DS-A80 Series Storage System

Quick Operation Guide

UD.6L0205B1019A01

Thank you for purchasing our product. If there is any question or request, please do not hesitate to contact dealer.

This guide may contain several technically incorrect places or printing errors, and the content is subject to change without notice. The updates will be added into the new version of this guide. We will readily improve or update the products or procedures described in the guide.

The figures shown in this manual are for reference only.

Regulatory Information

FCC Information

FCC compliance: This equipment has been tested and found to comply with the limits for a digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

FCC Conditions

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions:

1. This device may not cause harmful interference.
2. This device must accept any interference received, including interference that may cause undesired operation.

EU Conformity Statement

CE

This product and - if applicable - the supplied accessories too are marked with "CE" and comply therefore with the applicable harmonized European standards listed under the Low Voltage Directive 2006/95/EC, the EMC Directive 2004/108/EC, the RoHS Directive 2011/65/EU.

2012/19/EU (WEEE directive): Products marked with this symbol cannot be disposed of as unsorted municipal waste in the European Union. For proper recycling, return this product to your local supplier upon the purchase of equivalent new equipment, or dispose of it at designated collection points. For more information see: www.recyclethis.info

2006/66/EC (battery directive): This product contains a battery that cannot be disposed of as unsorted municipal waste in the European Union. See the product documentation for specific battery information. The battery is marked with this symbol, which may include lettering to indicate cadmium (Cd), lead (Pb), or mercury (Hg). For proper recycling, return the battery to your supplier or to a designated collection point. For more information see: www.recyclethis.info

Contents

Chapter 1 Introduction

1.1 Description

Developed on the basis of Linux operating system, the storage system is a kind of high-performance and cost-effective Gigabit network storage system and is mainly applicable to the medium and large-scale video surveillance system, featuring flexible allocation and facilitated configuration. Adopting the embedded modular design, the product promotes the stability and reliability of the storage system, and provides massive storage space with low cost.

1.2 Features

- Storage for NAS files;
- Storage for IP SAN block data;
- Redundant backup for RAID 0, RAID 1, RAID 5, RAID 10 and RAID 50 data;
- Network bonding and load balance;
- Support HDD hot-swap capability;
- Working status LED indicators and alarm by email notification;
- Logs saving and inquiry for working status and operation records.

Chapter 2 Installation and Working Environment

The device described in this manual should be installed in a standardized equipment room.

2.1 Power Supply System

The storage system is very sensitive to the change of a voltage, and an excessive high or low voltage, or a sudden change of the voltage may delete the data in the memory or even cause the damage of the components. To avoid of such damage, you must ensure the pure power supply and the power must be grounded. You are recommended to use the UPS, or the multiple power supply if permitted.

Requirements:

- The voltage should be 110V~220V+/-4%, and the sudden change cannot be more than 110V~220V +/-15%; Frequency: 50~60Hz+/-0.5Hz;
- Make correct Neutral Line and GND Line connections, and the voltage between them must be less than 1V.
- Grounding for AC power supply system: ensure the GND line is properly connected. The grounding for the chassis is recommended.
- Grounding for DC power supply system: the chassis must be properly grounded.
- Connect all power cords before applying power to the redundant power supply module.
- The storage system supports management for some UPS models.

2.2 Control of Working Environment

The over-high or over-low temperature and other unsatisfying installation and running environment factors can cause failures of the chip and mechanical components of the device, and thus they affect the stable and reliable running of the device as well as the data safety on the disks. Please follow the measurements shown below to take proper measurements:

- Use an air conditioner to control the temperature and the humidity at least 2 or 3 days before installing the device.
- The working environment of the device should meet the temperature of 23 ºC±2 ºC, humidity of 50%Rh ± 5%Rh and the temperature change rate of <5 ºC/h with non-condensing.

- The floor in the equipment room must be capable of loading more than 600kg/m^2, and the height between the floor and the ceiling must be more than 2.7 m. The loading capability of the rack can be computed in 10 kg/U, e.g., for a 4U chassis, the required loading capability of the rack is 40 kg.
- Ensure adequate air ventilation of the rack.
- Close all the doors and windows to prevent the dust or use a dust-filtering ventilation device. The dust particulate (≥5μm) must be less than 18,000 particulate / $(dm)^3$.
- In an conditions of non-working status of the device, the horizontal and vertical vibration acceleration value of the equipment room's floor surface must be lower than 0.5m/S^2 .
- The rack or surface on which the device is installed must be properly grounded, and ensure that each device is grounded as well. The resistance between the device casing and the ground must be less than 4Ω.

2.3 Installation and Initial Power-on

- The device shall be placed on the fixed flat surface. Tilting surface is not allowed.
- You can use the standard plate in the industrial cabinet or use the guide (not provided) to install the device to the rack. It is recommended to use the bolts to fix the device to the rack through the mounting screw holes on the rack.
- Connect all the power cords of the device to the power socket and wait for 12 hours before starting up. The temperature of the device and the equipment room must be consistent to prevent the damage caused by a huge temperature difference.
- If the device has been transported and stored for more than 10 days; perform the previous operation and then start up and run the device for 30 minutes without the hard disks. And then you shut down the device, insert the hard disks and start the device again.

2.4 Notes for Installation

- The device is high-precision equipment. Please keep stable and gentle when moving it.
- Multiple people are required to carry the heavy-weight device.
- Installation and running environment must meet standards. Take regular investigations and records for the equipment room, or apply a remote monitoring for the working status of the device.
- Do not unplug the power cord when the device is running.
- In case of alarm beeper produced during the system running, please take immediate check and solution.

2.5 Device Reliability

To enhance the reliability of the operating of the device, you can take the following measurements:

- Use the mobile alarm software installed on the storage system, and the message will be sent to your mobile phone as SMS.
- Add the Email alarm software module and the alarm information can be sent to the dedicated Email address.
- Use the StorOS Manager software to realize the online management and monitor for all the storage devices.
- Connect to the NTP server to adjust time for the storage server to avoid the inaccuracy of record time or record loss.
- Add a SNMP software module, the system alarm can be sent to the SNMP client on a PC.

Chapter 3 Hardware Installation

3.1 Hardware System

The Network Storage System includes hardware system and software system, which can be installed separately. The software storage system is an IP-based system which can manage the network storage devices online.

The hardware system adopts rack-mounted chassis which provides LED indicators for the status of power, network and HDD.

3.1.1 Front View

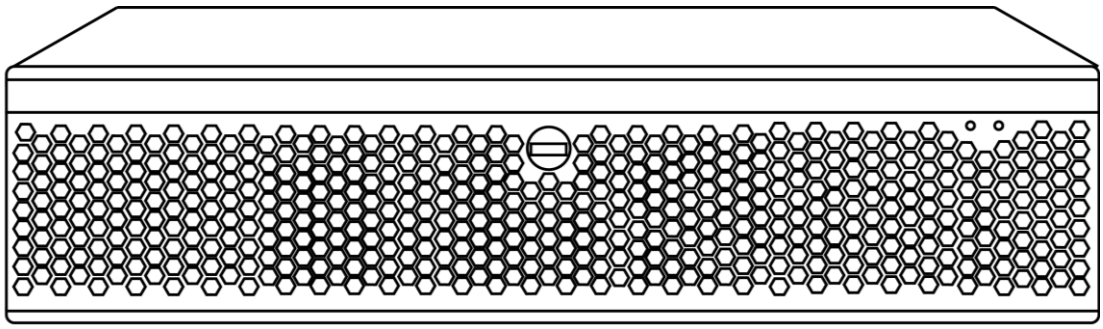


Figure 3. 1 Front View

3.1.2 HDD Slot Number

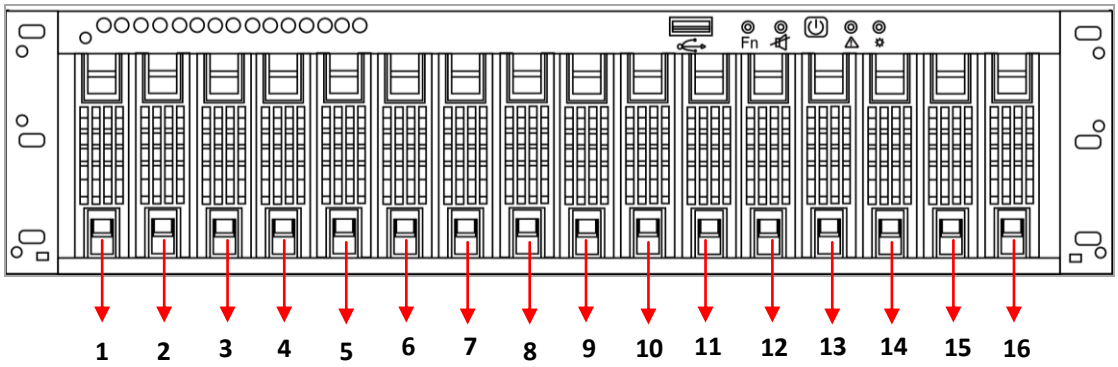


Figure 3. 2 HDD Slot Number

The storage device can be plugged with 3.5-inch hard disks, and the HDD slot No. is numbered from left to right and top to bottom.

3.1.3 Description of Front Panel

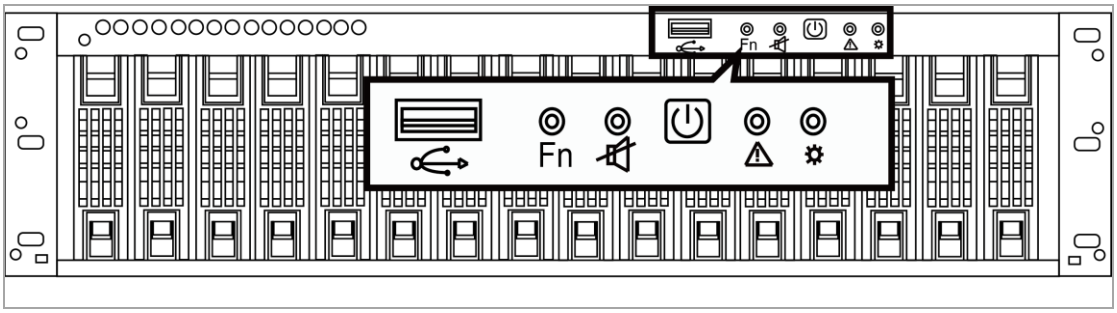


Figure 3. 3 Front Panel

Table 3-1 Description of Front Panel

Icon	Name	Description
	Mute	This button is used to clear the beep sound when the Fan and power failure alarm occurs.
	Power Switch	Turn on/off the system.
	Alarm LED Indicator	The indicator lights in red in case of Fan or power supply failure alarm.
	Power LED Indicator	Indicates the power connection status. When the device is powered up, the indicator lights in green.

NOTE

The USB interface and FN Device Positioning button are reserved and not available on the front panel of DS-A80 series storage system.

3.1.4 Description of Rear Panel

Rear Panel of Single Power Supply

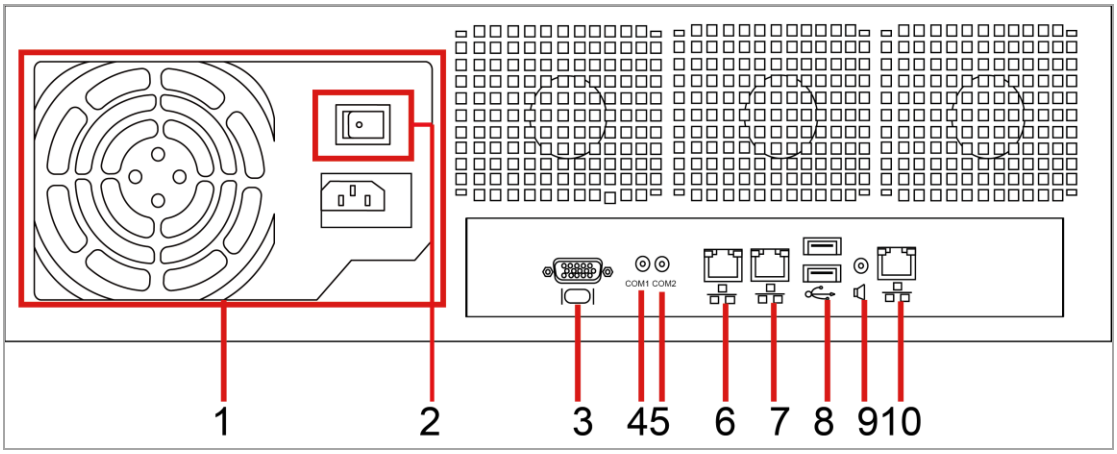


Figure 3. 4 Rear Panel of Single Power Supply

Table 3-2 Description of Rear Panel

Icon	Description
1	Power Supply
2	Power Switch
3	VGA Interface
4	COM 1: Hyper Terminal
5	COM 2: UPS
6	Data Port 1
7	Data Port 2
8	USB Interface
9	Audio Out
10	Management Port

Rear Panel of Redundant Power Supply

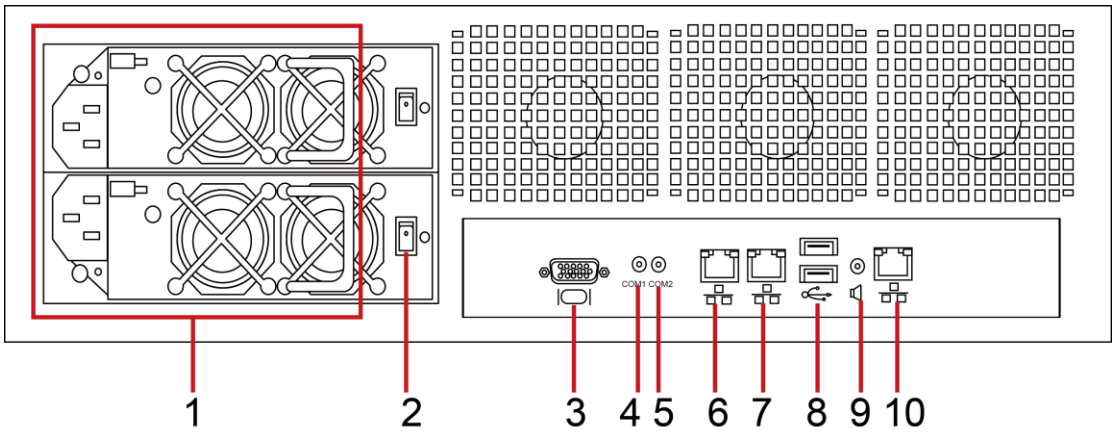


Figure 3. 5 Rear Panel of Redundant Power Supply

Table 3-3 Description of Rear Panel

Icon	Description
1	Power Supply
2	Power Switch
3	VGA Interface
4	COM 1: Hyper Terminal
5	COM 2: UPS
6	Data Port 1
7	Data Port 2
8	USB Interface
9	Audio Out

10	Management Port

3.2 Installation Requirement

Before installation, please prepare the following equipment and accessories:

1. Network Storage System
2. Power cord
3. 100M/1000M network cable (CAT 5e recommended)

The following accessories are optional or user-provided:

1. Gigabit Ethernet switch (second-layer switch, user-provided)
2. Rack guide apparatus (optional)

NOTE

Please refer to the packing list for the attached accessories.

3.3 HDD Installation

3.3.1 Selecting HDD Model

Adopt the certificated professional HDD models to ensure the stable running of the system and the reliable data storage. It is highly recommended to purchase the enterprise-class hard disks, e.g., Seagate Constellation™ ES, Western Digital WD RE3 and WD RE4 series hard disk. The use of non-enterprise-class hard disks for establishing RAID may cause instability of the system, thus leading to the data damage. In case of hard disk failure, please replace it with the functional one immediately so as to prevent the data loss or performance degradation.

Please refer to the List of Compatible HDD Models of our company for recommended HDD models.

NOTE

In order to avoid damages during transportation, it is recommended to package and transport the hard disks separately from the chassis of network storage system.

3.3.2 Installing HDD

To install the HDD on the brackets:

1. Insert the key and turn in clockwise direction to open the panel lock.

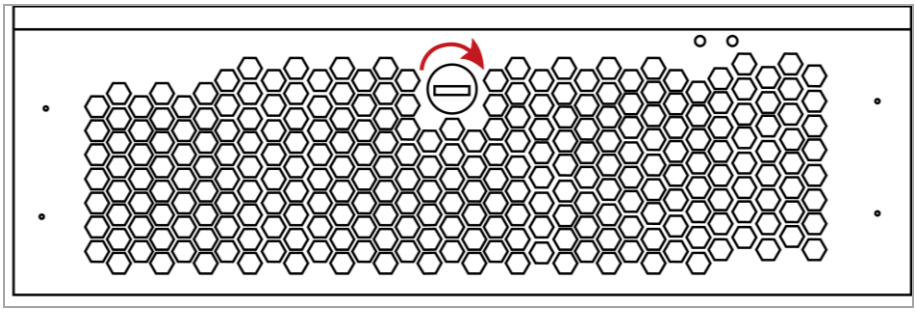


Figure 3. 6 Open Panel Lock

2. Separate the top edge of the front panel from the chassis, about 1cm in distance. And then lift and disassemble the front panel.

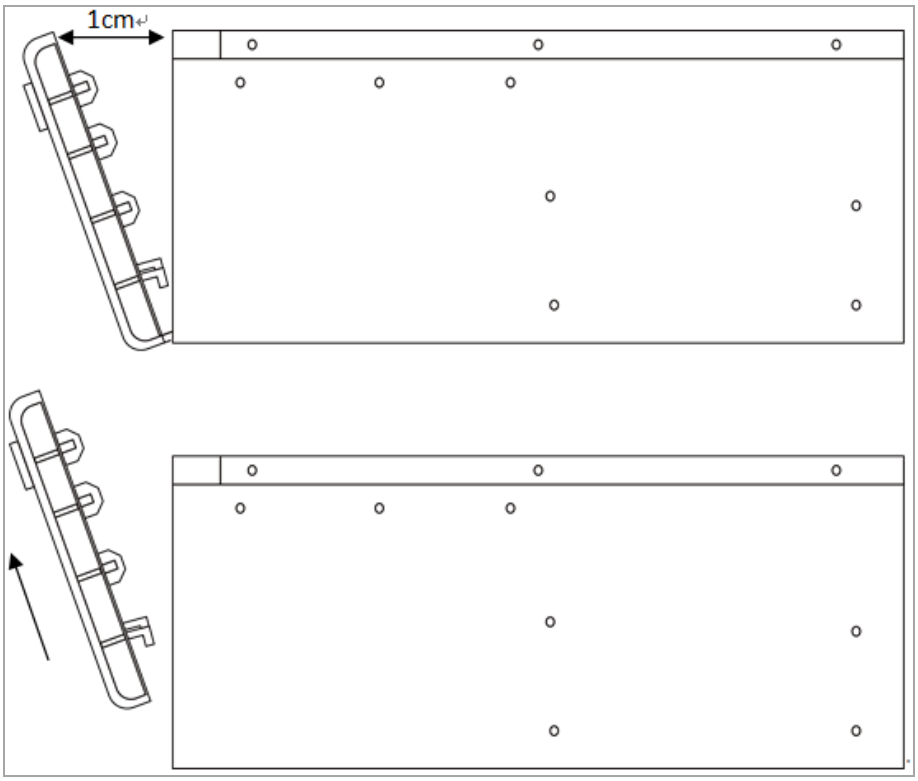


Figure 3. 7 Disassemble Front Panel

NOTE

To avoid the bayonet damage under the front panel, the separation distance between the front panel and chassis cannot be too long.

3. Press the spring lock of the HDD, and then pull out the HDD bracket from the chassis along the guide apparatus.

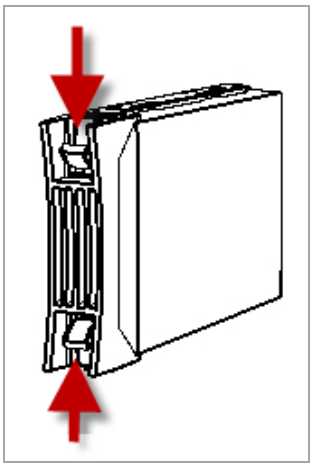


Figure 3. 8 Pull Out HDD Bracket

4. Remove the plastic module from the HDD bracket.

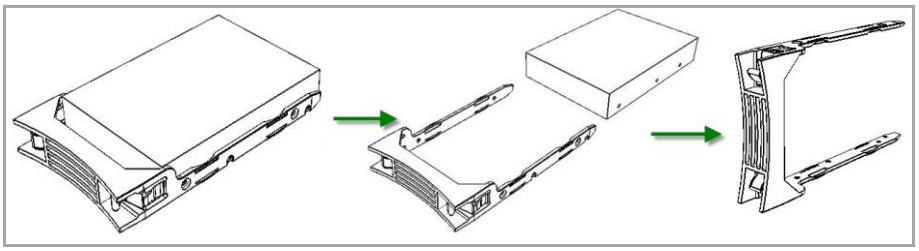


Figure 3. 9 Unplug HDD Bracket

5. Use four screws to secure the HDD to the bracket (with the HDD label facing up).

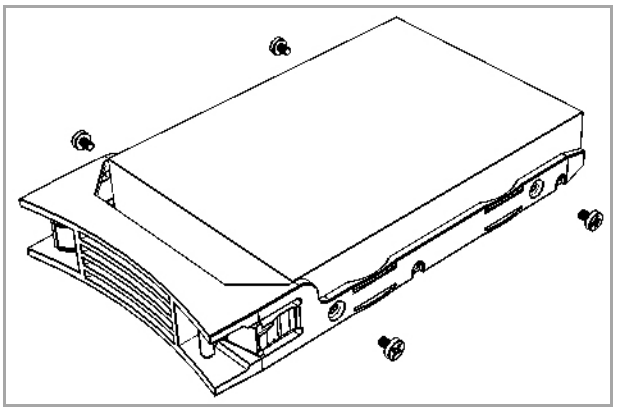


Figure 3. 10 Install HDD to Bracket

6. Press the spring lock of the HDD, insert the HDD bracket to the chassis and push it along the guide apparatus until to the bottom, to ensure the bracket being seated into position and locked.
7. Repeat the steps to install all the other HDDs.
8. Finally, close the front panel and lock it with the key again.

3.3.3 Precautions for HDD Installation

Before you plug or unplug the hard disks, please take the following precautions:

1. After you have plugged the hard disk to its mounting bracket, please use the provided screws to fix the four edges of the mounting bracket.
2. Make sure the HDD mounting bracket is steadily plugged to the chassis along the slot.
3. When you unplug the hard disk, unplug it about 3cm away from the chassis and then make it stay about 30 seconds on the guide apparatus before totally unplug it from the chassis. Since the discs of the hard disk are still spinning at high speed just after powering off, unplugging the hard disk immediately will damage the discs.
4. The system supports disk hot swapping, yet the data storage safety is not ensured.
5. Please avoid frequent plugging/unplugging of the hard disks during the system running so as to maintain long service life of the hard disks.
6. Check and examine the working status of the hard disks every two months, or configure the system with auto check and examine task.
7. The certification for the new hard disk is required when it is plugged to the system for the first time. Please refer to *Chapter 11 Bad Disk Management* for details.

Please avoid unplugging a hard disk when it is writing/reading data so as to prevent data loss.

3.4 Hardware Installation

Prior to starting the system, please make sure the following connections have been correctly made:

1. HDD installation.
2. Power cord connection: connect the power cord to 220VAC power supply.
3. Management port: use a CAT 5e network cable (supplied) to connect the management port to the Internet, so that the management PC or server is able to access the network storage system.
4. Data port: use a CAT 5e network cable to connect the data port to the Internet, to transmit and receive the data.
5. Serial port: initialize the storage system via serial port if needed (not for users).

3.5 Power On/Off

1. Make all power connections before the redundant power supplies.
2. Press the power switch on the front panel to start the system.
3. It takes about 5 minutes to start the system. The device beeps after the startup is complete.
4. If the unit fails to start up, please check whether all connections have been properly made.

5. As the unit has the power-off protection capability, the data will be automatically recovered when it starts up again if the unit encounters power-off failure in running.
6. To turn off the system, click the **Power off** button on the System Monitor interface (Maintenance > System monitor) of the management system.
7. To reboot the system, click the **Reboot** button on the System Monitor interface (Maintenance > System monitor) of the management system.

Chapter 4 System IP Address Configuration

4.1 Login

Management port (mainly for parameter settings) and data port (mainly for data transmission) are provided. The administrator is allowed to access the system via web browser and then configure the network parameters if needed.

Before you start:

1. Set the IP address of your PC (e.g., 10.254.254.10), making sure that the PC and the management port of storage system are in the same network segment.
2. Use a crossover network cable to connect the Ethernet port of your PC and the management port of the storage system.
3. Make sure the network communication between the storage system and PC has been successfully established.

NOTE

The default IP address of the system management port is 10.254.254.254.

Steps:

1. Input the IP address of the storage system in the address bar of the web browser, e.g., https://10.254.254.254:2004, and press the Enter key. A login window will pop up.
2. Input the user name *web_admin* and the default password *123, and* click the **Login** button to log in the Basic Storage Management system.

Figure 4. 1 Login

NOTE

The default IP address of the data port is 192.168.0.100.

4.2 Configuring Network Settings

4.2.1 Modifying Network Parameters

Steps:

1. Click System > Network to enter the Network Management interface.
2. Check the checkbox to select the data or management NIC on the NIC List for configuration.
3. Click **Modify** to open the Modify NIC Info dialog box.
4. Input the IP address, subnet mask, gateway and MTU for the selected NIC.
5. Click **OK** to save the new settings.

When the MTU value is higher than 1500, the network transmission performance will be improved effectively, yet it needs support of the connected router and other network devices.

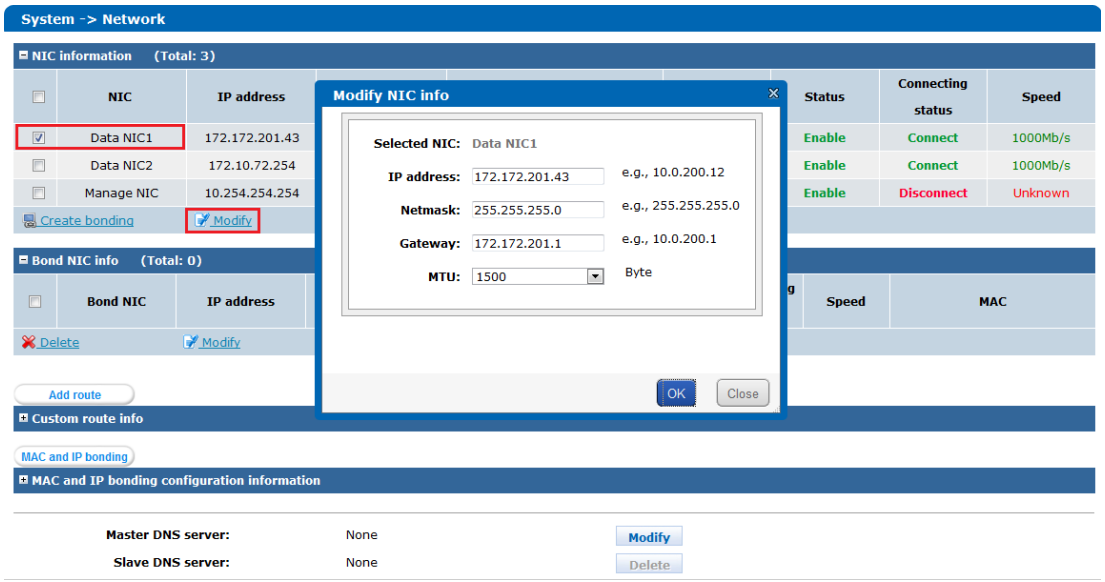


Figure 4. 2 Modify NIC Information

4.2.2 Configuring Bonding Mode

Steps:

1. Click System > Network to enter the Network Management interface.
2. Click the **Modify** button of **Current NIC bonding mode** at the bottom of the interface, and a drop-down list pops up.

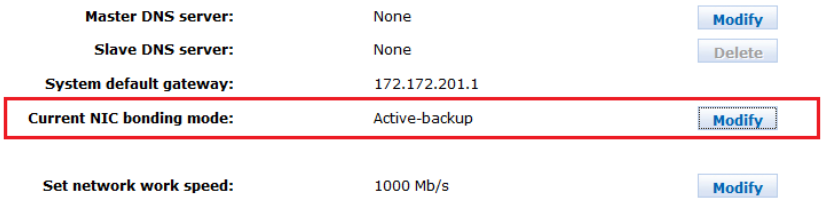


Figure 4. 3 Current NIC Bonding Mode

3. Select the bonding mode from the drop-down list to meet the actual needs, and then click **OK** to save the settings.

Figure 4. 4 Modify NIC Bonding Mode

NOTE

Restart the system after the NIC bonding mode is modified to activate the new settings.

4.2.3 Configuring Multi-NIC Bonding

Purpose:

Multi-NIC bonding is supported by the storage system, to realize the functionalities such as data transmission bandwidth expansion, fault-tolerance, flow control, etc. Only the data NICs can be

Steps:

1. On the Network Management interface, select the NICs from the NIC List for bonding.

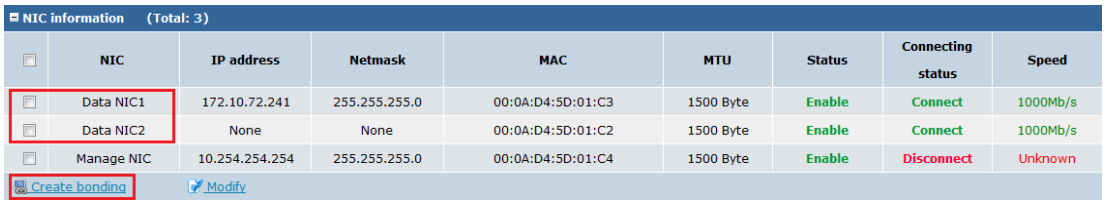


Figure 4. 5 NIC Information

2. Click **Create Bonding** in the **NIC information** field, and a dialog box pops up.

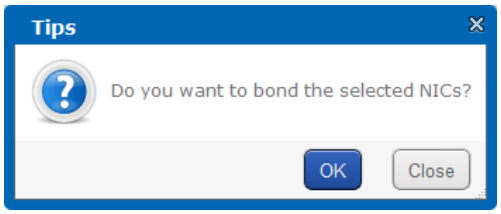


Figure 4. 6 Bond Selected NICs

3. Click **OK** to confirm the settings. It takes a few seconds to bond the selected NICs, and a message box will pop up after the NIC bonding is complete.

NOTE

- Please stop the data access to the storage system during NIC bonding process in case of data loss.
- The IP address of the first data NIC will be adopted for the bond

4.2.4 Deleting Multi-NIC Bonding

Steps:

1. On the Network Management interface, select the bond NIC from the list in the **Bond NIC info** field.

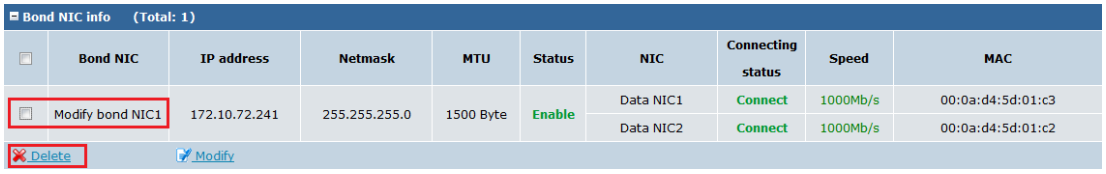


Figure 4. 7 NIC Bonding Information

2. Cick **Delete** to delete the selected bond NIC and a dialog box pops up.

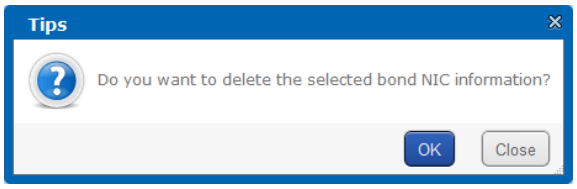


Figure 4. 8 Delete Bond NIC

3. Click **OK** to confirm the settings. And a message box will pop up after the selected bond NIC is deleted.

You can also select the bond NIC, and click **Modify** to modify the network parameters of the selected bond NIC, including IP address, subnet mask, gateway and MTU.

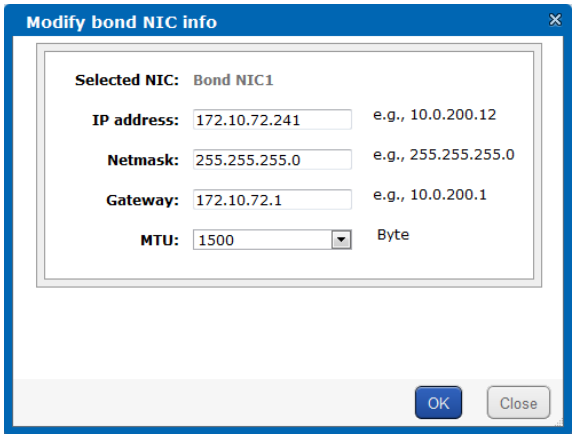


Figure 4. 9 Modify Bond NIC Information

4.2.5 Network Connection

Perform the following 4 principles to connect the storage system and the client server (your PC, laptop or server) to the network.

1. For the network connection stability, it is highly recommended that the storage system and the client server should be in the same network segment.
2. Connect the client server and storage system to the switch directly.
3. Connect all the data NICs to the switch.
4. The IP address of management NIC (10.254.254.254) is used for debugging and it cannot be used for video streaming.

NOTE

Both management NIC and data NIC can be used for system debugging.

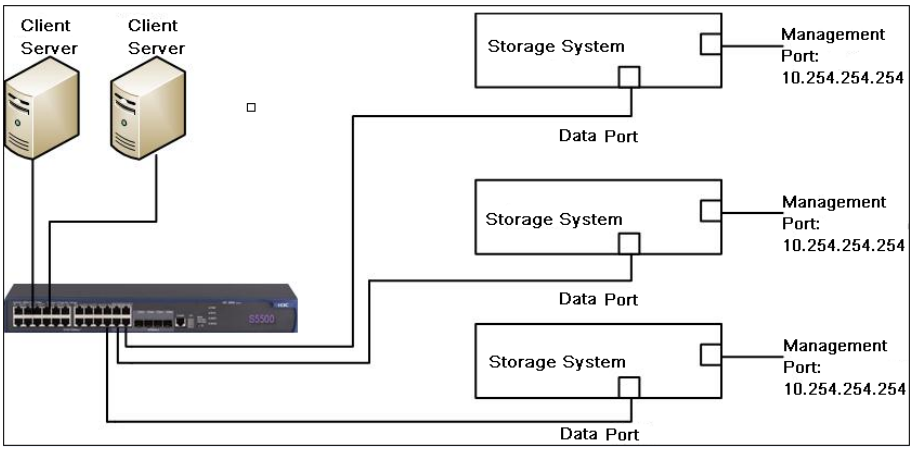


Figure 4. 10 Network Connection

Chapter 5 CVR Configuration

5.1 System Requirements

- Create private volume and record volume for management and record respectively.
- Establish private volume on the physical volume of RAID which is created on the enterprise-class HDD; and two private volumes are required.
- In large-scale projects, multiple record volumes are recommended, to reduce the recording pressure for each volume. Space of single LUN which constitutes the record volume is recommended to be no more than 8 TB.
- There is a certain mapping relation between the private volume and record volume. If the total capacity of record volumes exceeds 60TB, then the capacity of the private volumes should be configured as 20GB. While the total capacity of record volumes exceeds 120TB, then the capacity of the private volumes needs to be set as 30GB, and so on.
- CVR configuration mode:
  - Quick Settings. For details, see Section *5.2.1 Quick Settings*.

    NOTE

    You can also configure the CVR quick settings via iVMS-4200. Add the storage server to the client, click the **Remote Config** button and then click the **Quick Configuration** button on the HDD settings page.
  - Manual Configuration. For details, see Section *5.2.2 Manual Configuration*.

5.2 Configuring Private Volume

5.2.1 Quick Settings

If there are no virtual storage pools and RAID in the system, the **Quick-setting** button on the CVR Configuration page will be activated. Otherwise, the button is invalid.

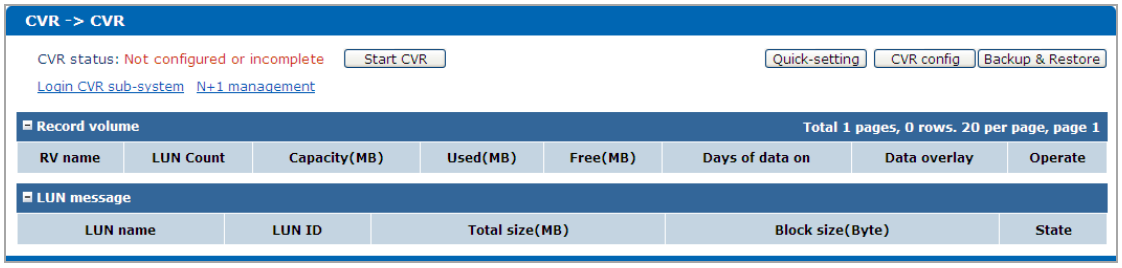


Figure 5. 1 CVR Configuration

Click the **Quick-setting** button and a message box pops up. Then click the **OK** button to confirm the settings and start the quick settings of CVR.

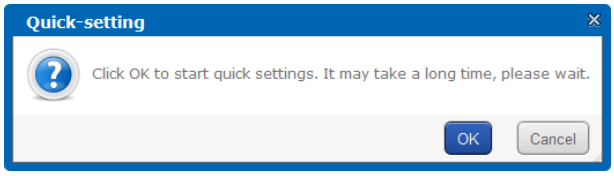


Figure 5. 2 Confirm the Quick Settings

Automatically, the physical volume or created RAID group will be added to the virtual storage pool first, and then the private volume, spare volume and record volume will be set.

NOTE

If there are more than 3 LUNs in the system, an archive volume will be created. Otherwise, no archive volume is provided.

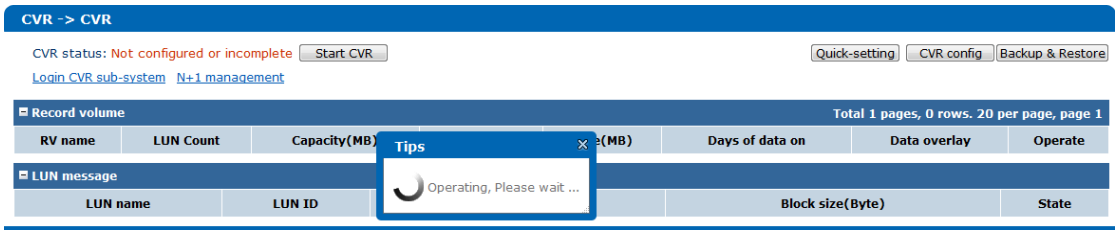


Figure 5. 3 Quick Settings Process

After the quick settings process is complete, no free LUNs are available in the system, and the service condition of the storage pool, CVR and LUN are displayed as follows:

Figure 5. 4 Service Condition of Storage Pool

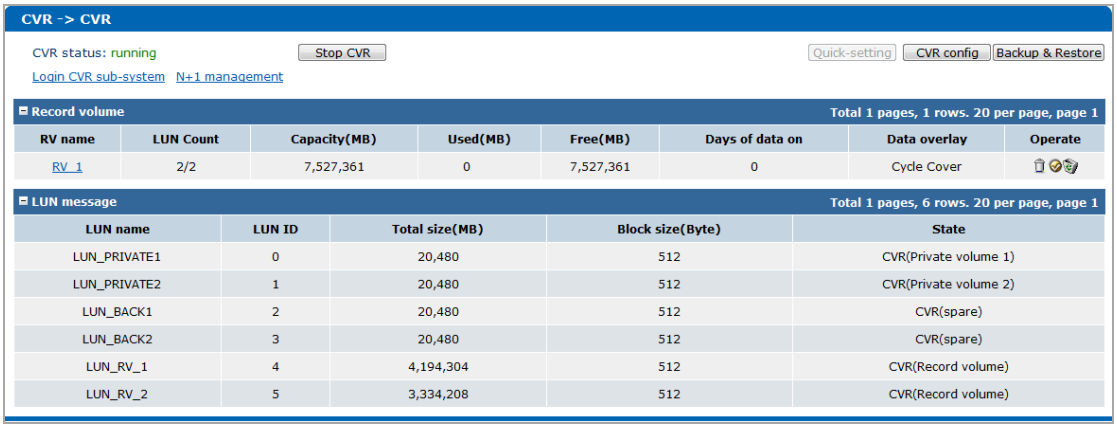


Figure 5. 5 Service Condition of CVR and LUN

- The bad disk and warning disk cannot be added to the virtual storage pool.
- If there is any non-enterprise-class disk in the system, adopt the single disk working mode.
- If there are less than 6 disks in the storage device, adopt single disk working mode without considering the disk number of expansion enclosure.
- If there are more than or equal to 6 disks in the storage device, adopt RAID working mode. Meanwhile, for the expansion enclosure, if there are more than or equal to 6 disks, adopt RAID working mode, too; otherwise, no settings are required for the disks.
- If there is only one disk in the system, no spare volume will be created; in the single disk working mode, no spare volume will be created on the last disk of storage device; in the RAID working mode, 2 spare volumes will be created on each RAID.

5.2.2 Manual Configuration

Steps:

1. Create the virtual storage pool.

   For details, see Section *6.4 Virtual Storage Pool Management*.

2. Create the LUNs.

   1) Enter the LUN Management interface.

      Storage>LUN

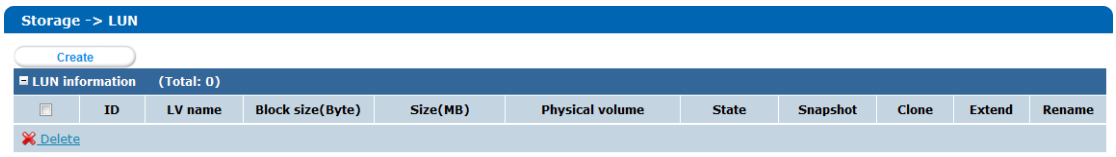


Figure 5. 6 LUN Management Interface

   2) Click the **Create** button to open the Create LUN page.

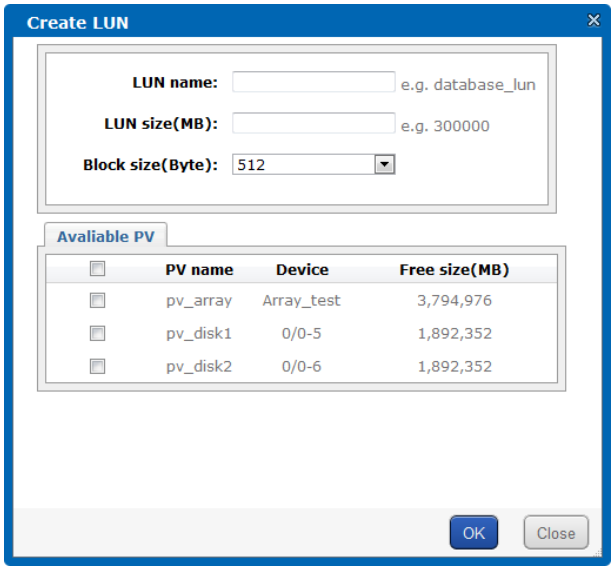


Figure 5. 7 Create LUN

3) Input the LUN name, LUN size in the text fields and select the block size from the drop-down list.

4) Check the checkbox to select a physical volume on which the LUN is created.

5) Click **OK** to confirm the settings.

NOTE

At least 5 LUNs are required for the CVR service, of which 4 LUNs with capacity over 20GB need to be set as private volumes and the corresponding spare volumes, and other LUNs need to be set as record volumes.

3. Create the private volumes.

1) Enter the Private Volume Settings interface, and the free LUNs in the system are displayed on the Free LUN list.

CVR > CVR > CVR config > Set private volume

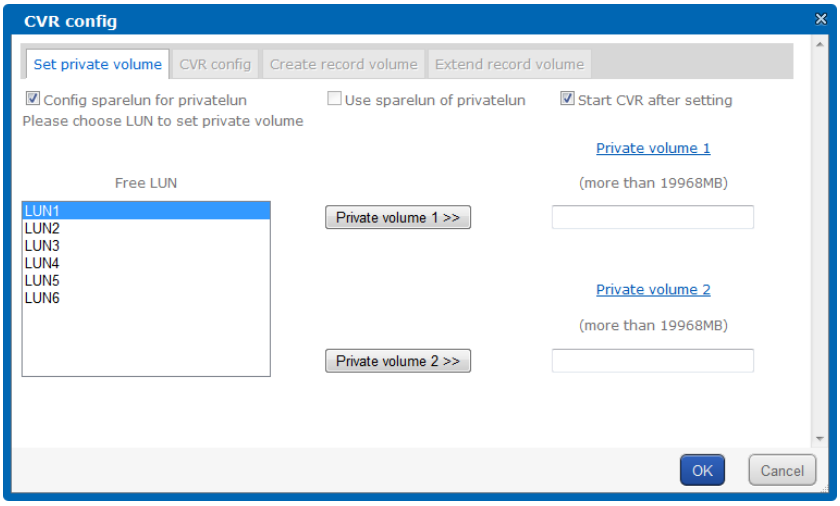


Figure 5. 8 Create Private Volume

2) Select the free LUN from the list and then click Private volume 1 >> or Private volume 2 >>

to set it as private volume 1 or private volume 2.

NOTE

Two LUNs will be automatically set as the spare volumes of the two private volumes. You can check the checkbox of **Use sparelun of privatelun** to enable the use of spare volume in case of private volume failure.

3) Optionally, you can check the checkbox of **Start CVR after setting** to start the CVR service after the private volume settings are complete.

4) Click **OK** to confirm the settings.

NOTE

It is recommended that the spare LUNs are in the different physical volume with the private LUNs. For details of physical volume, see Section *6.4 Virtual Storage Pool Management*.

4. Create the record volume.

1) Enter the Record Volume Settings interface.

CVR > CVR > CVR Config > Create record volume

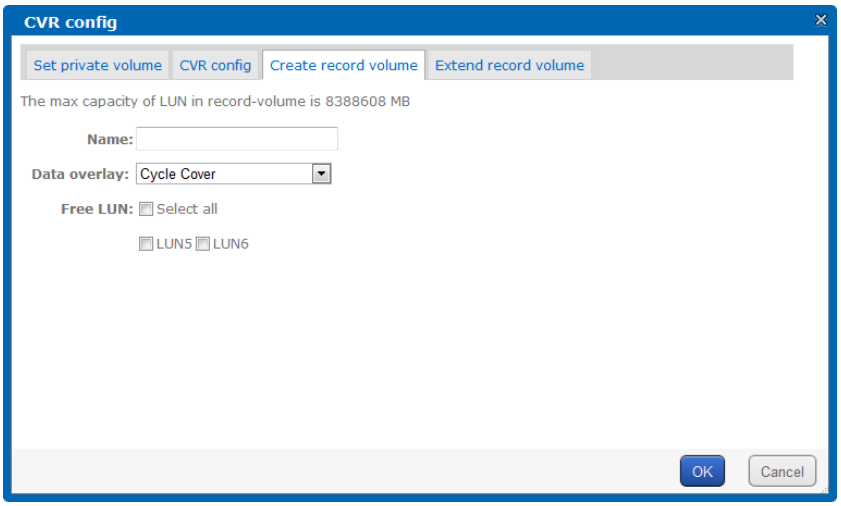


Figure 5. 9 Create Record Volume

2) Input the name for the record volume, select the Data overlay mode and select the free LUN(s) to be set as the record volume.

3) Click **OK** to confirm the settings.

NOTE

- The name should be no longer than 24 characters, and blank space and quotation marks are invalid.
- You can select multiple LUNs and merge them as a record volume.
- **Cycle Cover** and **No Cover** can be selected for Data overlay. In **Cycle Cover** (default) mode, the record files stored in the record volume will be overwritten when the record volume becomes full. In **No Cover** mode, the record process will stop when the record volume

becomes full.

5.3 Configuring Record Settings

5.3.1 Logging in the CVR System

Steps:

1. Input the IP address of the storage system in the address bar of the web browser, and press the Enter key. The address is formatted as: https://IP address of the storage server:2004.

   Example: If the IP address of the storage server is 192.0.0.64, then the address you should enter is https://192.0.0.64:2004.
2. Select *CVR* as the login system from the drop-down list.
3. Input the user name and password in the corresponding text fields. The default user name and password are *nvr_admin* and *123*.
4. Click the **Login** button to enter the CVR system.

   You can also click **Login CVR sub-system** on the CVR Management interface to enter the system login interface.

Figure 5. 10 Log in CVR System

5.3.2 Adding the Encoding Device

Steps:

1. Enter the Encoding Device Management interface.

   Device Management > Device

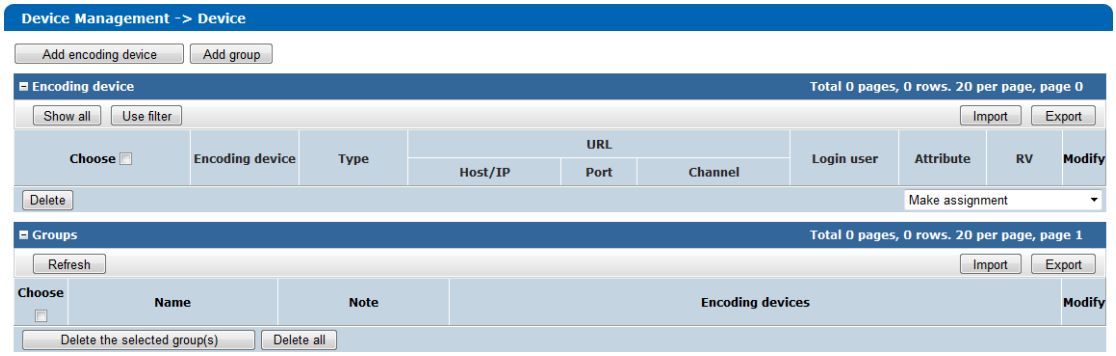


Figure 5. 11 Encoding Device Management

2. Click the **Add encoding device** button to open the Add Encoding Device page. Configure the corresponding settings for the device.

   Name: Edit a name for the encoding device as desired.

   Type: The encoding protocol of the encoding device.

   IP/Host: The IP address of the encoding device.

   Port: Input the port number of the encoding device. The port is *8000* by default.

   Channel: Set the channel No. for accessing. Multiple channels can be configured. E.g., enter 1, 3-5, 7 to represent the 1, 3, 4, 5, 7 channel of the device.

   Stream Media Server: Input the IP address of stream media server (optional).

   Login user: The user name of the encoding device.

   Password: The password of the encoding device.

   Options: Check the checkbox to enable the corresponding function of the device.

   Related to: Set the related record volume. If no record volume is related, the video of the device cannot be recorded.

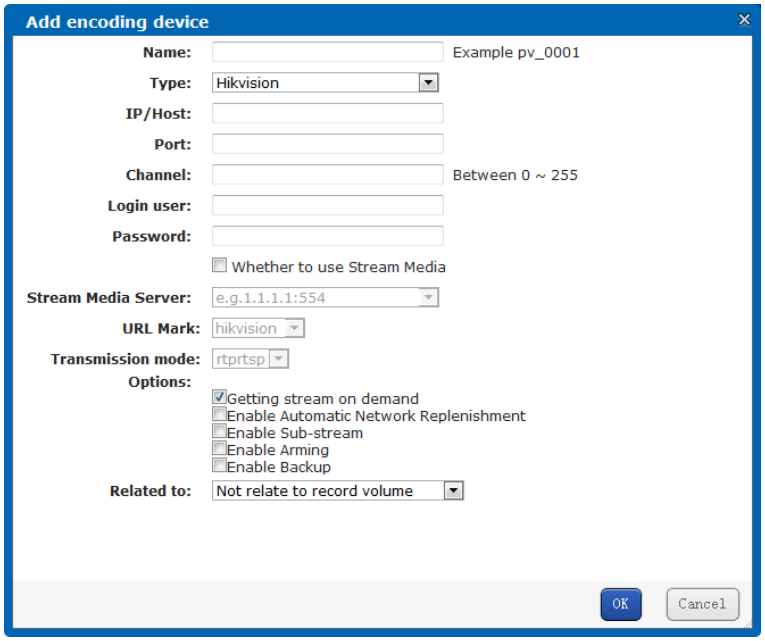


Figure 5. 12 Add Encoding Device

3. Click **OK** to confirm the settings.

   You can view the status of the added encoding devices on the Information interface (Information > Information). The status will be displayed as **Ready** after device is connected.

5.3.3 Editing the Record Schedule

Steps:

1. Enter the Schedule Management interface.

   Schedule & Alarm > Schedule

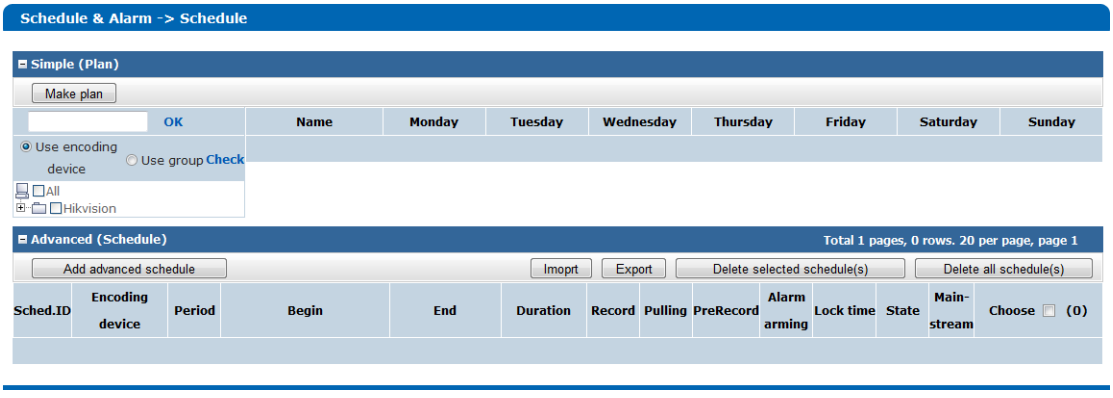


Figure 5. 13 Schedule Management

2. Click the **Make plan** button to open the Record Schedule Settings page.

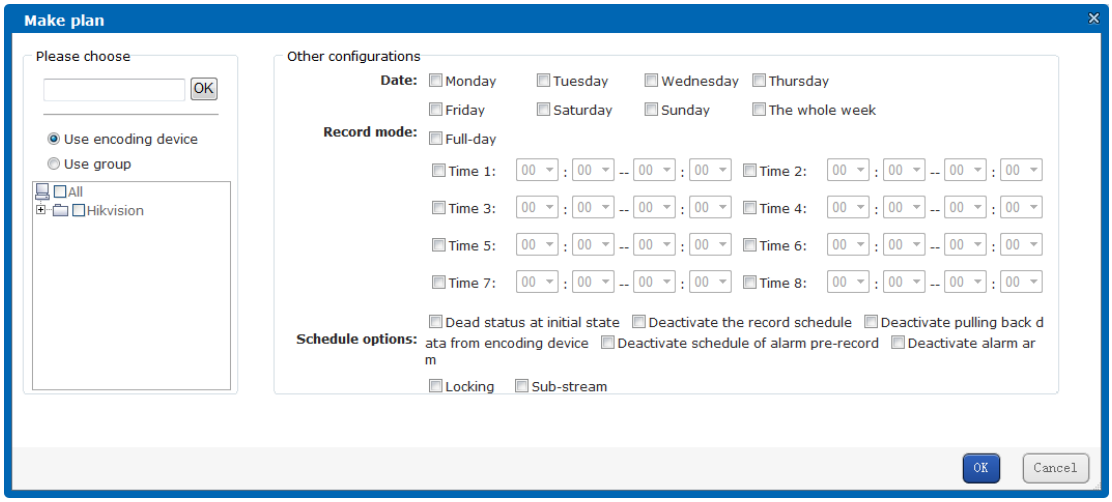


Figure 5. 14 Configure Record Schedule

3. Select **Use encoding device** or **Use group** to show the added encoding devices or groups, and then check the checkboxes to select the encoding device(s) for schedule settings.
4. Select the day(s) of the week, and then set full-day recording as the record mode or customize time periods for recording as desired.

   NOTE

   Up to 8 time periods can be configured for each day.
5. Select the schedule options for the record schedule.
6. Click **OK** to confirm the settings.
7. Repeat steps 2-6 to configure the schedule settings for other encoding devices. Optionally, you can check the checkbox of **All** to set the same schedule for all devices.

5.4 Live View and Playback

5.4.1 Live View

Before you start:

1. Add trusted sites. On the IE browser menu bar, navigate to Tools > Internet Options > Security > Trusted sites and click the **Sites** button to add the IP address of the CVR system to the list of trusted sites.

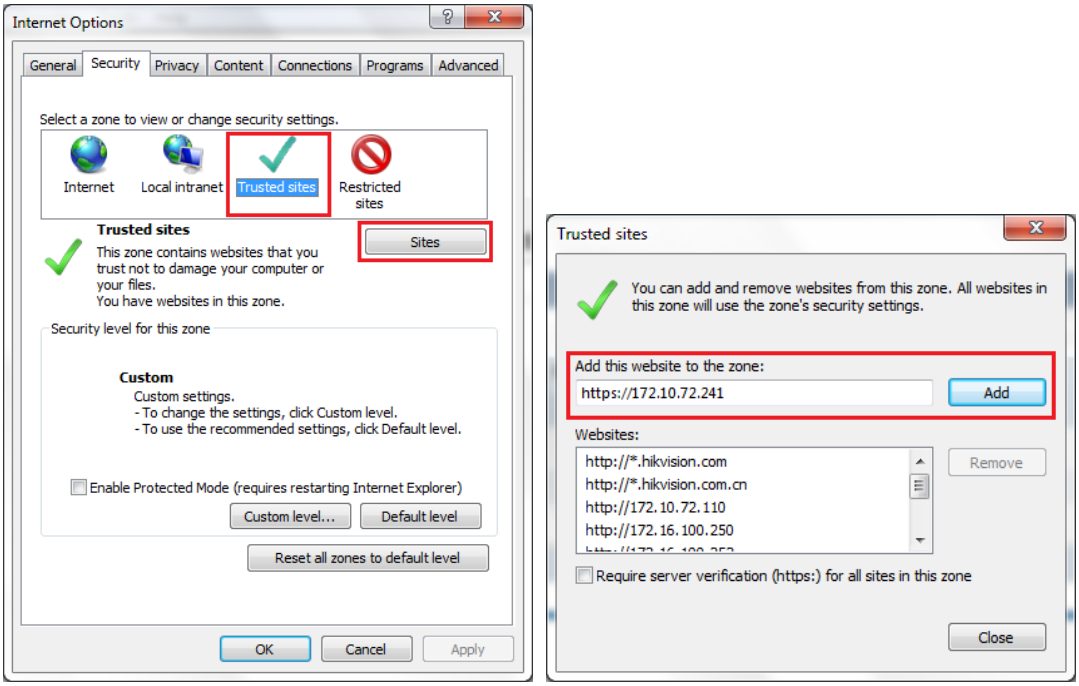


Figure 5. 15 Add Trusted Sites

2. On the IE browser menu bar, navigate to Tools > Internet Options > Security > Custom level to enable the all the ActiveX and plug-ins.

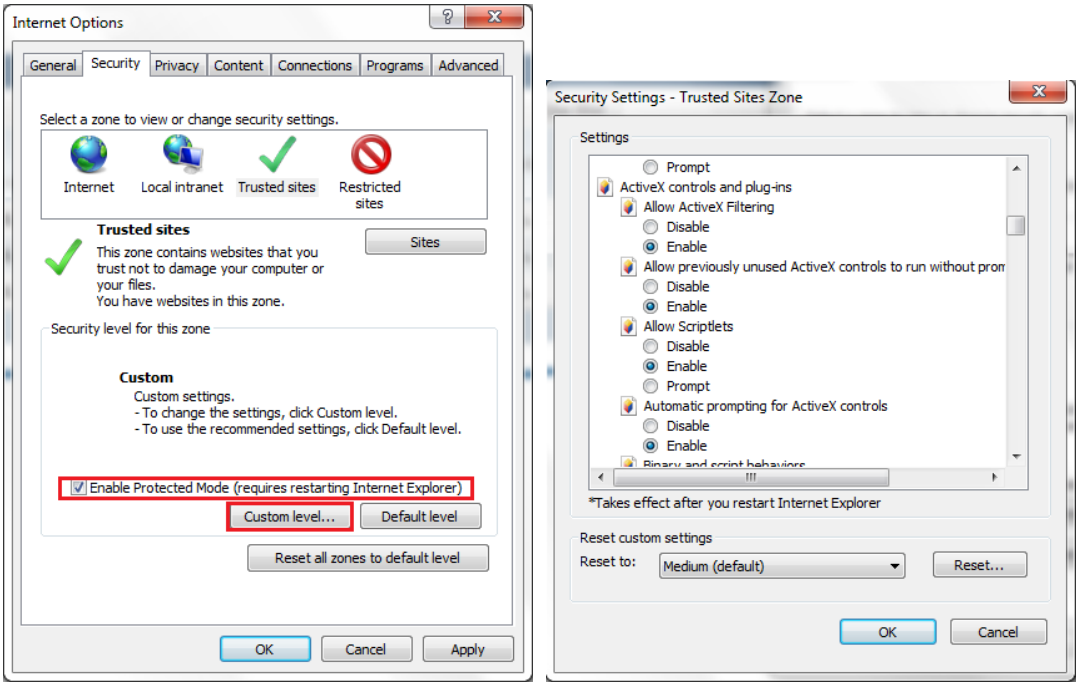


Figure 5. 16 Enable ActiveX

Steps:

1. Enter Encoding Device List interface.

   Live View & Record > Device List

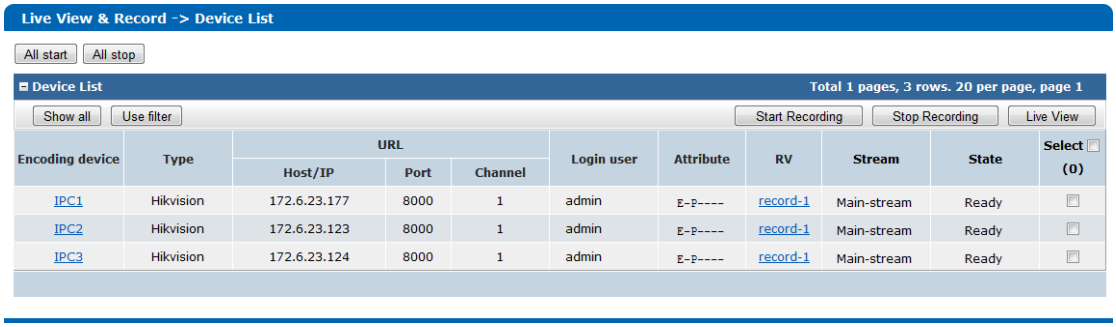


Figure 5. 17 Encoding Device List

2. Check the checkbox in the Select column to select the encoding device for live view, and then click the **Live View** button to view the live video of the selected encoding device.

NOTE

You need to install the plug-in before viewing the live video.

After adding the encoding devices to the storage system, you can select the encoding device from the list and then click the **Start Recording** / **Stop Recording** button to start / stop the recording process for the selected device.

5.4.2 Searching & Playing Back Record Files

Before you start:

The video files of the encoding devices need to be recorded on the storage system.

Steps:

1. Enter the Record Search interface.

   Play & Download > Record Search

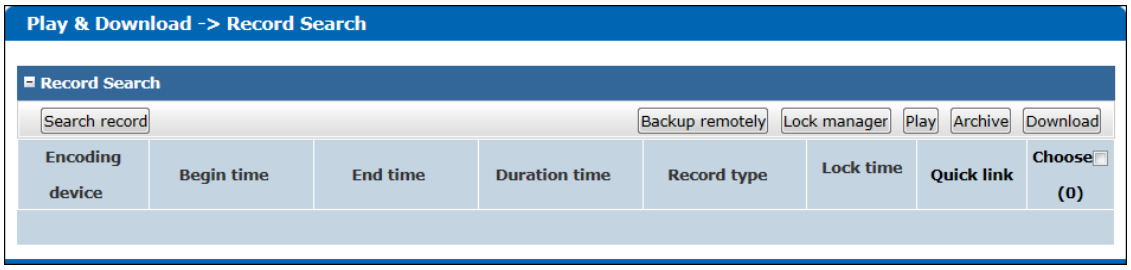


Figure 5. 18 Record Search

2. Click the **Search record** button to open the Search Record Files page.

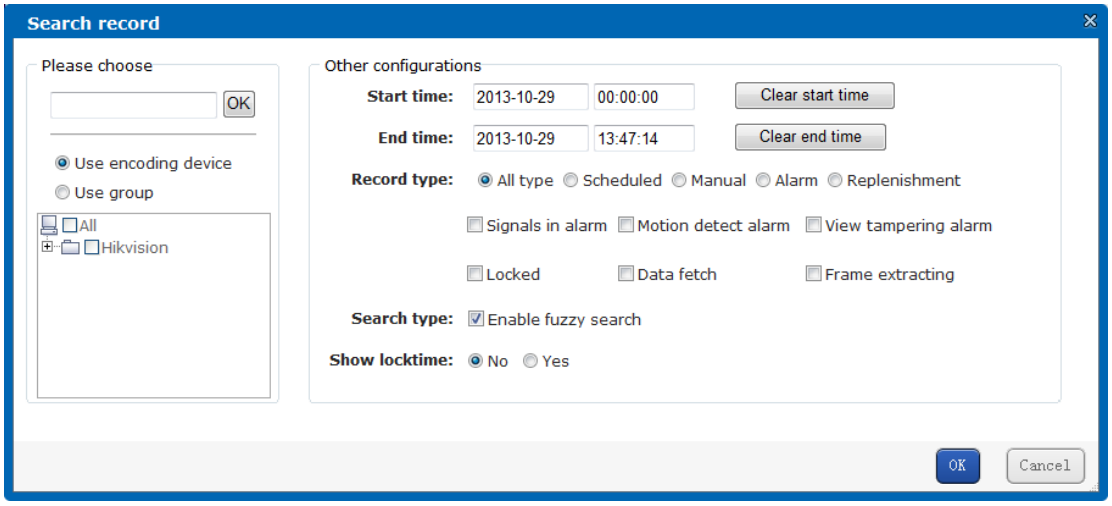


Figure 5. 19 Search Record Files

3. Select the encoding device(s) for search, and then specify the search conditions including start time, end time, record type, etc. Click **OK** to start the search and the matched record files will be displayed on a list.

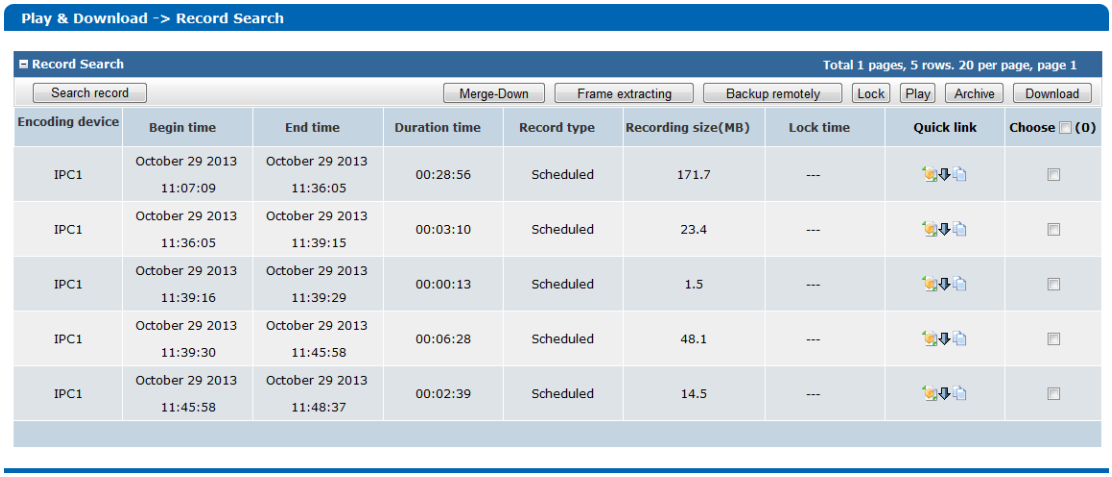


Figure 5. 20 Search Result

4. Check the checkbox in the Choose column to select the record file(s) for playback, and click the **Play** button to play back the selected record file(s).

Figure 5. 21 Record File Playback

Chapter 6 Creation and Use of RAID

The system supports RAID (Redundant Array of Independent Disks) service which provides redundant storage for the data on disks. When the RAID 5 is adopted, there will be no data loss in case of one disk failure in this RAID group.

Before providing the network storage service by single physical disk or RAID group, add the single physical hard disk or RAID group to a virtual storage pool, to work as the physical volume, and then create LUNs (logical unit number) on the physical volume to for the NAS, CVR or iSCSI service.

6.1 Logging in Basic Storage Management System

Steps:

1. Input the IP address of the storage system in the address bar of the web browser, e.g., https://10.254.254.254:2004, and press the Enter key. A login window will pop up.
2. Select *Basic* as the login system from the drop-down list.
3. Input the user name *web_admin* and the default password *123, and* select *Advanced* as the mode.
4. Click the **Login** button to log in the Basic Storage Management system.

Figure 6. 1 Login

6.2 Disk Management

6.2.1 Viewing Disk List

Steps:

1. Enter the Disk Management interface (Storage > Disk). The hard disks will be displayed on a list. You can view the disk information including the supplier, model, size, state and group.

If there are no hard disks installed in the storage system, no disk information is available.

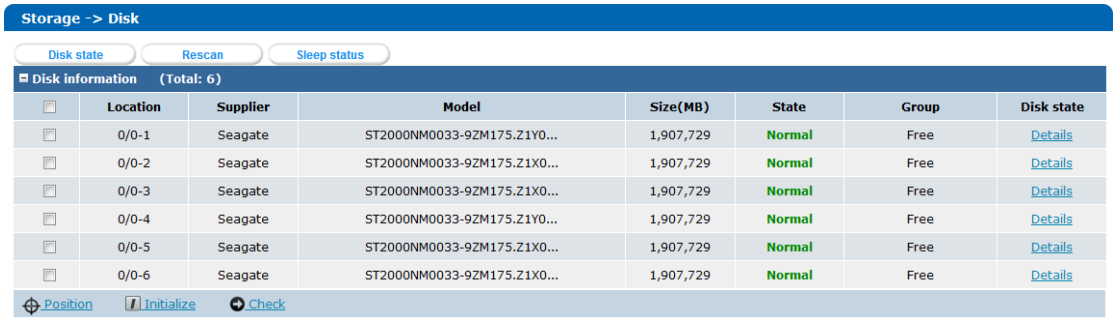


Figure 6. 2 Disk Management Interface

2. Click **Details** in the Disk State column, and you can view status of each disk.

   Click **Disk state**, and you can view the status of all disks in the list.

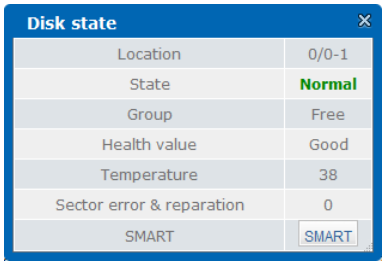


Figure 6. 3 Status of Each Disk

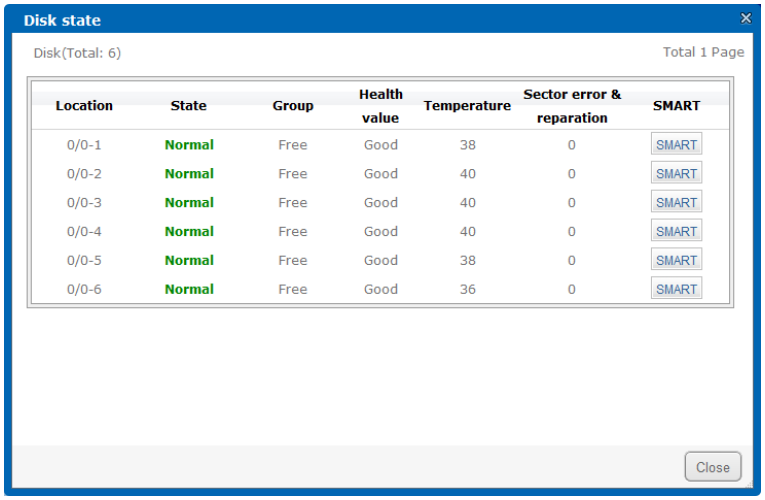


Figure 6. 4 Status of All Disks

3. You can click the **Rescan** button to refresh all the disks available in the system.
4. You can click the **Sleep status** button to view the sleep status of all the disks.

6.2.2 Viewing Disk Checking Status

On the Disk Management interface, click the **Check** button above the disk list to view the disk checking status of all the disks.

The **Check** button above the disk list is only available in the checking process of some disks.

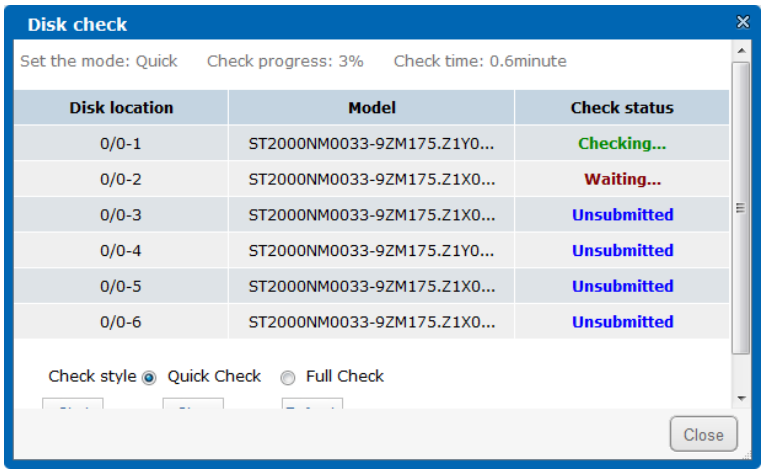


Figure 6. 5 Check Status of Disk

There are 3 types of check status available in the system: checking, unsubmitted and waiting.

Unsubmitted: the current disk has not been submitted for checking.

Waiting: the disk is waiting in the queue to be checked.

Checking: the current disk is under checking.

6.2.3 Checking Disk

Purpose:

When a physical disk is used in the storage system for the first time, the disk status will be shown as *Unauthorized*. You should check the disk before use.

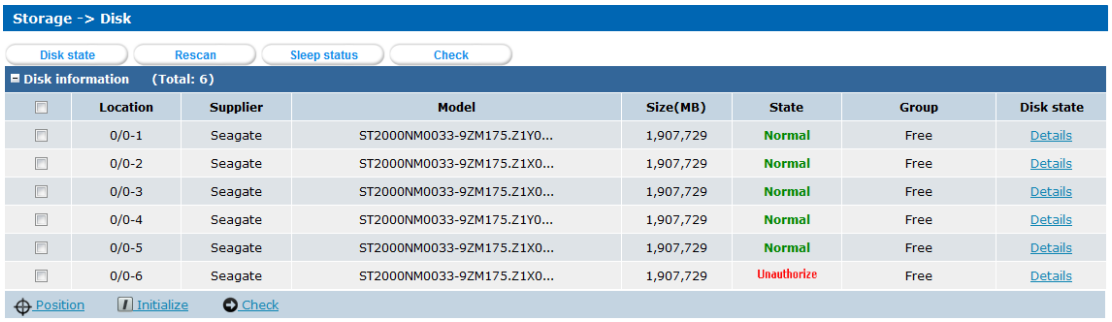


Figure 6. 6 Check Disk

Steps:

1. Select the disk(s) to be checked from the list.
2. Click **Check** under the disk list to open the Disk Check page.

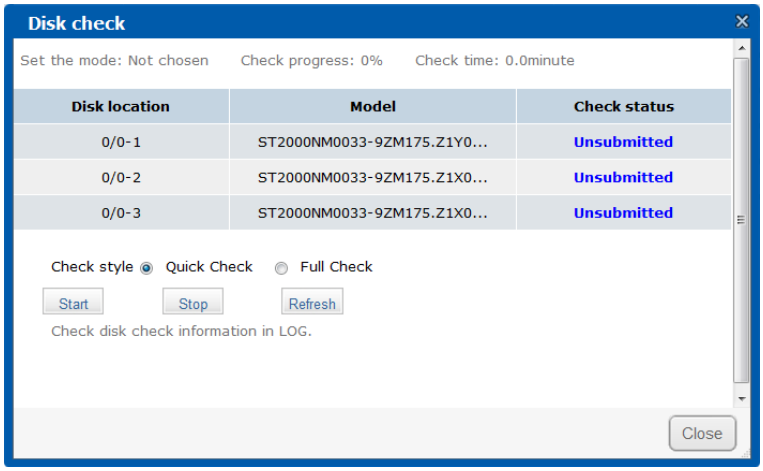


Figure 6. 7 Set Disk Check

3. Select *Quick Check* or *Full Check* as the check style.

   Quick Check: check all disks simutanously and it takes a short time.

   Full Check: check the disks one by one in details which may take a long time. It is recommended when the disks are used for the first time.

4. Click the **Start** button to start checking the selected disk(s). You can view the check progress and check time on the top of the page.

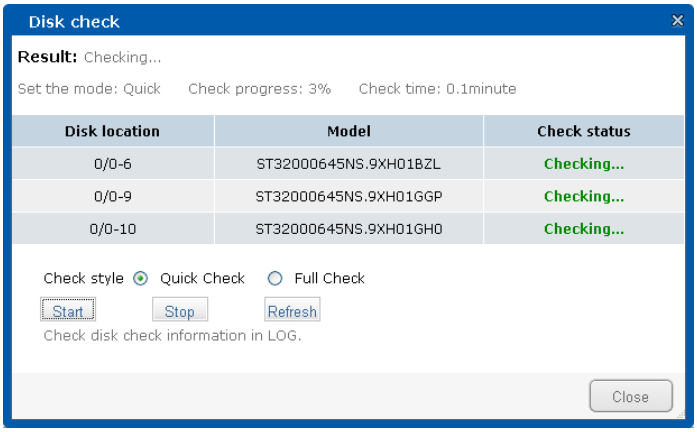


Figure 6. 8 Check Disk

5. You can click the **Stop** button to stop checking all the disks.

   You can also click the **Refresh** button to refresh the latest status of the disks.

6. After the checking process is complete, you can view the disk status in the disk management interface.

6.3 Array Management

6.3.1 Creating an Array

Steps:

1. Enter the Array Management interface.

   Storage > Array

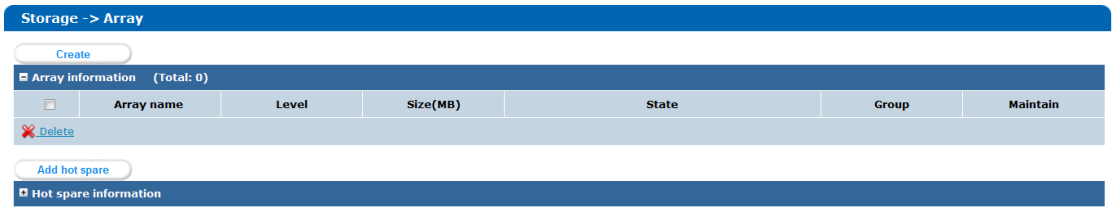


Figure 6. 9 Array Management Interface

2. Click the **Create** button to open the Create Array page.

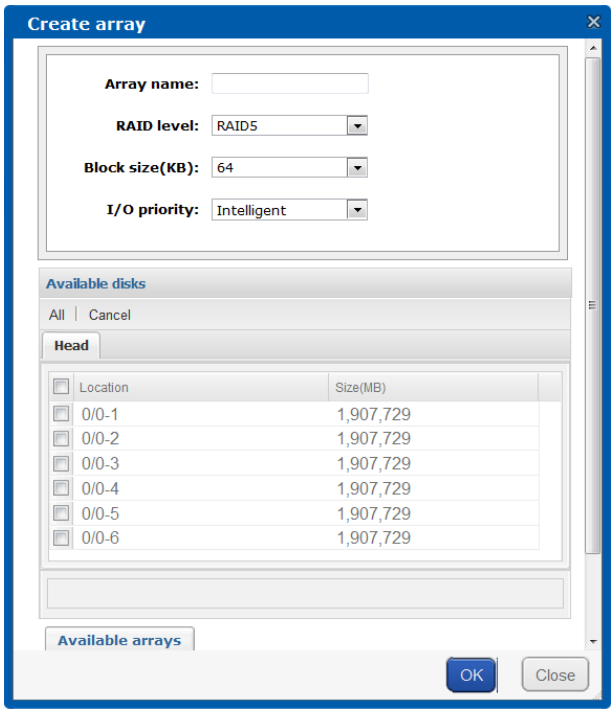


Figure 6. 10 Create Array Interface

3. Edit the array name. Only the letters and numeric are allowed.
4. Set the RAID level from the drop-down list. The RAID 5 is recommended.
5. Select the block size (default: 64KB) and the I/O priority.

   - **Block Size**: The basic unit of the RAID data. When large volume of input/output business data is required, select the larger block size; when small volume of input/output business data is required, select the smaller block size. The default size is 64KB and it is the most balanced option at present.

     NOTE

     When the *Video Surveillance RAID* is set as the block size in RAID 5, you can still play back the current recordings with the first disk in case that the RAID is unavailable.

   - **I/O Priority**: Set the priority for the internal I/O (RAID I/O) and external I/O (Business

I/O), and four options are available.

Intelligent (default): When the business I/O is small, the RAID I/O will be increased automatically; when the business I/O increases, the RAID I/O will be decreased automatically.

Balance: Balance the business I/O and the RAID I/O to guarantee 3MB/s minimum speed for the RAID I/O. This option is usually used when the business I/O is large and the array rebuilding or array initialization needs to be ensured.

Performance Priority: The RAID I/O will be stopped as long as business I/O is processed. This option is commonly used for business test with high performance requirement.

Protection Priority: Keep the RAID I/O as a priority and the business I/O will be affected. This option is mainly used to complete the array rebuilding or array initialization as soon as possible when there is no business I/O.

6. Select the physical disks from the list for creating the array.
7. Click the **OK** button, and confirm the following pop-up dialog box.

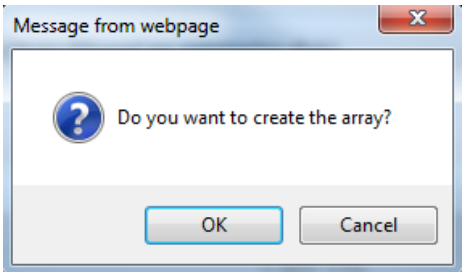


Figure 6. 11 Pop-up Dialog Box

8. Click the **Close** button to finish the settings. And the created array will be displayed on the list on the array management interface.

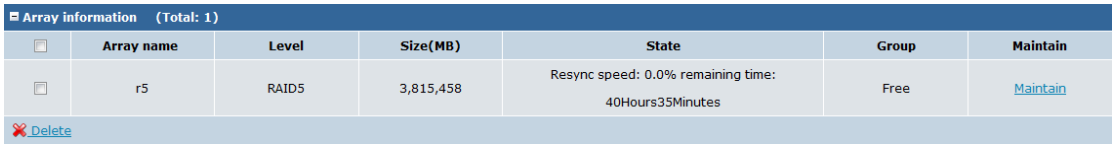


Figure 6. 12 Successfully Added Array

- Only the enterprise-class disks are allowed for creating the array.
- At least 3 physical disks must be selected for creating RAID 5.
- While creating RAID, it is recommended to select the physical disks with the same model and capacity to maintain better performance of RAID.
- Array initialization may bring some pressure on the system and cause an effect to the performance of the current business.

6.3.2 Rebuilding an Array

Purpose:

The array rebuilding function helps to protect the data saved on the unstable or failure physical disk in the array, to ensure the high security and stability of the system.

A hot spare disk is required for the array rebuilding.

NOTE

Array rebuilding may bring some pressure on the system and cause an effect to the performance of the current business.

Auto-rebuilding with Hot Spare Disk

Purpose:

The hot spare disk replaces the disconnected or failure disk in the array automatically, to ensure the high security and stability of the data. It is recommended to add the hot spare disk during RAID configuration.

Two hot spare modes are available**: Global** and **Local**.

- **Global Hot Spare**

Steps:

1. On the Array Management interface, click the **Add hot spare** button to open the Add Hot Spare page, and select *Global* as the group.

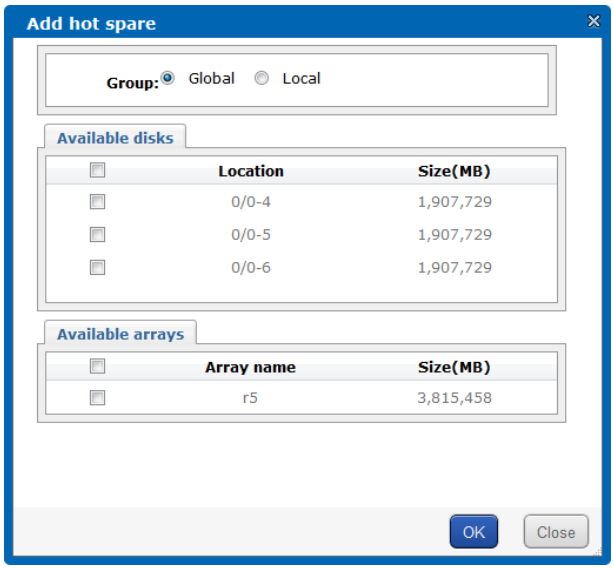


Figure 6. 13 Add Global Hot Spare

2. Select the available disk to be used as hot spare disk.
3. Click the **OK** button and confirm the following pop-up dialog box to add the global hot spare.

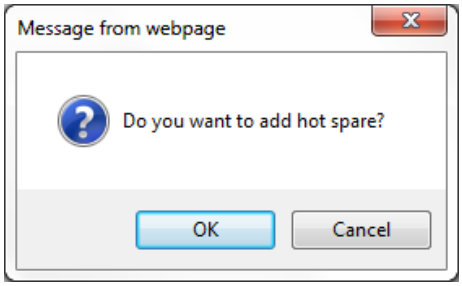


Figure 6. 14 Pop-up Dialog Box

4. Click the **Close** button to finish the adding of hot spare disk. You can view the information of the added hot spare on the Hot Spare Disk List:

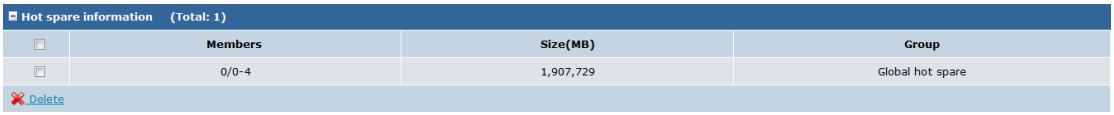


Figure 6. 15 Hot Spare Disk List

When there is a disk disconnected or failed, the array status will change to *Degraded*. With the global hot spare disk configured, the system will automatically start to rebuild the array and the rebuilding speed and remaining time will be displayed in the State column.

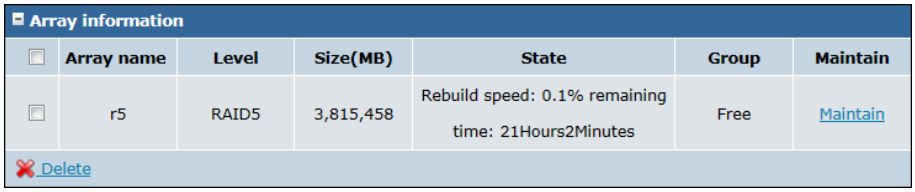


Figure 6. 16 Array Status

- **Local Hot Spare**

Steps:

1. On the Array Management interface, click the **Add hot spare** button to open the Add Hot Spare page, and select *Local* as the group.

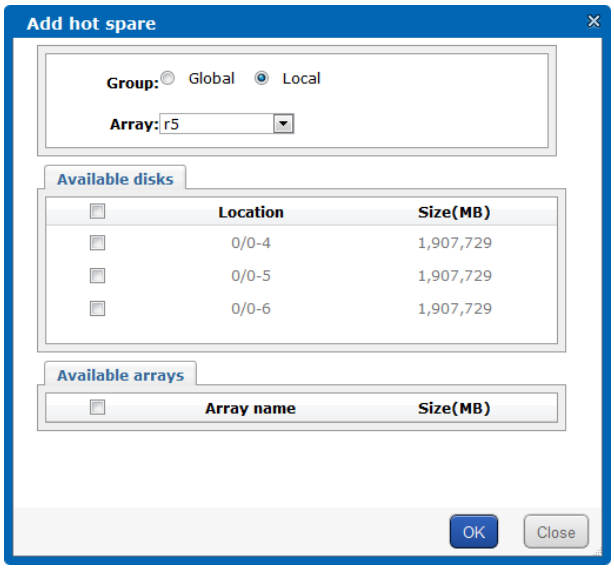


Figure 6. 17 Add Local Hot Spare Disk

2. Select the array to which the hot spare is added.
3. Select the available disk to be used as hot spare disk.
4. Click the **OK** button and confirm the following pop-up dialog box to add the local hot spare.

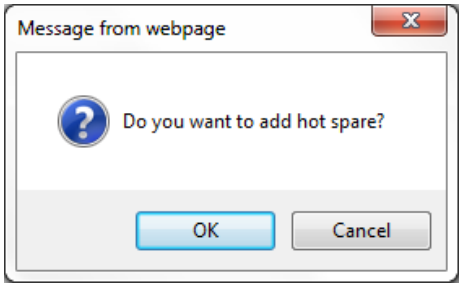
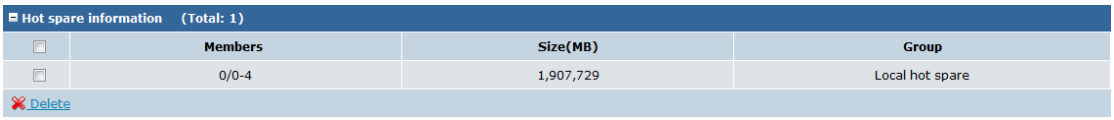


Figure 6. 18 Pop-up Dialog Box

5. Click the **Close** button to finish the adding of hot spare disk .You can view the information of the added hot spare on the Hot Spare Disk List.



Hot spare information (Total: 1)

	Members	Size(MB)	Group
	0/0-4	1,907,729	Local hot spare

Delete

Figure 6. 19 Hot Spare Disk List

When the specified array status changes to *Degraded*, the system will automatically start to rebuild the array.

Manual-rebuilding

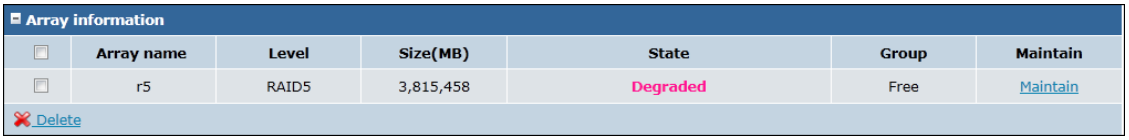
Purpose:

When there is a free disk in the system while no hot spare disk is available, you can start the array rebuilding manually.

Steps:

1. Enter the Array Management interface.

   Storage > Array



Array information

	Array name	Level	Size(MB)	State	Group	Maintain
	r5	RAID5	3,815,458	Degraded	Free	Maintain

Delete

Figure 6. 20 Array List

2. If the array state is displayed as *Degraded*, click **Maintain** on the Array List to enter the array maintenance interface.

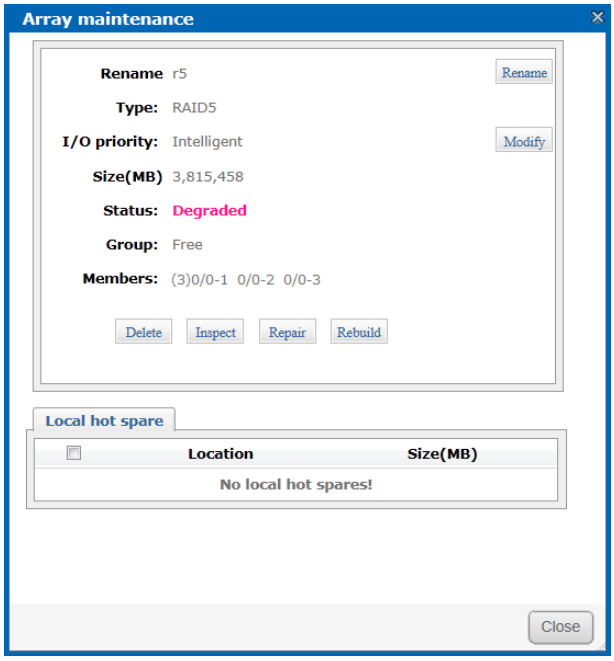


Figure 6. 21 Array Maintenance Interface

3. Click the **Rebuild** button.

Select the available free disk and click the **OK** button to start the array rebuilding.

Auto-rebuilding (optional)

Purpose:

When the array is degraded due to disk disconnection or failure, you can insert a new disk to the system and the system will start to rebuild the array automatically.

Steps:

1. Click Storage > Settings to enter the device settings interface:
2. Click the **Open** button to enable the **Auto-rebuild** function.

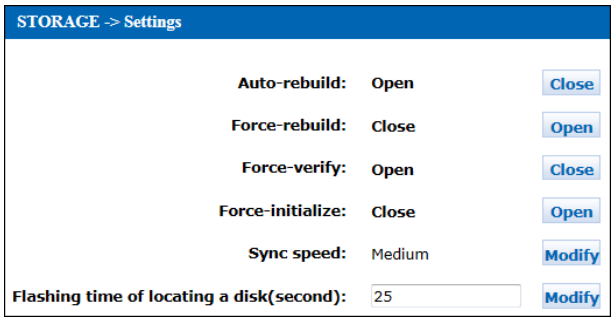


Figure 6. 22 Enable Auto-rebuild

Force-rebuilding (optional)

Purpose:

After the force-rebuild is enabled, the array rebuilding process will continue in case of disk I/O

error. You will be prompted to replace this non-rebuilt disk in the operation log after the array rebuilding is complete, to avoid data loss and enhance the data security.

Steps:

1. Click Storage > Settings to enter the device settings interface,
2. Click the **Open** button to enable the **Force-rebuild** function.

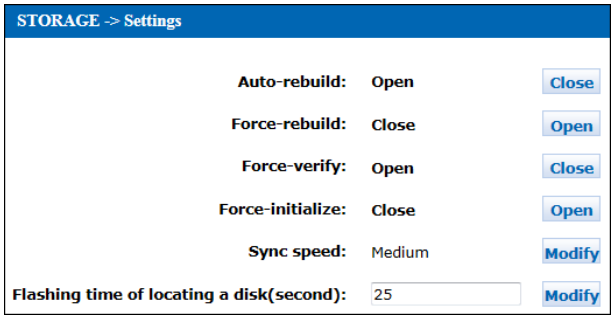


Figure 6. 23 Enable Force-rebuild

6.3.3 Array Verification

Purpose:

Array verification function helps to avoid the data error and file loss in the data storage process. A regular check and maintenance for the disk array is recommended, thus to ensure the high stability and security of the data stored in the array.

There are 2 types of verification modes available: checking the array and repairing the array.

NOTE

Array verification may bring some pressure on the system and cause an effect to the performance of the current business.

Checking the Array

- **Checking Array Manually**

Steps:

1. Click Storage > Array to enter the array management interface.
2. When the array state is *Normal*, click **Maintain** to enter the array maintenance interface.

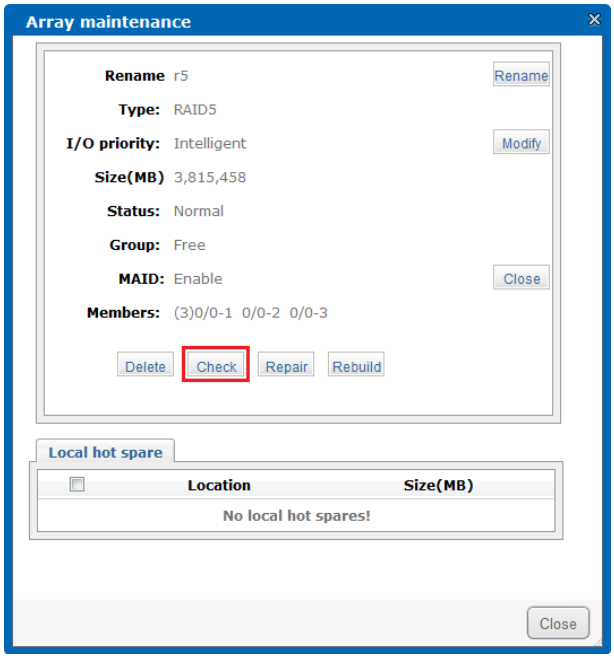


Figure 6. 24 Check Array Manually

3. Click the **Check** button to start checking the selected array.
4. When the array is in checking process, you can view the checking status on the Array List, including the checking speed and remaining time.

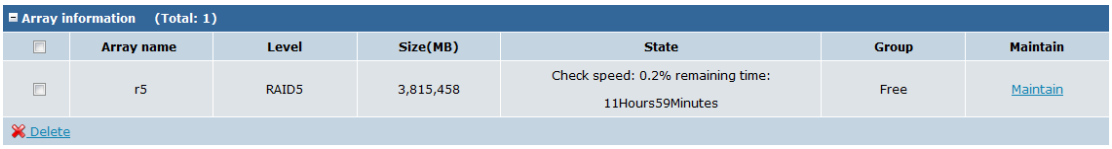


Figure 6. 25 View Checking Status

- **Checking Array by Strategy**

Purpose:

When the array is created, a verification strategy is added automatically to check the array every 3 months (cycle time) since then. You can also add the verification strategy manually for the array.

Steps:

1. When the array status is *Normal*, click Maintenance > Common to enter the Common Maintenance interface.
2. Click the **Add strategy** button to open the Add Strategy page.

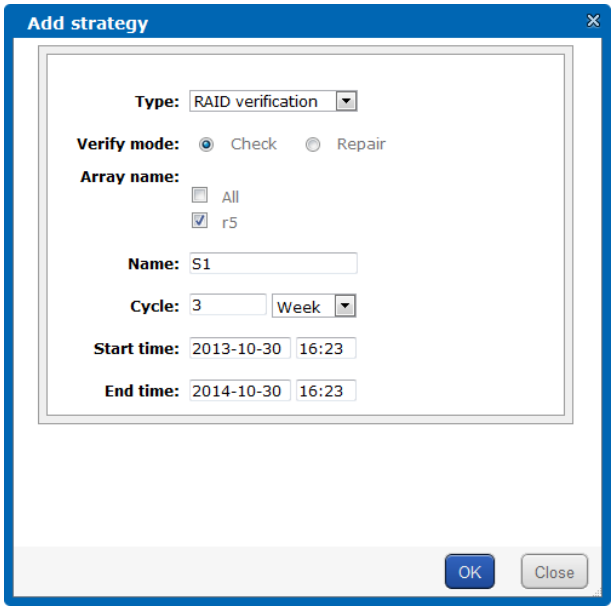


Figure 6. 26 Add Strategy

3. Select the type to *RAID verification* from the drop-down list and the verify mode to *Check*.
4. Select the array for verification form the array list.
5. Edit the name of the strategy as desired, and then set the cycle time and the start time/end time for verification.
6. Click **OK** to confirm the settings. You can view the added strategy on the RAID Verification Strategy List.

RAID verify strategy info (Total: 1)

Event	Name	Object	Cycle	Start time	End time
RAID check	S1	r5	3Week	2013-10-30 16:23	2014-10-30 16:23

Figure 6. 27 RAID Verification Strategy List

Repairing the Array

- **Repairing Array Manually**

Steps:

1. Click Storage > Array to enter the array management interface.
2. When the array status is *Normal*, click **Maintain** to enter the array maintenance interface.

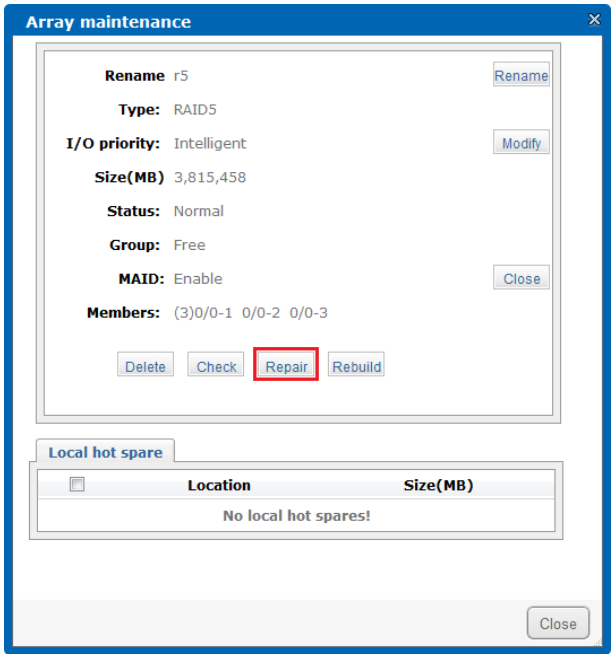


Figure 6. 28 Repair Array

3. Click the **Repair** button to start repairing the selected array.
4. When the array is in repairing process, you can view the repairing status on the Array List, including the repairing speed and remaining time.

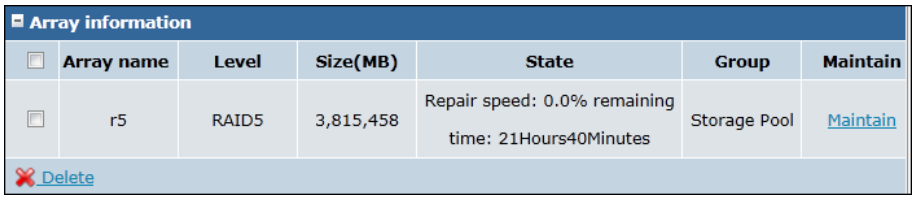


Figure 6. 29 View Repairing Status

- **Repairing Array by Strategy**

Steps:

1. When the array status is *Normal*, click Maintenance > Common to enter the maintenance interface.
2. Click the **Add strategy** button to open the Add Strategy page.

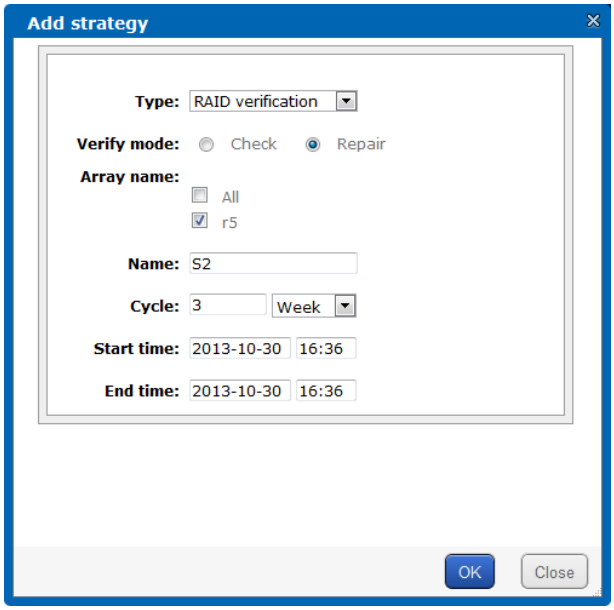


Figure 6. 30 Add Strategy

3. Select the type to *RAID verification* from the drop-down list and the verify mode to *Repair*.
4. Select the array to repair.
5. Edit the name of the strategy as desired, and then set the cycle time and the start time/end time for repairing verification.
6. Click **OK** to confirm the settings. You can view the added strategy on the RAID Verification Strategy List.

RAID verify strategy info (Total: 2)

Event	Name	Object	Cycle	Start time	End time
RAID check	S1	r5	3Week	2013-10-30 16:23	2014-10-30 16:23
RAID reparation	S2	r5	3Week	2013-10-30 16:36	2013-10-30 16:36

Delete

Figure 6. 31 RAID Verification Strategy List

6.4 Virtual Storage Pool Management

The Virtual Storage Pool is a list of physcial volumes, contributing to the management of multiple physical disks and RAID group. A physical volume can be divided into logic volumes (LUN) for different data storage service.

6.4.1 Creating Physical Volumes

Purpose:

The arrays and disks in the system can be added to a virtual storage pool as the physical volume.

Steps:

1. Click Storage > Storage Pool to enter the storage pool management interface.

Figure 6. 32 Storage Pool Management

2. Click the **Add** button to open the Add Storage Pool page.

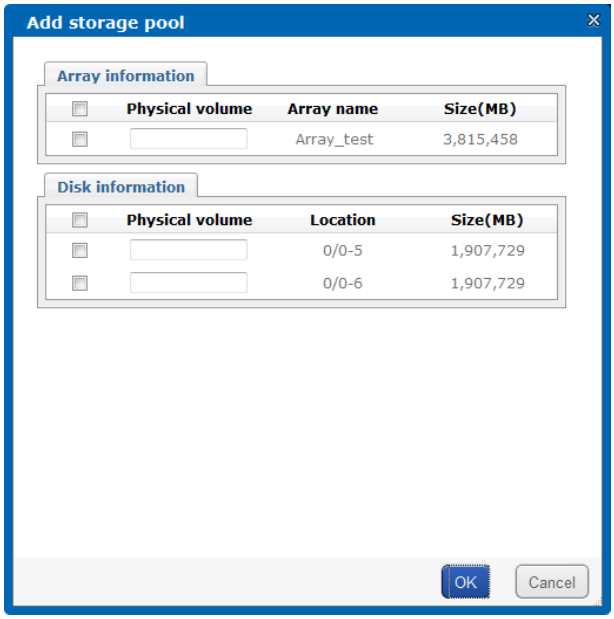


Figure 6. 33 Add Storage Pool

3. Check the checkboxes to select the arrays or physical disks to be added into the virtual storage pool.
4. Input the physical volume name in the corresponding text fields.
5. Click **OK** to confirm the settings. You can view the information of added physical volumes on the Physical Volume List.

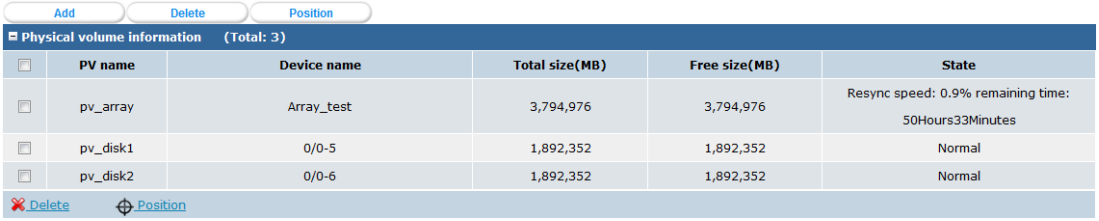


Figure 6. 34 Physical Volume List

Select the physical volume, click **Delete** under the Physical Volume List, and you can delete the selected physical volume from the virtual storage pool.

Select the physical volume, click **Position** under the Physical Volume List, and you can positioning all the disks in the selected physical volume.

Click the **Delete** button above the Physical Volume List, and you can delete the virtual storage pool from the storage system.

Click the **Position** button above the Physical Volume List, and you can positioning all the disks in the virtual storage pool.

NOTE

To positioning a disk, the indicator on the HDD bay bracket flickers for notification.

6.4.2 Creating LUNs

Purpose:

After physical volumes are added into the virtual storage pool, you can partition the volume space and create some logic volumes (LUNs) to be assigned to NAS, iSCSI, CVR and other storage service, to take highly use of the storage space.

Steps:

1. Enter the LUN Management interface.

   Storage > LUN

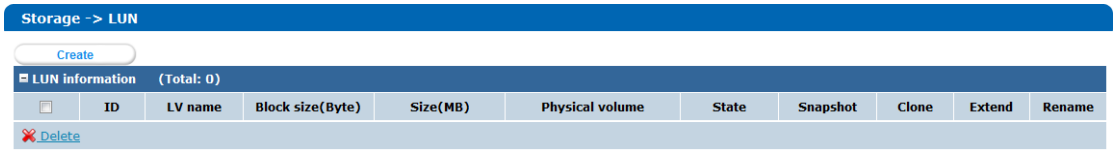


Figure 6. 35 LUN Management Interface

2. Click the **Create** button to open the Create LUN page.

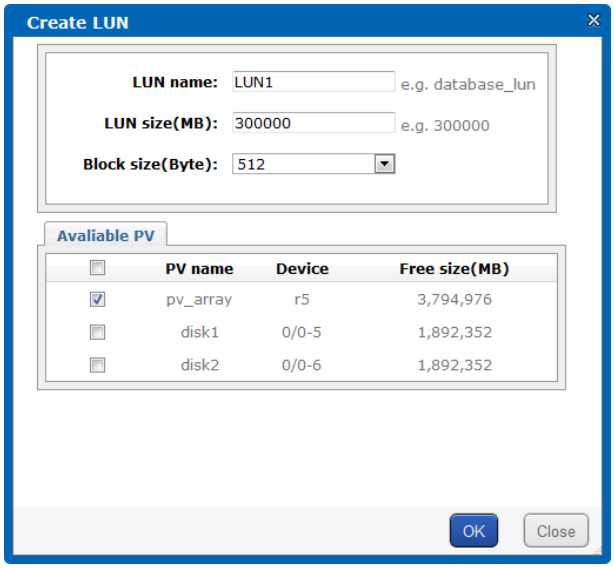


Figure 6. 36 Create a LUN

3. Input the LUN name, LUN size and block size in the corresponding text fields.

4. Check the checkbox to select a physical volume in which the LUN is located.
5. Click the **OK** button, and then confirm the pop-up dialog box.

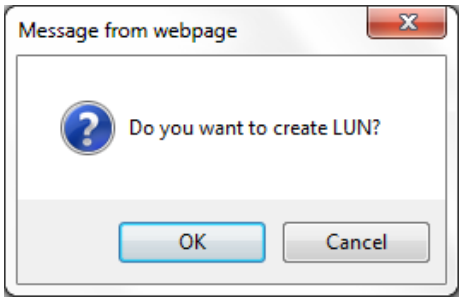
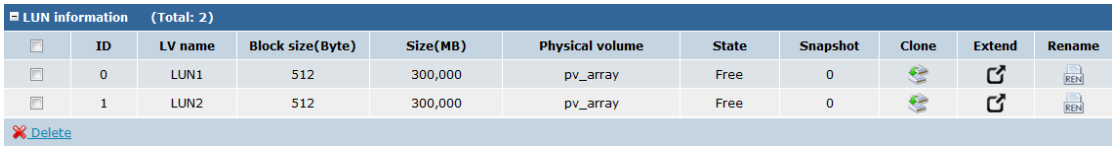


Figure 6. 37 Pop-up Dialog Box

6. Click the **Close** button to finish creating the LUN. You can view the information of Added LUNs on the LUN List.



LUN information (Total: 2)

	ID	LV name	Block size(Byte)	Size(MB)	Physical volume	State	Snapshot	Clone	Extend	Rename
	0	LUN1	512	300,000	pv_array	Free	0			
	1	LUN2	512	300,000	pv_array	Free	0			

Delete

Figure 6. 38 LUN List

Chapter 7 Configuring iSCSI Settings (optional)

Purpose:

The iSCSI connection is capable of mapping the storage space to the local client server, thus to provide the local management and operations for the system.

Before you start:

Insert the hard disks into the device, and then create the virtual storage pool and some logic volumes (LUNs). For details, see Section *6.4 Virtual Storage Pool Management*.

7.1 Creating iSCSI Volume

Purpose:

Some logic volumes (LUNs) can be assigned to the iSCSI network storage service and work as iSCIS volumes.

Steps:

1. Enter the iSCSI Management interface.

   SAN > iSCSI

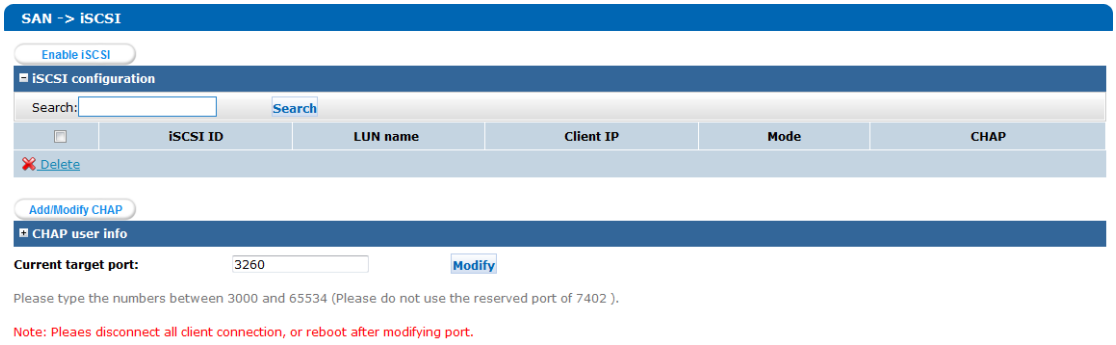


Figure 7. 1 iSCSI Management Interface

2. Click the **Enable iSCSI** button to open the Enable iSCSI page.

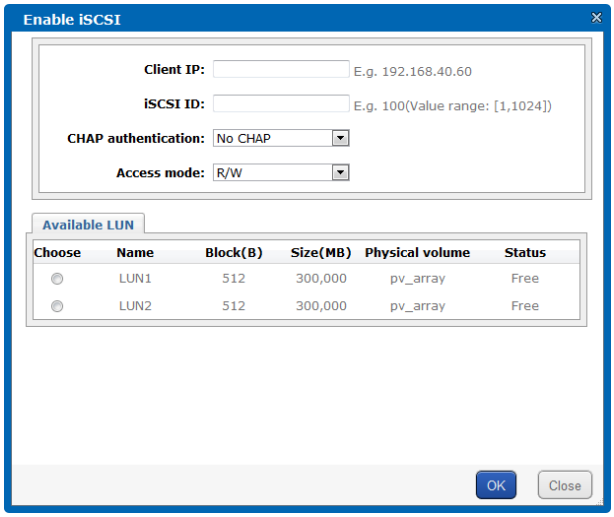


Figure 7. 2 Enable iSCSI

3. Input the client IP and iSCSI ID in the corresponding text fields, set the CHAP authentication and select the access mode.
4. Select a LUN from the list to work as the iSCSI volume.
5. Click the **OK** button, and then confirm the pop-up dialog box.

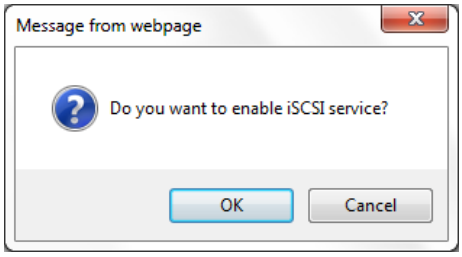


Figure 7. 3 Pop-up Dialog Box

6. Click the **Close** button to finish creating the iSCSI volume. You can view the information of the added iSCSI volumes on the iSCSI Volume List.

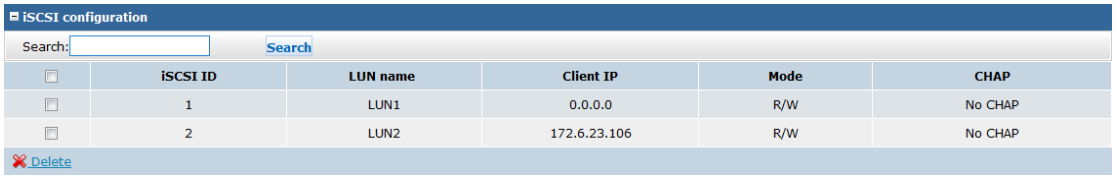


Figure 7. 4 iSCSI Volume List

NOTE

Only the client server specified by the IP address you input can connect the iSCSI volume. If multiple servers need to access the iSCSI service, you can input 0.0.0.0 as the Client IP.

7.2 Creating iSCSI Connection in Windows 2008

Use the iSCSI Initiator software in Windows 2008 to configure and establish the iSCSI connection to the storage system.

In Windows XP or Windows 2003, you need to click **Help** to enter the Help interface and download the corresponding software and install it on your PC. If the downloaded software cannot be installed properly, or the latest software is needed, you can log on to the Microsoft official website to download the corresponding software and install it.

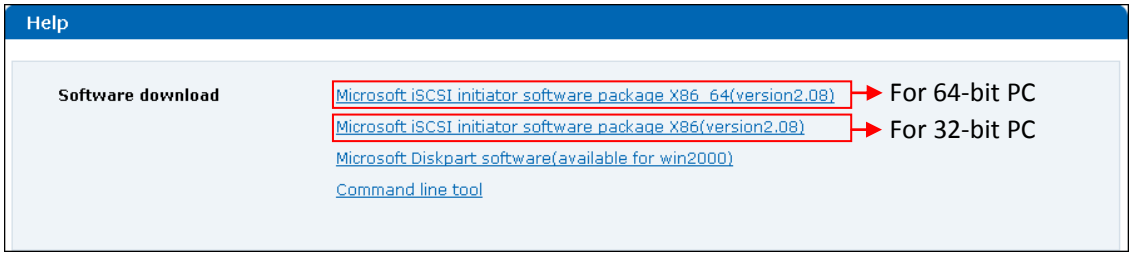


Figure 7. 5 Download iSCSI Initiator Software

Task 1: Connecting iSCSI Service

Steps:

1. Enter the Start menu, and select iSCSI Initiator to enter the following interface.

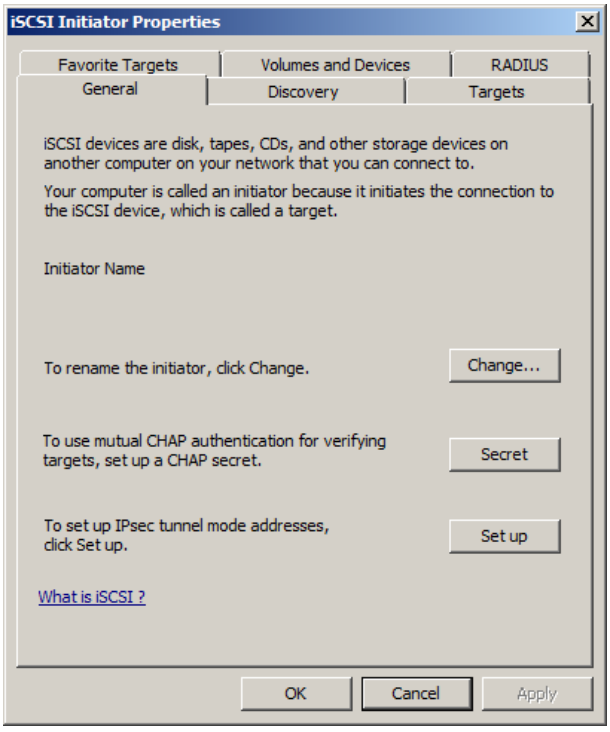


Figure 7. 6 Initiator Software Interface

2. Click the **Discovery** tab and click the **Add Portal…** button. The Add Target Portal dialog box will pop up.

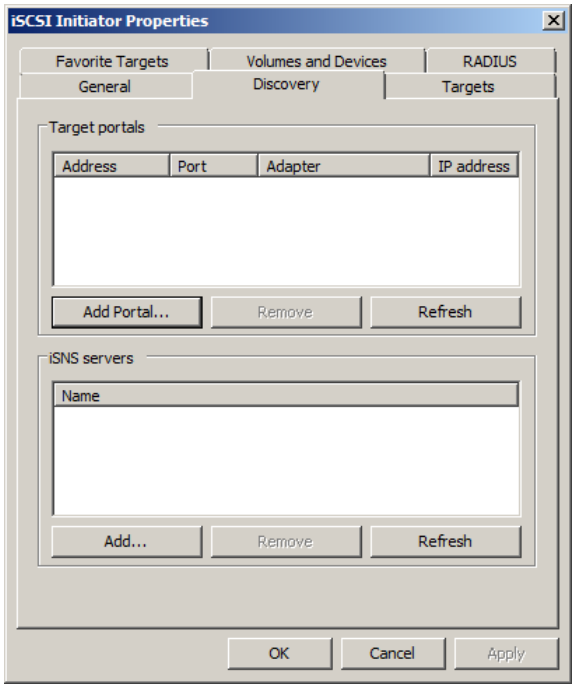


Figure 7. 7 iSCSI Initiator Properties

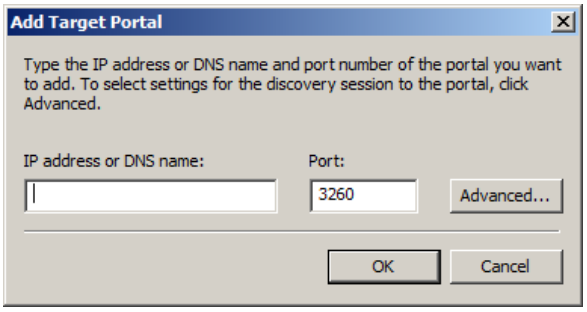


Figure 7. 8 Add Target Portal

3. Enter the IP address and port of the storage system, and click **OK** to confirm the settings. Click the **Targets** tab to enter the following interface.

NOTE

Inactive indicates that the storage target is discovered but not connected. You can connect multiple storage targets. You can refer to the following steps to configure the connection of iSCSI service

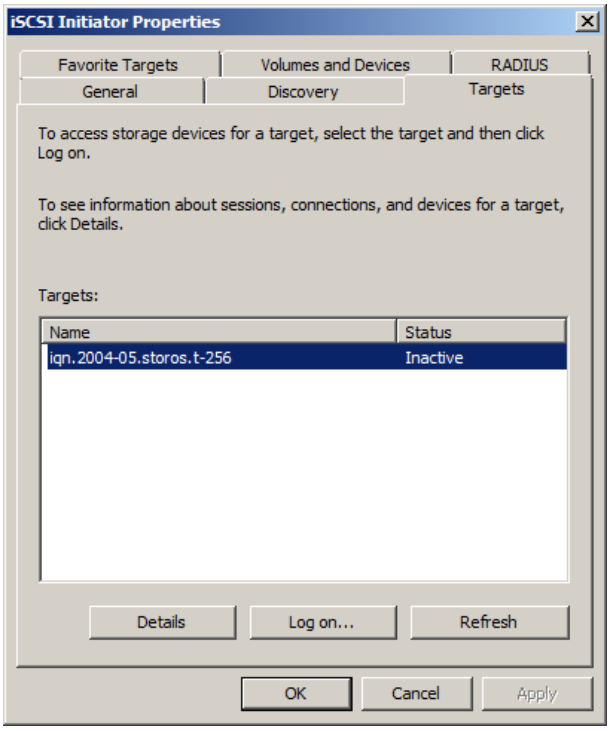
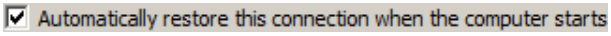


Figure 7. 9 Targets

4. Click the **Log on…** button and the Log On to Target dialog box will pop up. If you check  checkbox, the iSCSI storage system will be automatically connected when the PC starts next time. Click **OK** to complete the connection.

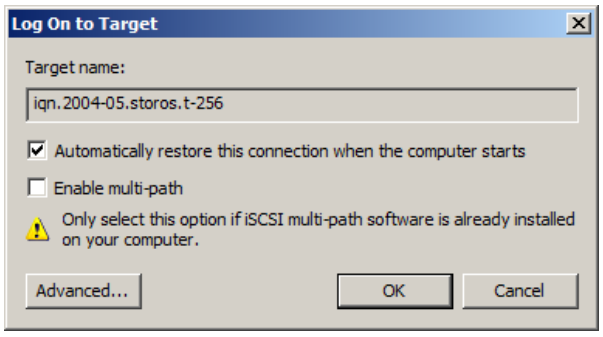


Figure 7. 10 Log On to Target

5. After connecting the storage system successfully, the status of the storage target will change to **Connected**.

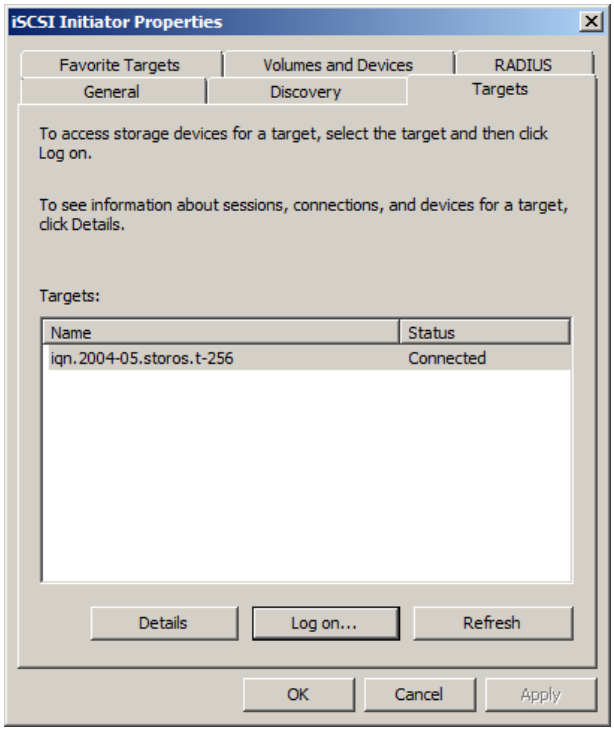


Figure 7. 11 iSCSI Connected

Task 2: Disconnecting iSCSI Service

Steps:

1. Select the storage target and click the **Details** button.
2. In the pop-up Target Properties interface, check ☑ checkbox for the Identifier and click the **Log off…** button to disconnect the connection.
3. Click **OK** to confirm the settings.

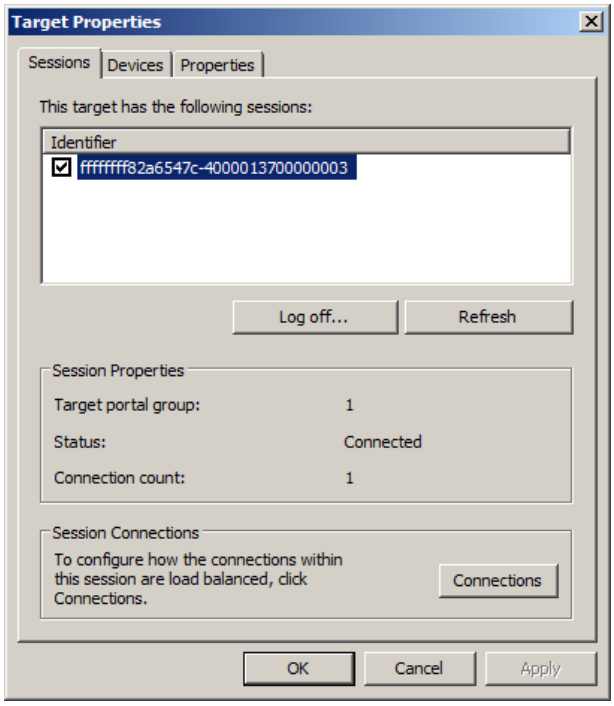


Figure 7. 12 Disconnect Storage Target

7.3 Mapping to Local Disk & Formatting iSCSI Disk

After iSCSI connection, the storage system can be considered as a local disk.

Steps:

1. Enter the Start menu, and select Administrative Tools > Computer Management > Storage > Disk Management. The Initialize Disk guide will pop up.

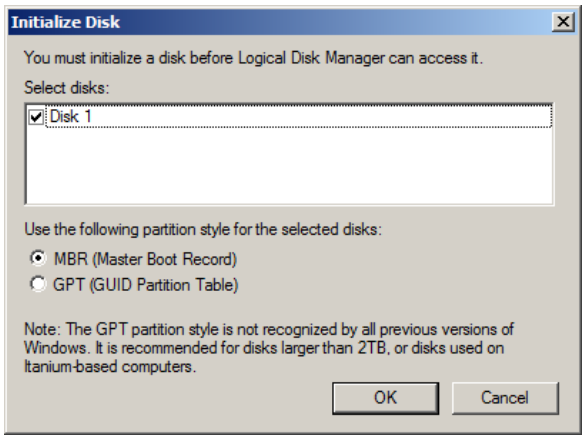


Figure 7. 13 Initialize Disk Guide

2. Check ☑ checkbox to select disk(s) and click **OK** to confirm initializing the disk(s).

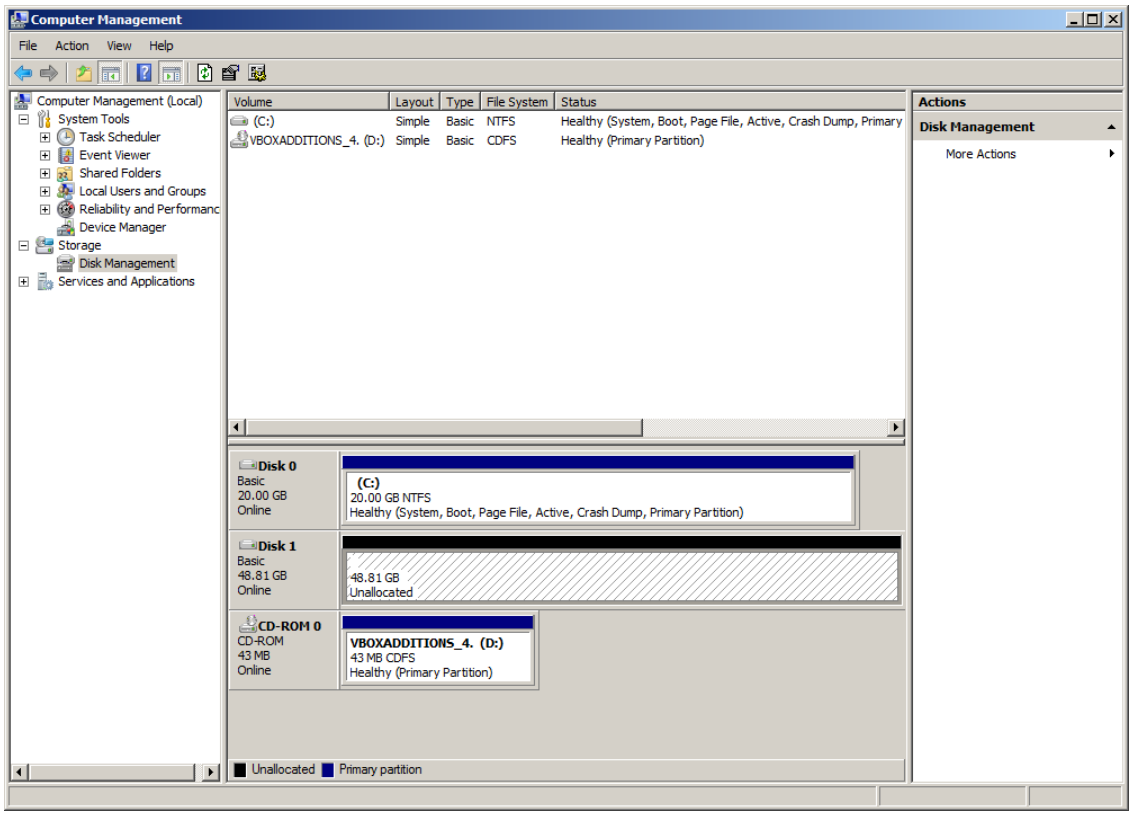


Figure 7. 14 Disk Management

3. You can map the storage system to a basic disk or a dynamic disk. The basic disk is accessible when the device is started, and the dynamic disk processes more features than the basic disk, e.g., extended dynamic volume and multiple disk volumes.
4. Right-click an iSCSI disk and select New Simple Volume to start activating the disk. Follow the pop-up guide to map the disk to local storage.
5. After formatting successfully, you can access the disk(s) in **Computer**.

7.4 Creating iSCSI Connection in Redhat5

The following content is the introduction of creating iSCSI connection in Redhat5.

Steps:

1. Discover the target.

   # iscsiadm -m discovery -t sendtargets -p 10.192.52.166

   10.192.52.166:3260, 1 iqn.2004-05.storos.t-111

2. Log on the target.

   # iscsiadm -m node -T iqn.2004-05.storos.t-111 -p 10.192.52.166:3260 -l

   Login session [iface: default, target: iqn.2004-05.storos.t-111, portal: 10.192.52.166, 3260]

3. View the disk information.

   # fdisk -l

```
Disk /dev/sda: 8589 MB, 8589934592 bytes
255 heads, 63 sectors/track, 1044 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         128      923737+  82  Linux swap / Solaris
/dev/sda3             129        1043     7349737+  83  Linux
/dev/sda4            1044        1044        8032+   5  Extended
/dev/sda5            1044        1044        8001   8e  Linux LVM

Disk /dev/sdb: 13.6 GB, 13623099392 bytes
64 heads, 32 sectors/track, 12992 cylinders
Units = cylinders of 2048 * 512 = 1048576 bytes

   Device Boot      Start         End      Blocks   Id  System
/dev/sdb1               1       12992    13303792   83  Linux
```

Figure 7. 15 Disk Information

4. Use the fdisk command for disk partitioning.

   fdisk [-l] [-b SSZ] [-u] device

   -l: View the status of partition table of the device.

   -b SSZ: Display the partition size on the standard output.

   -u: Used with -l, replace the cylinder number with partition number to indicate the start address of each partition.

   device: The name of the device.

NOTE

The fdisk command is the most common partition tool and is defined as the Expert partition tool. A second-level menu is included in the fdisk command.

5. Enter the command: # fdisk /dev/sdb. And the command prompts will come out: Command (m for help).

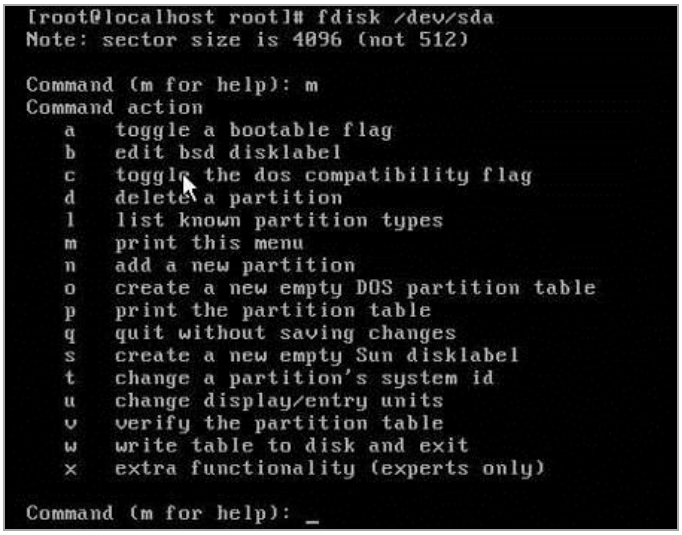


Figure 7. 16 fdisk Command for Partitioning

6. Enter **n** to create a partition and the prompt for selecting primary partition or extended partition will come out. We often use the primary partition. And then enter the partition number, first cylinder and partition size. Enter **w** to write the disk information.

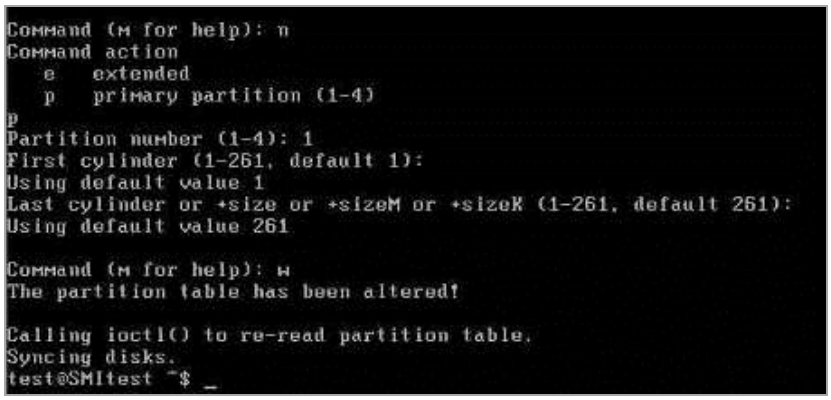


Figure 7. 17 Partition Disk

7. Format the partition.

   # mkfs.ext3 -b 4096 /dev/sdb1

8. Set the mount point.

   # mkdir /mnt/scsi01

   # mount /dev/sdb1 /mnt/scsi01

   Now the Linux server has connected the iSCSI disk and you can do the same operation as the local SCSI disk of the Linux server.

9. Mount an iSCSI disk automatically.

   Modify /etc/rc.local through the vi editor. Use the command *Shift + G* to locate the cursor at the last line. Use the command *o* and then enter #mount /dev/sd1 /mnt/scsi01. After saving the file and rebooting the Linux server, the server can mount the iSCSI disk automatically.

7.5 Creating iSCSI Connection in Suse 10

This section introduces the procedure iSCSI connection in Suse 10.

Steps:

1. Discover the target.

   # iscsiadm -m discovery -t sendtargets -p 10.192.52.166

   [1b72d5] 10.192.52.166:3260,1 iqn.2004-05.storos.t-123

2. Log on the target.

   # iscsiadm -m node -r 1b72d5 -l

3. View the disk information.

   # fdisk –l

```
Disk /dev/sda: 8589 MB, 8589934592 bytes
255 heads, 63 sectors/track, 1044 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         128      923737+  82  Linux swap / Solaris
/dev/sda3             129        1043     7349737+  83  Linux
/dev/sda4            1044        1044        8032+   5  Extended
/dev/sda5            1044        1044        8001   8e  Linux LVM

Disk /dev/sdb: 13.6 GB, 13623099392 bytes
64 heads, 32 sectors/track, 12992 cylinders
Units = cylinders of 2048 * 512 = 1048576 bytes

   Device Boot      Start         End      Blocks   Id  System
/dev/sdb1               1       12992    13303792   83  Linux
```

Figure 7. 18 Disk Information

4. Use the fdisk command for disk partitioning, and then format the disk.

   # fdisk /dev/sdb

   # mkfs.ext3 -b 4096 /dev/sdb1

5. Set the mount point.

   # mkdir /mnt/scsi01

   # mount /dev/sdb1 /mnt/scsi01

Now the server has connected the iSCSI disk and you can do the same operation as the local SCSI disk of the Linux server.

Chapter 8 Configuring NAS Settings (optional)

Purpose:

The NAS space can be used as the network shared disk within the office network to realize the share of data, software tools and other materials.

Before you start:

Insert the hard disks into the device, and then create the virtual storage pool and some logic volumes (LUNs). For details, see Section *6.4 Virtual Storage Pool Management*.

8.1 Creating NAS Net Disk

8.1.1 Creating NAS Volume

Steps:

1. Enter the NAS Disk Management interface.

   NAS > NAS Disk

Figure 8. 1 NAS Disk Management Interface

2. Click the **Create NAS volume** button to open the Create NAS Volume page. Select the LUN to work as the NAS volume from the drop-down list.

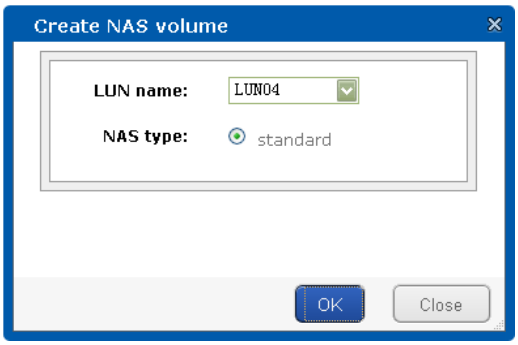


Figure 8. 2 Create NAS Volume

3. Click **OK** to confirm the settings. You can view the information of added NAS volumes on the NAS Volume List.

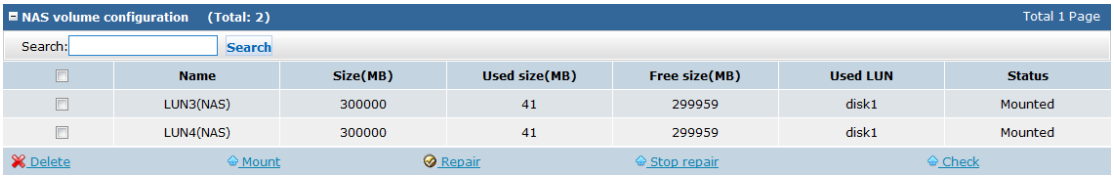


Figure 8. 3 NAS Volume List

8.1.2 Configuring Basic NAS Settings

Steps:

1. Enter the NAS Configuration interface.

   NAS > NAS Config

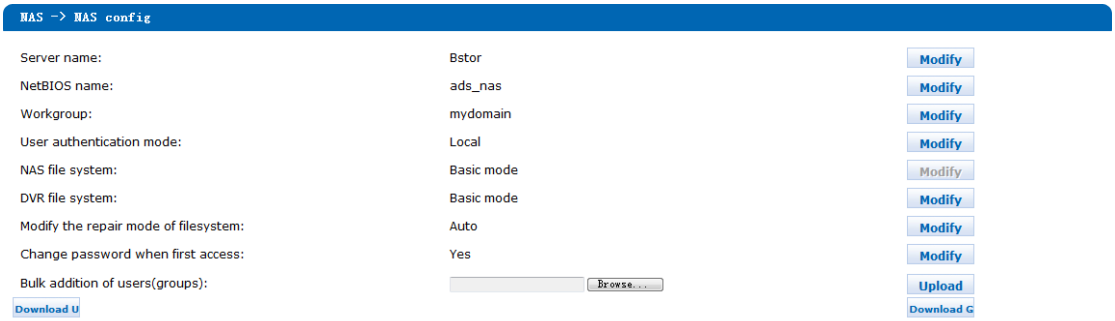


Figure 8. 4 NAS Configuration

2. You can configure the **Server name**, **NetBIOS name** and **Workgroup** to meet the actual needs in office.
3. For user authentication mode, you can select Local, Share or ADS.

   Local: This mode adopts the local user management system of the storage device, and the user name and password are saved in the storage server.

   Share: It allows any user to log in the system with no need of user name authentication.

   ADS: Based on the domain, all users are required to adopt the Active Directory for authentication. The ADS mode is optional.

8.1.3 Adding NAS User

If you set the user authentication mode as Local, you need to create the NAS user before creating NAS disk.

Steps:

1. Enter the NAS User Management interface.

   NAS > Users (Groups)

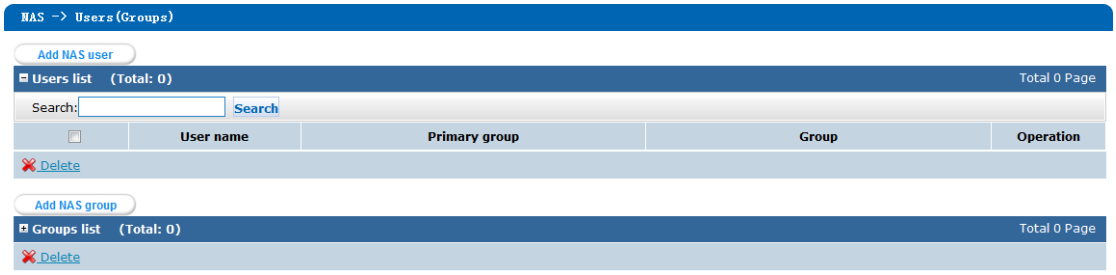


Figure 8. 5 NAS User Management

2. Click the **Add NAS user** button to open the Add NAS User page.

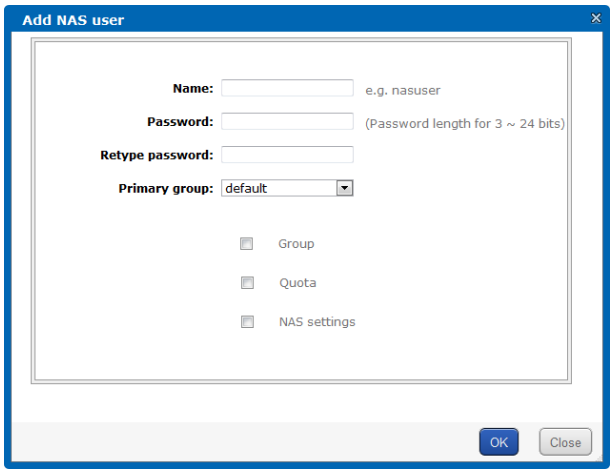


Figure 8. 6 Add NAS User

3. Input the name, password and confirm password in the corresponding text fields.
4. Set the group, quota and NAS settings for the NAS user.

   Primary group: *Default* and pre-defined group(s) can be selected.

   Group: Select the group for the user. The settings of the group define the permission of user, like quota and read-write permission of the user.

   Quota: Set the available storage space for the created user.

   - If no quota is set for the user (or the quota value is set as 0) and the user is in the default primary group, then the user can use the total capacity of the NAS volume.
   - If the quota of the primary group in which the user locates is not 0 and another quota is set for the user specially, then the usable disk capacity for the user is the smaller one of the two quotas.

     Example: if the total capacity of the NAS volume is 20G and the quota configured for the user is 0, and the quota of the primary group in which the user locates is 600M, then the usable disk capacity for the user is 600M.

   NAS settings: Set the protocol for file service and configure the NAS disk permission for the user.
5. Click **OK** to conform the settings.

8.1.4 Creating NAS Disk

Steps:

1. Enter the NAS Disk Management interface.

   NAS > NAS Disk

Figure 8. 7 NAS Disk Management

2. Click the **Add NAS disk** button to open the Add NAS Disk page.

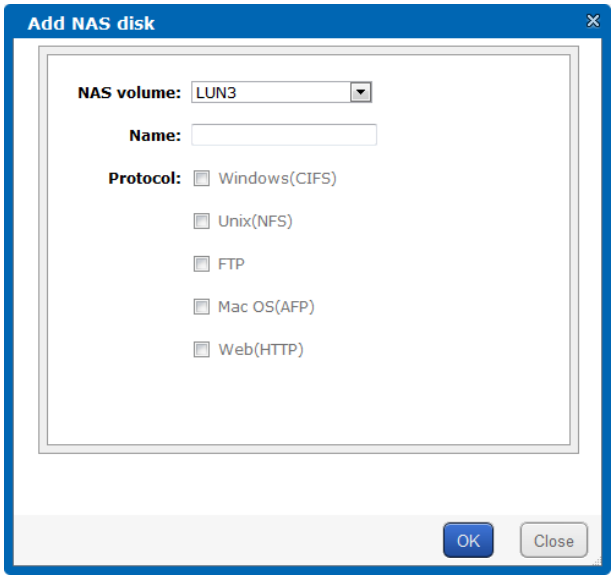


Figure 8. 8 Add a NAS Disk

3. Select the NAS volume from the drop-down list and input the name for the NAS disk.
4. Check the checkbox to select the protocol, and then set the read/write access to the NAS disk for the added NAS users or specified IP address segment.

   NOTE

   If the user authentication mode is set as S**hare** and the protocol is selected as **Windows (CIFS)**, you need only select the access mode to *read-write* or *read-only* for all the users.

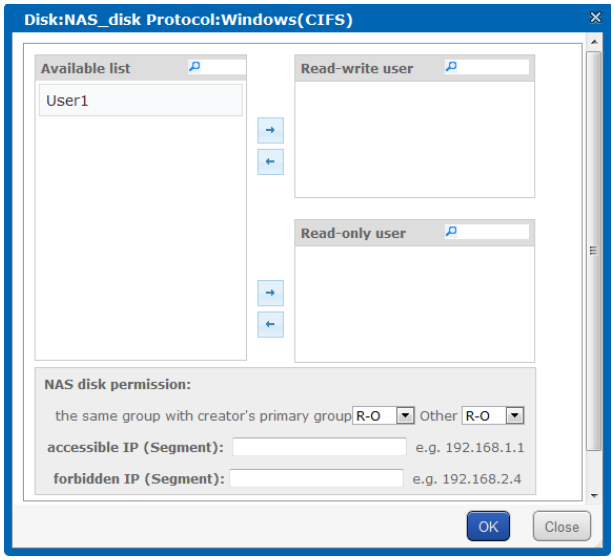


Figure 8. 9 Protocol Settings

5. Click **OK** to confirm the settings. You can view the information of added NAS disks on the NAS Disk List.

8.2 Creating NAS Disk Connection

NOTE

We take the Windows 7 operating system as an example in this section.

Steps:

1. Right-click **Computer** icon on the desktop of your PC and select **Map Network Drive**. The guide for Map Network Drive will pop up.

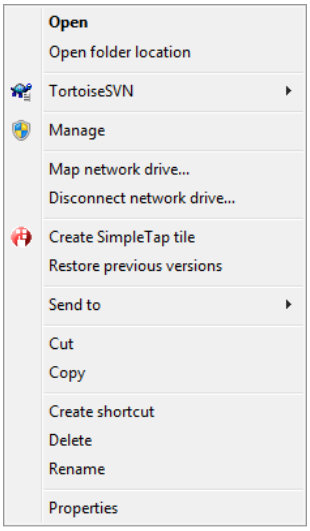


Figure 8. 10 Right-click Menu

2. Select a letter for the network drive from the drop-down list, and input the IP address and NAS disk name in the Folder text field.

Example: If the IP address of the storage system is 172.8.72.241 and the NAS disk name is NAS_disk1, then you should enter *\\172.8.72.241\NAS_disk1* in the Folder text field.

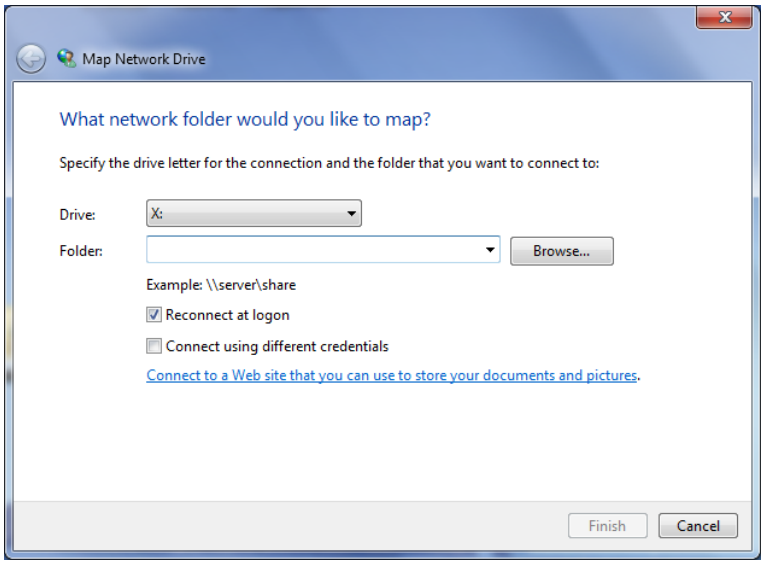


Figure 8. 11 Map Network Drive Guide

3. Optionally, you can check the checkbox of **Reconnect at logon** to connect the NAS disk automatically after the system startup.
4. Click the **Finish** button to confirm the settings. And then input the user name and password of the NAS disk in the pop-up dialog box, and click **OK**.

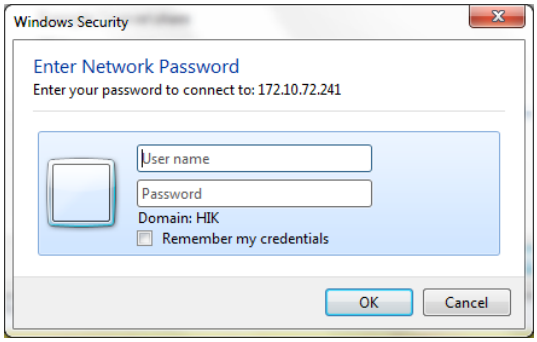


Figure 8. 12 User Name and Password

5. After mapping the NAS disk to the network drive successfully, you can view the NAS disk in the Network Location area of Computer.

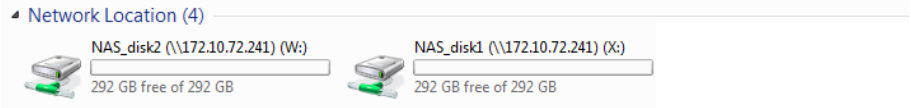


Figure 8. 13 Connected NAS Disk

6. To disconnect the NAS disk, you can select **Disconnect Network Drive** on the Right-click Menu**.**

8.3 Cautions for Proper Use of NAS Disk

- Due to the system settings of Windows, one client can use only one NAS user to access the

storage server. Disconnect all the NAS disks from the PC before you switch the NAS user. Please refer to the following table for detailed information.

Table 8-1 Relation between Client and User

Client	User	Support
Single	Single	Yes
Single	Multiple	No
Multiple	Single	Yes
Multiple	Multiple	Yes

- One client can connect multiple NAS disks and storage servers.
- Due to the cache mechanism of the Windows OS, wait a moment for the next connection after the NAS disk is disconnected from the PC.

Chapter 9 Configuring NAS Settings for DVR (optional)

The DVR storage share mode is applicable to the embedded encoding devices, e.g., DVR, DVS, IP camera, IP dome, etc. The DVR in the following section refers to the embedded encoding device.

The topological structure of the storage systems and DVR units are shown below. This is a recommended structure in network video surveillance deployment, considering the increasing business requirement in practical applications.

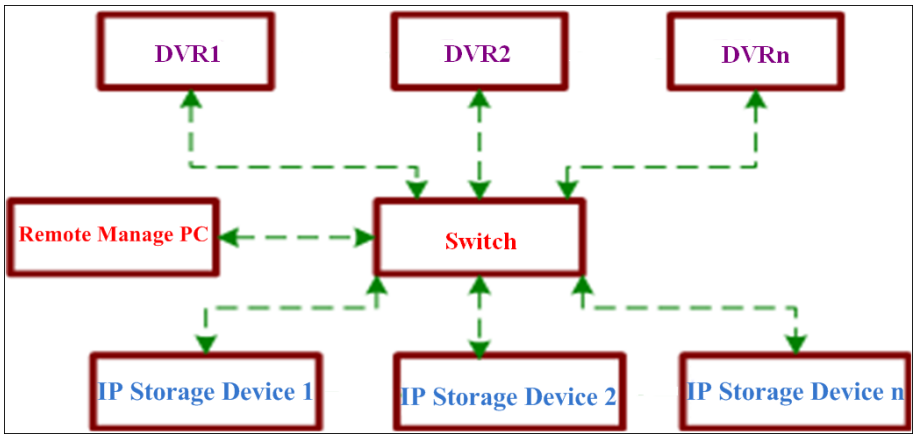


Figure 9. 1 Topological Structure

9.1 Creating DVR Storage Space

Before you start:

Add virtual storage pool before you configure the DVR settings. For more details, see Section *6.4 Virtual Storage Pool Management*.

Steps:

1. Enter the DVR Settings interface.

   NAS > DVR

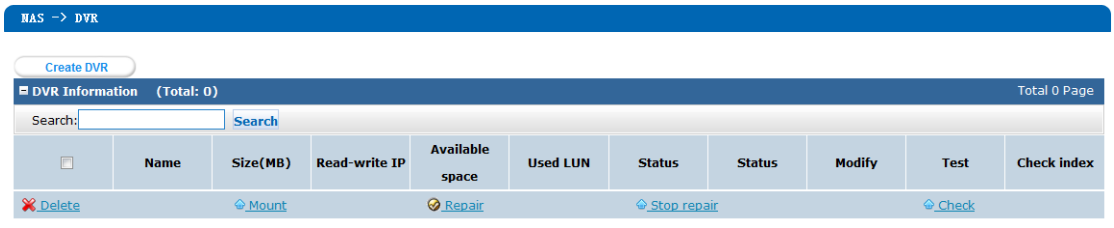


Figure 9. 2 DVR Settings Interface

2. Click the **Create DVR** button to open the Create DVR page.

   Name: Edit the name of the DVR NAS disk as desired.

   Size: Set the capacity of each DVR NAS disk.

R/W IP: Input the IP address of the DVR to which the DVR NAS disk is to be connected.

Number: Input the number of the DVR NAS disks to be created. (The default value is 1.)

Available physical volume: Select the physical volume on which the DVR NAS disk(s) is located.

NOTE

- The size of the DVR NAS disk should be set between 20GB and 8TB.
- If you specify the R/W IP, only the device with the specified IP address can access the DVR NAS disk. If you leave the field empty, then multiple devices can access the DVR NAS disk.
- The DVR NAS disk cannot be used by two DVRs at the same time.

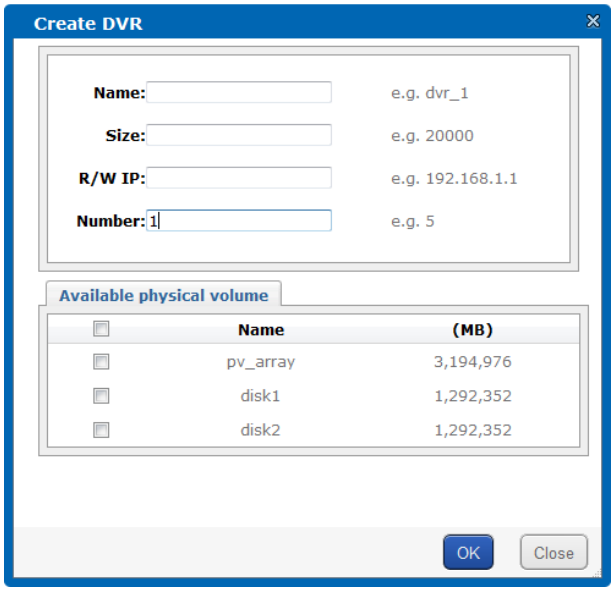


Figure 9. 3 Create DVR

3. Click the **OK** button to create the DVR NAS disk. You can view the information of the added DVR NAS disks on the DVR NAS disk List.

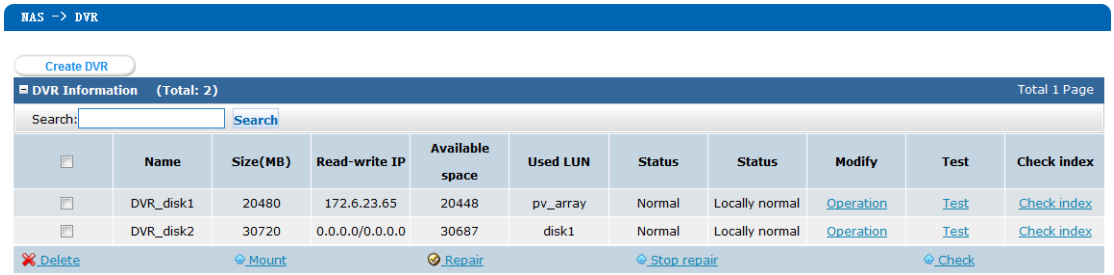


Figure 9. 4 DVR NAS Disk List

4. You can select a DVR NAS disk and click **Operation** in the Modify column to modify the name and R/W IP address for the DVR NAS disk. Click **OK** to confirm the settings.

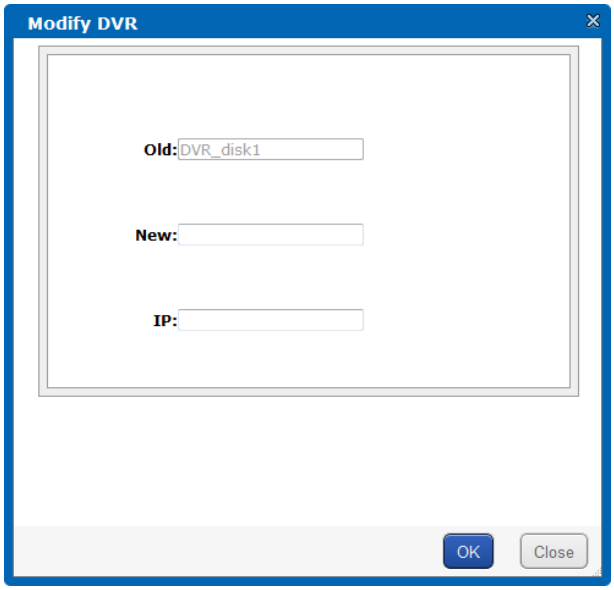


Figure 9. 5 Modify the DVR NAS Disk

5. You can check the checkbox to select the DVR NAS disk, click **Delete** under the list, and then confirm the pop-up dialog box to delete the selected DVR NAS disk.

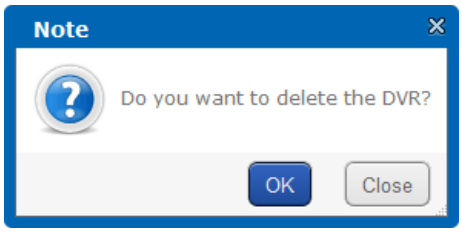


Figure 9. 6 Pop-up Dialog Box

6. You can select a DVR NAS disk and click **Test** in the Test column to test the communication status between the storage server and DVR.

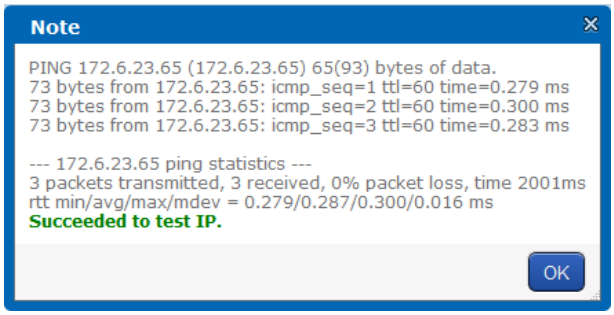


Figure 9. 7 Test Connection

9.2 DVR Configuration

Purpose:

DVR NAS disks in the network storage system can be added to the DVR units as the network HDDs, via the DVR local menu or the client software.

Here we take the DVR local menu as an example.

Steps:

1. Enter the Add NetHDD interface of the DVR local menu. For details, see the user manual of the DVR.
2. Select NAS from the drop-down list as the network HDD type.
3. Input the IP address and directory of the NAS disk. You can also click the **Search** button to search the NAS disks available, and select the NAS disk to be added.

   The directory format is: /dvr/DVR NAS disk name.

   Example: If DVR NAS disk name is DVR_disk1, then the directory should be /dvr/DVR_disk1.
4. Click **OK** to confirm the settings. And then the DVR NAS disk will be added to the HDD list of DVR.

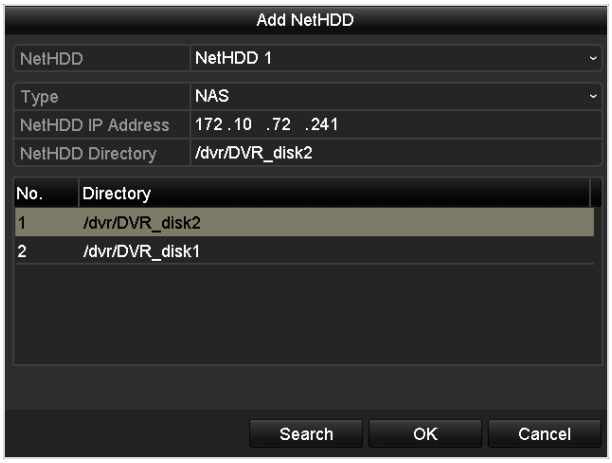


Figure 9. 8 Add NetHDD

Chapter 10 System Monitoring and Alarm

10.1 System Monitoring

After logging in the storage system, the administrator can view the basic status and the running information of the system. The current status of the system is displayed in the upper-right corner of the web page. If the storage system is running normally, the status is displayed as follows:

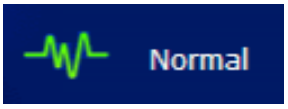


Figure 10. 1 Normal System

When the system is exceptional, you can see the abnormal information in the upper-right corner of the web page. Click 

to unfold the alarm message box and you can view the details of the abnormal information.

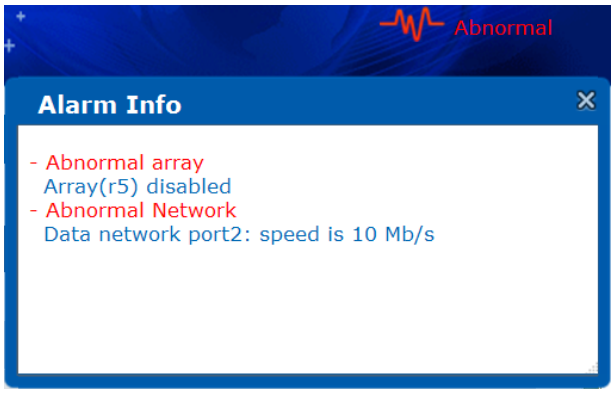


Figure 10. 2 Abnormal System

The alarm information of the system includes but is not limited to the following conditions:

1. Hard Disk: The status and connection condition of the disks installed on the chassis or expansion enclosure.
2. Environmental Control Information: The temperature, fan and power supply of the chassis or expansion enclosure.
3. System Business Status: iSCSI, NAS and CVR.
4. Network: The connection status of the data port or management port.

10.2 Environmental Information

In the Environmental Information interface (Maintenance > Control Message), the motherboard information, the chassis information, the expansion enclosure information and the audio warning information are listed.

Motherboard Information

The information of CPU fan speed, CPU temperature, motherboard fan speed and system temperature will be monitored. When the fan is abnormal (e.g., low speed) or the temperature is abnormal (e.g., high temperature), the system shows the corresponding alarm messages.

Chassis Information

The information of the fan speed, temperature information and power supply information of the chassis will be monitored. Up to 8 chassis fans can be connected depending on different models.

Expansion Enclosure Information

The manufacturer, type, bay number, version, fan speed, temperature and other information of the expansion enclosure are displayed.

Fan Speed Control

The fan speed of the chassis can be set according to the ambient temperature, to adjust the internal working temperature of the chassis. Low temperature can help to extend the system life and reduce the failure rate, but also increase the noise and power consumption. Our storage system provides 3 working modes of the fan, including high speed, medium speed (default) and low speed. In the same circumstance, comparing to medium speed, the high speed can decrease the temperature and the low speed can reduce the noise.

Audio Warning

The system makes the audible warning when the system is in abnormal status. You can click the mute button to enable/disable the audible warning.

Chapter 11 Bad Disk Management

Purpose:

The failure possibility of hard disk increases with increment of its working time. That is the reason why we set RAID as the HDD working mode. When RAID 5 working mode is adopted, the storage system will keep running in case of single hard disk failure, in an unstable status. Replace the bad disk to avoid the data loss and performance reduction.

11.1 Configuring Alarm for Bad Disks

Steps:

1. Enter the Disk Management interface.

   Storage > Disk

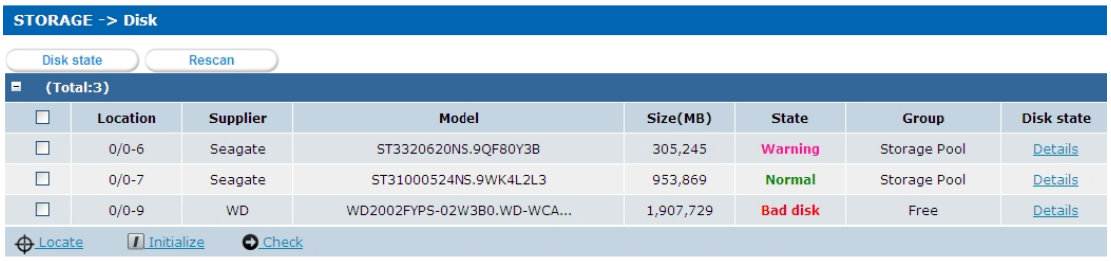


Figure 11. 1 Disk Information

2. If the disk is abnormal, the system will automatically detect the disk. After the detection is complete, the alarm information will be displayed with the disk No. and model.

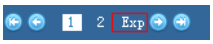
Figure 11. 2 Alarm Information

11.2 Replacing the Bad Disks

Steps:

1. Before replacing the bad disk(s), you need to check the new disks.
2. To check all the disks, click the Exp icon on the navigation bar 1 2 Exp and all the disks will be displayed.
3. Select all the disks, and click **Check** under the list to start the checking process for all disks. You can also check the selected disks partly. For details, see Section *6.2.3 Checking Disk*.

NOTE

The navigation bar  will be displayed when more than 10 disks are installed in the storage system.

4. Replace the bad disk with a new one in normal status after the checking process is complete. You can send the bad disk to disk manufacturer or the engineer of our company for detecting. Do not reuse the bad disk, for it may cause RAID instability or data loss.
5. Rebuild the array after replacing the bad disk. For details, see Section *6.3.2 Rebuilding an Array*.

Chapter 12 Appendix

- IE6, IE7, IE8 and IE9 browsers are supported by the storage system.
- The default IP address of Data NIC is 192.168.0.100, and the default working mode is Active-backup.
- If you forget the IP address of the device, you can obtain it by inputting command “ifconfig” in the Hyper Terminal(Baud rate should be set as 115200).
- You may enter the manage system through https://10.254.254.254:2004, with the user name web_admin and default password 123.
- It is recommended to connect two network interfaces to the Ethernet network when the storage device are equipped with several Gigabit NICs.
- After you modifying the IP address of an network interface, the Management system may be disconnected. log in to the system again with the new IP address in this condition.
- If you forget the modified IP address, configure a PC with IP address of 10.254.254.xxx, connect it to the storage system via the Manage NIC (https://10.254.254.254:2004), and then check and modify the IP address of Gigabit Network interface.

0203001031114