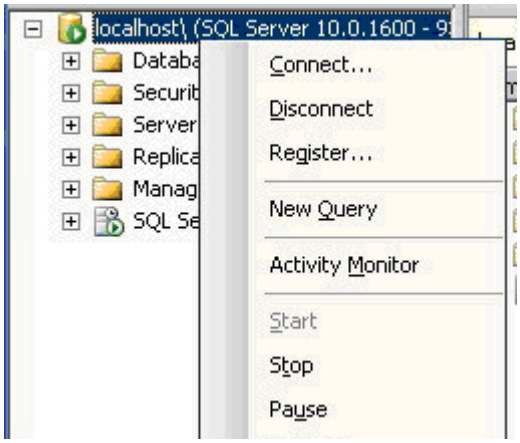
Open SANWatch Manager and create snapshot schedule.

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. For this procedure, you need to enable (check) this option.

Step 2: Rollback Snapshot Images

Here we assume that the database has been corrupted and we need to recover the database to a certain point.

Stop the database service. In Microsoft SQL server, right-click and select Stop.



In the SANWatch Manager, unmap the database volume.

Refer to the "Recovering Source Volume from a Snapshot (Rollback)" section for more information.

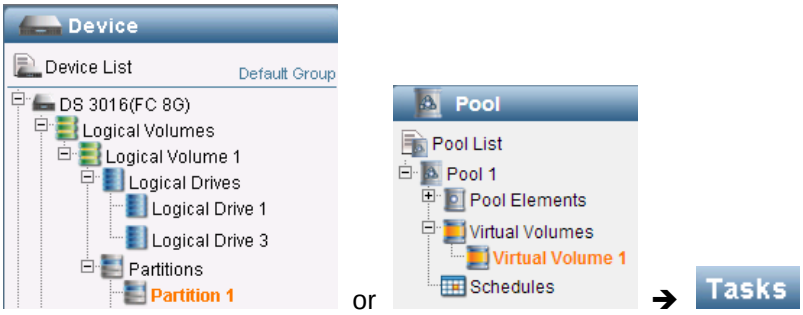
Creating a Volume Copy from a Snapshot Image

To create a volume copy, you must have at least one snapshot image ready.

Go to

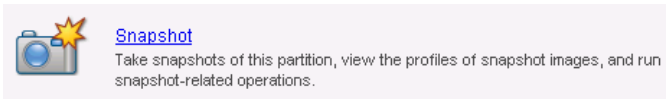
EonStor DS subsystems: SANWatch Home > Device sidebar > Device List > device name > Logical Volumes > LV name > Partitions > partition name > Tasks corner

ESVA subsystems: SANWatch Home > Pool sidebar > Pool List > Virtual Volumes > LV name > Tasks corner

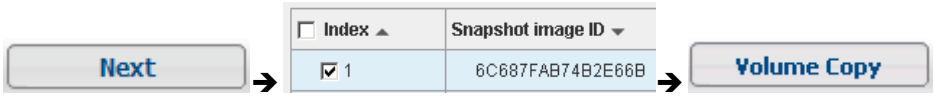


Steps

Click Snapshot in the Tasks corner.



Click Next, check the box next to the snapshot image ID, and click Volume Copy.



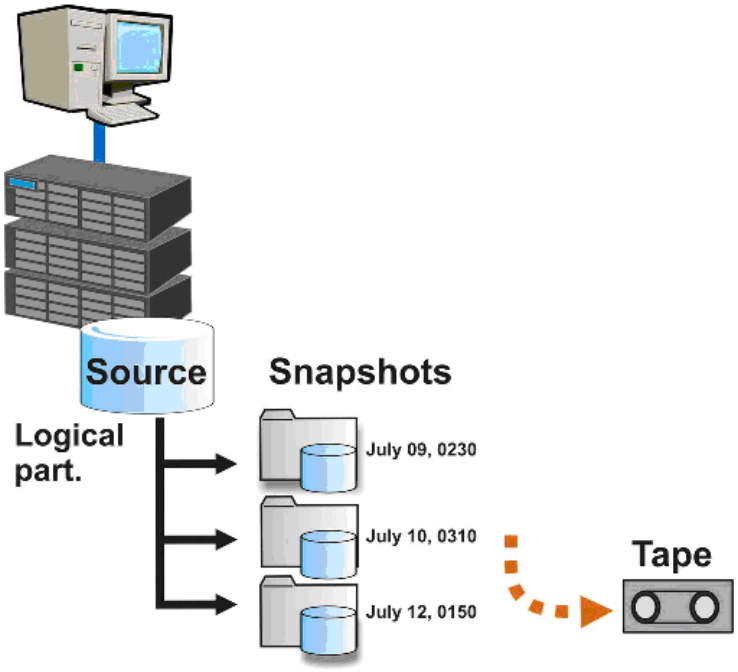
Follow the instructions.

Taking Backup of Snapshot Images

Here are three ways to take backups of snapshot images using tape storage and/or Volume Copy/Mirror functions described later in this manual.

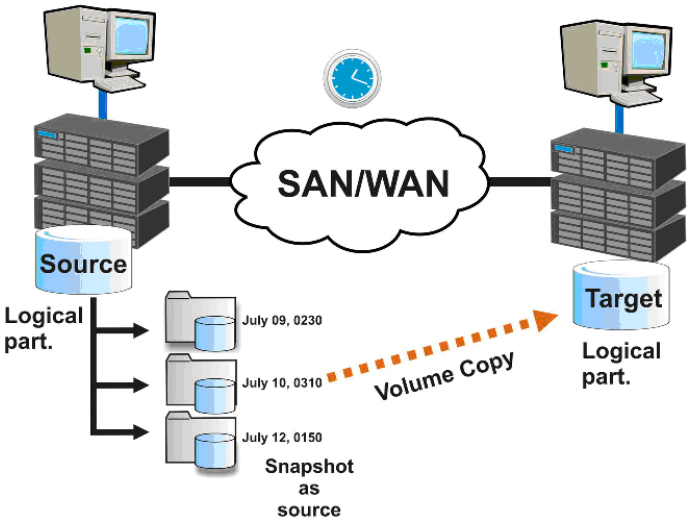
Using Tape Backup

Snapshots are saved to tape media during system low time.



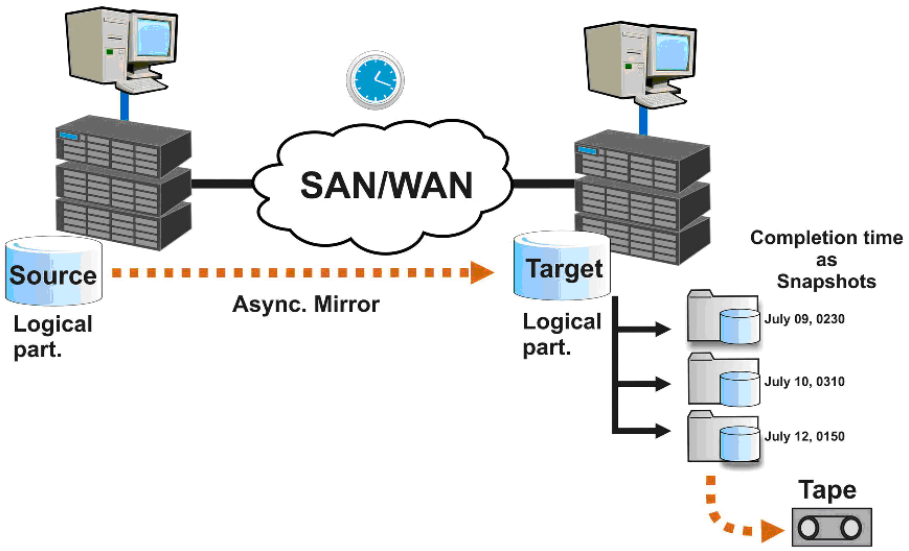
Using Volume Copy

After snapshot images are taken, they are copied to another location using the Volume Copy function.

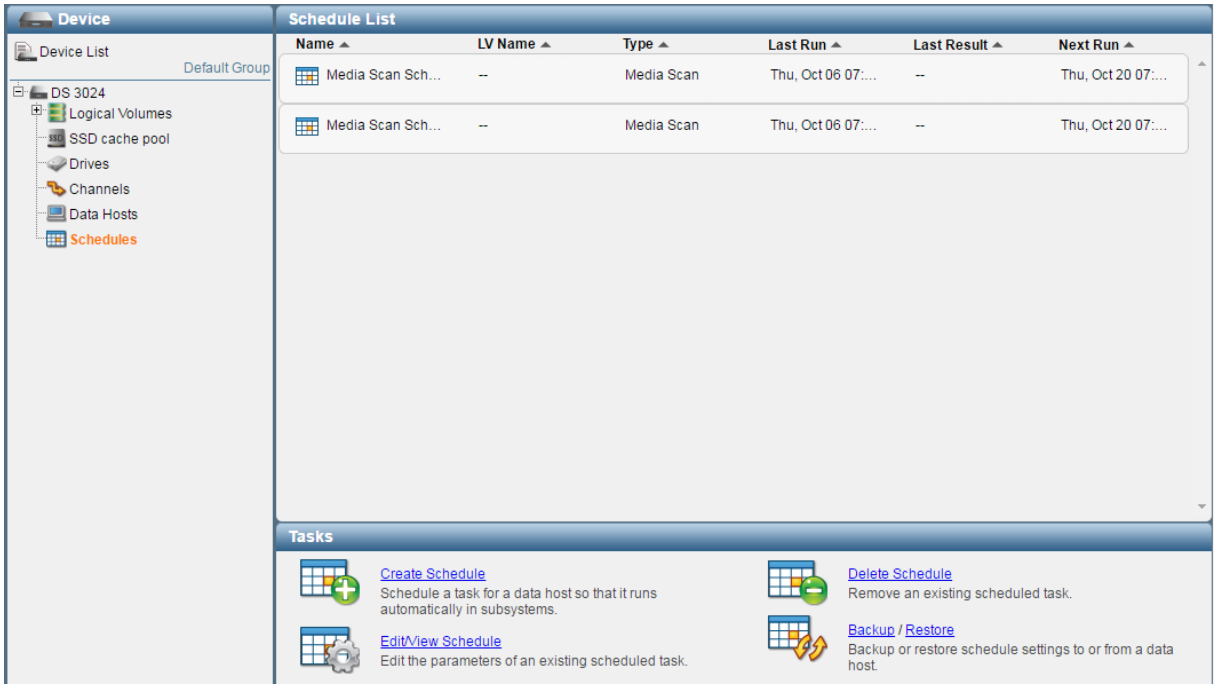


Using Asynchronous Mirror

Snapshots can be saved (mirrored) to a remote location using the Asynchronous Mirror function. Other backup methods, such as tape media, can be used in the remote site.


SAN/WAN
Source
Logical part.
Async. Mirror
Target
Logical part.
Completion time as Snapshots
July 09, 0230
July 10, 0310
July 12, 0150
Tape

Working with Schedules

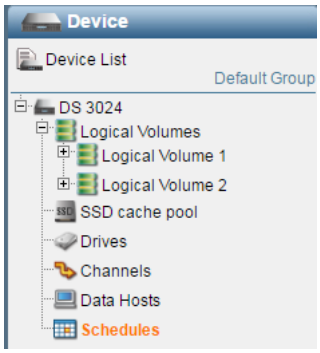


This chapter describes how to create a scheduled task (snapshot, volume mirror) and backup or restore schedule settings.

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 corner.

Parameters

Name	Shows the name of the scheduled task.
LV Name (or Pool Name)	Shows the name of logical volume (for EonStor DS subsystems) or pool (for ESVA subsystems) 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 previous date and time when the scheduled task was executed.
Last Result	Shows the result of the last execution of the scheduled task.
Next Run	Shows the next date and time when the scheduled task will be executed.

Creating Schedules: General Rules

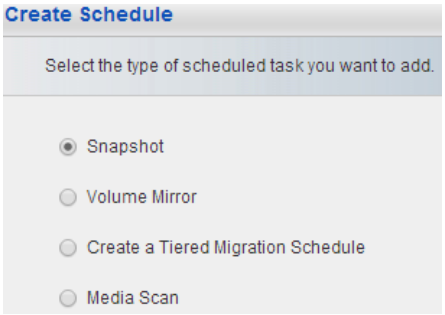
Go to

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

Steps

Click Create Schedule in the Tasks corner.

Select the schedule option.



Changing the IP Address

Scheduled asynchronous volume mirror 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 async volume mirror begins

It is best if you can keep the IP address fixed after creating the volume pair, but if you need to change it, follow these steps.

1. Restart SANWatch.
2. Re-discover the new IP address or add it manually.
3. Open SANWatch Manager from the subsystem with the updated IP address.
4. Remove the existing schedule.
5. Sync/async the volume pair to fix the broken link due to the changed IP address.
6. Create a new schedule with the updated IP address.

You can change the remote IP from the firmware (LCD menu or text interface) after creating a volume mirror (remote replication) pair. Note that if you do this, the remote pair will be broken. In order to remove a broken pair,

you must first unassign the target in SANWatch.
Changing the remote IP after creating a remote replication pair is not allowed in SANWatch. If you wish to change the IP, you need to first un-assign the target volume of the remote replication pair. After changing the IP, you can safely re-assign the pair by syncing/asyncing it manually.

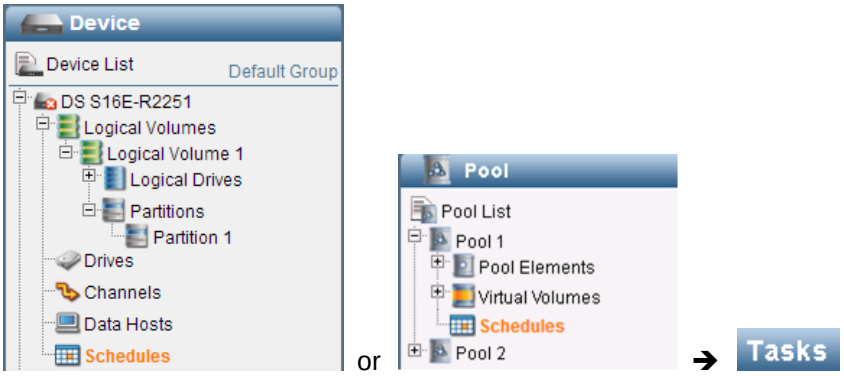
Taking Snapshots by Schedule

Notes

- The interval between two snapshots must be 10 minutes or longer.
- 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 take place at the same time, both schedules will fail.

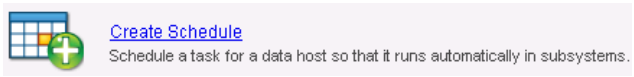
Go to

EonStor DS subsystems: SANWatch Home > Device sidebar > Device List > device name > Schedules
ESVA subsystems: SANWatch Home > Pool sidebar > Pool List > pool name > Schedules

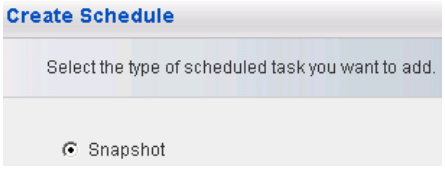


Steps

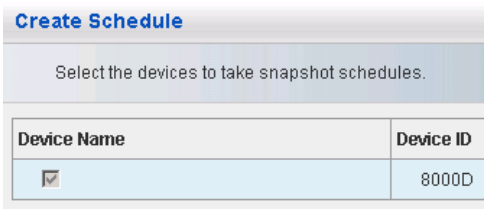
Click Create Schedule in the Tasks corner.



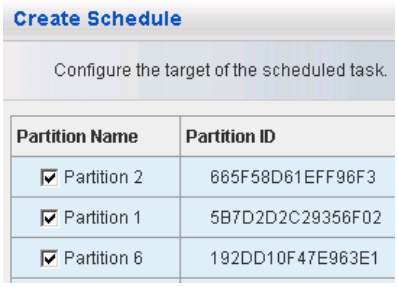
Select Snapshot and click Next.



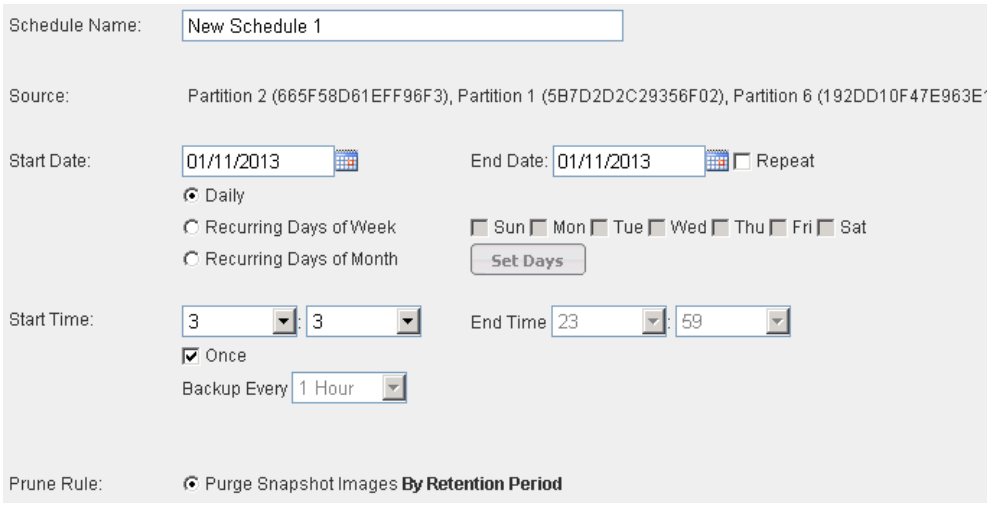
Check the box next to the device that contains the partition(s) (for EonStor DS subsystems) or virtual volume(s) (for ESVA subsystems) you wish to take snapshots of and click Next.

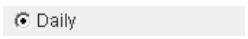


Select partition(s) or virtual volume(s), and click on Next.

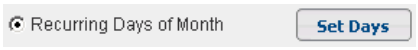


Enter your schedule parameters.

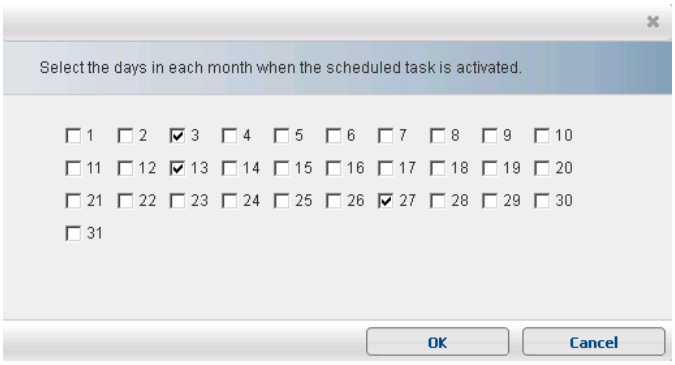


Parameters	**Schedule Name**	Enter a name for the snapshot schedule.
	Source	Shows the selected source for snapshot.
	Start/End Date	Specifies the duration of this schedule. To configure, click the part you want to configure (for example the year). If there is no stop date, check the Repeat box.
	Daily / Recurring Week Day / Recurring Days of Month	Specifies the recurrence of this schedule. Daily Check the Daily checkbox. The scheduled task will be executed every day.  Weekly Check on which day the scheduled task will be executed.  Monthly

Click Set Days.

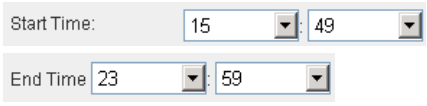


Select the days of each month on which the scheduled task will be executed.



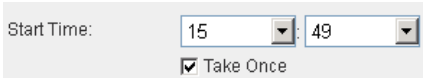
Start / End Time

Specifies the starting and ending hour/minute of the scheduled task.



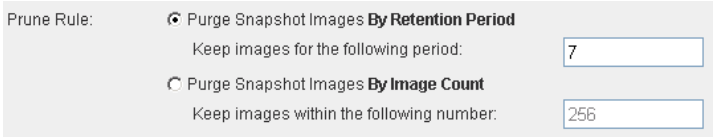
Configure the interval (frequency) using the drop-down list.

If you execute the task only once, check the Take Once box. The task will be executed on the Start Time.

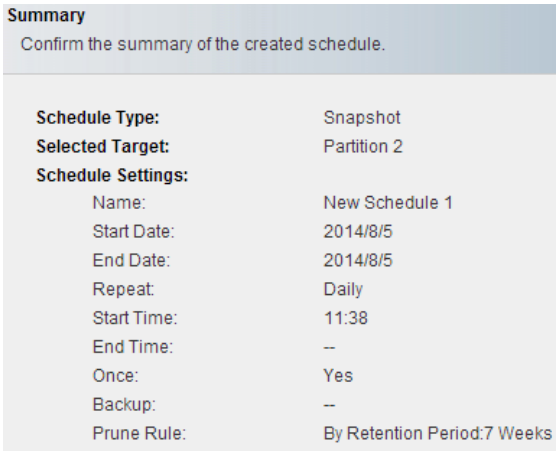


Prune rule

Specifies the amount (Snapshot Image Count) or period (Retention Period) of snapshots that will be stored in the system.



Click Next when done and confirm summary settings and click OK.



The snapshot schedule should appear in the Schedule List area.

Exporting/Importing Scheduled Backup Tasks	Click the Help icon at the top-right corner and look for "Backing Up or Restoring Schedule Settings."

Creating 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 "Creating a Volume Mirror" for more information about volume mirror.

Go to

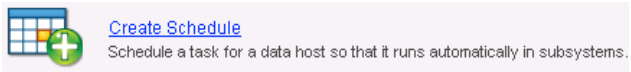
EonStor DS subsystems: SANWatch Home > Device sidebar > Device List > device name > Schedules > Tasks corner
ESVA subsystems: SANWatch Home > Pool sidebar > Pool List > pool name > Schedules > Tasks corner

or

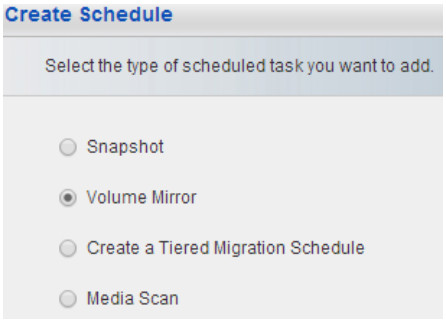
➔ Tasks

Steps

Click Create Schedule in the Tasks corner.

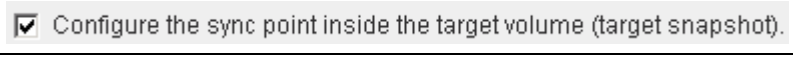


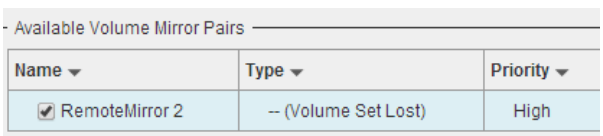
The list of tasks will appear. Check Volume Mirror and click Next.



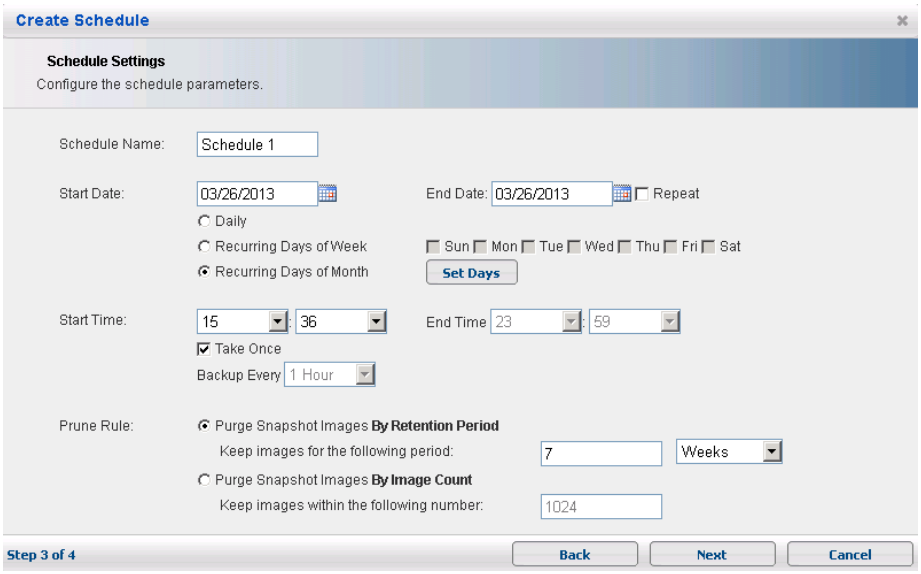
The list of volume mirror pairs will appear. Select a pair and click Next.

You may locate the sync point inside the target volume.





The schedule parameters will appear.



Parameters

Name

Enter the name of the scheduled task.

Start/End Date

Specifies the duration of this schedule. To configure, click the calendar icon and select the date.

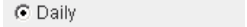
If there is no end date, check the Repeat box.

Daily / Recurring Week Day / Recurring Days of Month

Specifies the recurrence of this schedule.

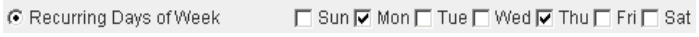
Daily

Check the Daily checkbox. The scheduled task will be executed every day.



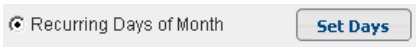
Weekly

Check on which day the scheduled task will be executed.

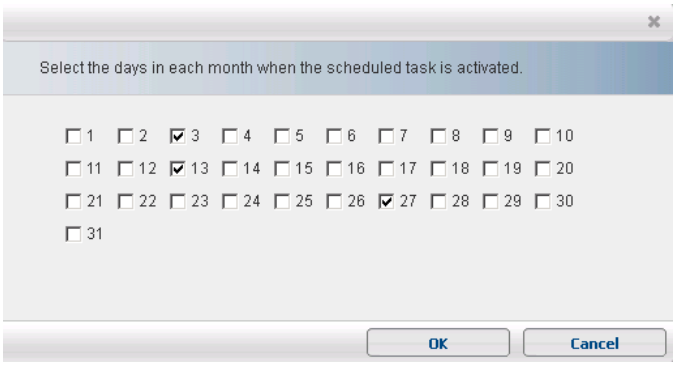


Monthly

Click Set Days.



Select the days of each month on which the scheduled task will be executed.

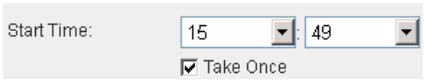


Start Time / End Time

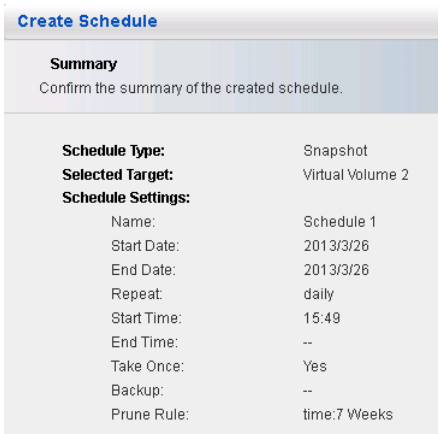
Specifies the starting and ending hour/minute of the scheduled task.

Configure the interval (frequency) using the drop-down list.

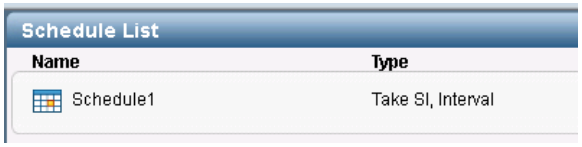
If you execute the task only once, check the Take Once box. The task will be executed on the Start Time.



Click Next. The summary of the scheduled task will appear.



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



Changing the IP Address

Scheduled asynchronous volume mirror 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 async volume mirror begins

It is best if you can keep the IP address fixed after creating the volume pair, but if you need to change it, follow these steps.

1. Restart SANWatch.
2. Re-discover the new IP address or add it manually.
3. Open SANWatch Manager from the subsystem with the updated IP address.
4. Remove the existing schedule.
5. Sync/async the volume pair to fix the broken link due to the changed IP address.
6. Create a new schedule with the updated IP address.

You can change the remote IP from the firmware (LCD menu or text interface) after creating a volume mirror (remote replication) pair. Note that if you do this, the remote pair will be broken. In order to remove a broken pair, you must first unassign the target in SANWatch. Changing the remote IP after creating a remote replication pair is not allowed in SANWatch. If you wish to change the IP, you need to first un-assign the target volume of the remote replication pair. After changing the IP, you can safely re-assign the pair by syncing/asyncing it manually.

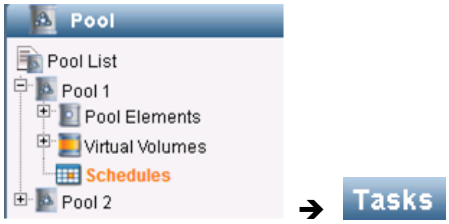
Creating Data Migration by Schedule (ESVA subsystems only)

This feature is different from tiered data migration, of which the purpose is to adjust the capacity ratio in a multi-tiered virtual volume according to the tier ratio settings.

The Data Migration feature helps with automatic data migration between pool elements after the pool is expanded or shrunk.

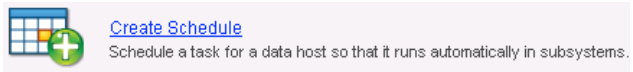
Go to

SANWatch Home > Pool sidebar > Pool List > pool name > Schedules > Tasks corner

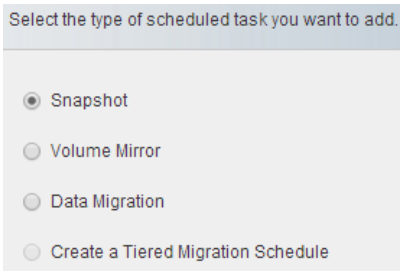


Scheduling Data Migration

Click Create Schedule in the Tasks corner.



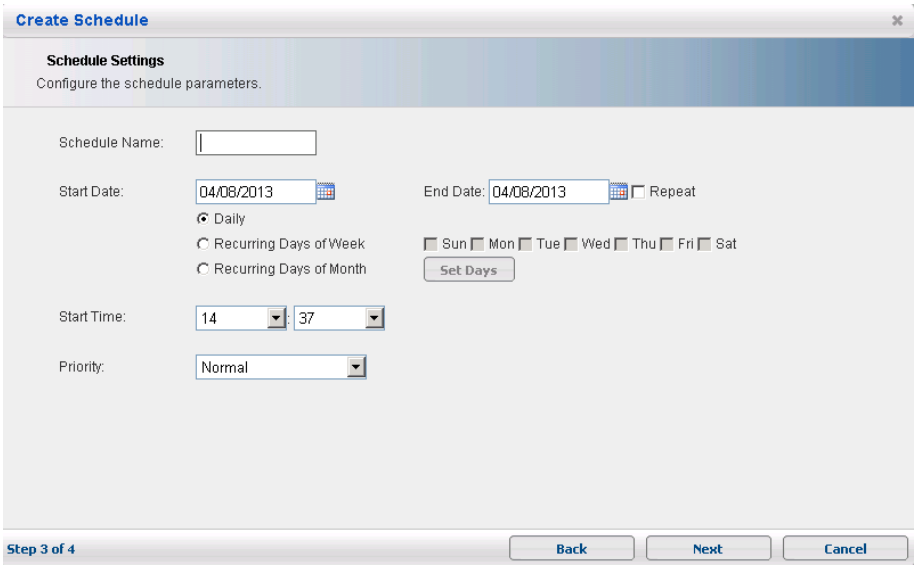
Select Data Migration and click Next.



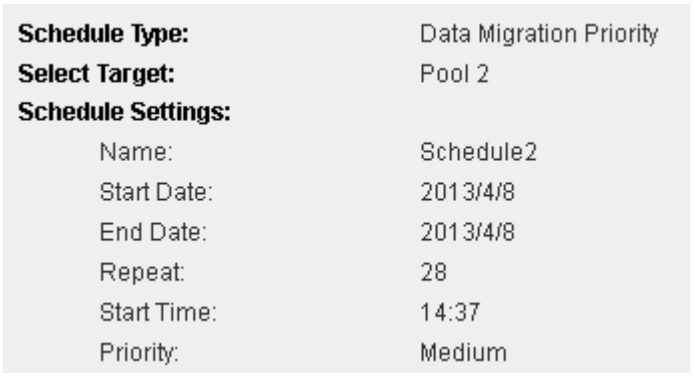
Highlight the pool in migration list and click Next.

Name	ID	Size	Available	Progress	Status
Pool 2	5618CEA460FD946B	559.49 GB	557.1 GB	Data migrating paused (1%)	On-line

Configure the schedule and click OK.



The summary will appear. Confirm and click OK.



The new schedule will appear.

Scheduling Parameters	**Start/Stop Date**	Specifies the duration of this schedule. To configure, click the part you want to configure (for example the year) and use the Up/Down arrow buttons. If there is no stop date, check the Repeat box.
	Daily / Recurring Week Day / Recurring Days of Month	Specifies the recurrence of this schedule.
	Start Time	Specifies the starting time of the migration task.
	Migration Priority	Specifies the amount (Snapshot Image Count) or period (Snapshot Image Time) of snapshots that will be stored in the system.

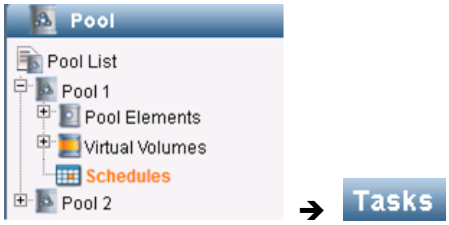
Creating Tiered Data Migration by Schedule

This feature only works when one or more logical volumes or pools that reside in multiple tiers exist in the subsystem.

Go to

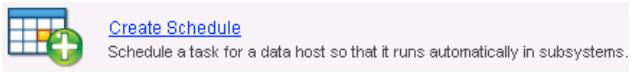
EonStor DS subsystems: SANWatch Home > Device sidebar > Device List > device name > Schedules > Tasks corner
ESVA subsystems: SANWatch Home > Pool sidebar > Pool List > pool name > Schedules > Tasks corner

or

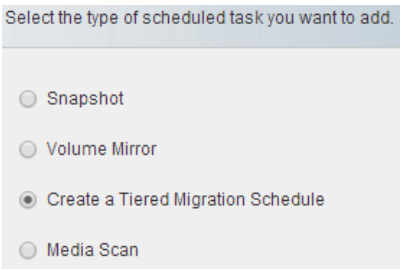


Steps

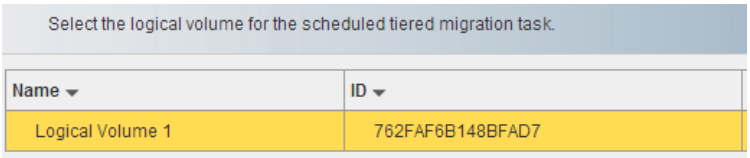
Click Create Schedule in the Tasks corner.



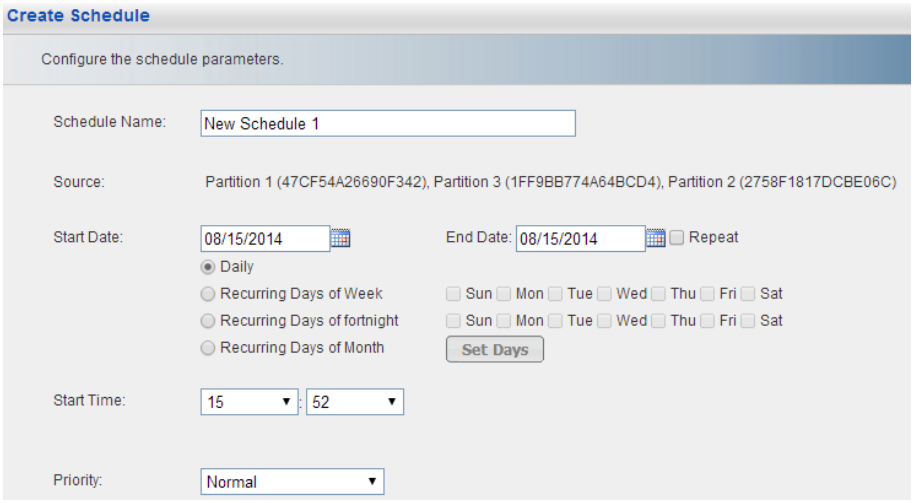
The list of tasks will appear. Check Create a Tiered Migration Schedule and click Next.



The list of tiered logical volumes or pools will appear. Select one of them and click Next.



The schedule parameters will appear.



Parameters

Schedule Name

Enter the name of the scheduled task.

Start/End Date

Specifies the duration of this schedule. To configure, click the calendar icon and select the date.

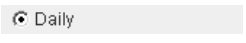
If there is no end date, check the Repeat box.

Daily / Recurring Week Day / Recurring Days of Month

Specifies the recurrence of this schedule.

Daily

Check the Daily checkbox. The scheduled task will be executed every day.

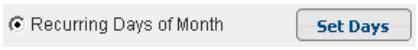


Weekly

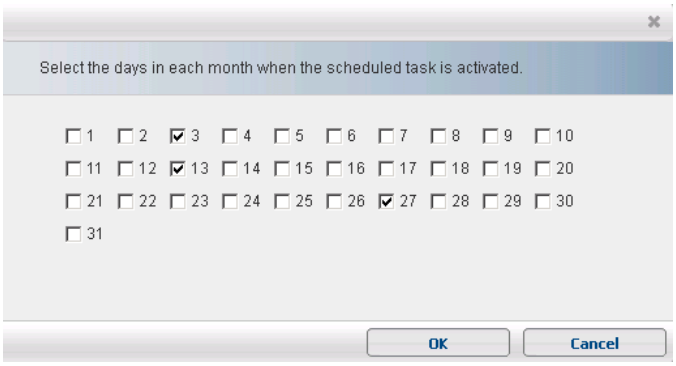
Check on which day the scheduled task will be executed.

Monthly

Click Set Days.

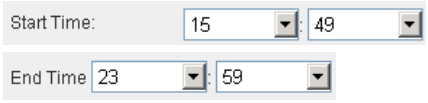


Select the days of each month on which the scheduled task will be executed.



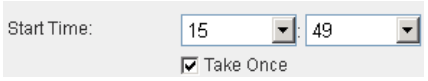
Start Time / End Time

Specifies the starting and ending hour/minute of the scheduled task.

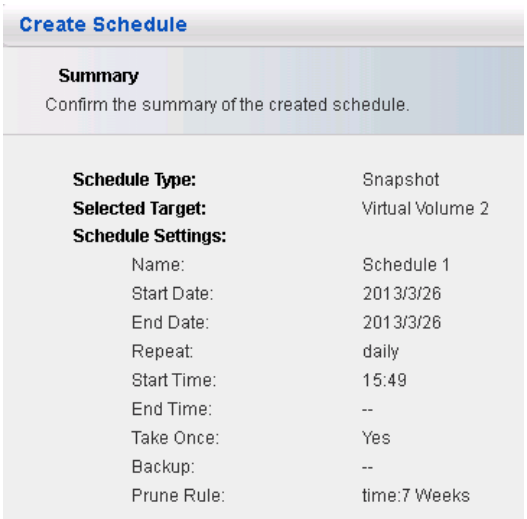


Configure the interval (frequency) using the drop-down list.

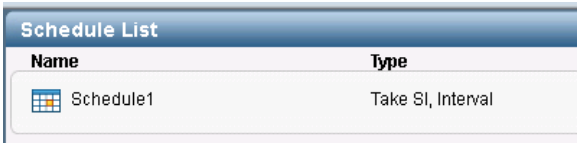
If you execute the task only once, check the Take Once box. The task will be executed on the Start Time.



Click Next. The summary of the scheduled task will appear.



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



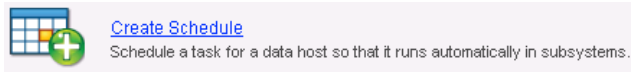
Scanning Disk Drives by Schedule (EonStor DS subsystems only)

Go to

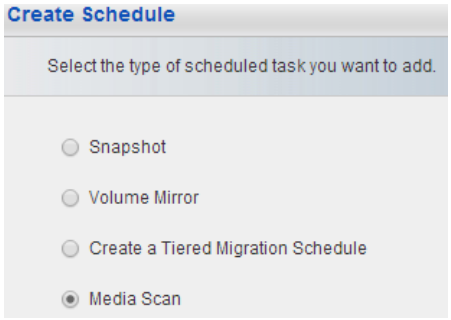
SANWatch Home > Device sidebar > Device List > device name > Schedules > Tasks corner

Steps

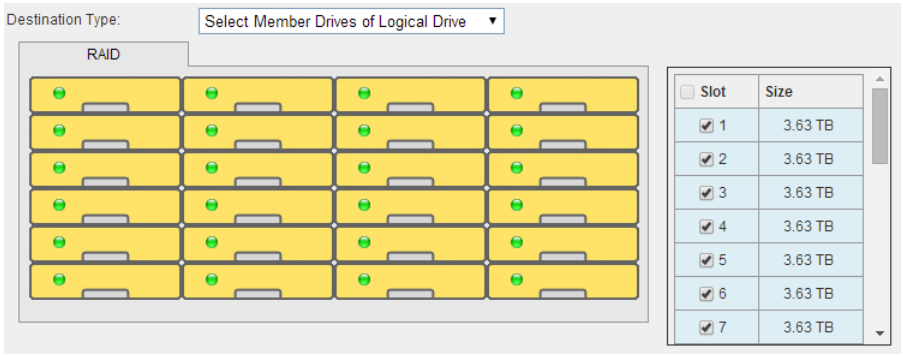
Click Create Schedule in the Tasks corner.



The list of tasks will appear. Check Media Scan and click Next.



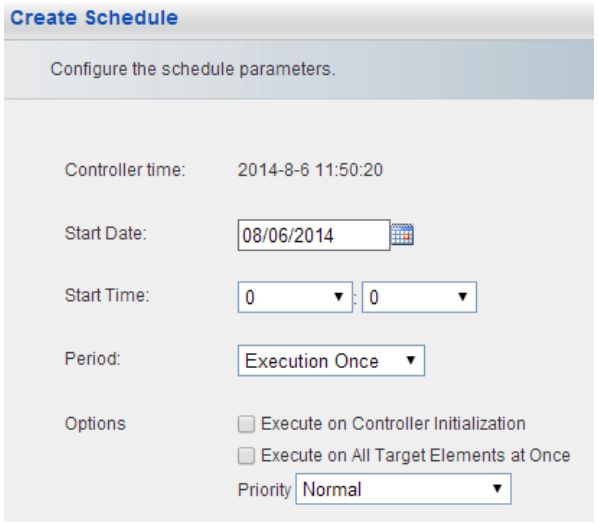
The front view of the device will appear. Select the drives that will be scanned.



- 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) for 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 (or pool element), logical volume (or pool), and partition (or virtual volume) will be selected.

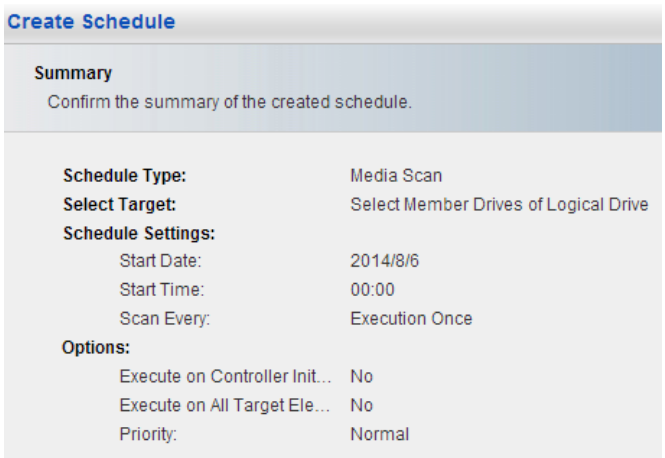
- All Eligible Drives: All healthy drives, whether a part of a logical drive or not, will be selected.

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 gets initialized ➢ All drives at once (if you choose the priority as high, scanning will be executed rapidly but the system performance may be affected)

Click Next. The summary of the scheduled task will appear.



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

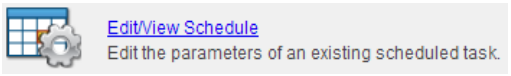
Editing/Deleting Schedules

Go to

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

Editing a Schedule

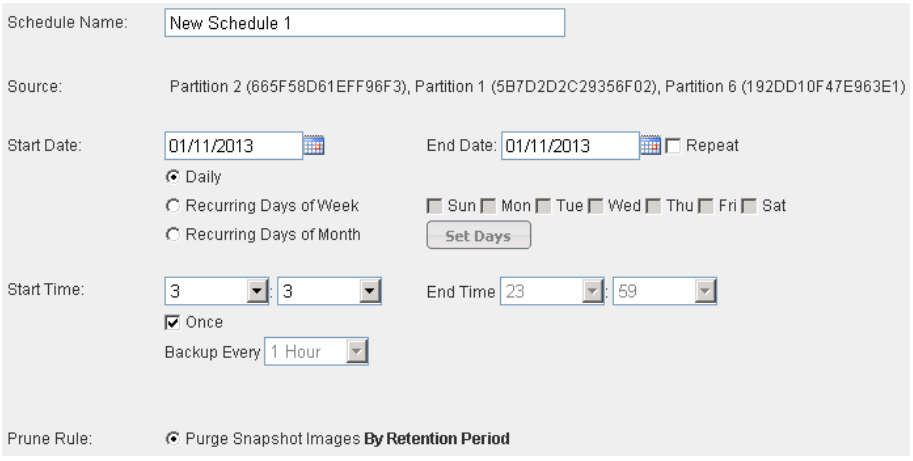
Click Edit/View Schedule in the Tasks corner.



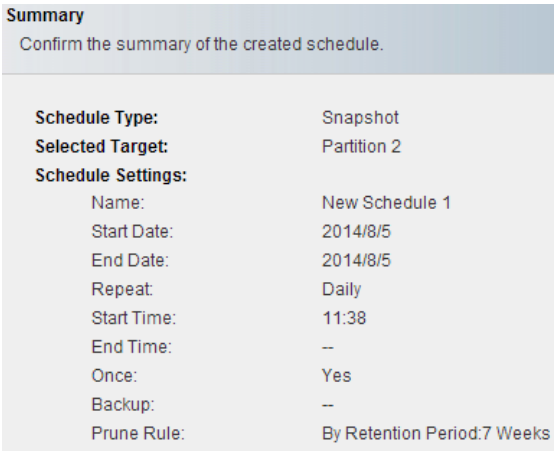
The list of scheduled task will appear. Highlight the task to be edited and click Next.

> For media scan related scheduled tasks, you are only allowed to click View to view their summary information.

The schedule parameters will appear. They are the same as those you configured while creating the schedule task. Reconfigure them and click Next.



The summary of the scheduled task will appear.

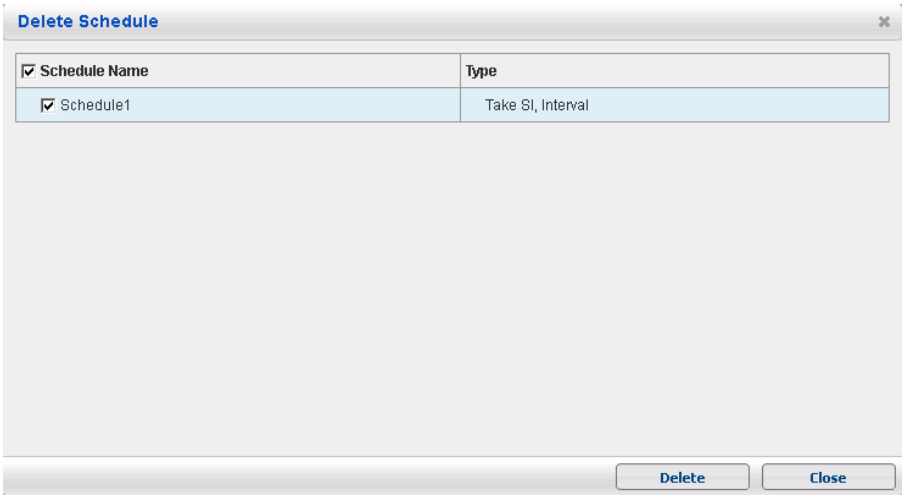


Click OK and Close. The scheduled task will reappear in the list.

Deleting a Scheduled Task

Click Delete Schedule in the Tasks corner.

The list of scheduled task will appear. Highlight the task to be deleted and click Delete.



The scheduled task will be removed from the list.

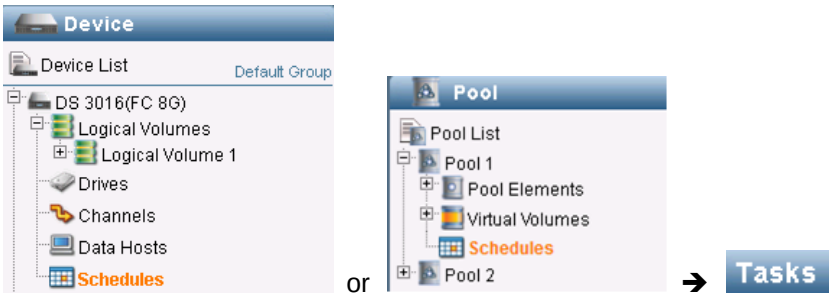
Backing Up or Restoring Schedule Settings

You may save the schedule settings to a local file, or import an existing settings into your subsystem. This feature is useful for moving your RAID environment from one subsystem (or controller) to another.

To use this feature: Your SANWatch must be connected to the subsystem via in-band connection. At least one backup schedule (snapshot or mirror) must exist.

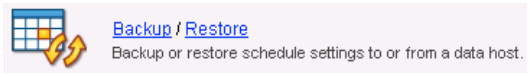
Go to

EonStor DS subsystems: SANWatch Home > Device sidebar > Device List > device name > Schedules
ESVA subsystems: SANWatch Home > Pool sidebar > Pool List > pool name > Schedules

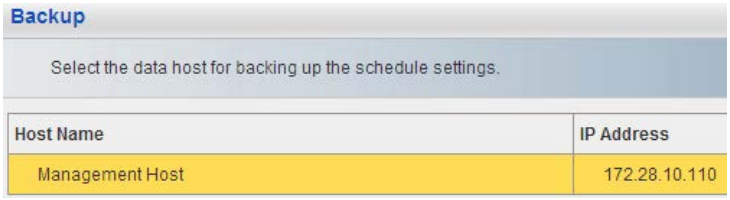


Backing up Settings

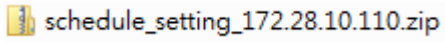
Click Backup in the Tasks corner.



The list of available hosts will appear. Highlight the host and click OK.

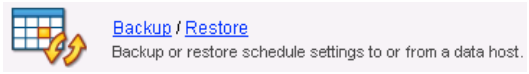


The settings of scheduled tasks will be exported as a zip file and downloaded to your computer.

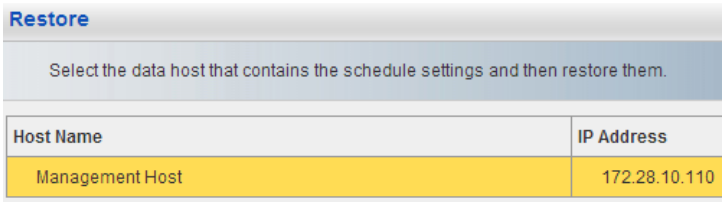


Restoring Settings

Click Restore in the Tasks corner.



The 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 is packed in zip format (*.zip). When you import a configuration data, do not unpack the zip file – select the original zip file and import it.

Appendix

TCP/IP and UDP Port Assignments

Use these ports if you manually configure secure access to SANWatch. Contact your network administrators if management access needs to span across protected networks.

Software	58630	SSL port for connecting RAID subsystem
	58632	Non-SSL port for connecting RAID subsystem
	58641	Port for receiving automatic discovery responses
	8818	Port for SANWatch
Management Host Agent	58634	Port for receiving requests from the Notification Manager
	58635	Port for redundant configurations when synchronizing Management Host Agent
	58641	Port for receiving automatic discovery responses
	58699	Port for receiving requests for portal access to SANWatch
In-Band Data Host Agent	58630	SSL port for a console to connect to Data Host Agent
	58632	Non-SSL port for a console to connect to 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