P3AM-7652-17ENZ0

FUJITSU Storage
ETERNUS DX100 S4/DX200 S4,
ETERNUS DX100 S3/DX200 S3
Hybrid Storage Systems

Configuration Guide (Basic)

Basic setup to start operations

FUJITSU

Table of Contents

List of Figures

List of Tables

Preface

Fujitsu would like to thank you for purchasing the FUJITSU Storage ETERNUS DX100 S4/DX200 S4, ETERNUS DX100 S3/DX200 S3 (hereinafter collectively referred to as ETERNUS DX).

The ETERNUS DX is designed to be connected to Fujitsu servers (Fujitsu SPARC Servers, PRIMEQUEST, or PRIMERGY) or non-Fujitsu servers.

This manual describes the basic setup of the ETERNUS DX and how to start the operation.

This manual is intended for use of the ETERNUS DX in regions other than Japan.

Please carefully review the information outlined in this manual.

Seventeenth Edition

January 2023

Trademarks

Third-party trademark information related to this product is available at:

https://www.fujitsu.com/global/products/computing/storage/eternus/trademarks.html

About This Manual

Intended Audience

This manual is intended for field engineers or storage system administrators who perform basic setups and start operations.

Related Information and Documents

The latest version of this manual and the latest information for your model are available at:

https://www.fujitsu.com/global/support/products/computing/storage/manuals-list.html

Refer to the following manuals of your model as necessary:

"Site Planning Guide" "Design Guide (Basic)" "Operation Guide (Basic)"

"Configuration Guide (Power Synchronized Unit)"

"Configuration Guide (Web GUI)" "Configuration Guide -Server Connection-" "Configuration Guide (NAS)"

"ETERNUS Web GUI User's Guide"

"ETERNUS CLI User's Guide"

Document Conventions

■ Third-Party Product Names

- Oracle Solaris may be referred to as "Solaris", "Solaris Operating System", or "Solaris OS".
- Microsoft® Windows Server® may be referred to as "Windows Server".

■ Notice Symbols

The following notice symbols are used in this manual:

Caution	Indicates information that you need to observe when using the ETERNUS storage system. Make sure to read the information.
Note	Indicates information and suggestions that supplement the descriptions included in this manual.

Warning Signs

Warning signs are shown throughout this manual in order to prevent injury to the user and/or material damage. These signs are composed of a symbol and a message describing the recommended level of caution. The following explains the symbol, its level of caution, and its meaning as used in this manual.

WARNING

This symbol indicates the possibility of serious or fatal injury if the ETERNUS DX is not used properly.

CAUTION

This symbol indicates the possibility of minor or moderate personal injury, as well as damage to the ETERNUS DX and/or to other users and their property, if the ETERNUS DX is not used properly.

IMPORTANT This symbol indicates IMPORTANT information for the user to note when using the ETERNUS DX.

The following symbols are used to indicate the type of warnings or cautions being described.

Electric Shock

△The triangle emphasizes the urgency of the WARNING and CAUTION contents. Inside the triangle and above it are details concerning the symbol (e.g. Electrical Shock).

No Disassembly

⃠The barred "Do Not..." circle warns against certain actions. The action which must be avoided is both illustrated inside the barred circle and written above it (e.g. No Disassembly).

Unplug

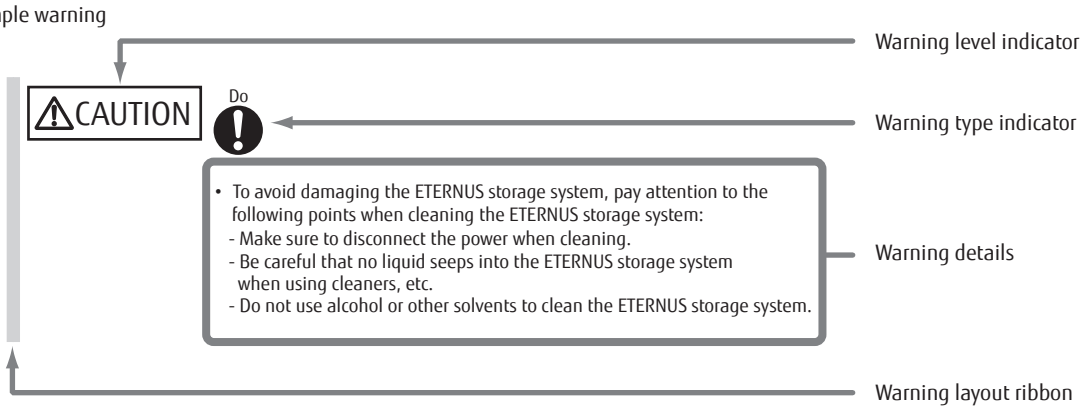
●The black "Must Do..." circle indicates actions that must be taken. The required action is both illustrated inside the black disk and written above it (e.g. Unplug).

How Warnings are Presented in This Manual

A message is written beside the symbol indicating the caution level. This message is marked with a vertical ribbon in the left margin, to distinguish this warning from ordinary descriptions.

A display example is shown here.

Example warning



Warning Labels and Manufacturer's Labels

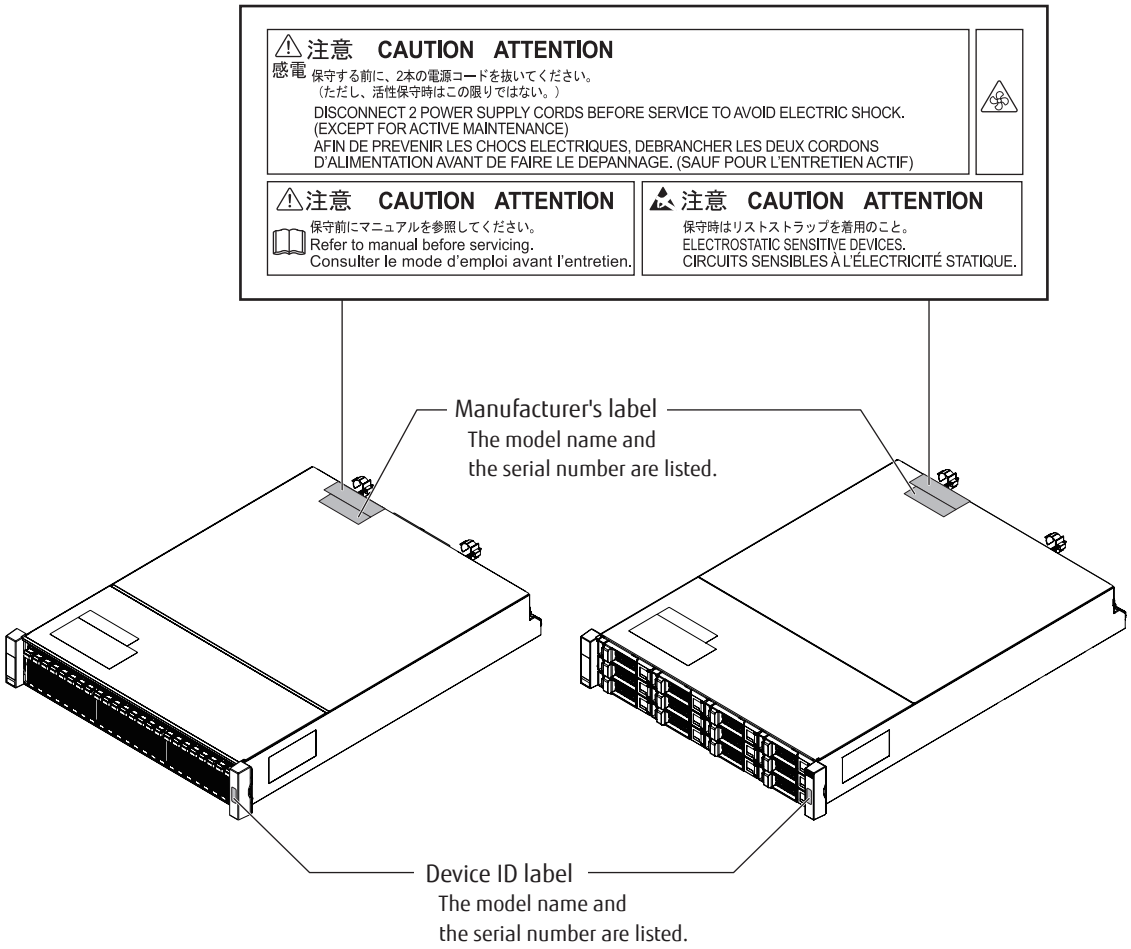
Warning labels, manufacturer's labels, and a device ID label are found in the ETERNUS DX, as shown in the example below.

Never remove these labels from the equipment or allow them to become dirty.

Controller Enclosure

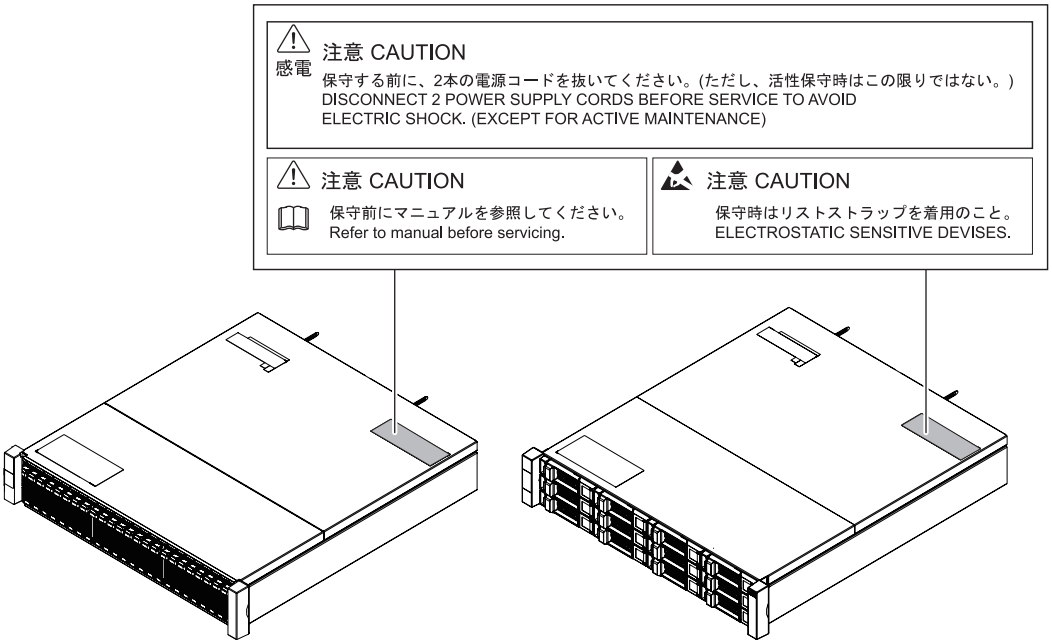
- 2.5"/3.5" type controller enclosure

  On the controller enclosure, warning labels and manufacturer's labels are attached to the rear or to the left side.

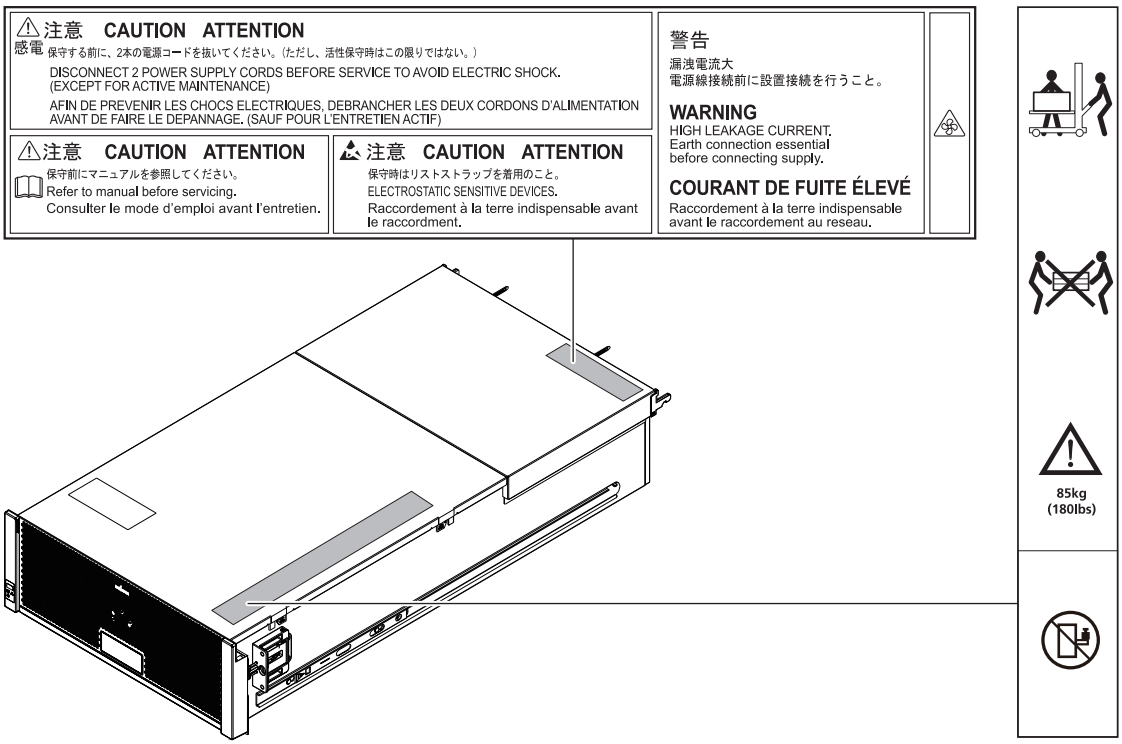


Drive Enclosures

- 2.5"/3.5" type drive enclosure



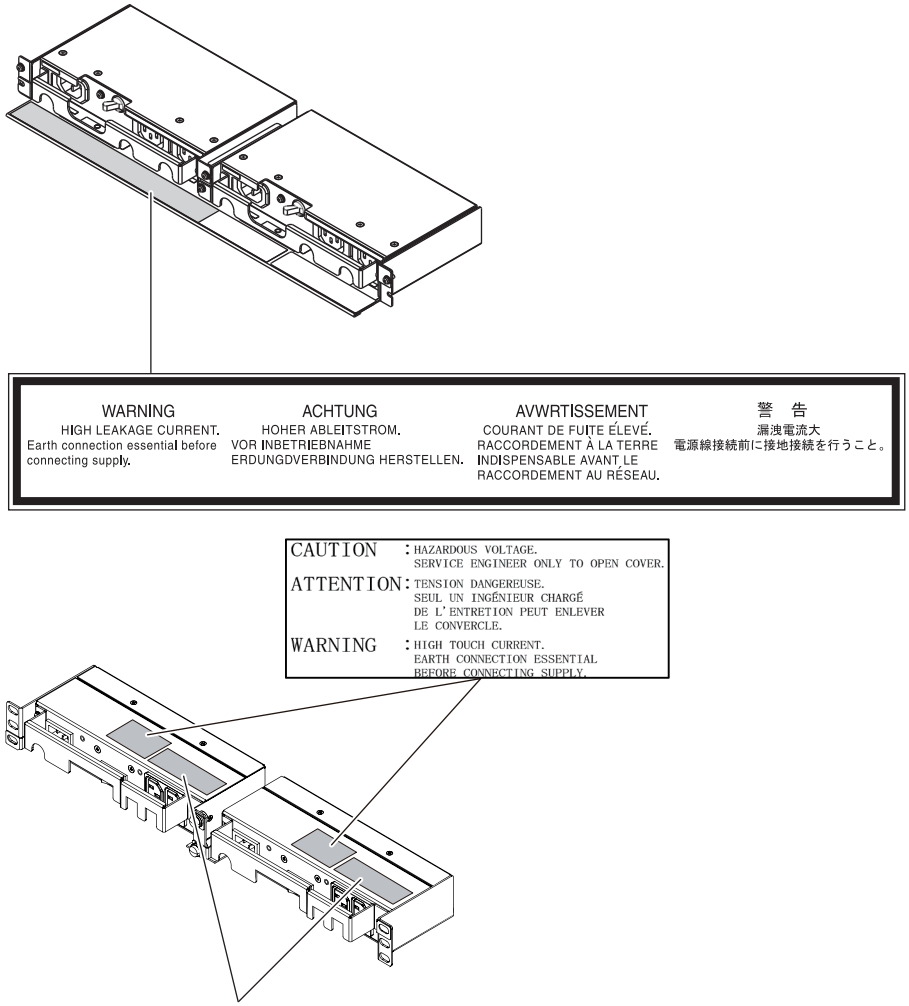
- High-density drive enclosure



Power Distribution Units (for Regions other than the EMEIA, Central American, and Caribbean Regions)

For power distribution units, there are two different types of exteriors.

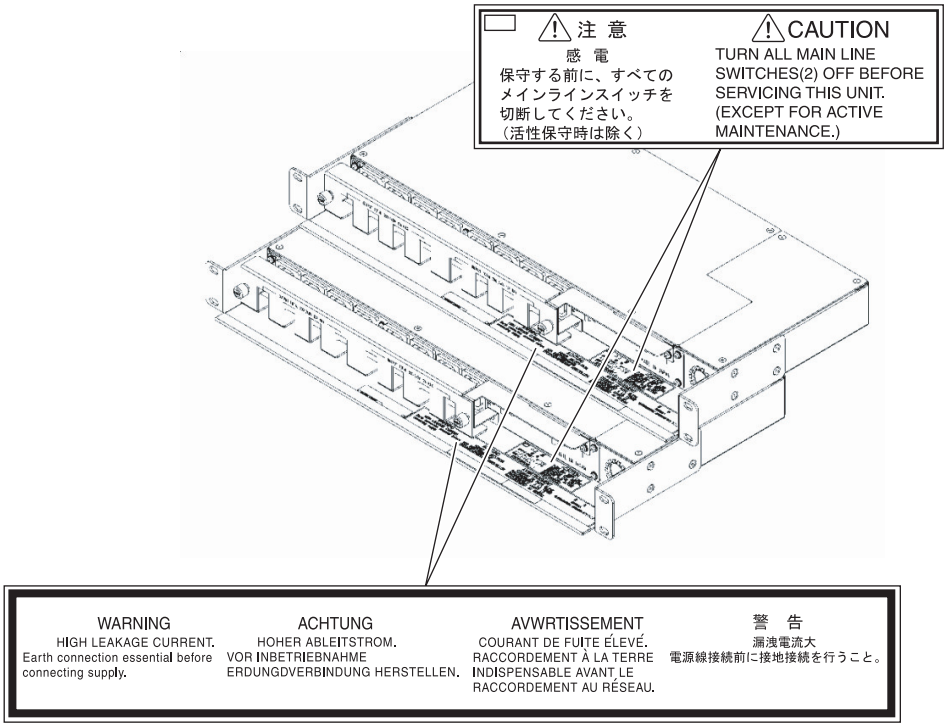
- Power distribution unit (AC200-240V, 1U)



Manufacturer's label

The model name and the serial number are listed.

- Power distribution unit (AC200-240V, 2U)



Manufacturer's label
The model name and the serial number are listed.

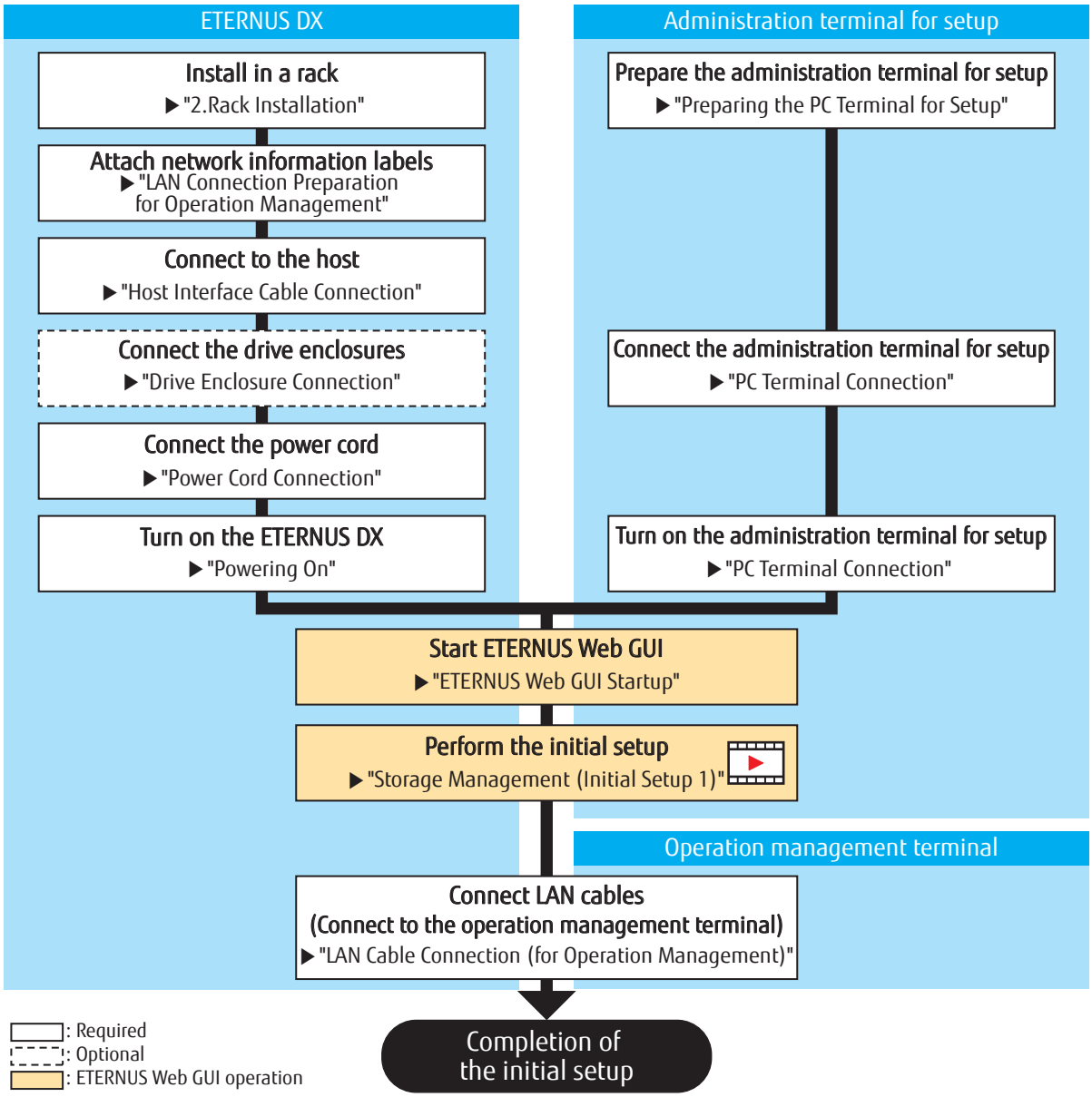
1. Configuration Workflow

This chapter describes the workflow from the installation of the ETERNUS DX in a rack to the completion of the configuration.

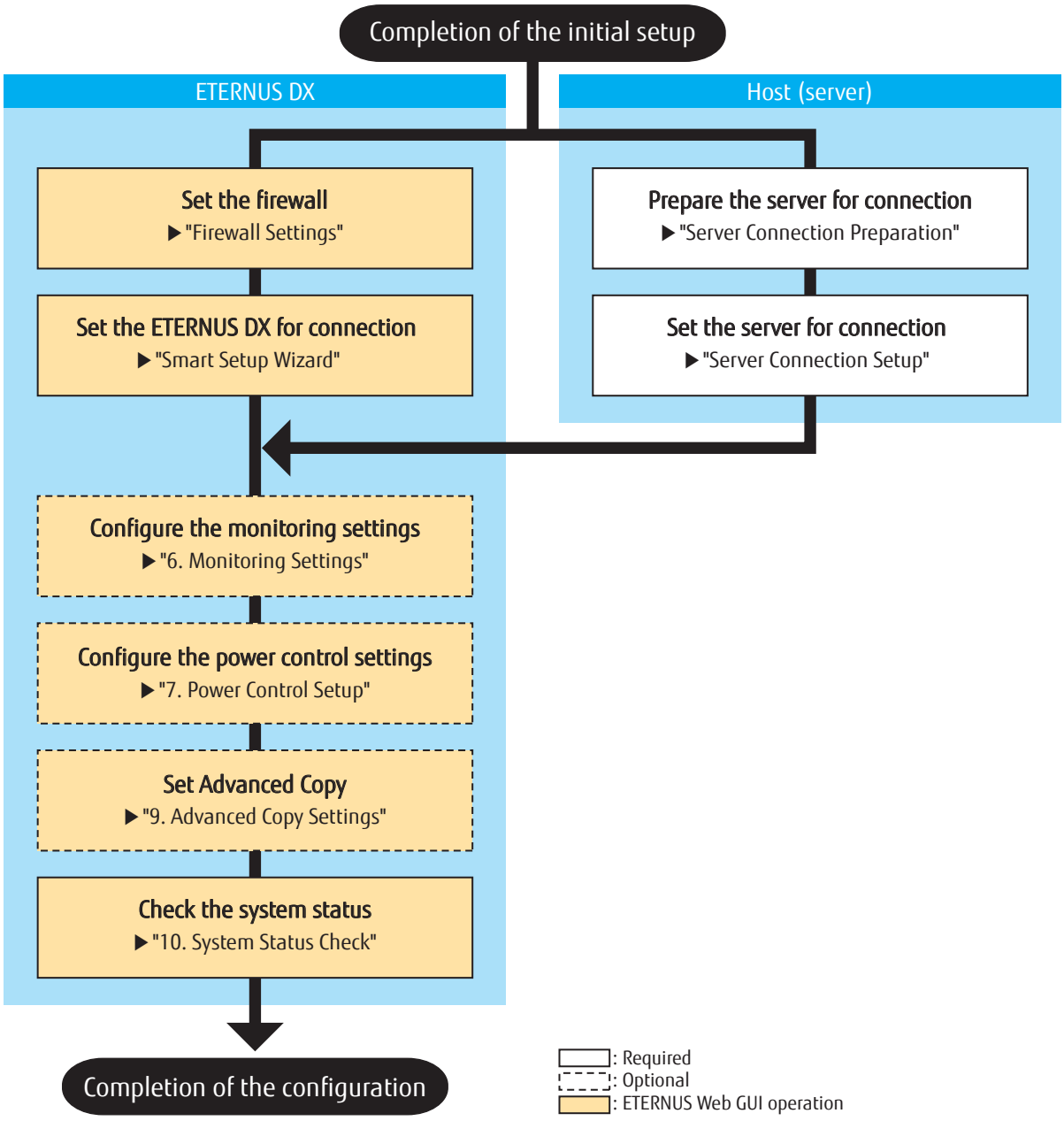
From Installation in a Rack to Completion of the Initial Setup

For details about the ETERNUS Web GUI operations affixed with the (▶) icon, refer to the FUJITSU Storage ETERNUS video site in addition to this manual. (See the "ETERNUS AF/DX Configuration Guide (Basic)" section in https://www.fujitsu.com/global/products/computing/storage/eternus/video-library/.)

When using power synchronization, perform the procedure described in "Power Synchronized Unit Connection" (page 60).

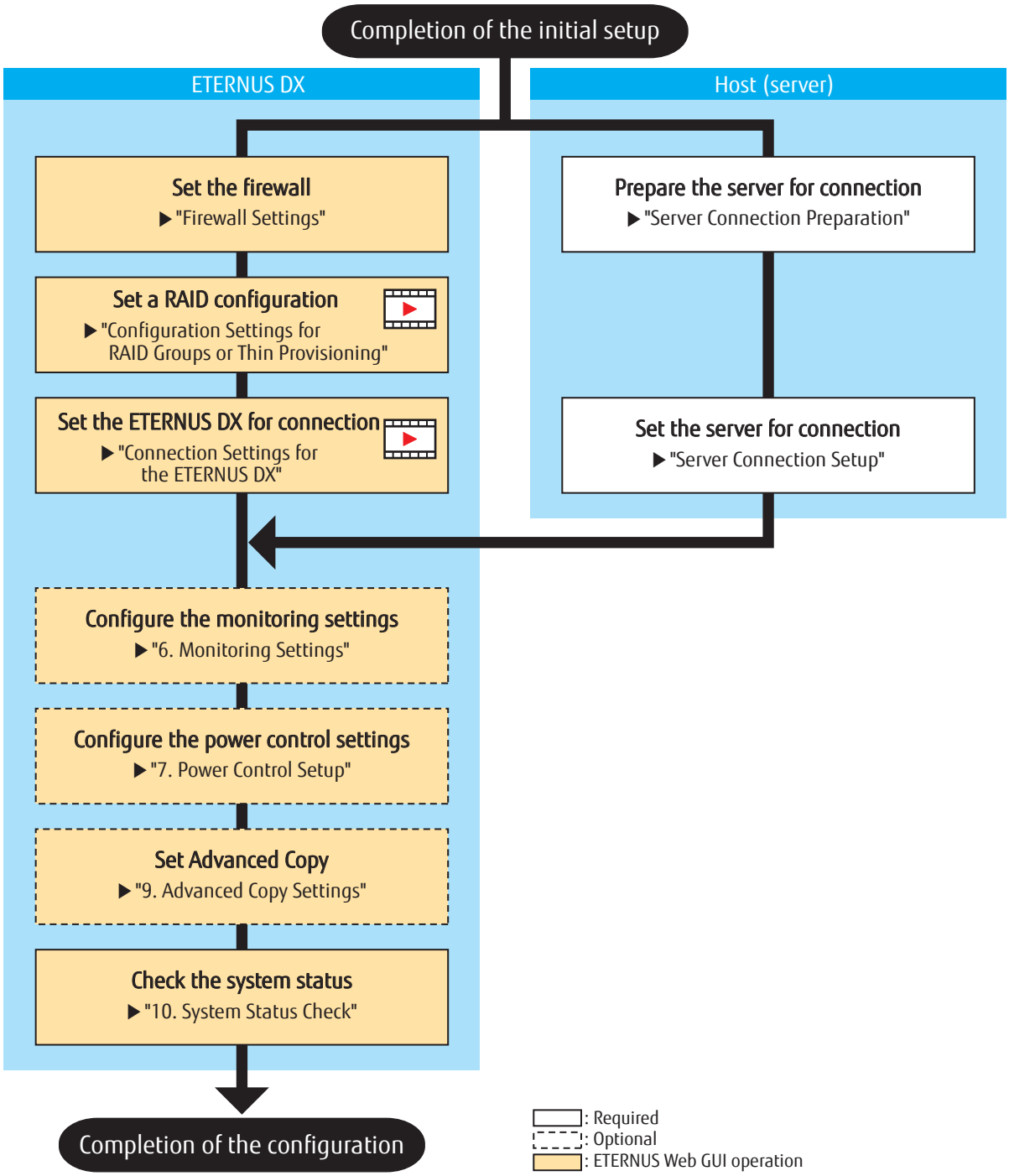


From Completion of the Initial Setup to Completion of the Configuration (When Using the Smart Setup Wizard)



From Completion of the Initial Setup to Completion of the Configuration (without Using the Smart Setup Wizard)

For details about the ETERNUS Web GUI operations affixed with the (▶) icon, refer to the FUJITSU Storage ETERNUS video site in addition to this manual. (See the "ETERNUS AF/DX Configuration Guide (Basic)" section in https://www.fujitsu.com/global/products/computing/storage/eternus/video-library/.)



2. Rack Installation

This chapter describes the procedure for installing the ETERNUS DX in a rack.

Make sure to check "Safety Notes and Regulations" before starting the installation. Also refer to the rack manual.

CAUTION

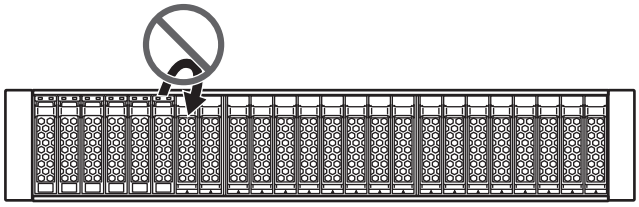
Do

- Wear a wrist strap or touch a metal part to discharge the human body's natural static electricity before starting each operation. Failure to discharge static electricity may cause failure in the ETERNUS DX.
- If components are installed in a way other than as described in this chapter, damage and/or device failure or electrical shock may occur.
- Do not install the ETERNUS DX in the rack with cables, such as power cords, connected.
- The ETERNUS DX contains delicate components, and should be handled gently. Do not drop or knock the ETERNUS DX against the rack when installing it. Also, do not knock the other devices installed in the rack.
- The center of gravity must be taken into consideration to prevent a rack from toppling over. Enclosures should generally be installed from bottom to top to lower the center of gravity and to ensure the safe use of racks.

Do Not

- Do not uninstall the drives that are installed by default or move them to any other slot.

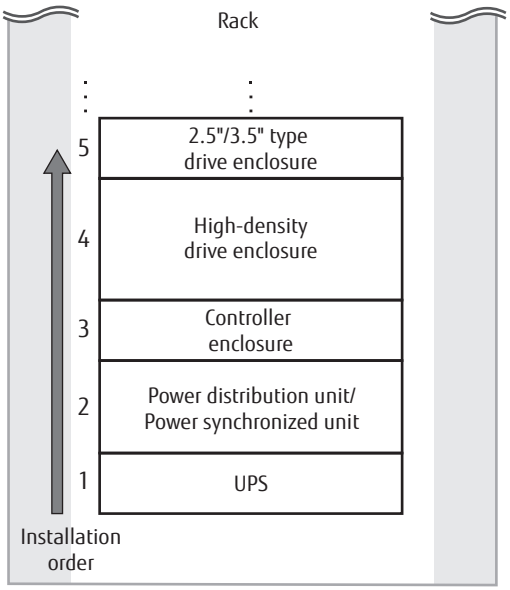
  Contact your sales representative or maintenance engineer if drives that are installed by default need to be uninstalled or moved to another slot.



Note

- If the storage system is installed at the bottom of a rack, a space for the surplus of cables may not be available in some racks, preventing the storage system from being pulled out when maintenance work is required. In this case, secure a space of 1U or more at the bottom when installing the storage system.
- To install an enclosure, power distribution units, power synchronized units, and UPS units in a single rack, mount the devices in the following order (from bottom to top).

  Drive enclosures must also be installed in order of DE-ID (DE_No. label). For details on the DE_No. label, refer to "2.5"/3.5" Type Drive Enclosure Installation (for Regions other than the EMEIA, Central American, and Caribbean Regions)" (page 31) and "High-Density Drive Enclosure Installation (for Regions other than the EMEIA, Central American, and Caribbean Regions)" (page 34).



Power Distribution Unit Installation (for Regions other than the EMEIA, Central American, and Caribbean Regions)

This section describes how to install a power distribution unit in a rack.

CAUTION

Do Not

- Do not connect any devices other than the ETERNUS DX to the power distribution unit.

Installing Power Distribution Unit (1U)

This section describes how to install a 1U power distribution unit in a rack.

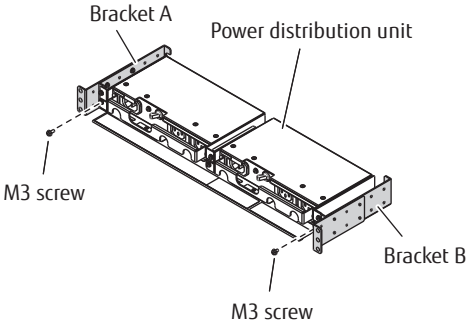
For power distribution units (1U), there are two different types of exteriors.

■ For Product ID ETFP4BU-L

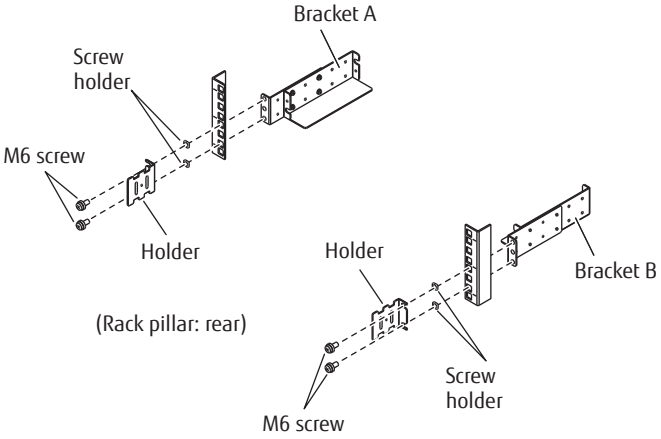
Procedure

1 Remove the two brackets temporarily attached to the power distribution unit.

Remove the two M3 screws from the front of the power distribution unit to free the brackets.

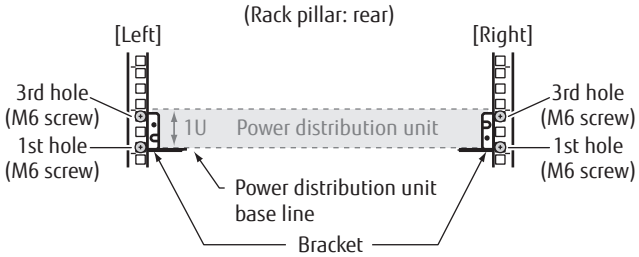


2 Attach the brackets and holders to the rack.



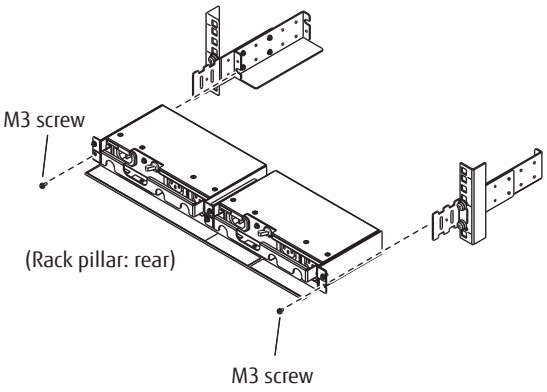
The four M6 screw positions for the brackets are determined relative to the power distribution unit base line.

The four M6 screws should be inserted in the 1st and 3rd holes above the base line.



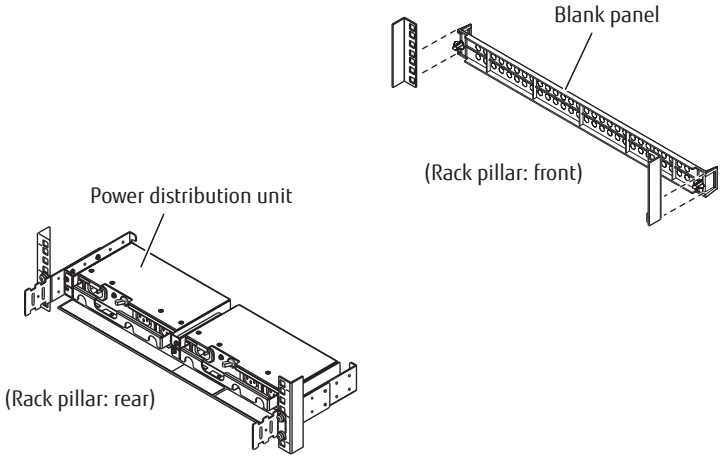
3 Install the power distribution unit in the rack.

Fasten the power distribution unit to the bracket with the two M3 screws removed in Step 1.



4 Attach the blank panel to the front side of the rack.

The blank panel should be attached at the same height as the power distribution unit.



End of procedure

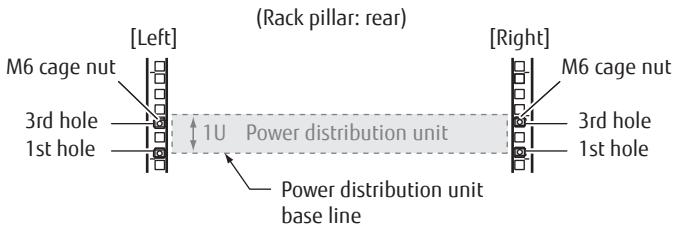
■ For Product ID ETFP4DU-L

Procedure

1 Attach the M6 cage nuts to the rear rack pillar.

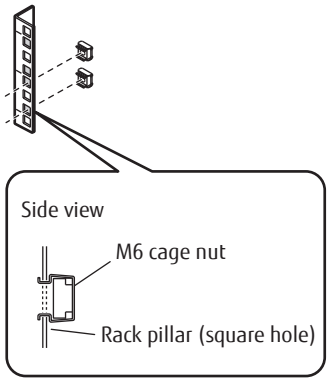
- Attachment positions

  On either side, insert four M6 cage nuts in the 1st and 3rd holes above the power distribution unit base line.



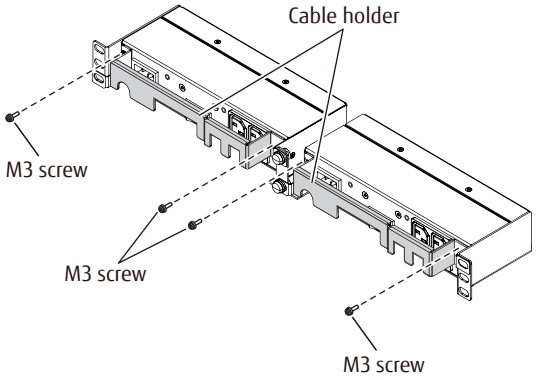
- Attachment procedure

  Clip the M6 cage nut tabs into the desired hole from the inside.



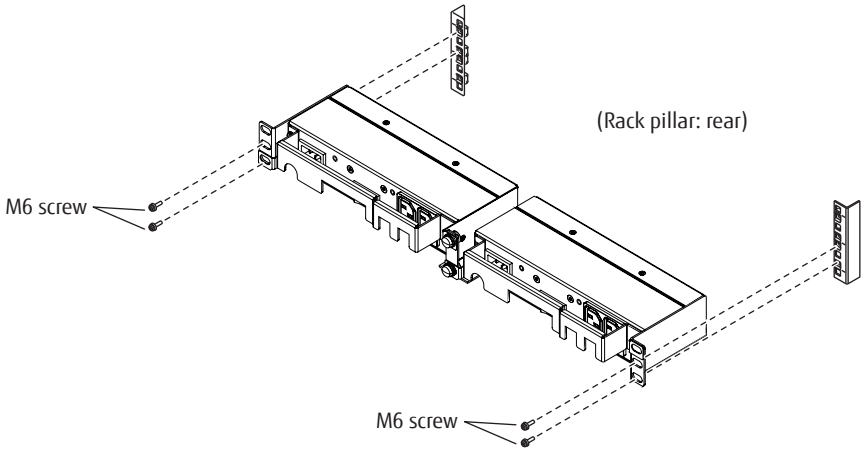
2 Attach the cable holders to the power distribution unit.

Use four M3 screws to attach the cable holders.



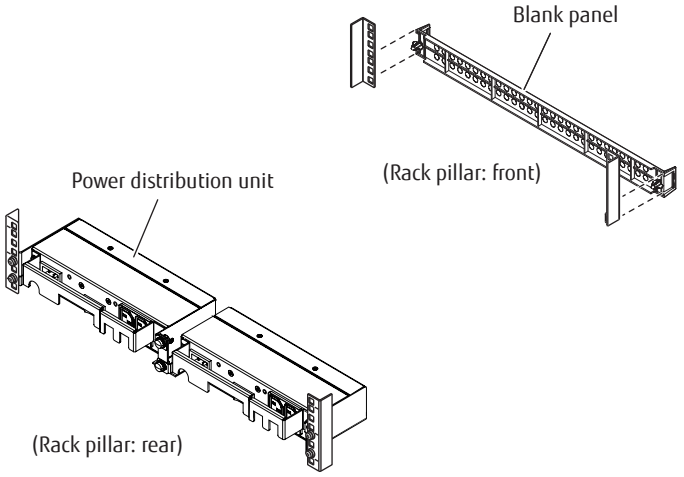
3 Install the power distribution unit in the rack.

Use four M6 screws to fasten it in the rack pillar.



4 Attach the blank panel to the front side of the rack.

The blank panel should be attached at the same height as the power distribution unit.



End of procedure

Installing Power Distribution Unit (2U)

This section explains how to install a 2U power distribution unit (12 outlet type or 16 outlet type) in a rack.

For power distribution units (2U), there are two different types of exteriors.

■ For Product ID ETFP12U-L/ETFP16U-L

Note

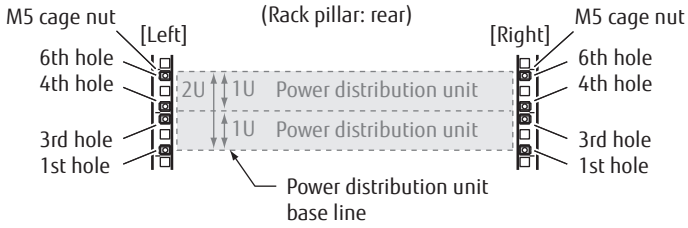
This section explains how to install a 12 outlet type power distribution unit (Product ID: ETFP12U-L) as an example. This installation method can also be applied to a 16 outlet type power distribution unit (Product ID: ETFP16U-L).

Procedure

1 Attach the M5 cage nuts to the rear rack pillar.

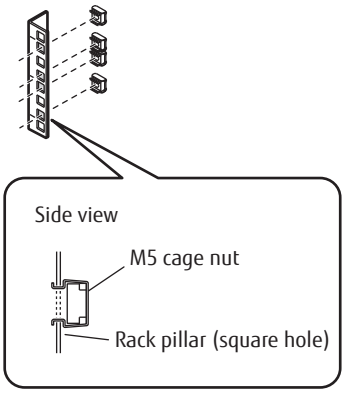
- Attachment positions

  On either side, insert eight M5 cage nuts in the 1st, 3rd, 4th, and 6th holes above the power distribution unit base line.



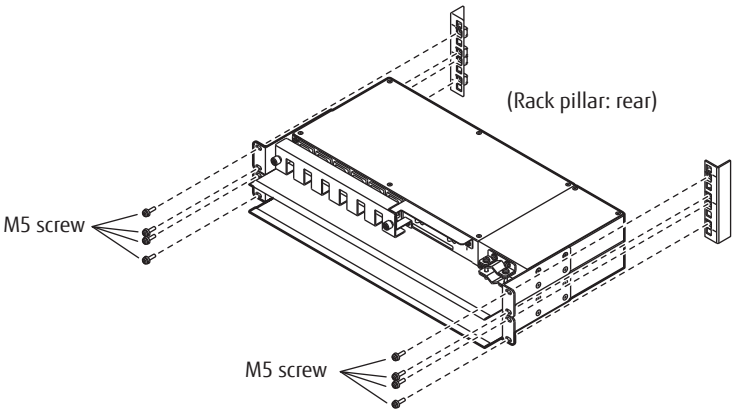
- Attachment procedure

  Clip the M5 cage nut tabs into the desired hole from the inside.



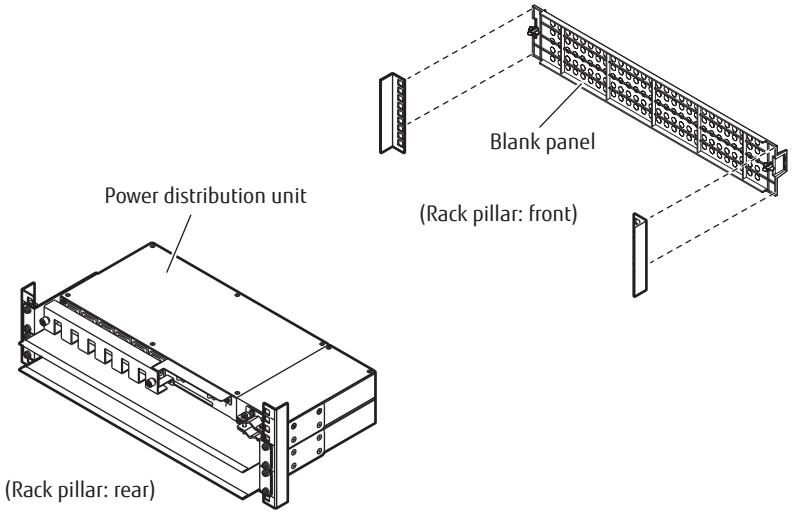
2 Install the power distribution unit in the rack.

Fasten it to the prepared holes in the pillars with eight M5 screws.



3 Attach the blank panel to the rack front.

The blank panel should be attached at the same height as the power distribution unit.



End of procedure

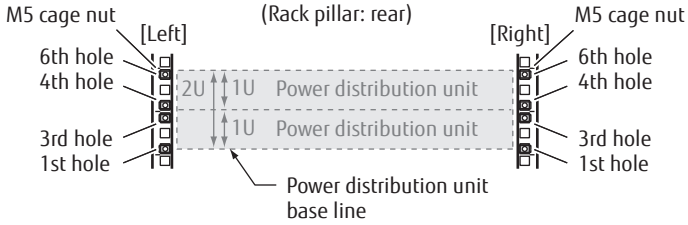
■ For Product ID ETFP32U-L/ETFP48U-L

Procedure

1 Attach the M5 cage nuts to the rear rack pillar.

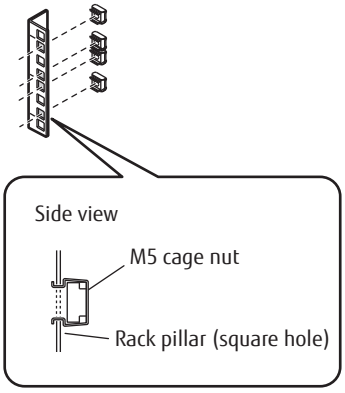
- Attachment positions

  On either side, insert eight M5 cage nuts in the 1st, 3rd, 4th, and 6th holes above the power distribution unit base line.



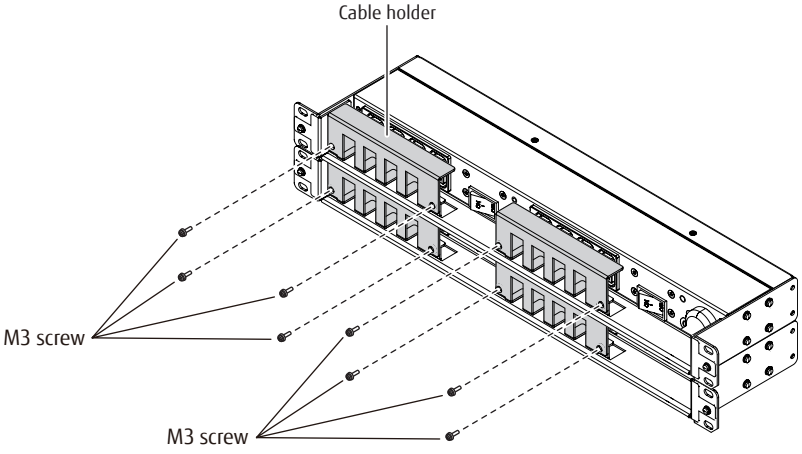
- Attachment procedure

  Clip the M5 cage nut tabs into the desired hole from the inside.



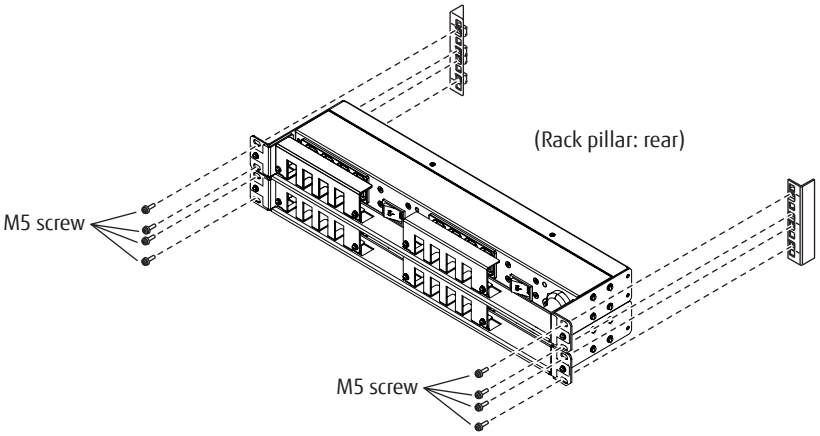
2 Attach the cable holders to the power distribution unit.

Use eight M3 screws to attach the cable holders.



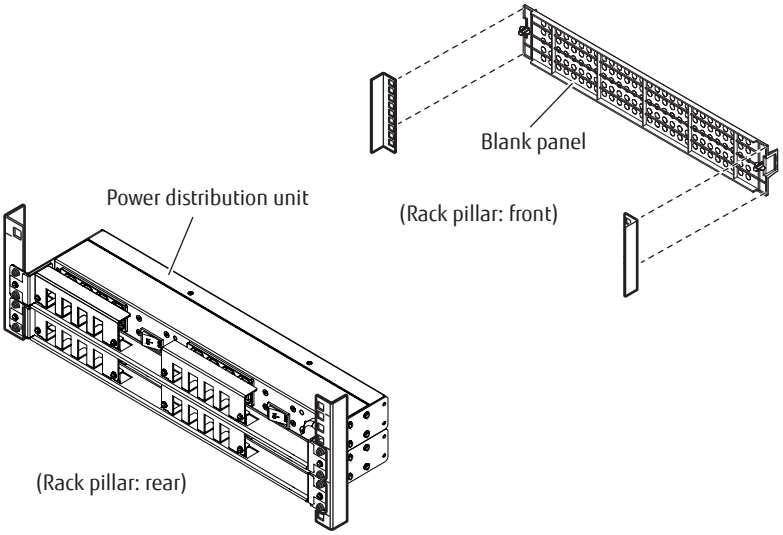
3 Install the power distribution unit in the rack.

Fasten it to the prepared holes in the pillars with eight M5 screws.



4 Attach the blank panel to the rack front.

The blank panel should be attached at the same height as the power distribution unit.



End of procedure

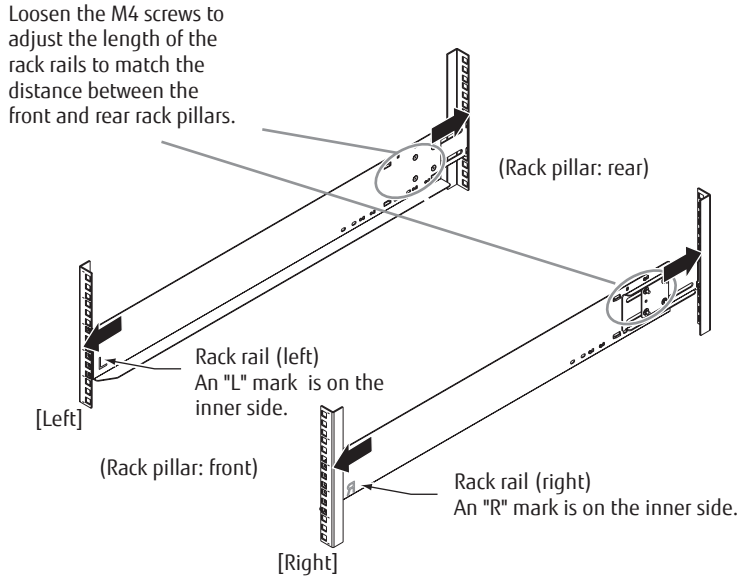
Controller Enclosure Installation (for Regions other than the EMEIA, Central American, and Caribbean Regions)

This section describes how to install a controller enclosure in a rack.

Procedure

1 Adjust the sizes of the rack rail (for left side) and the rack rail (for right side) to fit the rack.

Loosen the M4 screws to adjust the length of the rack rails to match the distance between the front and rear rack pillars. Leave the M4 screws slightly unscrewed, as the rack rails must be attached to the rack before they can be completely tightened.

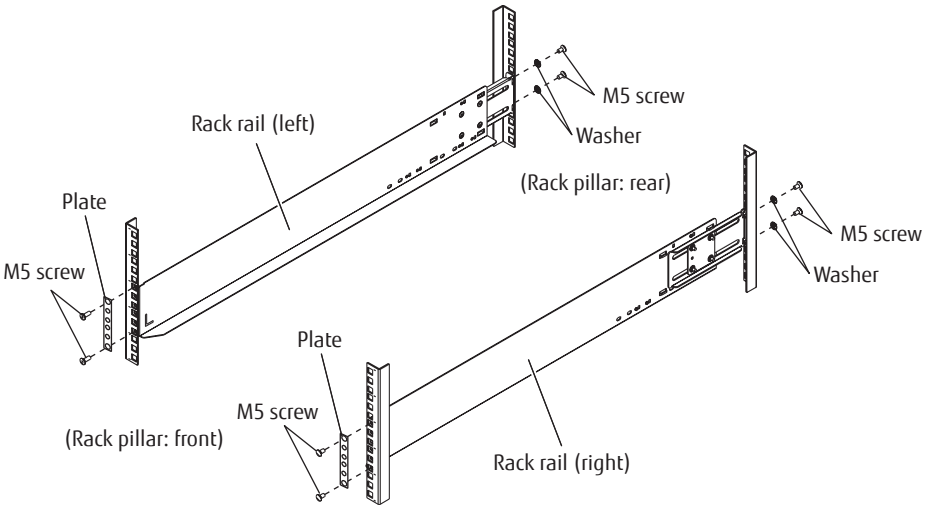


2 Attach the rack rails to the rack.

Use the two plates to fasten the rack rails to the front rack pillars. Use the washers to fasten the rack rails to the rear rack pillars.

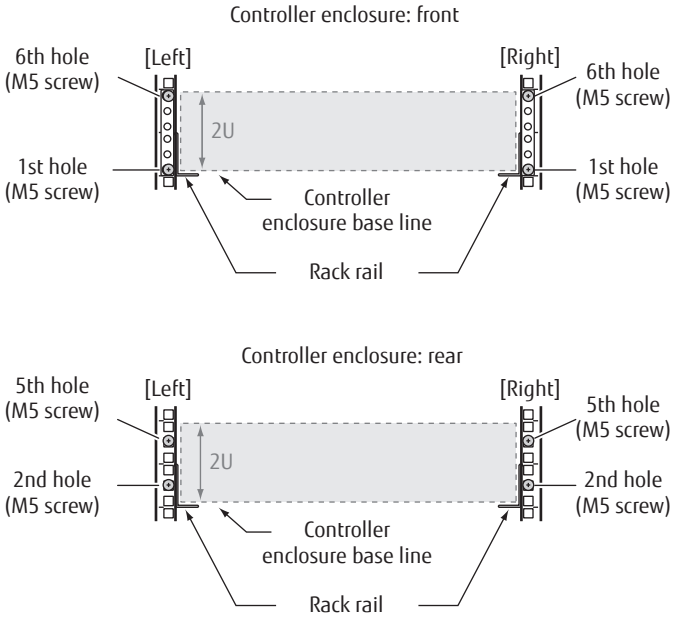
Note

Make sure to attach the rack rails to rack pillars so that they fit exactly together without any space between them.



The M5 screw positions for the rack rails are determined by the controller enclosure base line.

Insert the M5 screws in the 1st and 6th holes on the front rack pillars above the base line and in the 2nd and 5th holes on the rear rack pillars above the base line to fasten the rack rails.



3 Tighten the M4 screws of the rack rails that were slightly unscrewed in Step 1.

4 Install the controller enclosure in the rack.

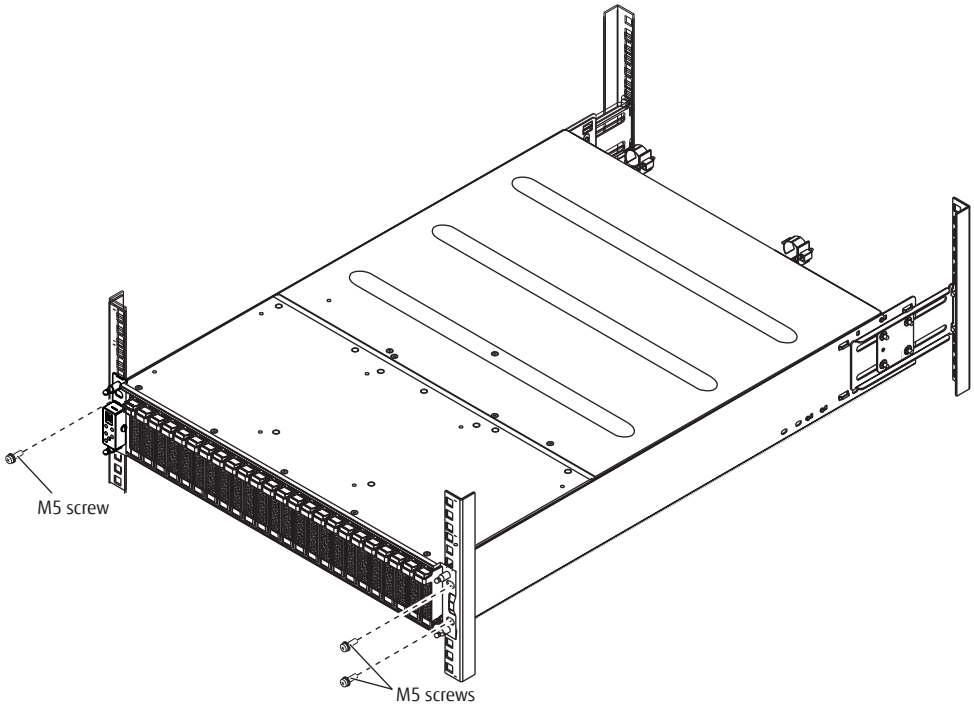
CAUTION

Do

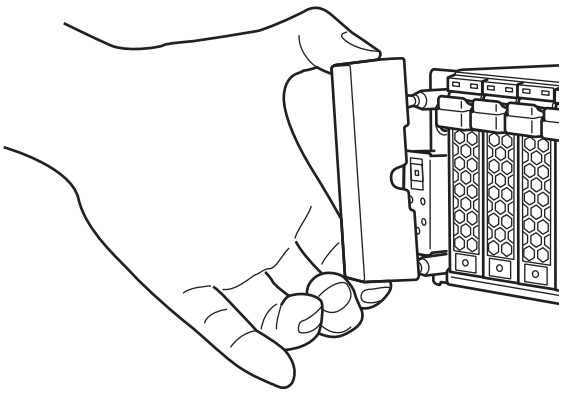
- When installing or removing the controller enclosure to or from the rack, make sure that the sides and the bottom of the controller enclosure are held by two or more people. Failure to do so may cause injury.

5 Fasten the controller enclosure in the rack.

Use three M5 screws to fasten it in the rack pillar.



6 Attach the flange cover.



End of procedure

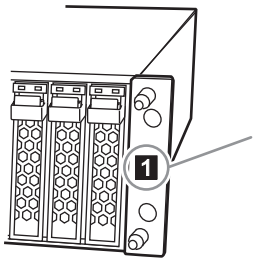
2.5"/3.5" Type Drive Enclosure Installation (for Regions other than the EMEIA, Central American, and Caribbean Regions)

This section explains how to install a 2.5"/3.5" type drive enclosure in a rack.

IMPORTANT

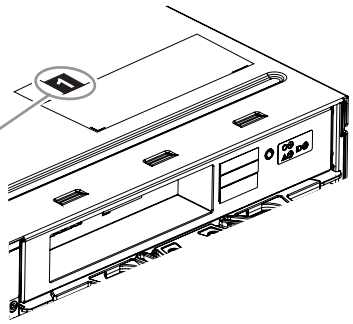
Drive enclosures must be installed above the controller enclosure. When installing multiple drive enclosures, install them in the order of the "DE_No. label" numbers that are attached to the drive enclosures. The DE_No. labels are attached on the following locations.

Right front side of the drive enclosure



DE_No. label

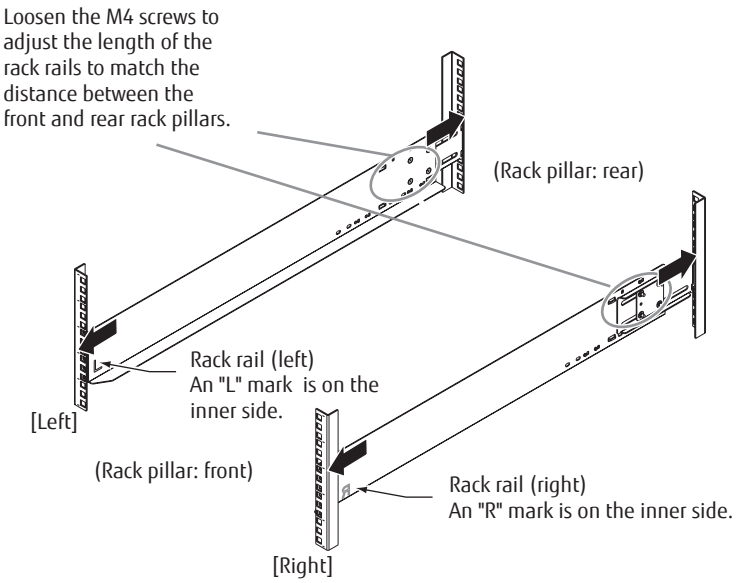
Upper right rear side of the drive enclosure



Procedure

1 Adjust the sizes of the rack rail (for left side) and the rack rail (for right side) to fit the rack.

Loosen the M4 screws to adjust the length of the rack rails to match the distance between the front and rear rack pillars. Leave the M4 screws slightly unscrewed, as the rack rails must be attached to the rack before they can be completely tightened.

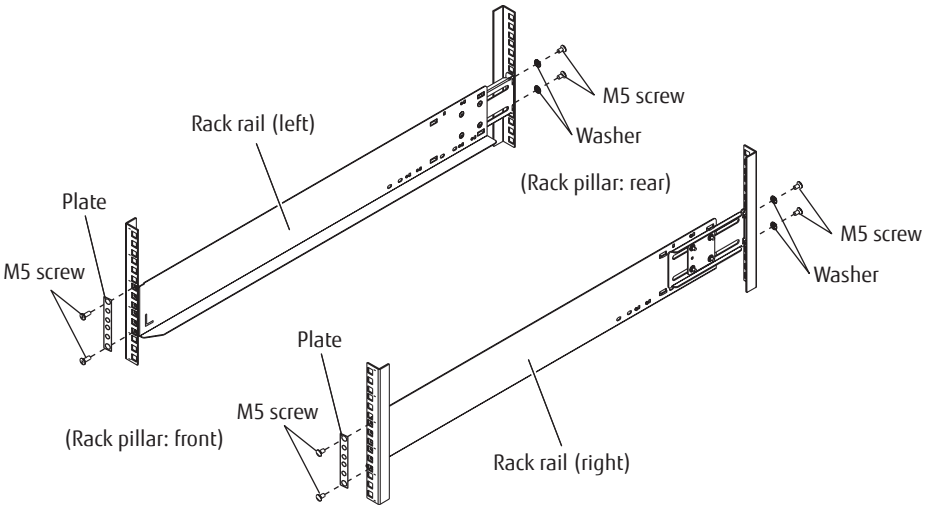


2 Attach the rack rails to the rack.

Use the two plates to fasten the rack rails to the front rack pillars. Use the washers to fasten the rack rails to the rear rack pillars.

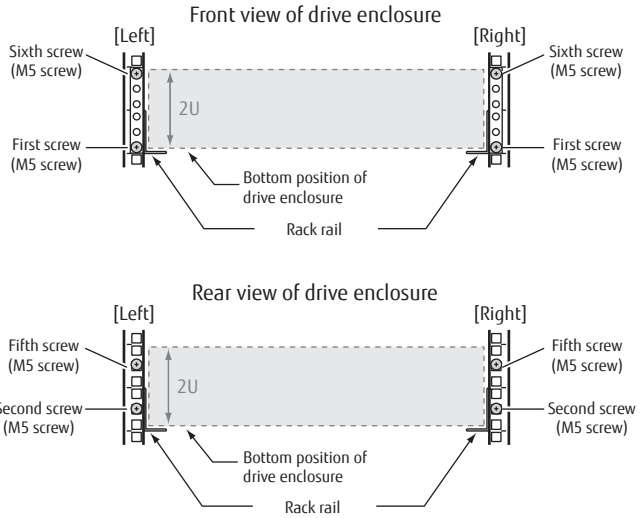
Note

Make sure to attach the rack rails to rack pillars so that they fit exactly together without any space between them.



The M5 screw positions for the rack rails are determined by the drive enclosure base line.

Insert the M5 screws in the 1st and 6th holes on the front rack pillars above the base line and in the 2nd and 5th holes on the rear rack pillars above the base line to fasten the rack rails.



3 Tighten the M4 screws of the rack rails that were slightly unscrewed in Step 1.

4 Install the drive enclosure in the rack.

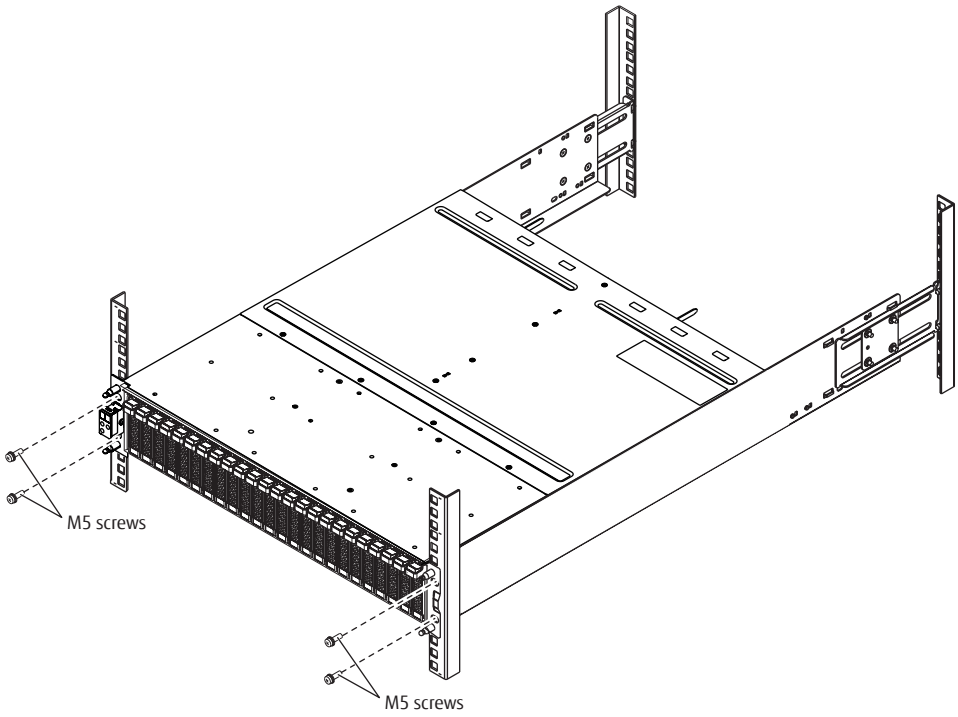
CAUTION

Do

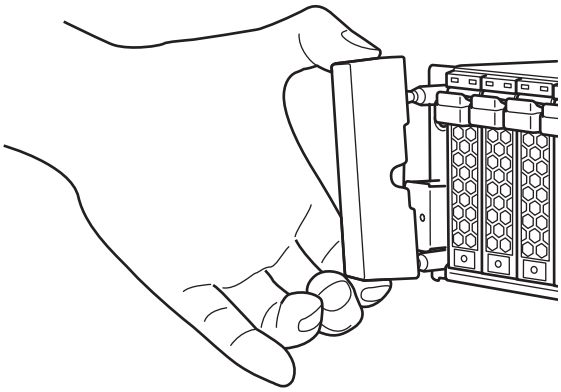
- When installing or removing the drive enclosure to or from the rack, make sure that the sides and the bottom of the drive enclosure are held by two or more people. Failure to do so may cause injury.

5 Fasten the drive enclosure in the rack.

Use four M5 screws to fasten it in the rack pillar.



6 Attach the flange cover.



End of procedure

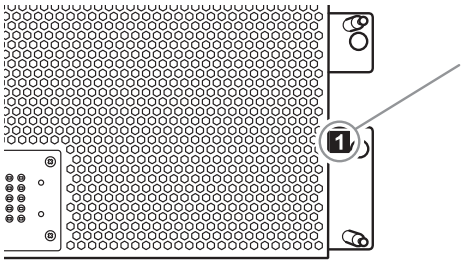
High-Density Drive Enclosure Installation (for Regions other than the EMEIA, Central American, and Caribbean Regions)

This section describes how to install a high-density drive enclosure in a rack.

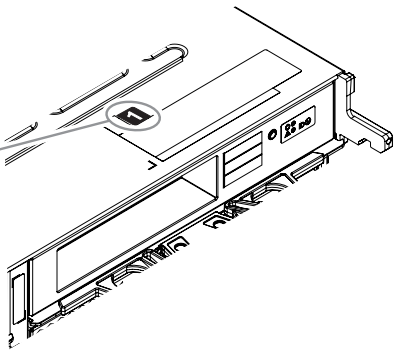
IMPORTANT

High-density drive enclosures must be installed above the controller enclosure. When installing multiple high-density drive enclosures, install them in the order of the "DE_No. label" numbers that are attached to the high-density drive enclosures. The DE_No. labels are attached on the following locations.

Right front side of the high-density drive enclosure



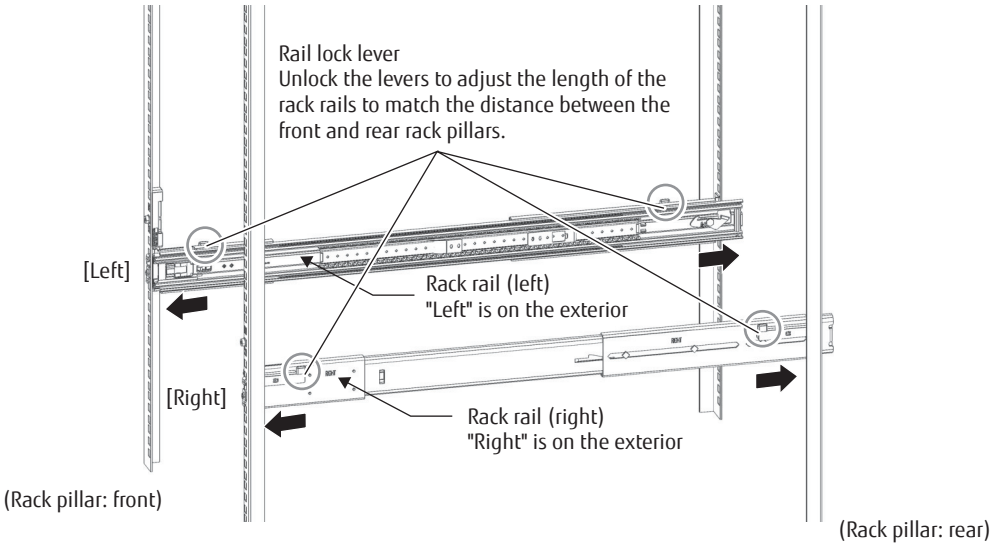
Upper right rear side of the high-density drive enclosure



Procedure

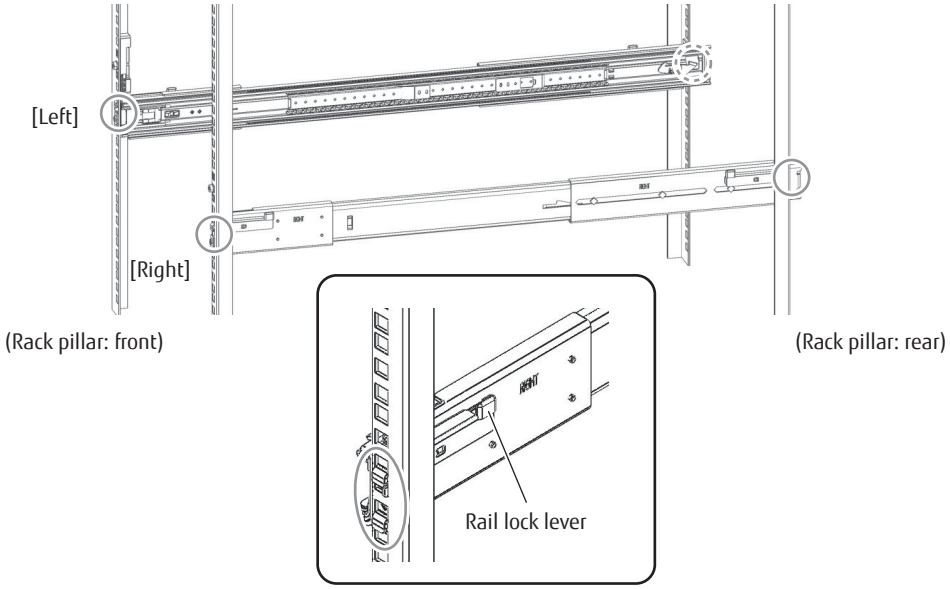
1 Adjust the sizes of the rack rail (for left side) and the rack rail (for right side) to fit the rack.

Pull the rail lock lever in the direction of the arrow and unlock it to adjust the length of the rack rails to match the distance between the front and the rear rack pillars. Leave the rail lock lever unlocked because the rail lock lever is locked after the rack rail is installed.



2 Attach the rack rails to the rack.

(1) Insert the rack rails into the holes of the front and the rear rack pillars to lock the rail lock lever.

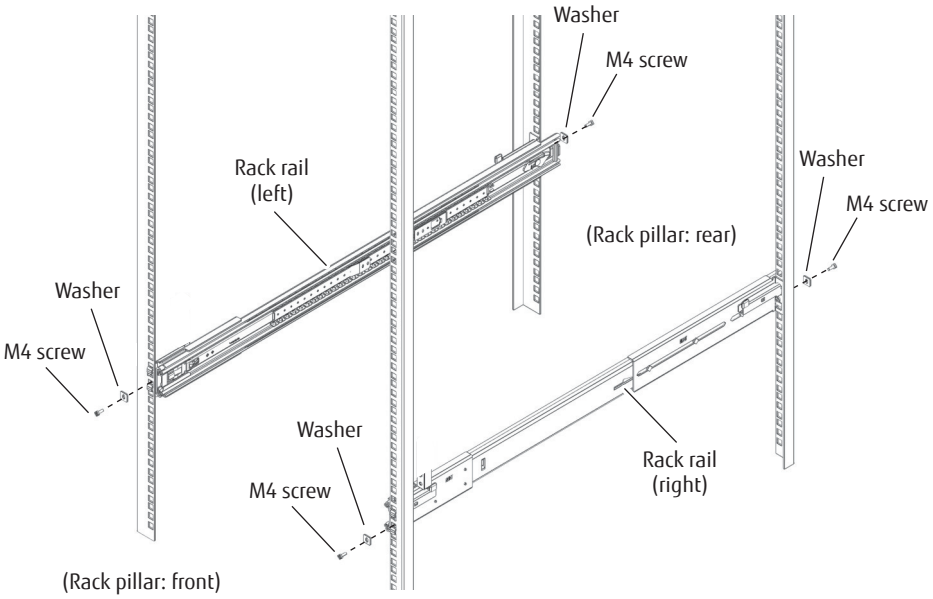


(2) Use the M4 screws to fasten the front and the rear rack rails.

Use the washers to fasten the rack rails to the front and rear rack pillars.

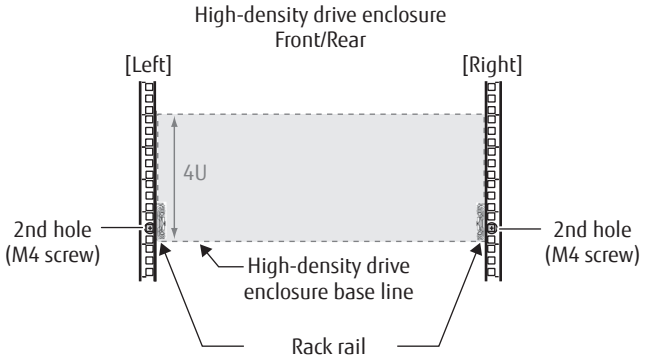
Note

Make sure to attach the rack rails to rack pillars so that they fit exactly together without any space between them.



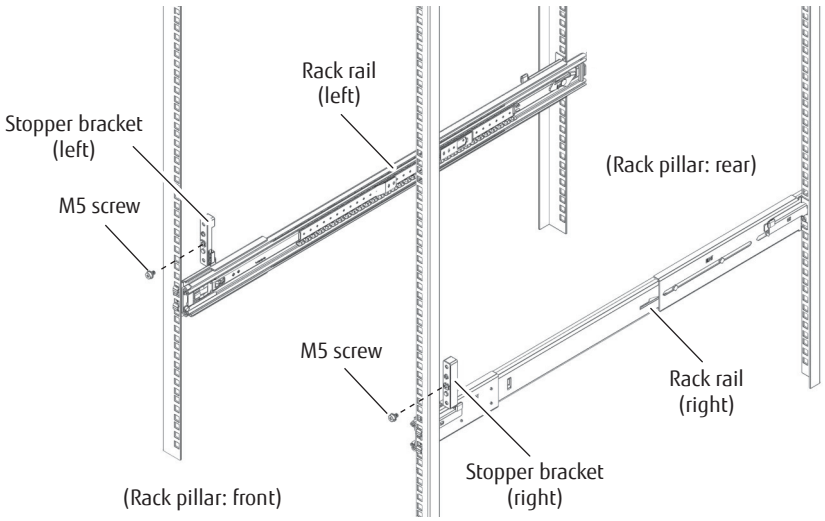
The M4 screw positions for the rack rails are determined by the high-density drive enclosure base line.

Insert the M4 screws in the second holes on the front and rear rack pillars above the base line to fasten the rack rails.



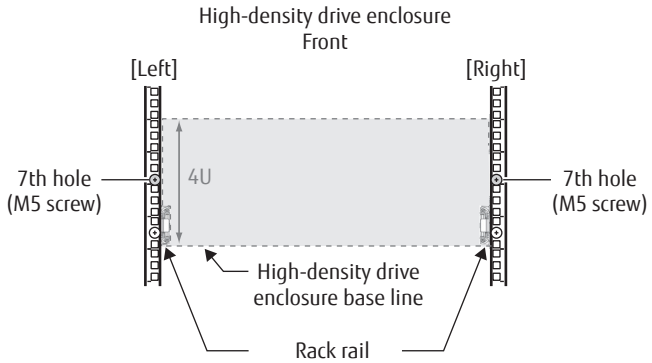
3 Install the stopper bracket (for left side) and the stopper bracket (for right side).

Attach the stopper bracket to the front rack pillar.



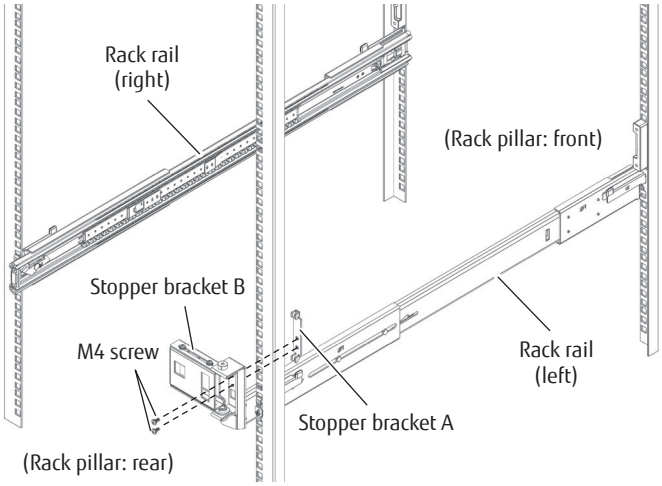
The M5 screw positions for the stopper brackets are determined by the high-density drive enclosure base line.

Insert the M5 screws in the seventh holes above the base line to fasten the stopper brackets.



4 Install the flap brackets.

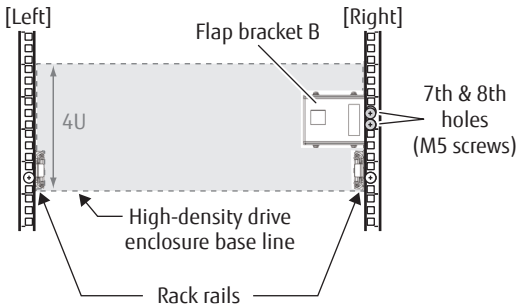
Attach flap bracket A and B on the right side of the rear rack pillar with the M4 screws.



The M4 screw positions for flap bracket A and B are determined by the high-density drive enclosure base line.

Insert the M4 screws in the seventh and eighth holes above the base line to fasten the flap brackets.

Rear view of a high-density drive enclosure



5 Install the high-density drive enclosure in the rack.

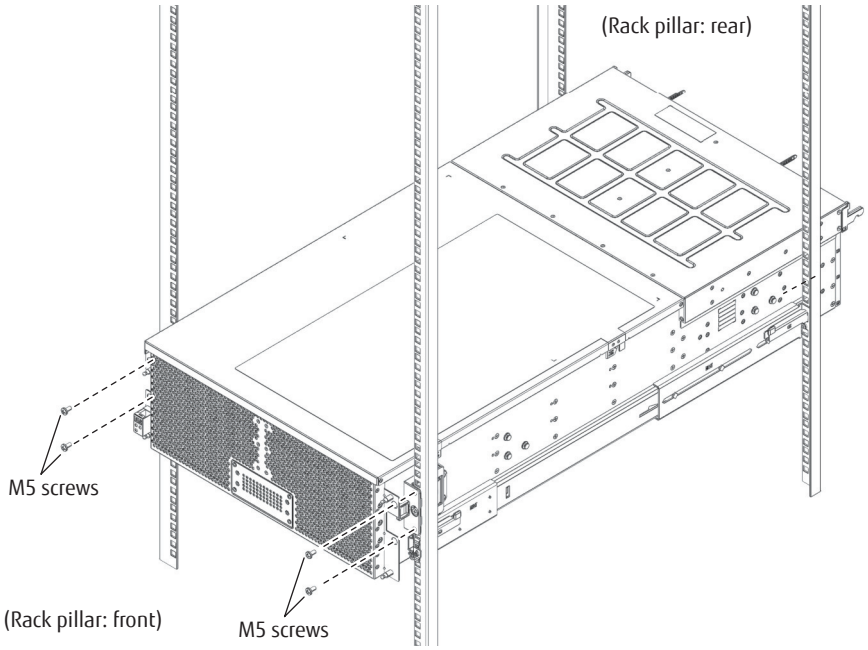
CAUTION

Do

- For safety and stability, use a lifter to install or remove high-density drive enclosures in the rack.

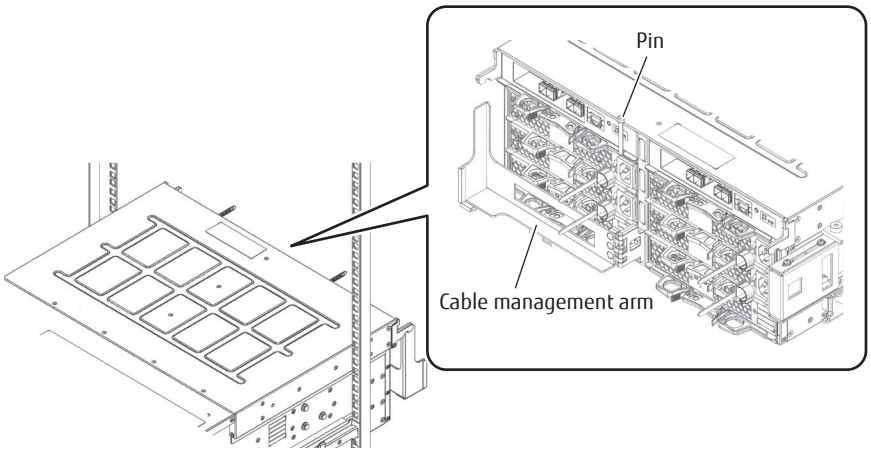
6 Fasten the high-density drive enclosure in the rack.

Use four M5 screws to fasten it in the rack pillar.

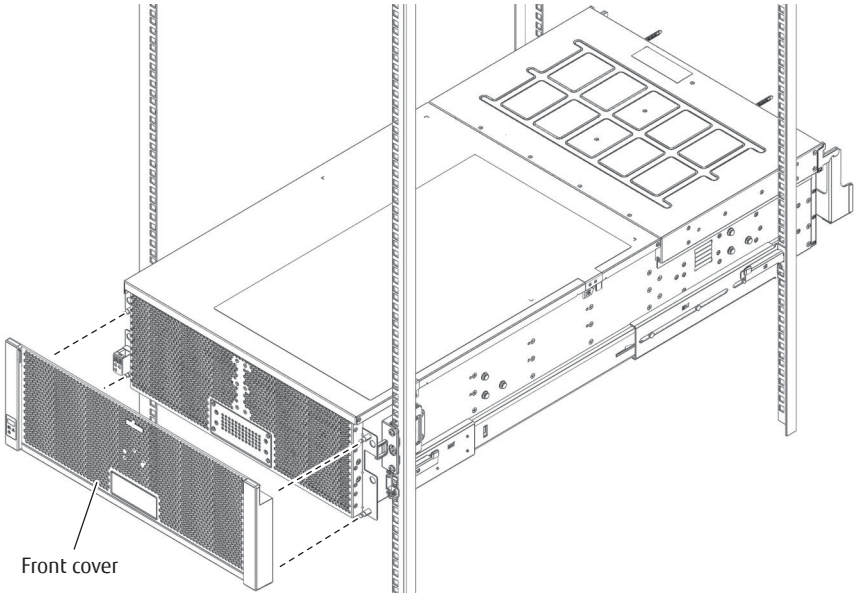


7 Attach the cable management arm.

To attach the cable management arm, place the arm in the bracket on the rear of the high-density drive enclosure. After placing the arm in the bracket, firmly attach the arm with the pin.



8 Attach the front cover.



End of procedure

3. Checking the Configuration Environment

This manual explains how to configure the system with the ETERNUS DX, taking a basic configuration as an example.

System Configuration Example

This section describes the procedure for the following system configuration as an example.

- iSCSI interface connection
- Multipath connection using the ETERNUS Multipath Driver
- Event notification (SNMP trap transmission, email notification, syslog notification, and remote support) via LAN
- Generation management of data by acquisition of backup based on the day of the week with generation copy using SnapOPC+

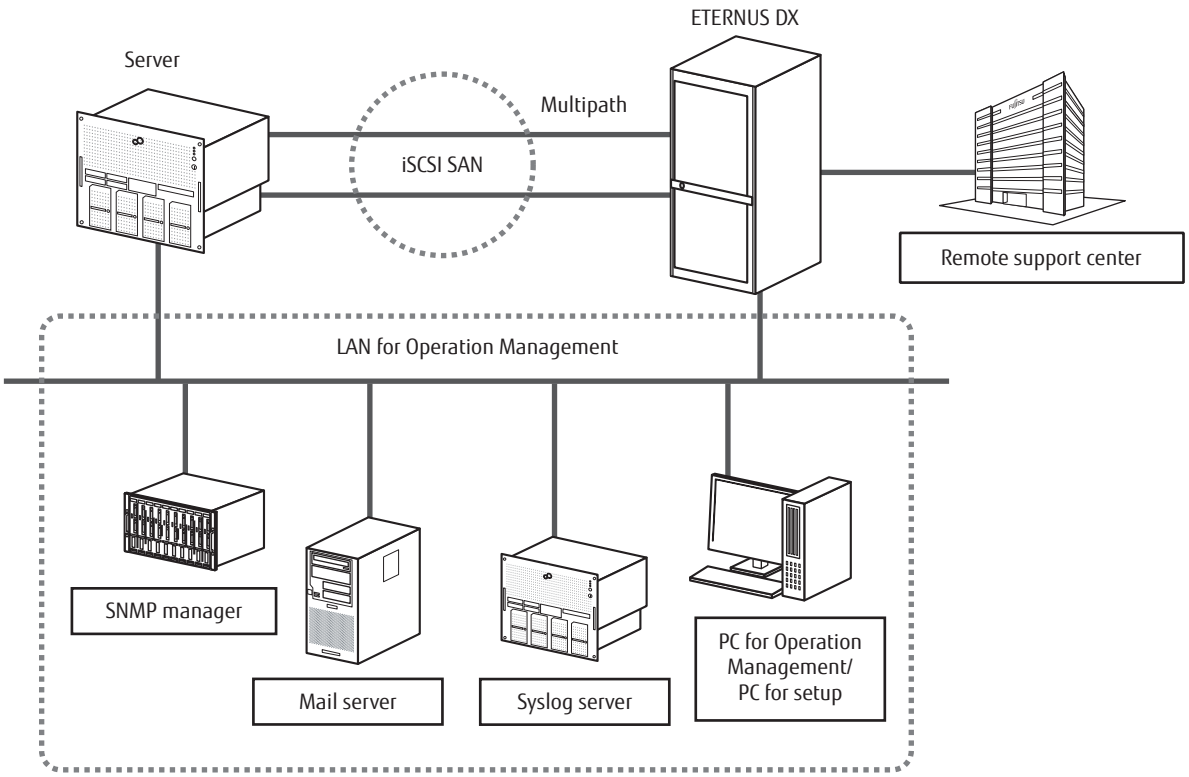
Note

For the settings for connection using other interfaces, refer to "Configuration Guide (Web GUI)" and "Configuration Guide -Server Connection-".

Configuration Diagram

The following diagram shows a system configuration example.

Figure 1 System Configuration Example



■ Server (Host) Environment

Table 1 Server (Host) Environment

Item	Explanation
Server OS	Windows Server 2008
Connection Configuration	iSCSI connection, duplicated with multipath connection
Multipath Driver	ETERNUS Multipath Driver

To connect the server and the ETERNUS DX via a switch, setting up of the switch must be performed. For details on this setting, refer to relevant manuals of the switch.

Server Connection Preparation

Prepare the server to connect to the ETERNUS DX.

A host bus adapter (HBA) that matches the connection interface that is to be used and a driver for the HBA are required. Some types of HBA require utility software. Prepare the required environment for the HBA that is to be used by referring to the HBA manual.

This section uses an iSCSI connection as an example to explain the required preparation for server connection.

Driver Preparation

Prepare required drivers and utilities.

- LAN card driver for iSCSI
  - LAN driver
  - Supported version of iSCSI Software Initiator

    This is already installed in a server that runs Windows Server 2008 or later.
- ETERNUS Multipath Driver

CAUTION

Do

- Before installing the ETERNUS Multipath Driver, make sure that the server is not connected to the ETERNUS DX. If the server is connected, shut down the server, remove the cable, and then restart the server.

Driver Installation

Install the LAN driver and the ETERNUS Multipath Driver.

LAN Driver Installation

The following procedure explains how to install the LAN driver.

When using the onboard LAN card, skip this procedure.

Procedure

1 To install a LAN driver, refer to the instructions for the LAN card.

2 Check that the driver has correctly been installed.

End of procedure

ETERNUS Multipath Driver Installation

The following procedure explains how to install the ETERNUS Multipath Driver.

Procedure

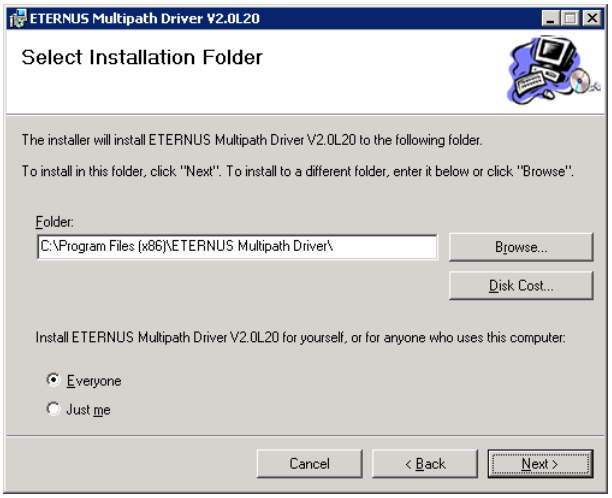
1 Insert the CD-ROM into the server, then from Windows Explorer double-click on "setup.msi" in the "English" folder of the CD-ROM.

A screen to confirm the start of installation appears.

2 Click the [Next] button.

A screen to specify the installation directory of the ETERNUS Multipath Driver and which user installs the driver appears.

3 To change the installation directory, click the [Browse] button and select the installation directory. To leave the settings unchanged, click the [Next] button.



Note

For the user who installs the driver, select [Everyone] for normal operations.

If [Just me] is selected, users other than the one who installed the driver are not allowed to uninstall or overwrite the installation of it.

The option that is selected here does not affect the operation of the ETERNUS Multipath Driver after installation.

A screen to confirm execution of the installation appears.

4 Click the [Next] button.

When installation is complete, a message appears.

5 Click the [Close] button.

A screen to confirm whether to restart the computer appears.

6 Restart the server.

End of procedure

iSCSI Initiator Parameter Settings

The following procedure explains how to set the iSCSI initiator parameters. This section shows how to set an iSCSI initiator name.

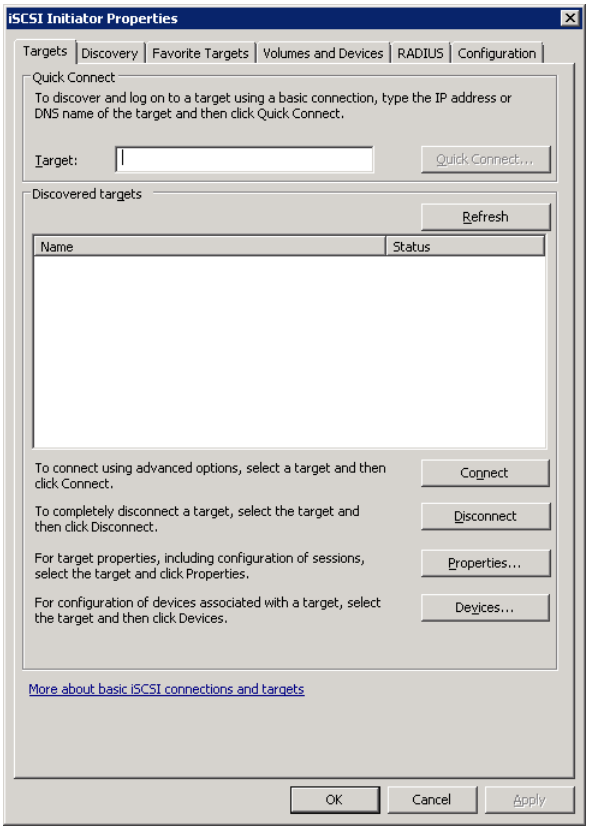
Procedure

1 In [Administrative Tools], click [iSCSI Initiator].

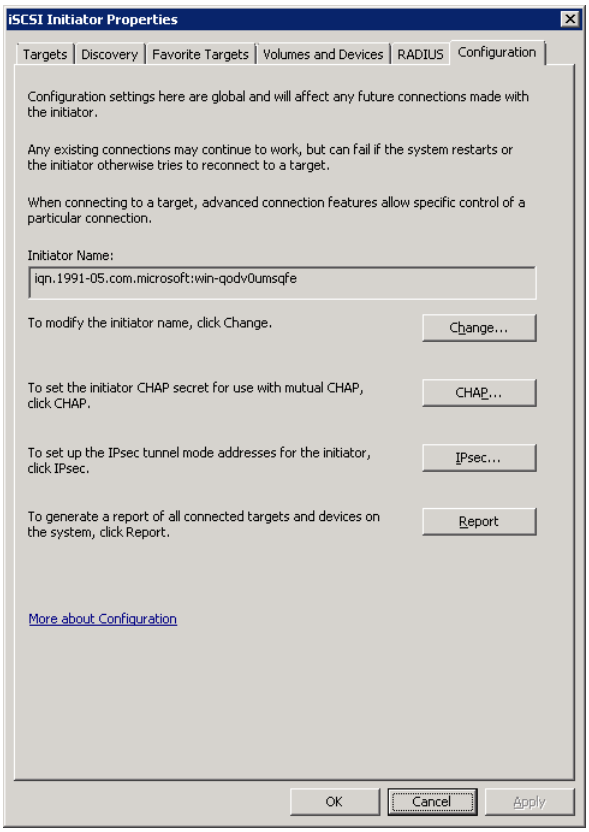
2 For the first startup, the following dialog appears.

If there is no problem with service startup settings, click the [Yes] button.

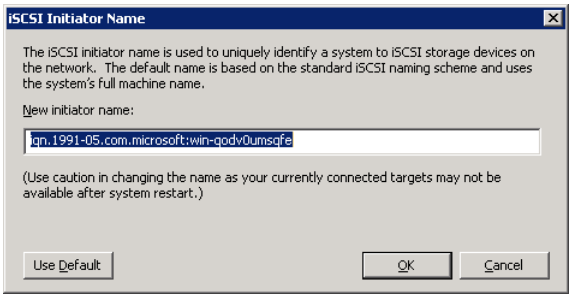
3 On the [iSCSI Initiator Properties] screen, click the [Configuration] tab.



4 The currently set initiator name is displayed.
Click the [Change] button.



5 On the [iSCSI Initiator Name] screen, specify the initiator name and click the [OK] button.
To leave the initiator name unchanged, click the [OK] button.



Note

To use the default initiator name, also click the [Change] button.
This allows you to continue to use this initiator name even after changing the "server name".

6 Shut down the server.

Note

After this, the settings for the ETERNUS DX must be completed before connecting the ETERNUS DX to the server. In order to perform these settings, turn off the server.

End of procedure

Preparing the PC Terminal for Setup

The initial settings of the ETERNUS DX are performed by using a Web browser on the PC terminal.

Prepare and set up the PC terminal before the initial settings.

Preparing the PC terminal

Prepare the PC terminal that contains the following environment:

- Web browser

  For details on the operating environment of ETERNUS Web GUI, refer to "ETERNUS Web GUI User's Guide" or "Configuration Guide (Web GUI)".

Setting up the PC terminal

Set up the PC terminal with the following procedure:

Procedure

1 Set the IP address and subnet mask of the PC terminal.

Set the following values.

IP address: 192.168.1.2

Subnet mask: 255.255.255.0

2 Check the settings of the Web browser.

For details on the required settings, refer to "Configuration Guide (Web GUI)".

End of procedure

LAN Connection Preparation for Operation Management

Completing and Attaching the Network Setting Label

Enter the network setting information on the Network Setting label. Attach the Network Setting label on the rack wall near the controller enclosure to avoid losing it.

Figure 2 Network Setting Label

Network Setting	
IP address of MNT port	:
IP address of FST port	: . . .
Subnet Mask of FST port	: . . .
IP address of RMT port	:

Complete the following items in the Network Setting label.

- IP address of MNT port

  Enter the IP address for the MNT port of the ETERNUS DX. The MNT port is a LAN port that is used to perform operation management connection.

- IP address of FST port

  This item is not used. No information needs to be entered for this item.

- Subnet Mask of FST port

  This item is not used. No information needs to be entered for this item.

- IP address of RMT port

  Enter the IP address for the RMT port of the ETERNUS DX. The RMT port is a LAN port that is used during initial setup and to connect to the remote support center.

LAN Related Specifications

■ Network Communication Protocols

The usable LAN ports and functions are different depending on the usage and protocol.

The following table shows how the LAN ports may be used (by usage and protocol).

Table 2 LAN Port Availability

Usage		Protocol	tcp / udp	Port number	Direction	Master CM		Slave CM		Remarks
						MNT	RMT	MNT	RMT	
ETERNUS Web GUI		http / https	tcp	80 / 443	from	○	○	△ (*1)	△ (*1)	Accessed from a Web browser
ETERNUS CLI		telnet / ssh	tcp	23 / 22	from	○	○	△ (*1)	△ (*1)	–
		ftp (client)	tcp	21	to	○	○	△ (*1)	△ (*1)	–
SNMP	agent	snmp	udp	161	from	○	○	○	○	–
	trap	snmp trap	udp	162 (*2)	to	○ (*3)	○ (*3)	×	×	–
SMI-S		http / https	tcp	5988 / 5989	from	○	×	×	×	Used for SMI-S client communication
		http / https	tcp	–	to	○	×	×	×	Used for event communications with the SMI-S listener, etc.
		SLP	udp	427	to	○	×	×	×	Used for service inquiry communication from the SMI-S client
		SLP	tcp	5993	from	○	×	×	×	
E-mail		smtp (client)	tcp	25 (*2)	to	○ (*3)	○ (*3)	×	×	Used for failure notification, etc.
NTP		NTP (client)	udp	123	to	○ (*3)	○ (*3)	×	×	–

Usage	Protocol	tcp / udp	Port number	Direction	Master CM		Slave CM		Remarks
					MNT	RMT	MNT	RMT	
REMCS (remote support)	smtp (client)	tcp	25 (*2)	to	○ (*3)	○ (*3)	×	×	Used for failure notification, etc.
	pop3 (client)	tcp	110 (*2)	to	○ (*3)	○ (*3)	×	×	Used for SMTP authentication
	http (client)	tcp	80 or 8080 (*2)	to	○ (*3)	○ (*3)	×	×	Used for firmware download, etc.
AIS Connect (remote support) (*4)	https (client)	tcp	443	to	○ (*3)	○ (*3)	×	×	–
Syslog (event notification and audit log sending)	Syslog	udp	514 (*2)	to	○ (*3)	○ (*3)	×	×	–
RADIUS	Radius	udp	1812 (*2)	to	○ (*3)	○ (*3)	×	×	–
ping	ICMP	–	–	from	○ (*3)	○ (*3)	×	×	–
KMIP (key management)	SSL	tcp	5696 (*2)	to	○ (*3)	○ (*3)	×	×	–
ETERNUS DX Discovery	Unique protocol	udp	9686	from	○	×	×	×	–

○: Possible / △: Partially possible / ×: Not possible

***1:** Only the following functions are available:

- Checking the ETERNUS DX status
- Switching the Master CM

***2:** Modifiable

***3:** May use either the MNT port or RMT port.

***4:** Service for AIS Connect was discontinued in December 2022.

For details on the port numbers for the ETERNUS SF Software, refer to the manual of each Storage Foundation Software ETERNUS SF.

■ Communication Modes

The default LAN operation mode is "Auto Negotiation" which allows the ETERNUS DX to automatically recognize 1000BASE-T/100BASE-TX/10BASE-T and Full/Half-Duplex connections. However, some devices may require that a fixed communication mode be set.

4. Connecting Cables

This chapter explains how to connect various cables to the ETERNUS DX.

CAUTION

- Wear a wrist strap or touch a metal part to discharge the human body's natural static electricity before starting each operation. Failure to discharge static electricity may cause failure in the ETERNUS DX.

Host Interface Cable Connection

Connect the ETERNUS DX to the connection destination using host interface cables. The connection procedure varies depending on the type of host interface that is used for the ETERNUS DX.

If the host interface in the ETERNUS DX100 S4/DX200 S4 is iSCSI 10Gbit/s (10GBASE-SR) or Ethernet 10Gbit/s, and an FC cable is used for the connection, the SFP+ module must be installed in the host interface port before the cable is connected.

Prepare the same number of host interface cables as the number of host interface ports.

IMPORTANT

- To help with host interface cable management and prevent incorrect connections, attach labels to the cables that show which end is for the connection origin and which end is for the connection destination.
- SAS 12Gbit/s host interface cables have the same connector type as the mini SAS HD cables between enclosures. To prevent accidental connections to a DI port on the drive enclosure or the controller enclosure with the host interface cable, check the connection destination port.

  In addition, the cable connector of the host interface is plugged in an orientation that is different from the connector of the mini SAS HD cables between enclosures. When connecting the host interface cable, make sure that the tab is facing up.
- When connecting a host interface cable, check the direction of the connector tab and insert it all the way in firmly.

  When disconnecting a host interface cable, pull out the connector while holding its tab.
- If the host interface ports and host interface cable connectors have covers, remove the covers. Keep the removed covers in a safe place where they will not be lost.
- When connecting the cables, position them so that they will not obstruct replacement of the power supply unit or controllers by the maintenance engineer.

Note

This section uses a controller enclosure with two controllers as an example to explain the connection procedure. When one controller is installed, this procedure is only applied to Controller 0 (CM#0).

SFP+ Module Handling Instructions

The following shows instructions for handling an SFP+ module.

About Condensation

CAUTION

Do

- When moving an SFP+ module from a cold place, such as an unconditioned store house in winter, to a warmer place such as an air-conditioned room, the severe temperature change may result in condensation forming.

  To avoid this, allow the packed SFP+ modules sufficient time in the warmer place (one hour for each 15°C of temperature difference) to adapt to the new temperature.

About Static Electricity

CAUTION

Do

- When handling SFP+ modules, wear a wrist strap or touch a metal part to discharge the human body's natural static electricity. Failure to discharge static electricity may cause failure in the ETERNUS DX.
- Leave the SFP+ module in its package until ready to install it.

About Shock

CAUTION

Do Not

- Do not handle the SFP+ module roughly or subject it to physical shocks when laying it down.
- Do not place any objects on top of SFP+ modules.
- Do not knock or drop the SFP+ module on hard objects.

This section uses an iSCSI 1Gbit/s host interface (CA) as an example to show the connection procedure.

Procedure

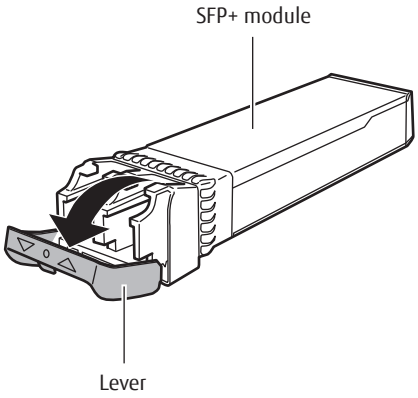
1 Install an SFP+ module in the host interface port.

This procedure is required only when an SFP+ module must be installed.

Note

Step 1 is not required if the host interface (CA) is iSCSI 1Gbit/s.

(1) Remove the connector cover attached to the port of the SFP+ module and open the lever.

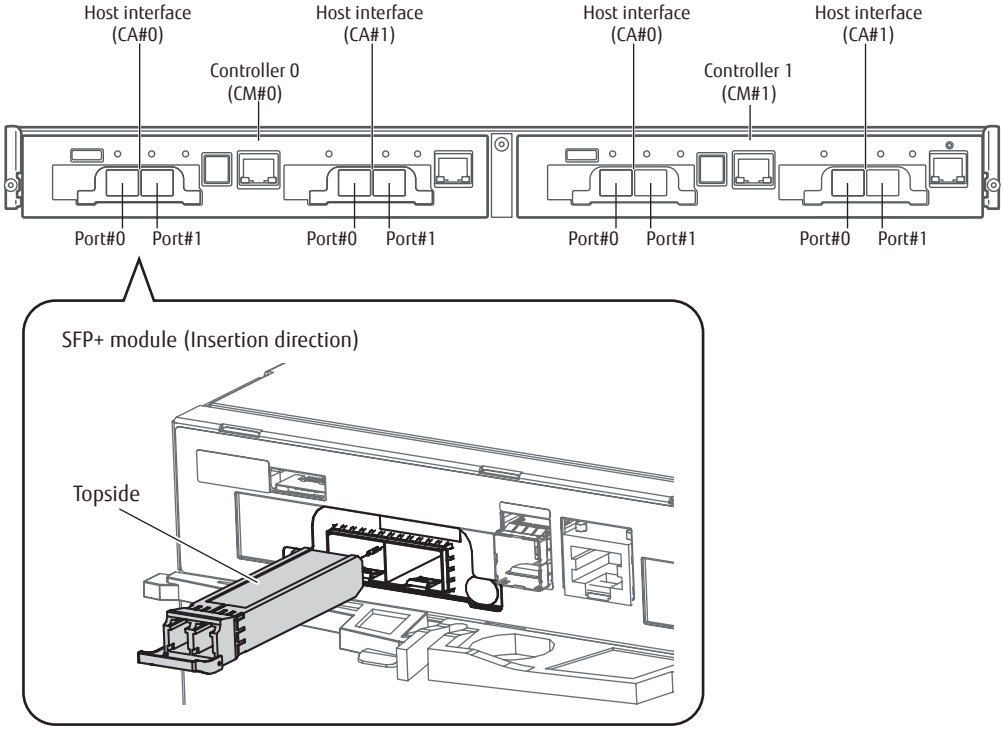


IMPORTANT

Keep the removed connector cover in a safe place where it will not be lost.

(2) Check the direction of the SFP+ module and insert it all the way into the port cage of the host interface.

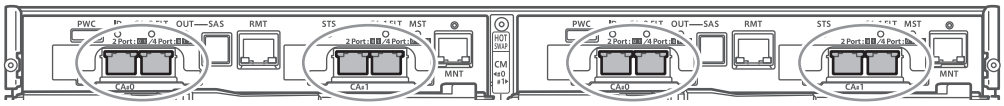
Install the SFP+ module in Port#0 first, and then Port#1.



(3) Close the SFP+ module's lever.

2 Connect a host interface cable to the ETERNUS DX.

Insert the host interface cable connectors in the host interface ports (iSCSI) of Controller 0 (CM#0) and Controller 1 (CM#1).



CAUTION

Do

- When connecting the host interface cables, position them so that they will not obstruct replacement of the power supply unit or controllers by the maintenance engineer.

3 Connect the host interface cable to the connection destination.

Connect the other end of the cable to the connection destination.

End of procedure

Drive Enclosure Connection

When a drive enclosure is installed, connect the drive enclosure to the controller enclosure with a mini SAS HD cable between enclosures. When multiple drive enclosures are installed, connect the drive enclosures with mini SAS HD cables between enclosures.

0.75m mini SAS HD cables between enclosures are provided with 2.5" type drive enclosures and 3.5" type drive enclosures. 2.5m cables between enclosures are provided with high-density drive enclosures.

The connection type between Controller 0 and the I/O modules for Controller 0 is different from that between Controller 1 and the I/O modules for Controller 1.

Between Controller 0 and I/O module line 0, connect the source DI (OUT) port and the destination DI (IN) port in ascending order of the drive enclosure numbers (DE-ID) of the drive enclosure.

Between Controller 1 and I/O module line 1, contrary to the line 0, connect the source DI (OUT) port and the destination DI (IN) port in descending order of the drive enclosure numbers (DE-ID) of the drive enclosure.

Do not connect anything to the last DI port that is nearest to the edge.

The last ports nearest to the edge are the DI (OUT) port of I/O module 0 in the drive enclosure of the largest DE-ID and the DI (OUT) port of I/O module 1 in the drive enclosure of the smallest DE-ID.

The connection configurations of cables between enclosures and the last DI port location when two drive enclosures are installed are shown below.

Figure 3 Connecting Cables between Enclosures (When Only One Controller Is Installed)

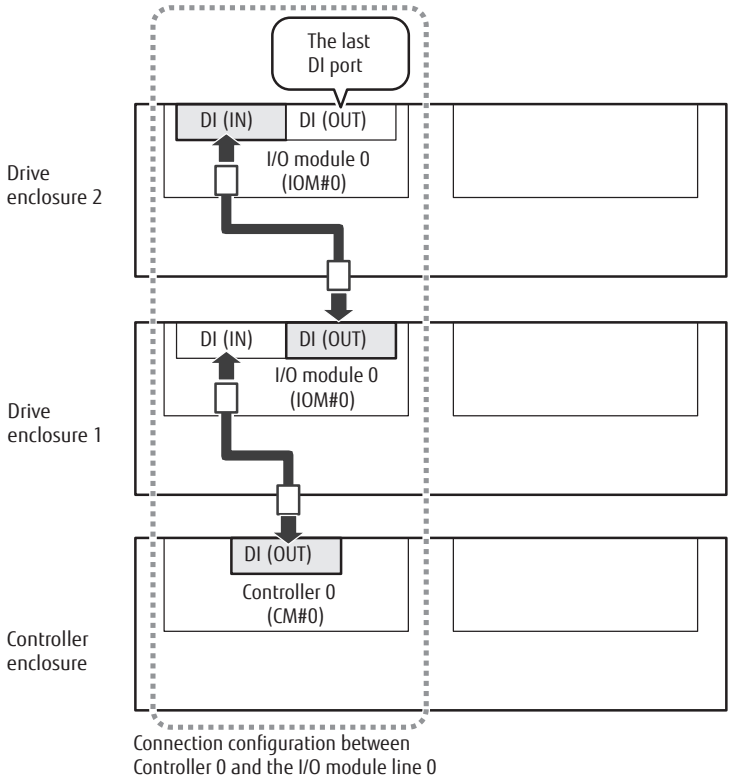
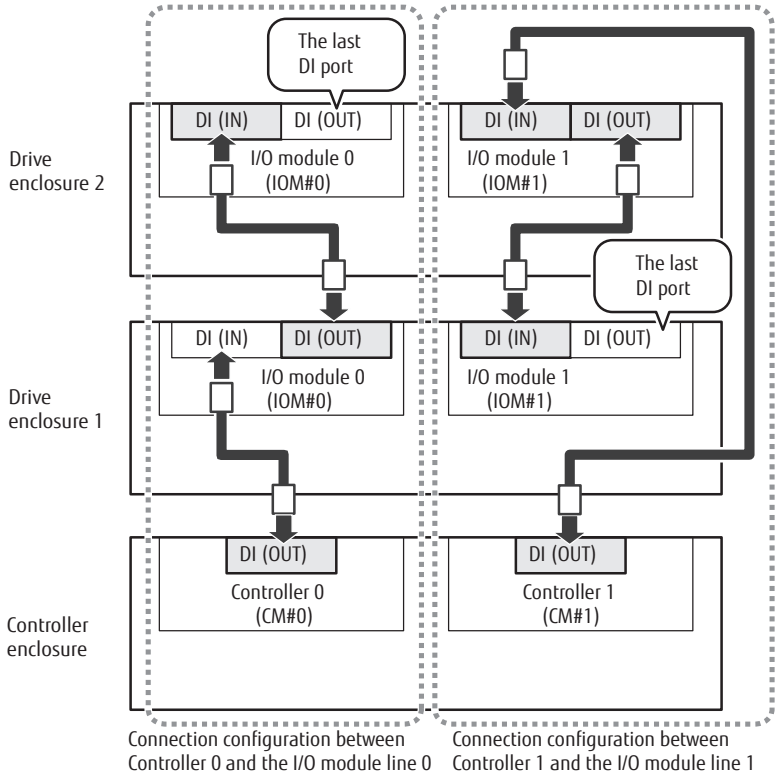


Figure 4 Connecting Cables between Enclosures (When Two Controllers Are Installed)

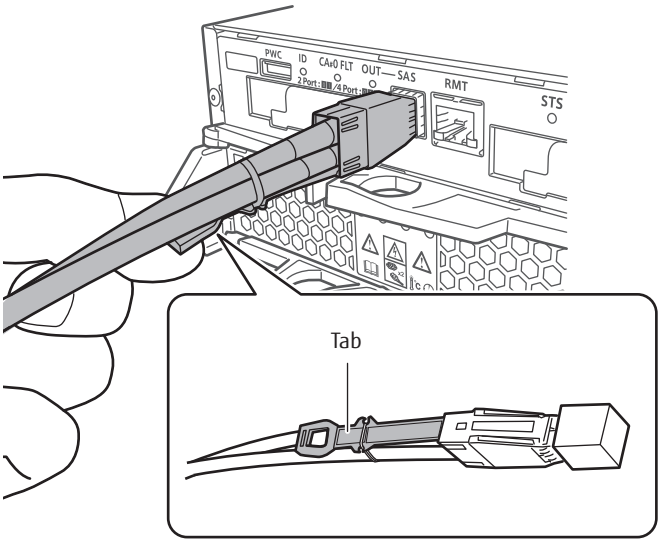


The following procedure explains how to connect the mini SAS HD cable between enclosures.

IMPORTANT

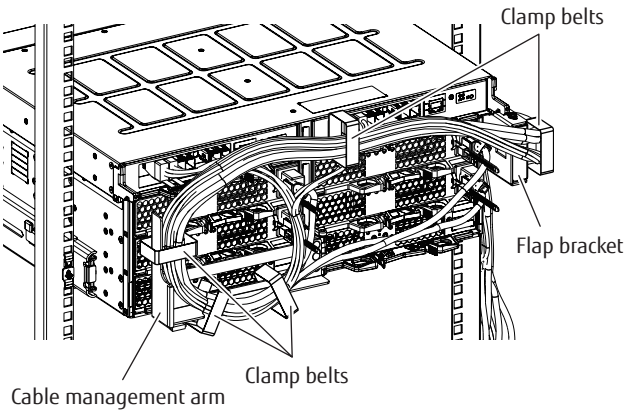
- To help with management of the mini SAS HD cable between enclosures and prevent incorrect connections, make sure to attach the destination labels to the connectors of the cables.
- When connecting the mini SAS HD cable between enclosures, check the direction of the connector (the tab must be pointed downward) and firmly insert all the way in.

  To disconnect the mini SAS HD cables between enclosures, hold the tab and then pull out the connector.



Note

When high-density drive enclosures are installed, fasten the high-density drive enclosure cable between enclosures with the clamp belts to the flap brackets and the cable management arm on the rear of the device.

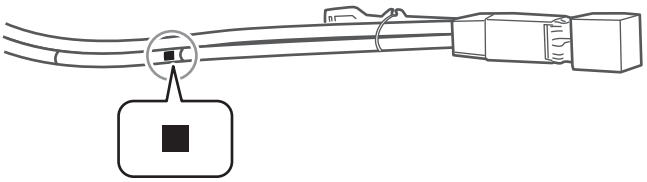


Procedure

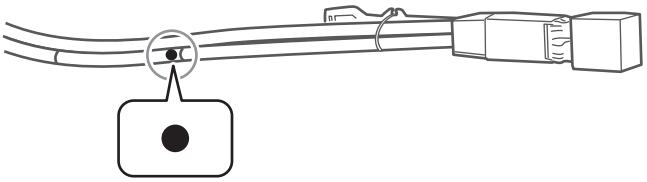
1 Attach the destination labels to the connectors of the mini SAS HD cables between enclosures.

(1) Before attaching the destination labels, check the connection destination of the mini SAS HD cables between enclosures.

- The connector on which the "■" symbol is printed is connected to the DI (OUT) port on the controller enclosure or the drive enclosure.

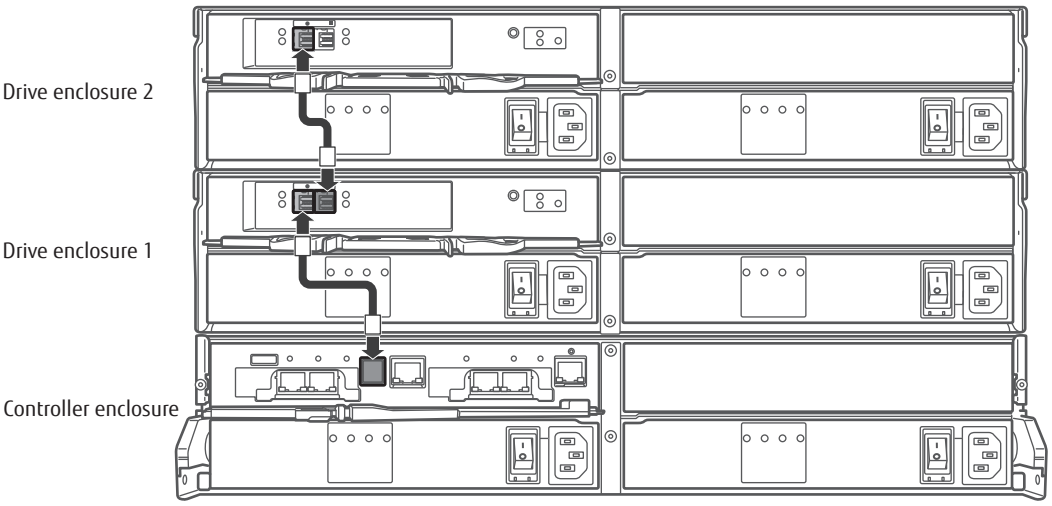


- The connectors on the cable with the "●" symbol are connected to the DI (IN) ports on the drive enclosure.

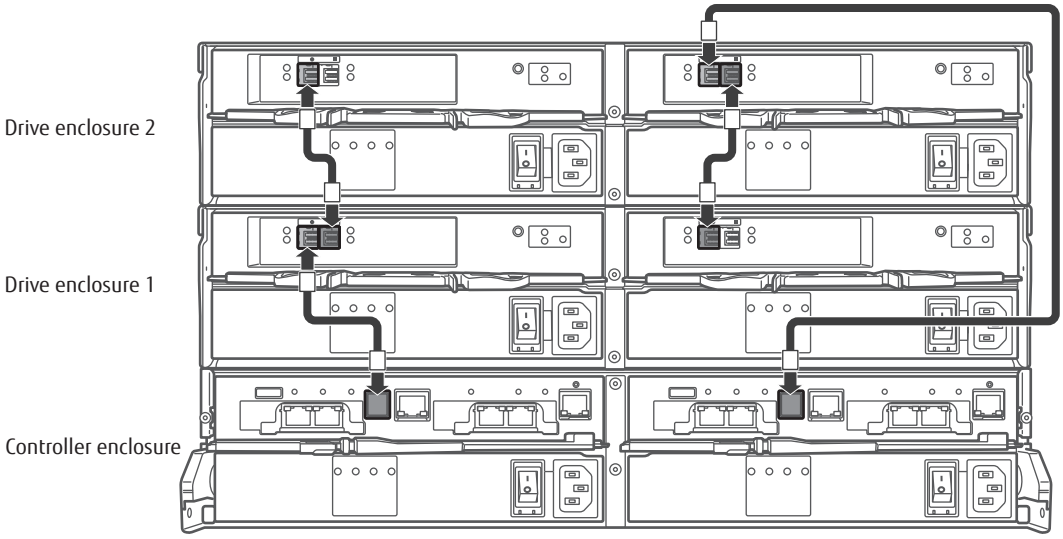


The following figures show the connection of the mini SAS HD cable between enclosures connecting the controller enclosure to drive enclosure 1 and connecting drive enclosure 1 to drive enclosure 2.

- When only one controller is installed



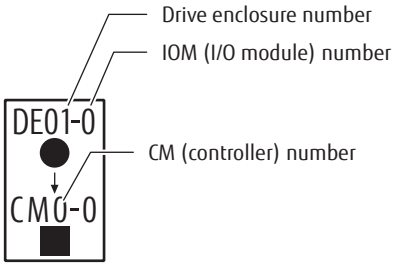
- When two controllers are installed



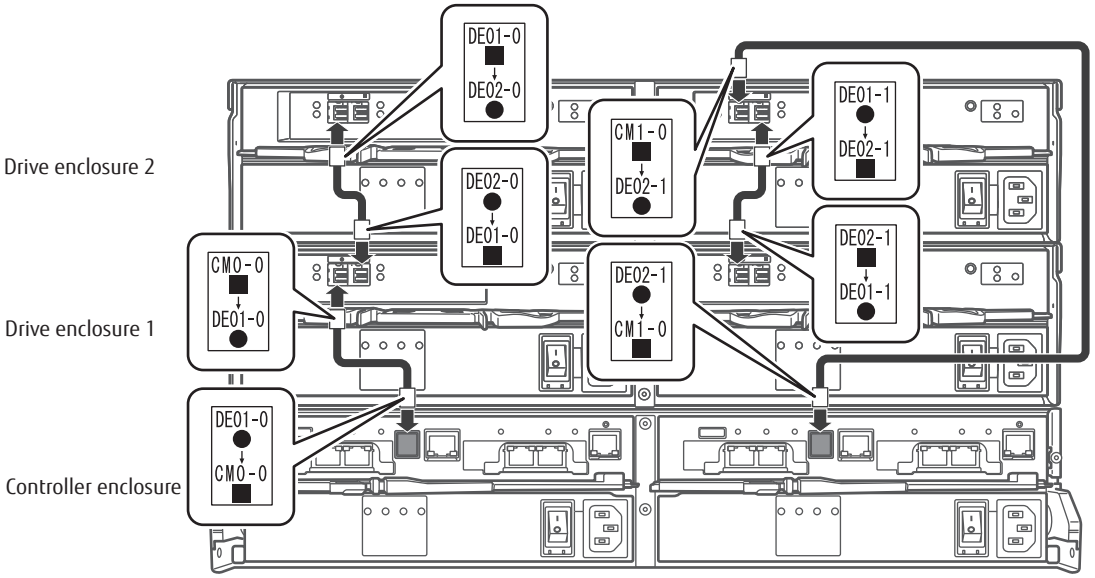
(2) Attach the destination labels to the connectors of the mini SAS HD cables between enclosures.

"Controller number" or "Drive enclosure number - IOM number" is printed on the destination labels in the "Connection origin DI port → Connection destination DI port" format. The "■" or "●" symbol is also printed on the destination labels.

Carefully check the connection origin and connection destination, and then attach the destination labels.



The following figure shows an example of the destination label attachments on the mini SAS HD cables between enclosures that connect the controller enclosure to drive enclosure 1 and that connect drive enclosure 1 to drive enclosure 2.



2 Connect the controller enclosure to the drive enclosure and connect between the drive enclosures.

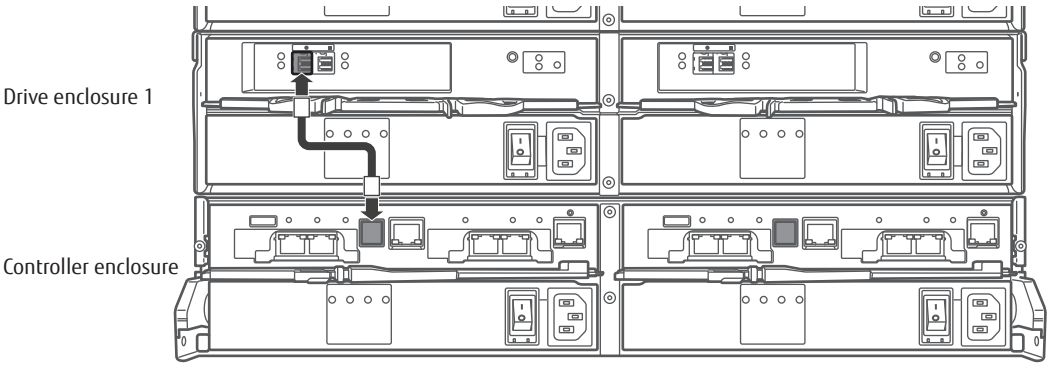
Connect Controller 0 first.

(1) Connect the controller enclosure to the drive enclosure.

Connect the DI (OUT) port of Controller 0 (CM#0) in the controller enclosure to the DI (IN) port of I/O module 0 (IOM#0) in drive enclosure 1 with the mini SAS HD cable between enclosures.

(i) Connect the plug to be connected to DI (OUT) port, to the DI (OUT) port of the Controller 0 (CM#0).

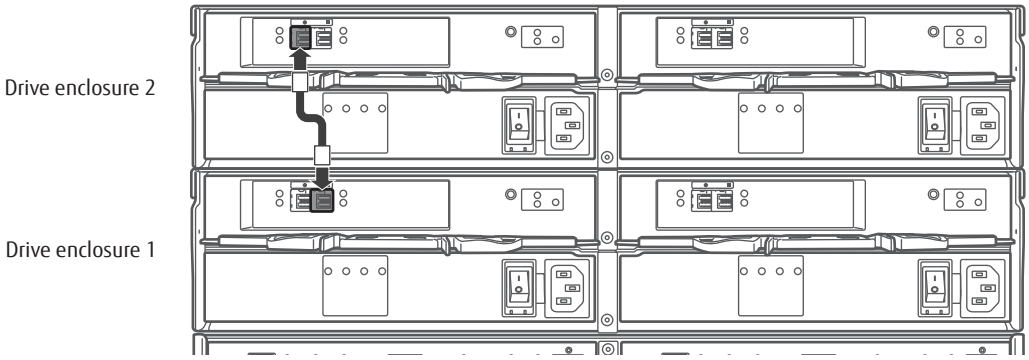
(ii) Connect the plug to be connected to DI (IN) port, to the DI (IN) port of the I/O module 0 (IOM#0).



(2) Connect between the drive enclosures.

Connect the DI (OUT) port of I/O module 0 (IOM#0) in drive enclosure 1 to the DI (IN) port of I/O module 0 (IOM#0) in drive enclosure 2 with the mini SAS HD cable between enclosures.

Connect the cable in the same way as Step (1).



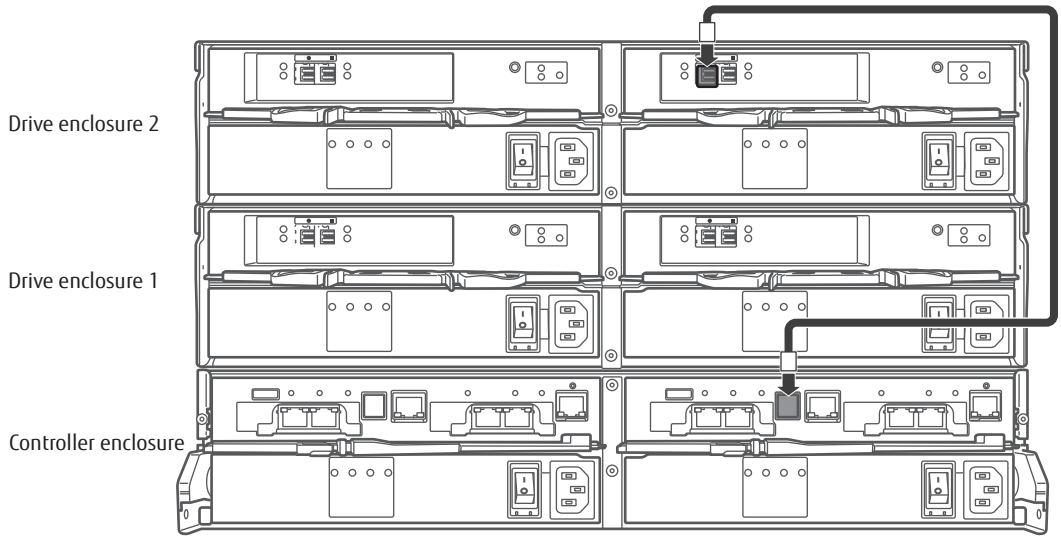
3 When two controllers are installed, connect Controller 1 next.

(1) Connect the controller enclosure to the drive enclosure.

Connect the DI (IN) port of I/O module 1 (IOM#1) in drive enclosure 2 to the DI (OUT) port of Controller 1 (CM#1) with the mini SAS HD cable between enclosures.

(i) Connect the plug to be connected to DI (OUT) port, to the DI (OUT) port of the Controller 1 (CM#1) in the controller enclosure.

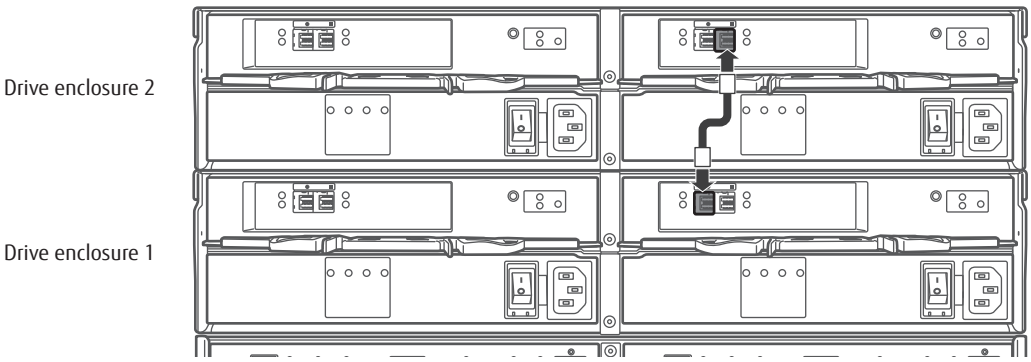
(ii) Connect the plug to be connected to the DI (IN) port, to the DI (IN) port of the I/O module 1 (IOM#1) in drive enclosure 2.



(2) Connect between the drive enclosures.

Connect the DI (OUT) port of I/O module 1 (IOM#1) in drive enclosure 2 to the DI (IN) port of I/O module 1 (IOM#1) in drive enclosure 1 with the mini SAS HD cable between enclosures.

Connect the mini SAS HD cable between enclosures in the same way as Step (1).



End of procedure

Power Synchronized Unit Connection

When using a power synchronized unit for power control, connect the power synchronized unit to the ETERNUS DX.

Refer to "Configuration Guide (Power Synchronized Unit)" for details about power synchronized units, the procedure for connecting power synchronized units to the ETERNUS DX, and required settings.

Power Cord Connection

Connect the power cords to the ETERNUS DX.

IMPORTANT

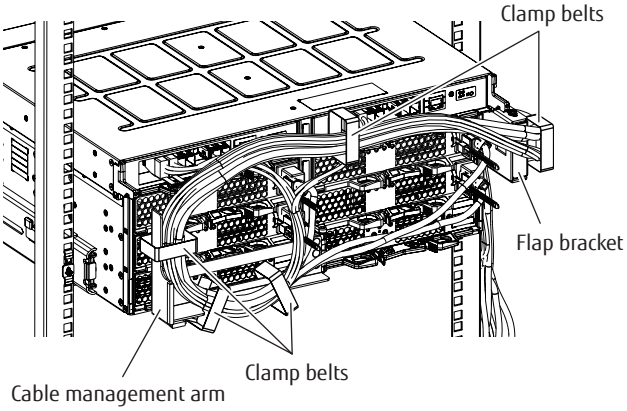
The controller enclosure and drive enclosure (2.5" type and 3.5" type) have two power supply units (PSU#0 and PSU#1).

The high-density drive enclosure has four power supply units (PSU#0, PSU#1, PSU#2, and PSU#3).

Make sure that the power cords are connected to all the power supply units.

Note

When high-density drive enclosures are installed, fasten the power cord of the high-density drive enclosure with the clamp belts to the flap brackets and the cable management arm on the rear of the device.



When No Power Distribution Units Are Installed

The following procedure explains how to connect the power cords when no power distribution units are installed.

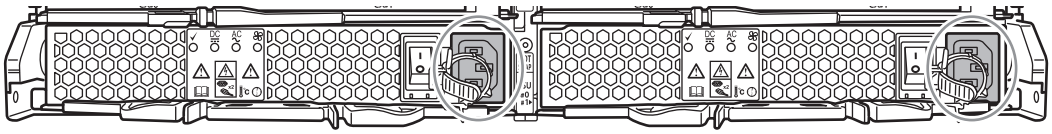
IMPORTANT

To help with power cord management and prevent incorrect connections, attach labels to the power cords and make a note of connection origins and destinations.

Procedure

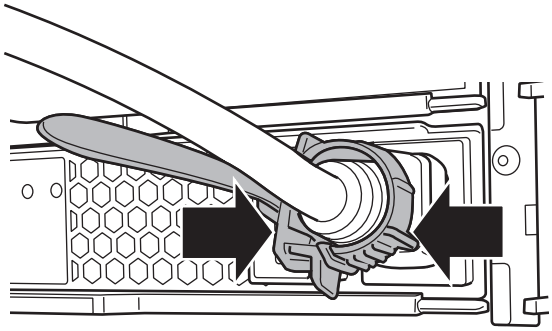
1 Connect the power cord to the ETERNUS DX.

(1) Connect the power cord plugs to the power inlets of the power supply units.



(2) Fasten the plug of the power cord with the release tie.

Wrap the release tie around the power cord and fasten the release tie from either side. Make sure that the release tie is not loose.



2 Connect the power cords to the socket.

Connect the plug at the other end of each power cord to the socket.

IMPORTANT

Connecting two or four power cords for each enclosure to different two power supply facilities improves the availability of the power supply facilities against failures.

CAUTION

Do Not

- Do not use the server service outlet to connect a power cord for the ETERNUS DX.

End of procedure

When 1U Power Distribution Unit Is Installed (for Regions other than the EMEIA, Central American, and Caribbean Regions)

The following procedure explains how to connect the power cord when a 1U power distribution unit is installed.

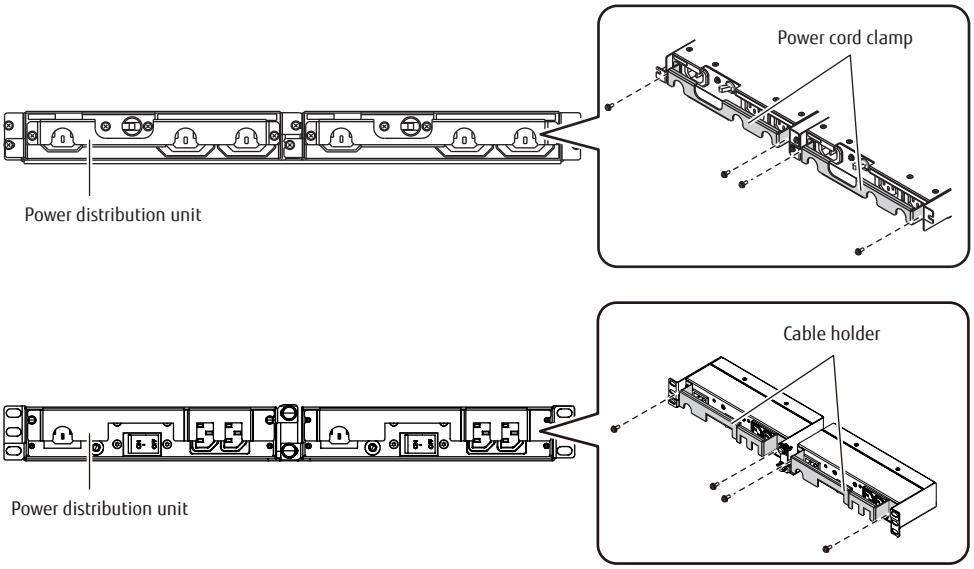
For power distribution units (1U), there are two different types of exteriors.

IMPORTANT

To help with power cord management and prevent incorrect connections, attach labels to the power cords and make a note of connection origins and destinations.

Procedure

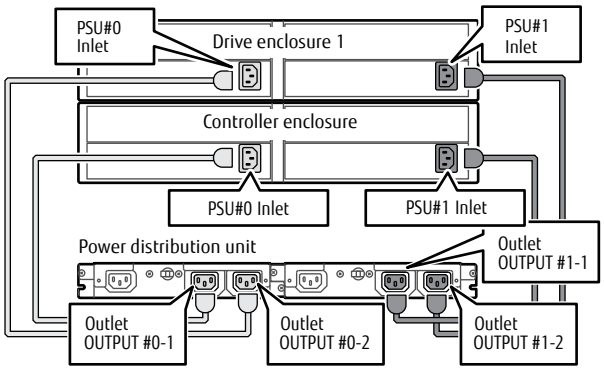
1 Remove the power cord clamps or the cable holders from the power distribution unit.



2 Connect the power distribution unit outlets and power supply unit inlets with the power cords (AC output cables).

The procedure to connect the power supply unit is same as Step 1 in "When No Power Distribution Units Are Installed" (page 61).

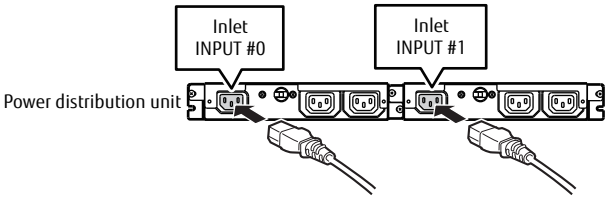
The following figure shows an example of AC output cable connection:



: Connect OUTPUT#0-n of the Power distribution unit to the PSU#0 inlet of the ETERNUS storage system.

: Connect OUTPUT#1-n of the Power distribution unit to the PSU#1 inlet of the ETERNUS storage system.

3 Connect the power cord (AC input cable) plugs to the inlets of the power distribution unit.



4 Use the power cord clamps to prevent the power plugs from coming unplugged.

Attach the power cord clamps removed in Step 1.

5 Connect the plugs on the other end of the power cords (AC input cables) that were connected in Step 3 to the sockets.

IMPORTANT

Power supply failure can be prevented by connecting the power cords (AC input cables) on the INPUT#0 side and the INPUT#1 side to different power sources.

End of procedure

When 2U Power Distribution Unit Is Installed (for Regions other than the EMEIA, Central American, and Caribbean Regions)

The following procedure explains how to connect the power cords when a 2U power distribution unit (12 outlet type or 16 outlet type) is installed.

For power distribution units (2U), there are two different types of exteriors.

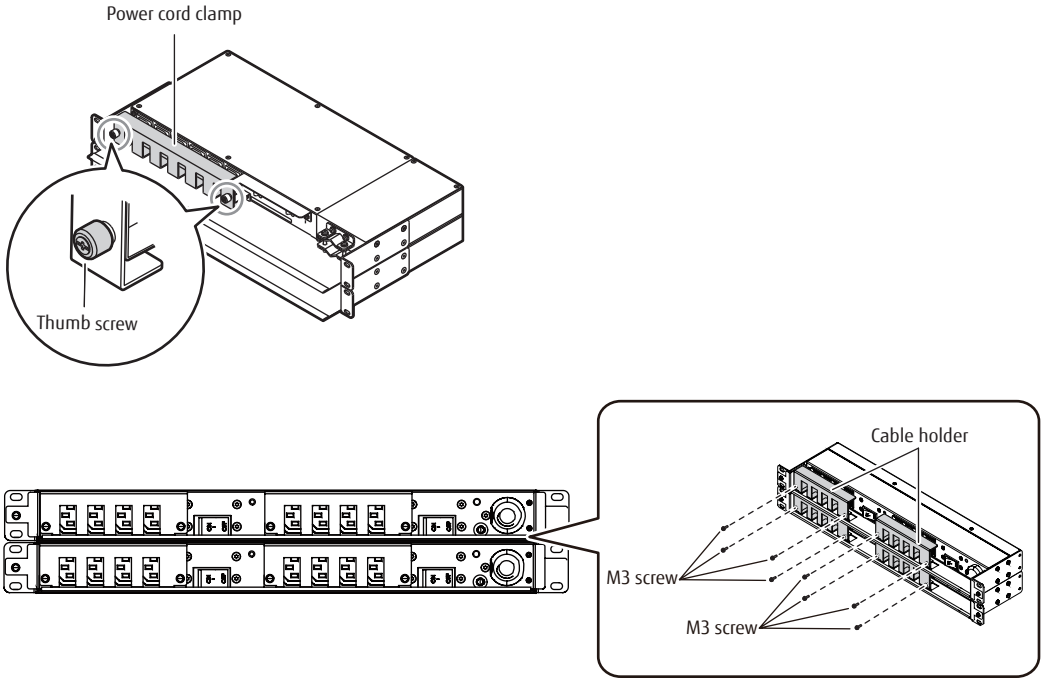
IMPORTANT

To help with power cord management and prevent incorrect connections, attach labels to the power cords and make a note of connection origins and destinations.

Procedure

1 Remove the power cord clamps or the cable holders from the power distribution unit.

Loosen the two thumb screws or the eight M3 screws on both sides of the power cord clamp or cable holder to remove it.



2 Connect the power distribution unit outlets and power supply unit inlets with the power cords (AC output cables).

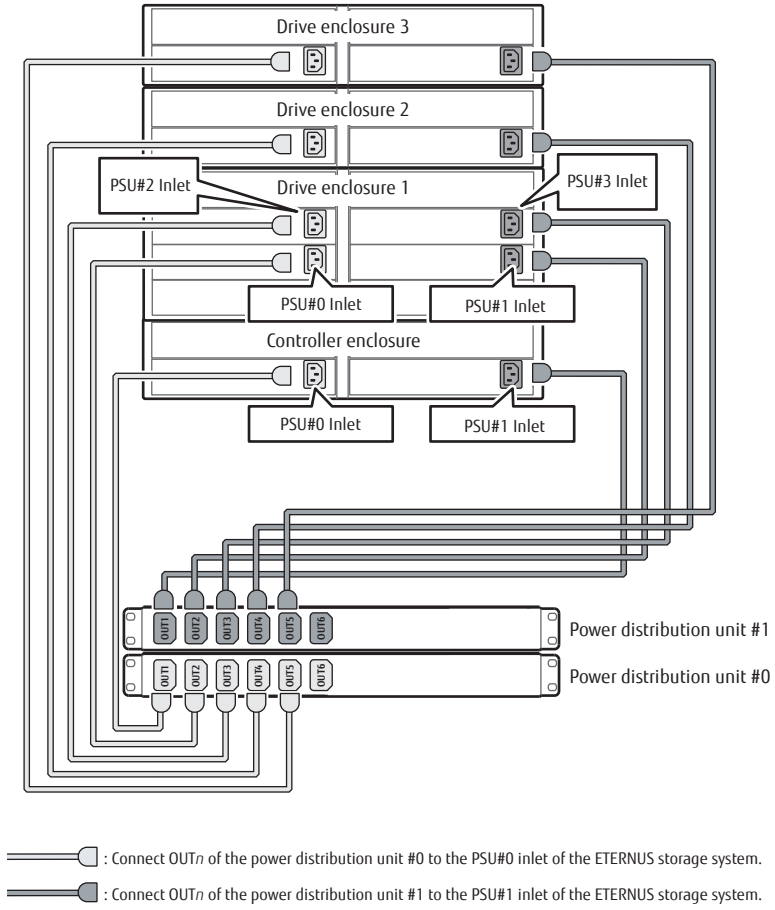
The procedure to connect the power supply unit is same as Step 1 in "When No Power Distribution Units Are Installed" (page 61).

IMPORTANT

- Connect the PSU#0 power cord to power distribution unit#0 (the lower power distribution unit). Connect the PSU#1 power cord to power distribution unit#1 (the higher power distribution unit).
- For the high-density drive enclosure, connect the PSU#0 and PSU#2 power cords to power distribution unit#0 (the lower power distribution unit). Connect the PSU#1 and PSU#3 power cords to power distribution unit#1 (the higher power distribution unit).

The following figures show a connection diagram of AC outlet cables.

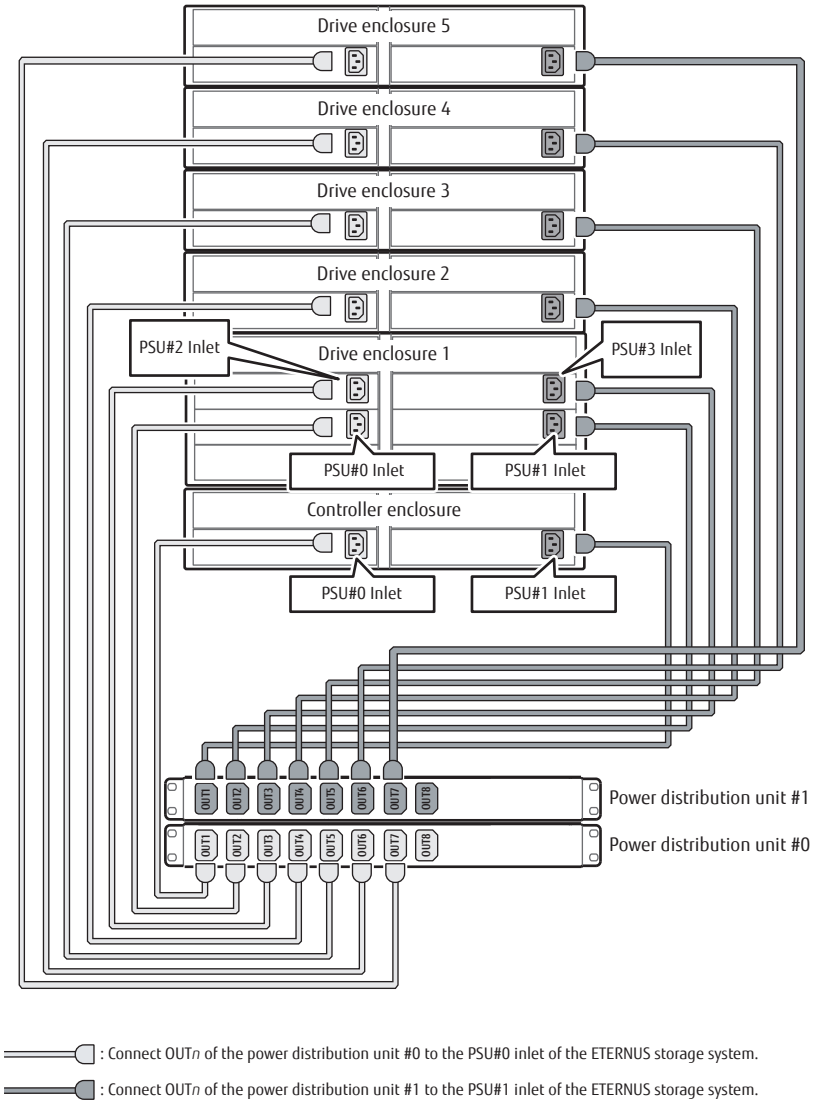
- For outlet × 12



: Connect OUT*n* of the power distribution unit #0 to the PSU#0 inlet of the ETERNUS storage system.

: Connect OUT*n* of the power distribution unit #1 to the PSU#1 inlet of the ETERNUS storage system.

- For outlet × 16

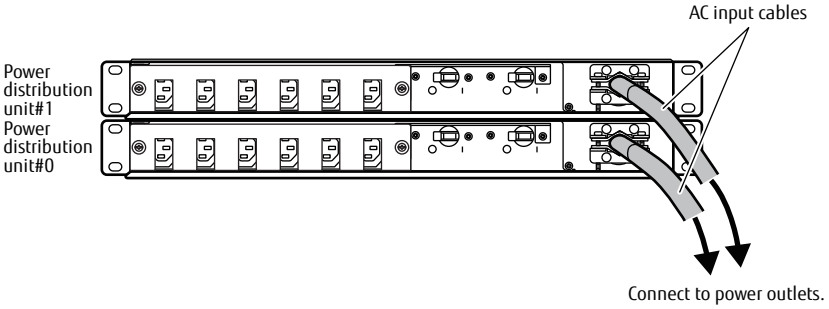


3 Use the power cord clamps to prevent the power plugs from coming unplugged.
Attach the power cord clamps removed in Step 1.

4 Connect the plugs on the other end of the power cords (AC input cables) that are attached to the power distribution unit to sockets.

IMPORTANT

Power supply failure can be prevented by connecting the power cords (AC input cables) on the power distribution unit #0 side and the power distribution unit #1 side to different power sources.



End of procedure

5. General Settings

This chapter explains how to set up the ETERNUS DX.

Initial Settings after Installation

The following settings must be performed when an ETERNUS DX is installed.

Storage Management

Perform the device information settings and the network connection settings All of the required settings can be performed by following the instructions that are displayed when the Initial Setup 1 wizard is used.

Firewall Settings

Select whether to enable or disable connections for each service that is to be used via the LAN for operation management.

RAID Configuration Settings

Register the RAID groups, the volumes, and the hot spares in the ETERNUS DX.

Monitoring Settings

Perform the settings to enable constant monitoring of the storage system status. For details on these settings, refer to "6. Monitoring Settings" (page 101).

Power Control Setup

Perform the storage system power control settings. For details on these settings, refer to "7. Power Control Setup" (page 122).

SAN Connection Settings

Perform the settings for SAN connections with the server. For details on these settings, refer to "8. SAN Connection Settings" (page 126).

Advanced Copy Settings

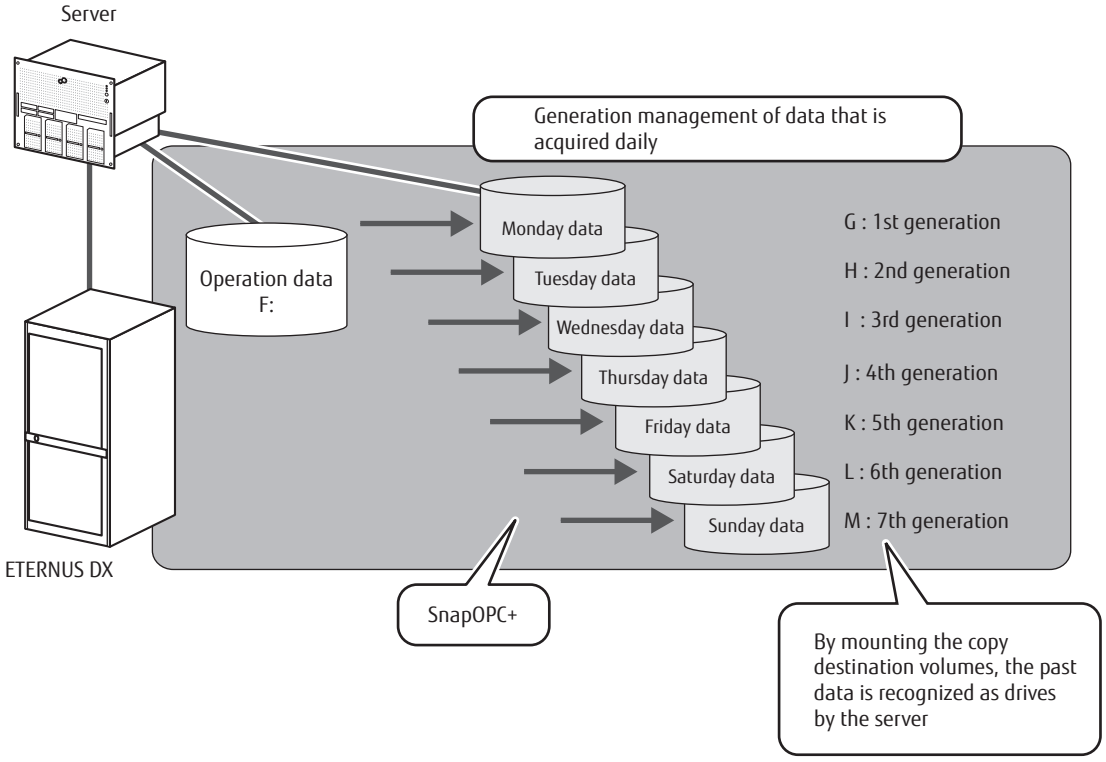
Perform the basic settings to use the Advanced Copy function. For details on these settings and performing SnapOPC+, refer to "9. Advanced Copy Settings" (page 163).

Example of Differential Backup Settings

This section describes the RAID configuration settings by using the settings for differential backing up with SnapOPC+ as an example.

In the ETERNUS DX, the differential copy function (SnapOPC+) can be used without needing any optional software. Mounting the copy destination volume on the server allows the past data to be seen as a drive, and the past data can be easily restored with copy & paste from the assigned drive.

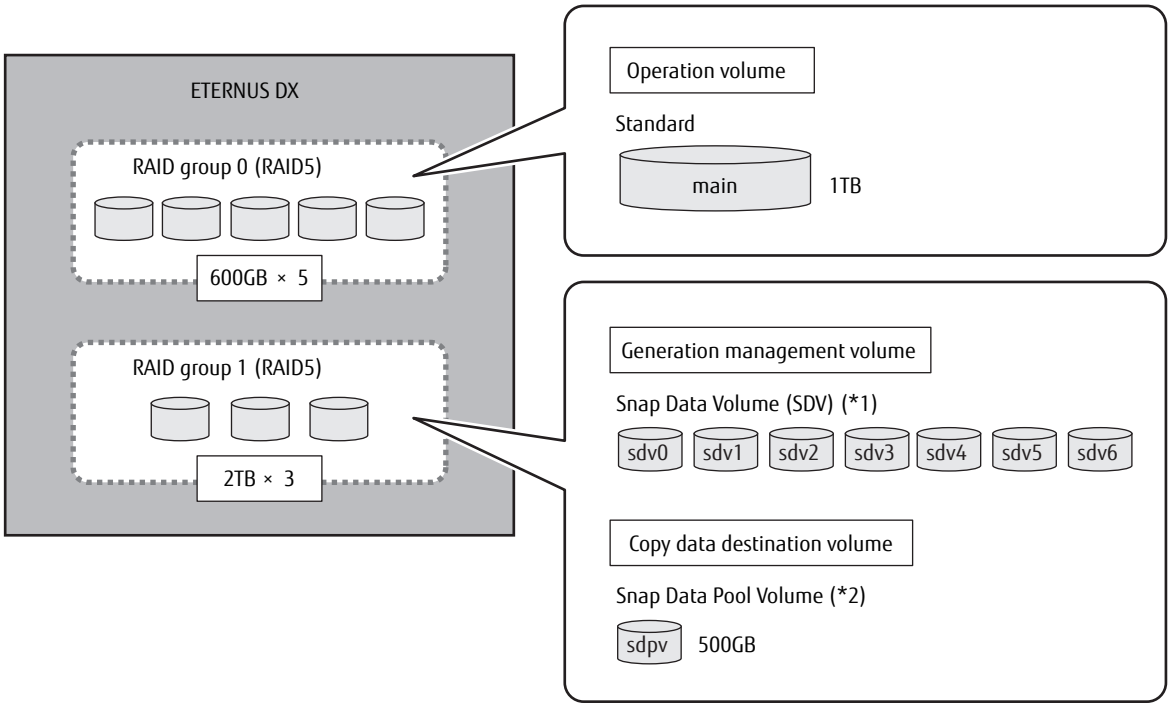
Figure 5 Example of Differential Backup Settings with SnapOPC+



● ETERNUS DX Environment

Create the operation volume and backup volume in the ETERNUS DX.

Figure 6 Example of Creating Operation Volume and Backup Volume



***1:** SDV is used as the copy destination for SnapOPC+ and stores generation data.

***2:** SDPV is the expansion area of the SDV and is used to configure the Snap Data Pool (SDP) area.

PC Terminal Connection

Connect a PC terminal to the ETERNUS DX.

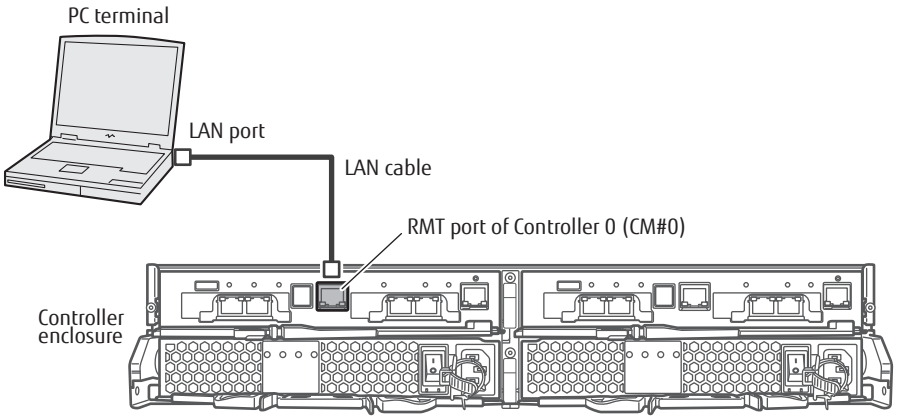
Connect the PC terminal to the RMT port of Controller 0 (CM#0) on the controller enclosure directly with the LAN cable (for operation management).

For the setup information of the PC terminal, refer to "Preparing the PC Terminal for Setup" (page 46).

Note

The ETERNUS DX and the PC terminal must be connected directly since the network environment of the ETERNUS DX is set using the PC terminal for the initial setup of the ETERNUS DX.

Figure 7 PC Terminal Connection for Initial Setup



Powering On

This section explains how to turn on the ETERNUS DX.

For power distribution units, there are two different types of exteriors.

Switching On and Off the Main Line Switch on the Power Distribution Unit

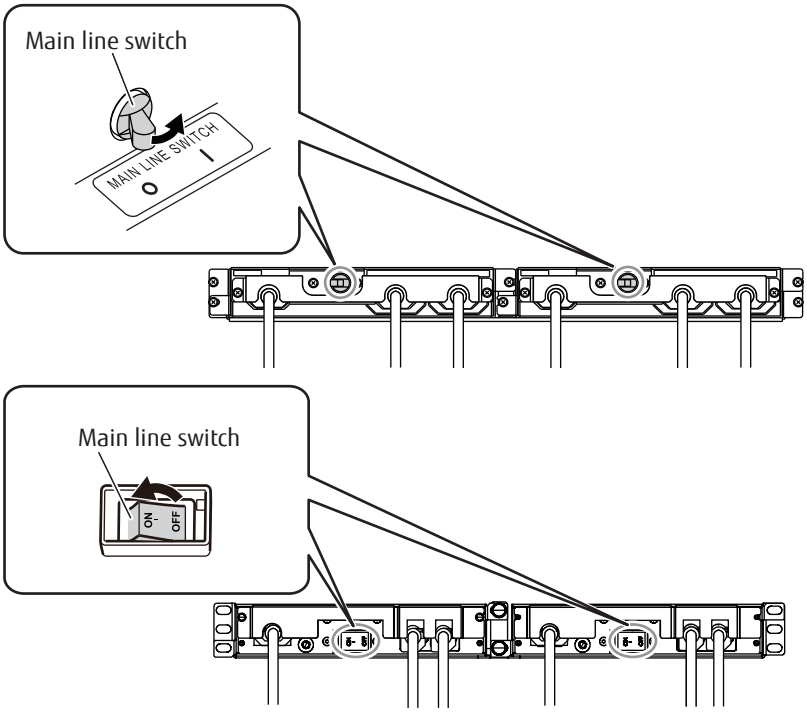
Turn the main line switch of the power distribution unit to the ON position (marked "|").

IMPORTANT

Make sure all of the main line switches are in the ON position.

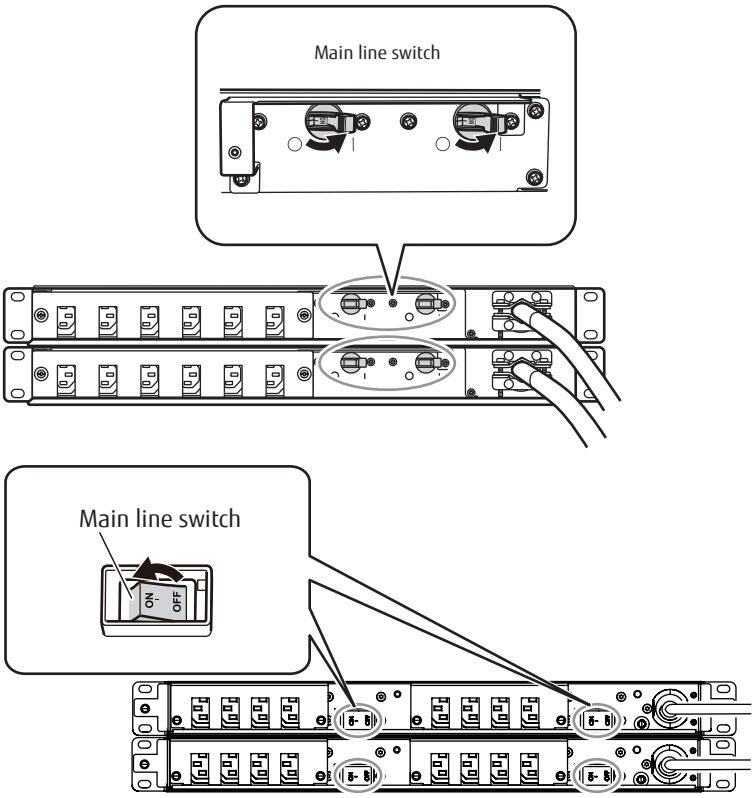
- For 1U

Figure 8 ON Position (Marked "|") of the Main Line Switches on a 1U Power Distribution Unit



- For 2U

Figure 9 ON Position (Marked "|") of the Main Line Switches on a 2U Power Distribution Unit



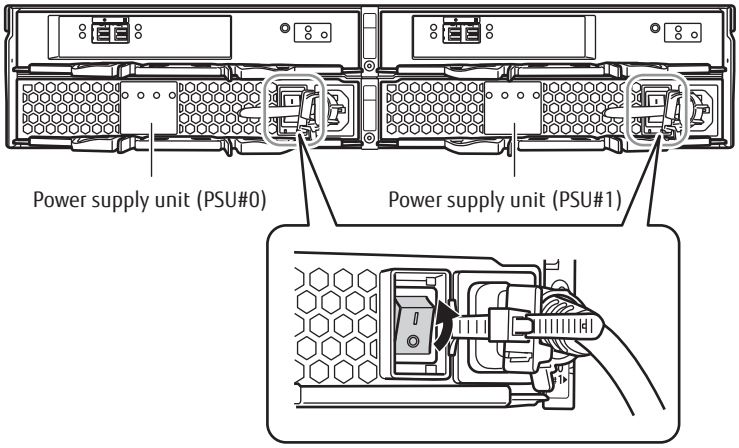
Switching On and Off the PSU Switch on the Power Supply Unit

Move the PSU switches of the power supply units in the controller enclosure and the 2.5"/3.5" type drive enclosures to the ON position (marked "|"). Note that power supply units for high-density drive enclosures do not have PSU switches.

IMPORTANT

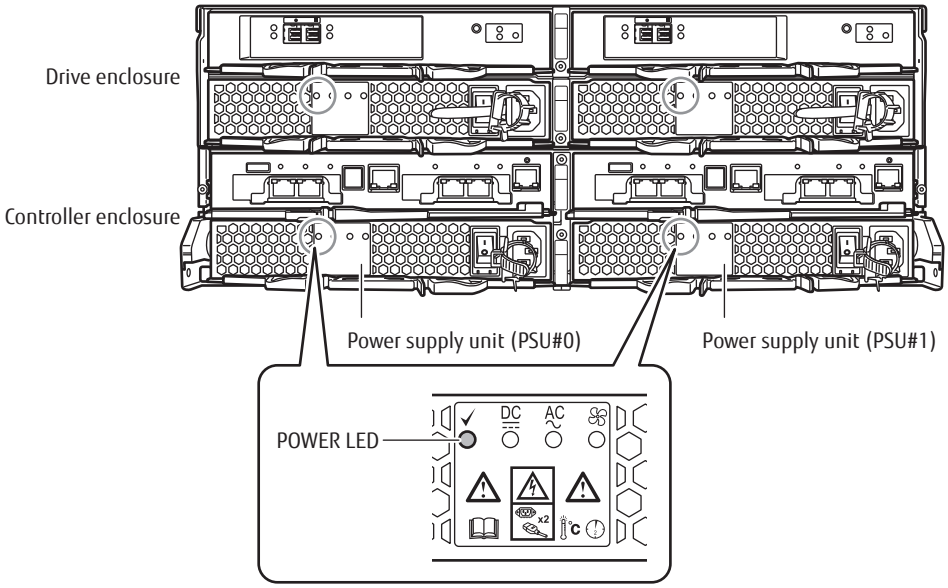
Make sure all of the PSU switches are in the ON position.

Figure 10 ON Position (Marked "|") of the PSU Switch on a Power Supply Unit



AC power is supplied to an enclosure.

- For the controller enclosure, the POWER LED on the power supply unit blinks green.
- For the drive enclosure, the POWER LED on the power supply unit emits green lights and the fan revolves at high speed for 30 seconds.



Powering On

Turn on the PC terminal and the ETERNUS DX.

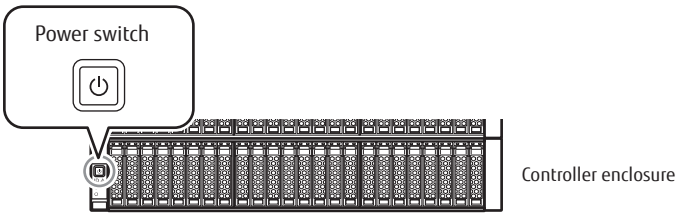
Follow the procedure below to turn on the ETERNUS DX.

IMPORTANT

- After turning on the power of the ETERNUS DX, it takes approximately five minutes (or approximately 10 minutes for a Unified configuration and approximately 20 minutes for a VLAN/Bonding maximum configuration) to reach the READY state (the READY LED [ ] turns on). If an error is detected in a component during the initial power-on diagnostics, it may take a longer time (of up to 10 minutes for a SAN configuration in which the Deduplication/Compression function is disabled, up to 11 minutes for a SAN configuration in which the Deduplication/Compression function is enabled, approximately 40 minutes for a Unified configuration, and approximately 50 minutes for a VLAN/Bonding maximum configuration) for the ETERNUS DX to reach the READY state. If a scheduled operation is being performed, make configurations by taking the operation into consideration.
- After power-off, wait for about one minute before turning power on again.
- If the ETERNUS DX is not turned off normally due to problems such as a power failure, it takes approximately five minutes (max.) longer to reach the READY state the next time the ETERNUS DX is turned on.

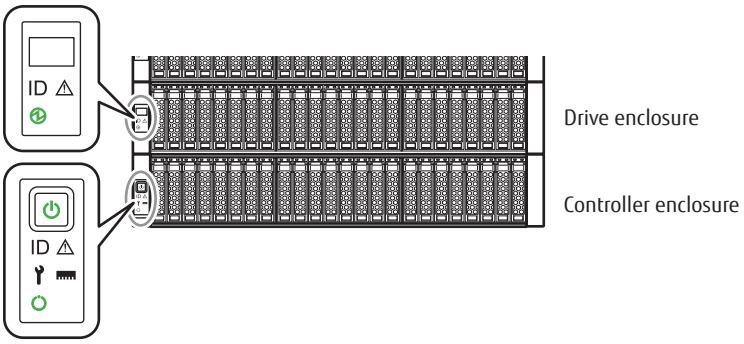
Procedure

1 Press the Power switch of the controller enclosure.



The POWER LED ( ) of the controller enclosure and the POWER LEDs ( ) of the drive enclosures are turned on.

2 After approximately five minutes (or approximately 10 minutes for a Unified configuration and approximately 20 minutes for a VLAN/Bonding maximum configuration), check that the READY LED ( ) of the controller enclosure is lit up.



When checking the connection between the PC terminal and the ETERNUS DX, execute the "ping" command at the PC command prompt. An example of ping execution is shown below. ("192.168.1.1" is the default IP address for the ETERNUS DX)

```
ping 192.168.1.1
```

If the execution results in an error, check the network settings of the PC terminal.

IMPORTANT

When communication cannot be established even after the RMT port of Controller 0 (CM#0) is connected to the LAN port of the PC terminal, make sure that the MASTER LED of Controller 0 (CM#0) is turned on. When two controllers are installed and the MASTER LED of Controller 1 (CM#1) is turned on, use the RMT port of Controller 1 (CM#1).

End of procedure

ETERNUS Web GUI Startup

Start up ETERNUS Web GUI via the Web browser of the connected terminal.

If the settings of the Web browser are incorrect, ETERNUS Web GUI may not be connected. For details on these settings, refer to "Configuration Guide (Web GUI)".

Procedure

1 Open the Web browser on the terminal.

2 Enter the following URL in the address bar of the Web browser:

```
https://192.168.1.1/
```

The login screen for ETERNUS Web GUI appears.

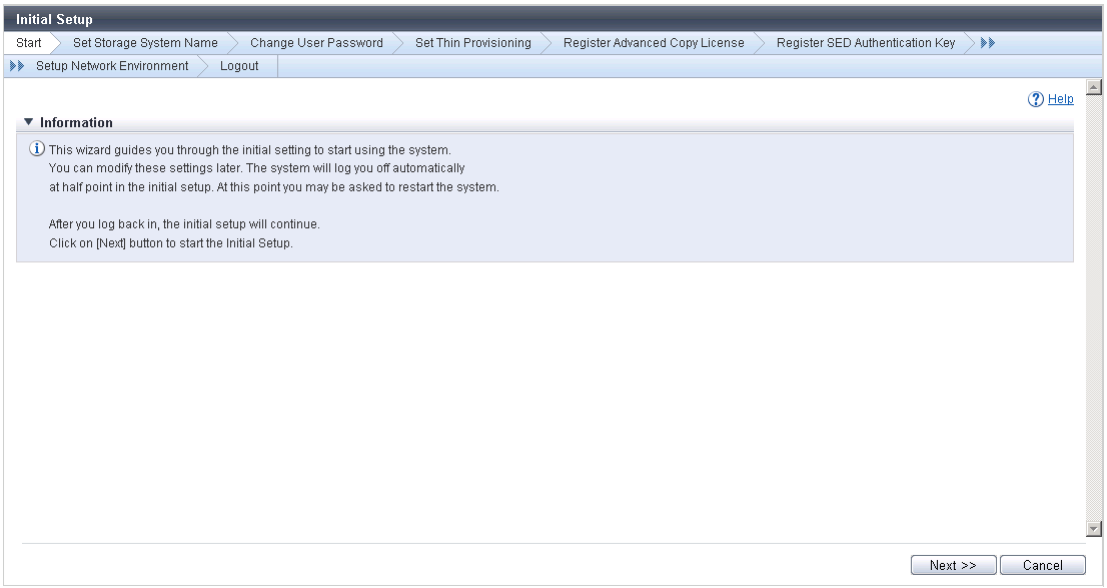
3 To change the language, click the [Option] button and select [English] or [Japanese] in [Language:].

4 Enter the User ID and Password.

User ID: root

Password: root (by default)

After logging in, the Initial Setup screen of ETERNUS Web GUI appears.



End of procedure

Storage Management (Initial Setup 1)

The settings that are required before operating the ETERNUS DX can be easily performed by using Initial Setup 1, Initial Setup 2, and the Smart Setup Wizard.

This section explains Initial Setup 1. For details on these settings, refer to "Configuration Guide (Web GUI)".

For details on the Initial Setup 2, refer to "Configuration Guide (Web GUI)".

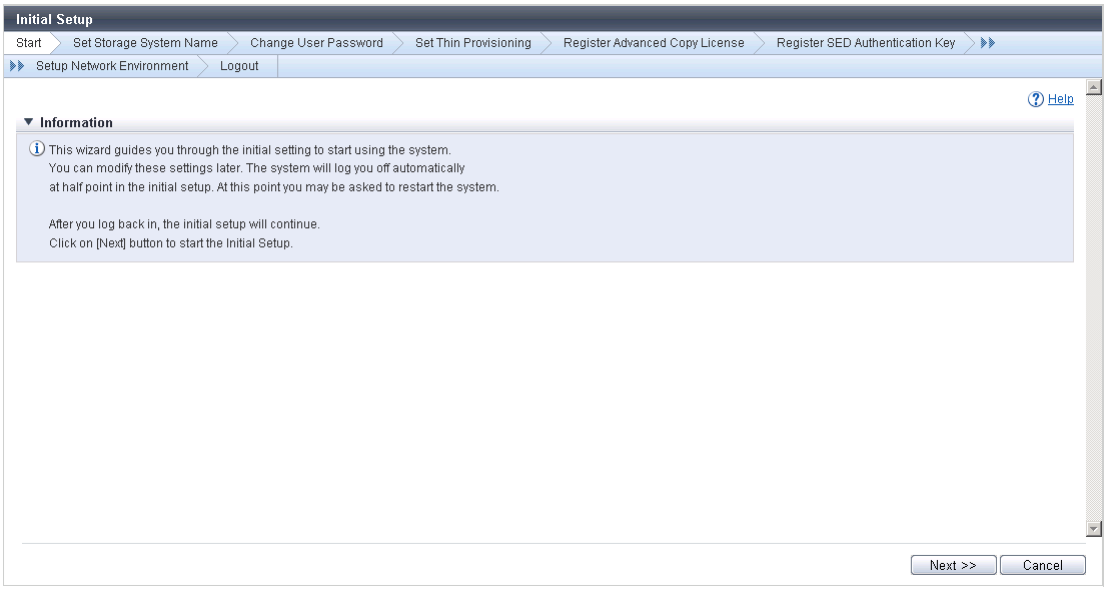
For details on the Smart Setup Wizard, refer to "Smart Setup Wizard" (page 134).

- Set Storage System Name
- Change User Password
- Set Thin Provisioning
- Register SED Authentication Key
- Setup Network Environment

The procedure for the initial setup is shown below. For details on the settings, refer to "Configuration Guide (Web GUI)".

Procedure

1 Click the [Next >>] button in the [Initial Setup] screen.



The [Set Storage System Name] screen appears.

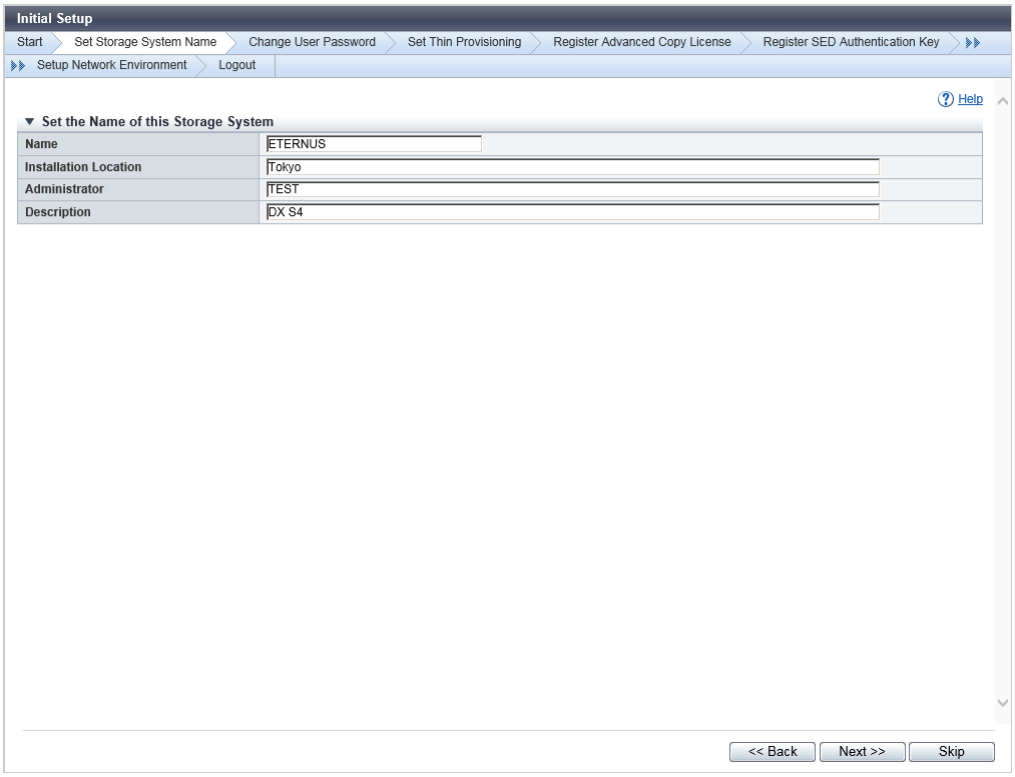
2 ETERNUS DX name setup

Set the name of the ETERNUS DX as well as other information.

Note

The information that is set here is used for network management by SNMP. The name of the ETERNUS DX is displayed in the login and operation screens of ETERNUS Web GUI.

(1) Set the required items and click the [Next >>] button.



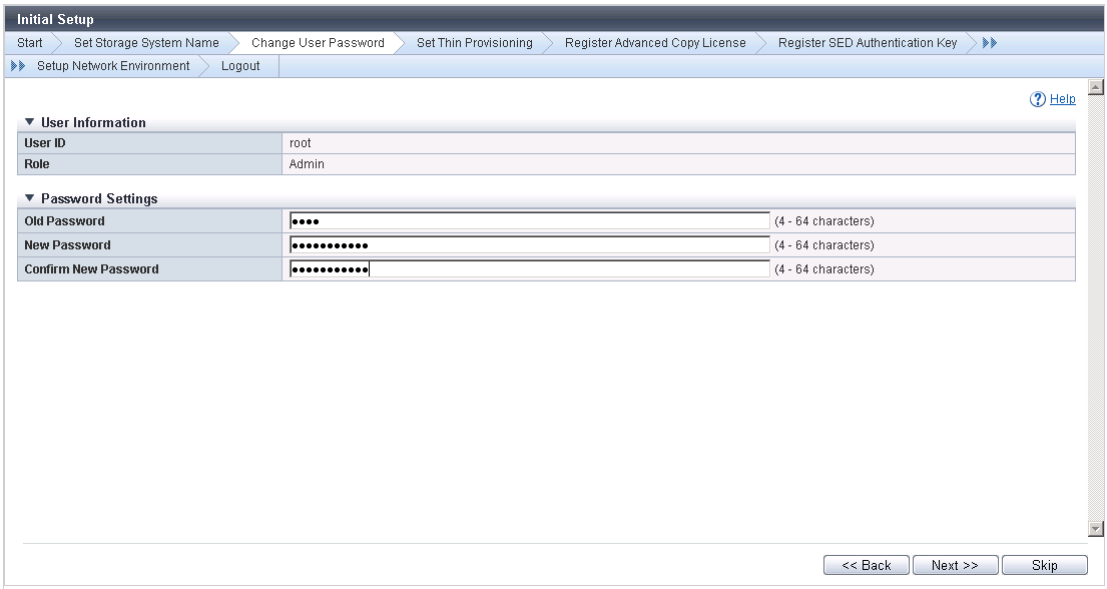
A confirmation screen appears.

(2) Click the [OK] button.
The name of the ETERNUS DX is set and the setting completion screen appears.

(3) Click the [Done] button.
The [Change User Password] screen appears.

3 Changing user passwords
Change the user password.

(1) Set the required items and click the [Next >>] button.



A confirmation screen appears.

(2) Click the [OK] button.

The password is changed and the change completion screen appears.

(3) Click the [Done] button.

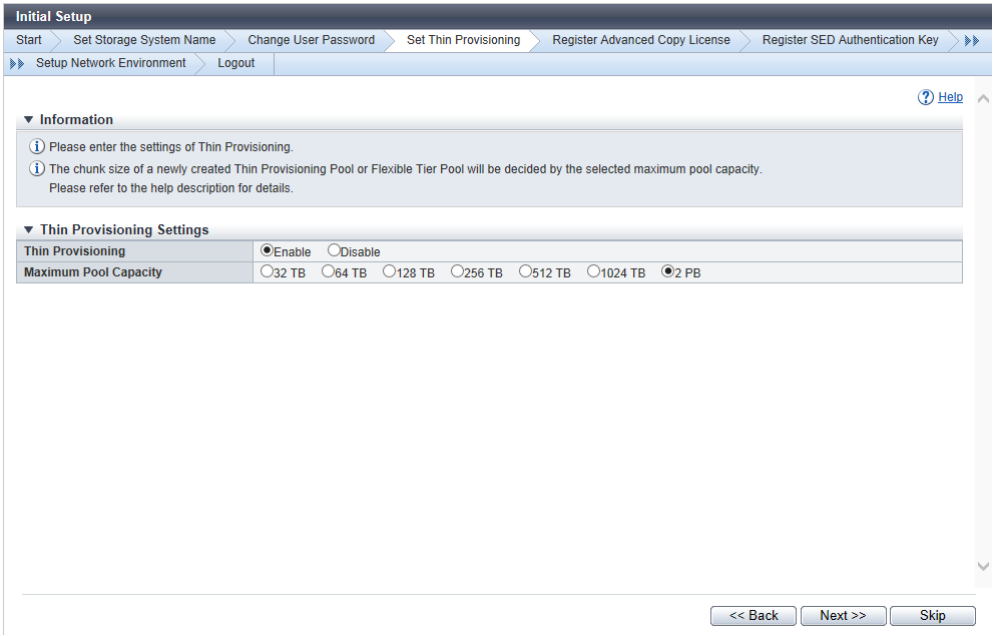
The [Set Thin Provisioning] screen appears.

4 Thin Provisioning setup

Enable or disable the Thin Provisioning function and set the maximum pool capacity.

If Thin Provisioning is enabled, creation of Thin Provisioning Pools and configuration of host affinity can be simplified by using the Smart Setup Wizard.

(1) Set the required items and click the [Next >>] button.



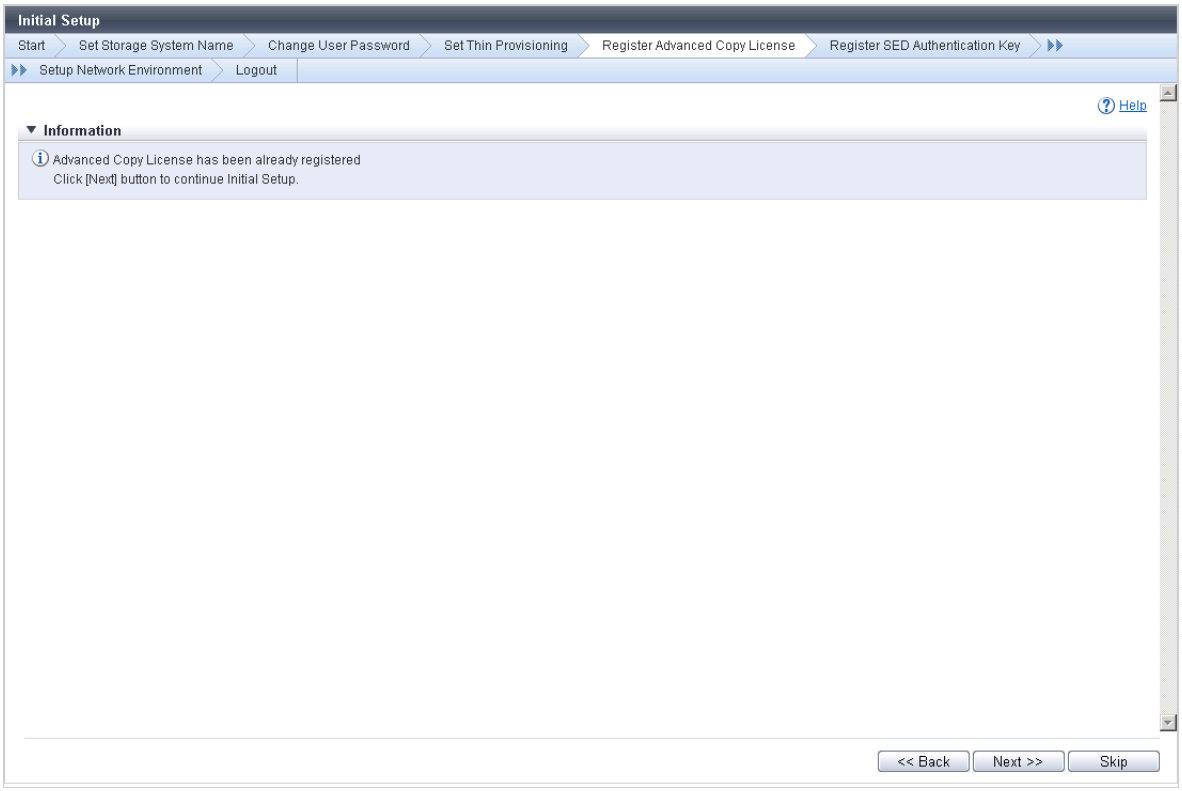
A confirmation screen appears.

(2) Click the [OK] button.
The Thin Provisioning is set and the change completion screen appears.

(3) Click the [Done] button.
The [Register Advanced Copy License] screen appears.

5 Advanced Copy license registration

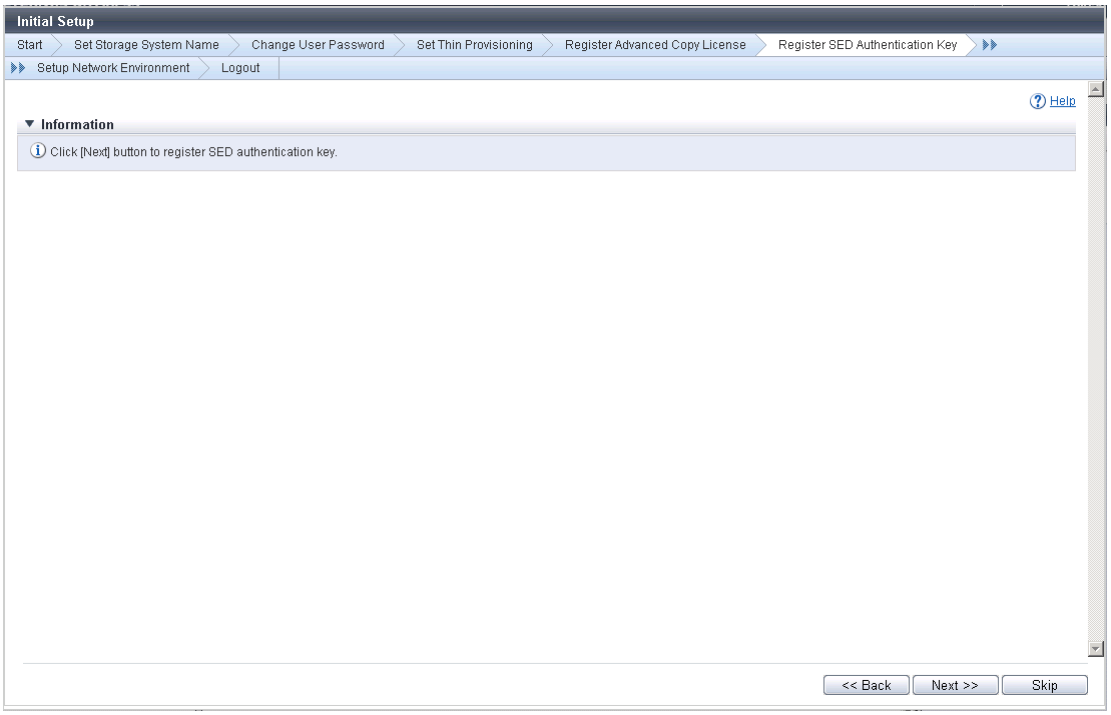
Click the [Skip] button to proceed to the [Register SED Authentication Key] screen.



6 SED authentication key registration

When Self Encrypting Drives (SEDs) are installed in the ETERNUS DX, register the SED authentication key.

(1) A message to confirm whether to register the SED authentication key is displayed. Click the [Next >>] button.



A confirmation screen appears.

(2) Click the [OK] button.

The SED authentication key is registered and the registration completion screen appears.

(3) Click the [Done] button.

The [Setup Network Environment] screen appears.

Note

- The SED authentication key can be registered even if no SEDs are or will be installed.
- When SEDs are already installed in the ETERNUS DX, a message that requests rebooting appears. Reboot the ETERNUS DX according to the displayed message.

7 Network environment setup

Set the ETERNUS DX environment for network communication.

Caution

If the network environment is set with the factory default, some functions are not available.

Make sure to set up the network environment for the MNT port.

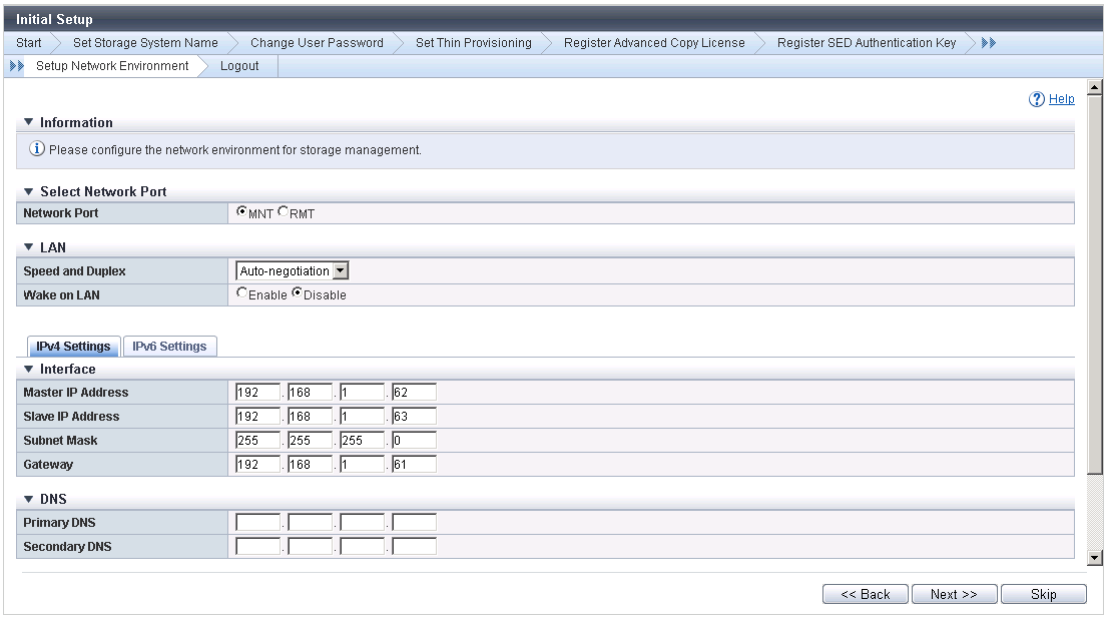
IMPORTANT

- Do not use the RMT port for an operation management LAN. Use the RMT port only for remote support.
- Configure the IP address for the MNT port with an IP address in a different subnetwork than the RMT port.
- When specifying the IP address of the Slave CM, specify an IP address that is in the same subnet but is different from the IP address of the Master CM.
- Either or both an IPv4 address and an IPv6 address can be specified for the MNT port and the RMT port.
- To connect to the devices in a network in which the ETERNUS DX does not belong, set "Gateway", and specify the IP address (or network address) or the connect IP address in "Allowed IP Address".

  If the ETERNUS DX is accessed from a system with the same network address (or same subnetwork), the IP address does not need to be set.

(1) Click the [IPv4 Settings] tab to specify an IPv4 address. Click the [IPv6 Settings] tab to specify an IPv6 address.

The following procedure shows an example when selecting the [IPv4 Settings] tab.



A confirmation screen appears.

(2) Click the [OK] button.

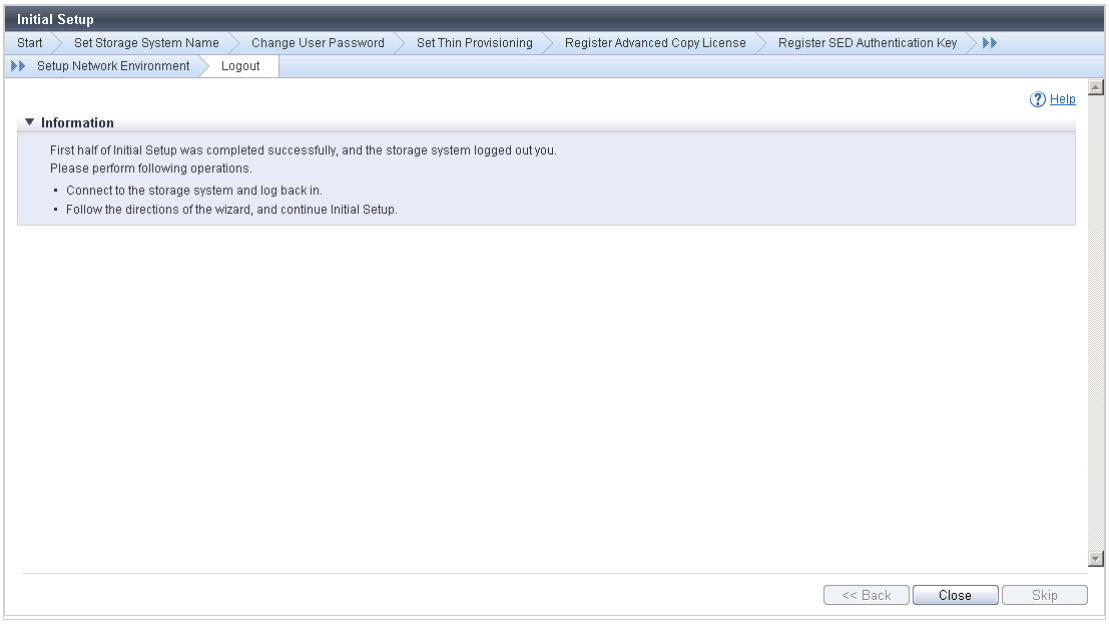
The network environment setting is applied and the setting completion screen appears.

(3) Click the [Finish] button.

The [Logout] screen appears.

8 Logout

(1) Click the [Close] button.



Initial setup 1 is complete and the screen returns to the [Login] screen.

(2) Close the Web browser.

9 Remove the LAN cable that connects the RMT port to the PC terminal.

End of procedure

LAN Cable Connection (for Operation Management)

The ETERNUS DX must be connected to a LAN to perform actions via ETERNUS Web GUI or ETERNUS CLI such as settings, maintenance operations, monitoring the device status, and using remote support.

Prepare the required number of LAN cables for the network environment of the customer.

The following procedure explains how to connect the LAN cable.

Caution

When the LAN switch that is to be used has the Spanning Tree Protocol (STP) function enabled, connection to the ETERNUS DX may fail. Use the following settings to disable the STP function:

- When the STP function is not necessary for the network configuration:

  Disable the STP function of the LAN switch.

- When the STP function is necessary for the network configuration:

  Disable the STP function of the LAN switch port only for the ETERNUS DX connection or perform the Port-Fast setting.

IMPORTANT

- To help with LAN cable management and prevent incorrect connections, attach labels to the LAN cables and make a note of connection origins and destinations.
- When connecting LAN cables, check the connector orientation and then firmly push it all the way in.

  When disconnecting LAN cables, depress the tab, then pull out the connector.

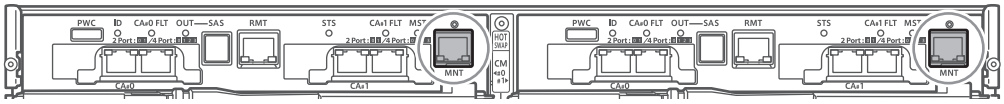
Note

This section uses a controller enclosure with two controllers as an example to explain the connection procedure. When one controller is installed, this procedure is only applied to Controller 0 (CM#0).

Procedure

1 Connect the LAN cable to the ETERNUS DX.

Connect the LAN cable connectors to the MNT ports of the Controller 0 (CM#0) and Controller 1 (CM#1) for the ETERNUS DX.

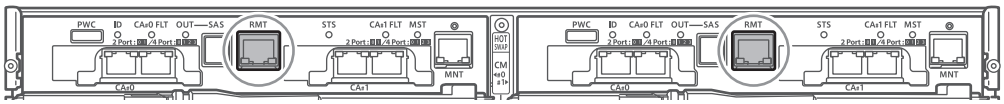


CAUTION

Do

- When connecting the LAN cables, position them so that they will not obstruct replacement of the power supply unit or controllers by the maintenance engineer.

2 When the RMT port is used, connect the connector of the LAN cable to the RMT port of Controller 0 (CM#0) and Controller 1 (CM#1).



3 Connect the LAN cables of the MNT port to the network of the customer. If the RMT port is used for remote support, connect the LAN cable of the RMT port to the network for remote support.

End of procedure

Firewall Settings

Set the firewall for each service. The settings are required respectively for the MNT port and the RMT port.

Caution

- If both HTTP connection and HTTPS connection are disabled, the device is inaccessible via ETERNUS Web GUI.
- If both Telnet connection and SSH connection are disabled, the device is inaccessible via ETERNUS CLI.
- If the network environment for the MNT port is not set up, some functions will be unusable. Make sure to set up the network environment.

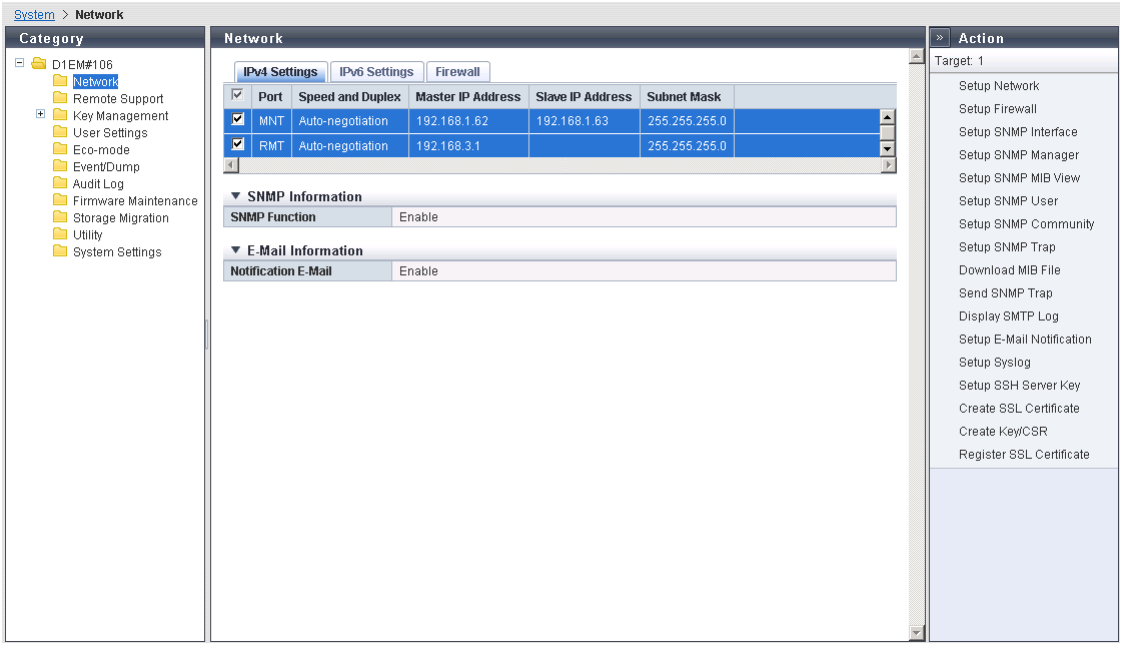
Procedure

1 Start the Web browser and log in to ETERNUS Web GUI with the IP address that is set in Step 7 in "Storage Management (Initial Setup 1)" (page 77).

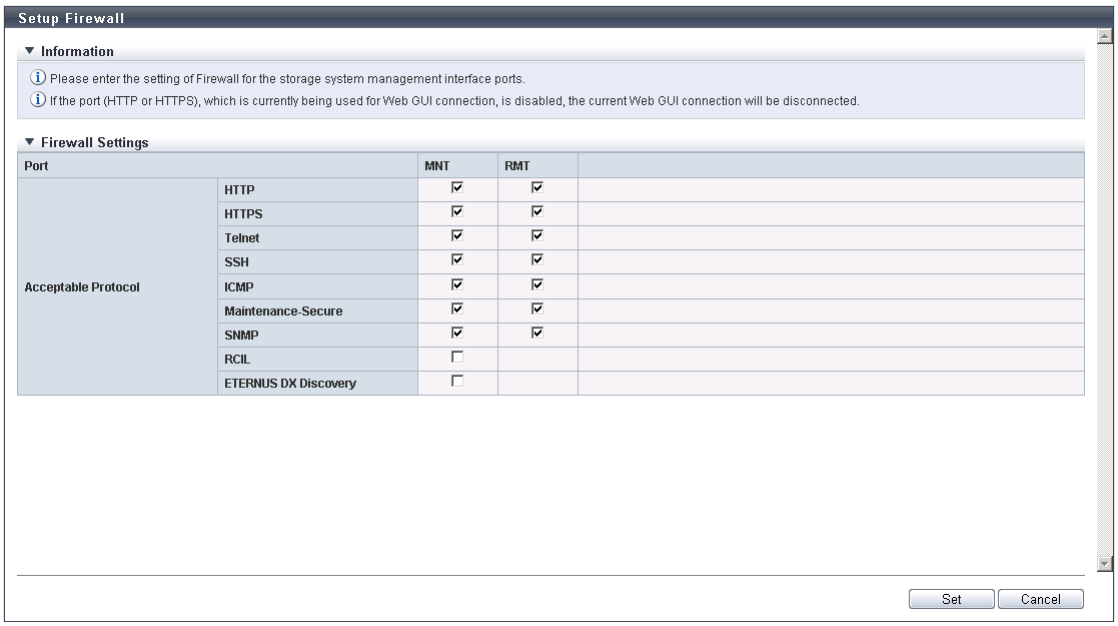
2 Click the [System] tab on the navigation of the ETERNUS Web GUI screen.

3 In [Category], click [Network].
The [Network] screen appears.

4 Select the port to be set. In [Action], click [Setup Firewall].



5 In the [Setup Firewall] screen, specify whether to enable/disable each service.
To enable a service, select the checkbox for that service.



- HTTP/HTTPS
  This service is enabled when an ETERNUS DX is connected via ETERNUS Web GUI.
  Data is encrypted and transferred for HTTPS.
- Telnet/SSH
  This service is enabled when an ETERNUS DX is connected via ETERNUS CLI.
  Data is encrypted and transferred for Secure SHell (SSH).
- ICMP
  This service is enabled when an ICMP connection is allowed.
- Maintenance-Secure
  This service is enabled for connections from things such as monitoring software or for using the remote support function to download firmware between storage systems.
  SSH encrypts and sends/receives data.
- SNMP
  This service is enabled when an ETERNUS DX is connected via the SNMP manager.
- ETERNUS DX Discovery
  Change the setting to "Disable".

6 Click the [Set] button.

7 In the confirmation screen, click the [OK] button.
The firewall settings are applied.

8 Check the setting completion message and click the [Done] button.
The screen returns to the [Network] screen.

End of procedure

Configuration Settings for RAID Groups or Thin Provisioning

This section describes the RAID groups that are used for operation volumes (Standard) and generation management volumes (SDV). For details on the settings of the Thin Provisioning Pools (TPPs) that are used for Thin Provisioning Volumes (TPVs), refer to "Configuration Guide (Web GUI)".

Creation of Thin Provisioning Pools and configuration of host affinity can be simplified using the Smart Setup Wizard. For details on the settings, refer to "Smart Setup Wizard" (page 134).

Usage for RAID Groups and Thin Provisioning

This section describes usage for RAID groups and Thin Provisioning.

RAID groups are areas for storing normal data that are used when the volume capacity requirements can be estimated in advance. Business volumes and Advanced Copy volumes (Standard type volumes, WSVs, Snap Data Volumes (SDVs), and Snap Data Pool Volumes (SDPVs)) can be created in RAID groups.

Thin Provisioning manages drives in a pool and assigns them to virtual logical volumes when data is written from the host. Thin Provisioning enables operations to be started with less drive capacity even if the capacity requirements cannot be estimated. Thin Provisioning Volumes (TPVs, NAS user volumes, and Deduplication/Compression Volumes) are created in Thin Provisioning Pools (TPPs).

RAID Configuration Settings

Use ETERNUS Web GUI to set RAID configurations in the ETERNUS DX.

Perform the following settings:

- RAID group creation
- Volume creation
- Hot spare registration

This section describes the configuration settings when the following volumes are created as an example.

- Operation volume

  Create an operation volume (Standard) in RAID5(4+1) RAID group.

- Backup volume

  Create a generation management volume (SDV) and copy data destination volume (SDPV) in RAID5(2+1) RAID group.

RAID Group Creation

Create RAID groups (groups of drives that configure RAID in the ETERNUS DX) to create volumes.

Create an operation RAID group and a backup RAID group.

Figure 11 RAID Group Creation

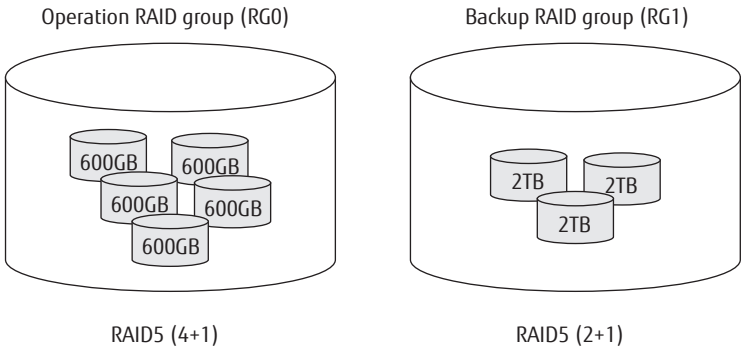


Table 3 RAID Group Creation

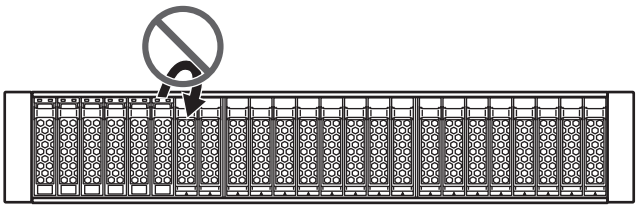
Usage	Item	Create mode	RAID level	Configuration drive
Operation RAID group (copy source)	RG0	Manual	RAID5	600GB SAS disk × 5
Backup RAID group (copy destination)	RG1	Manual	RAID5	2TB Nearline SAS disk × 3

CAUTION

Do Not

- Do not uninstall the drives that are installed by default or move them to any other slot.

  Contact your sales representative or maintenance engineer if drives that are installed by default need to be uninstalled or moved to another slot.



The procedure to register a RAID group is as follows:

Procedure

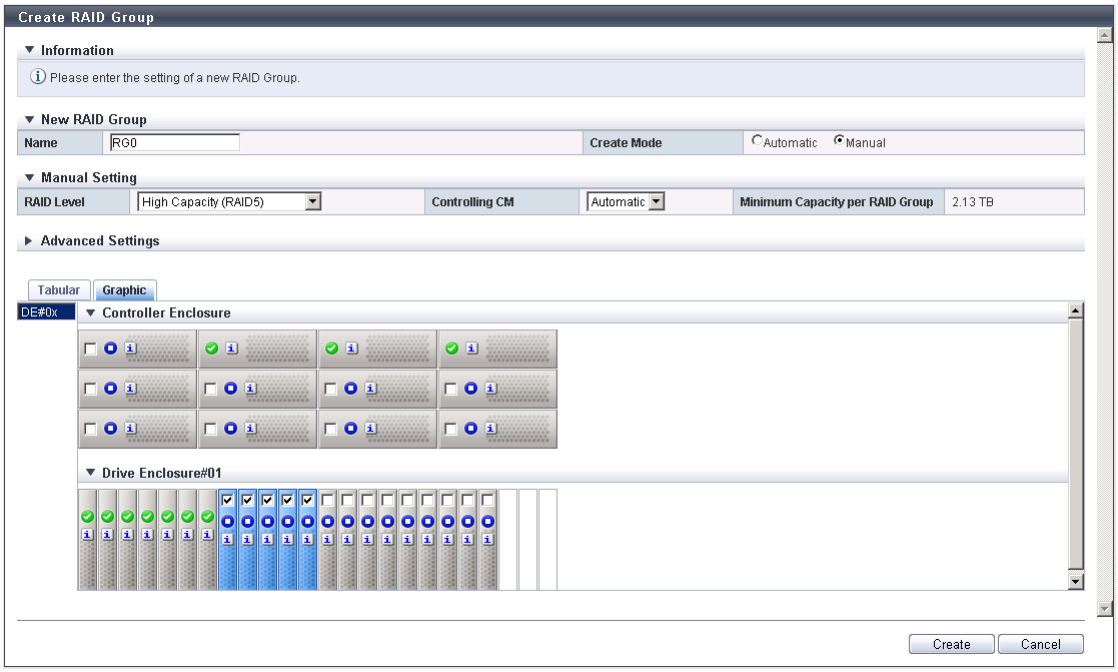
1 On the navigation of the ETERNUS Web GUI screen, click the [RAID Group] tab.
The [RAID Group] screen appears.

2 In [Action], click [Create].
The [Create RAID Group] screen appears.

3 Enter the name of the RAID group that is to be registered. Select "Manual" for "Create Mode".

4 Set the required items and click the [Create] button.

The following screen shows the settings that are displayed when creating a RAID group with the RAID group name "RG0" and the RAID level "RAID5(4+1)".



A confirmation screen appears.

5 Click the [OK] button.

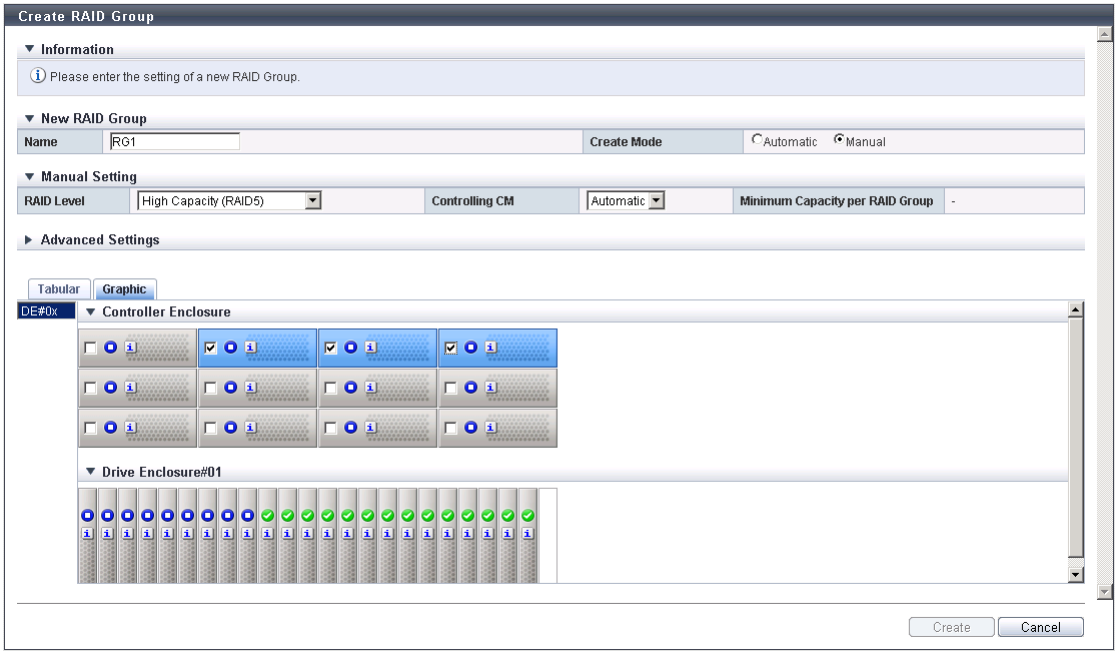
The RAID group is registered and the registration completion screen appears.

6 Click the [Done] button.

The screen returns to the [RAID Group] screen.

7 After creating an operation RAID group, repeat Step 1 and later steps to create a backup RAID group.

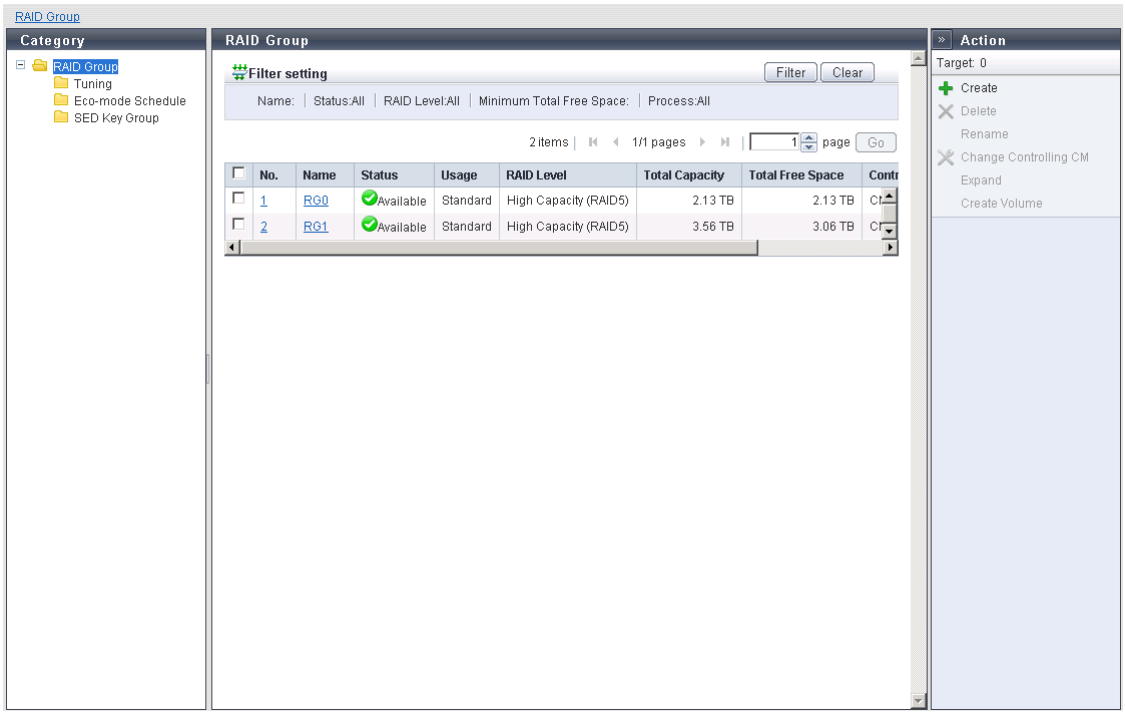
The following screen shows the settings that are displayed when creating a RAID group with the RAID group name "RG1" and the RAID level "RAID5(2+1)".



End of procedure

The following screen shows the RAID group information that is displayed after the RAID group is created.

Figure 12 RAID Group Information after Creation

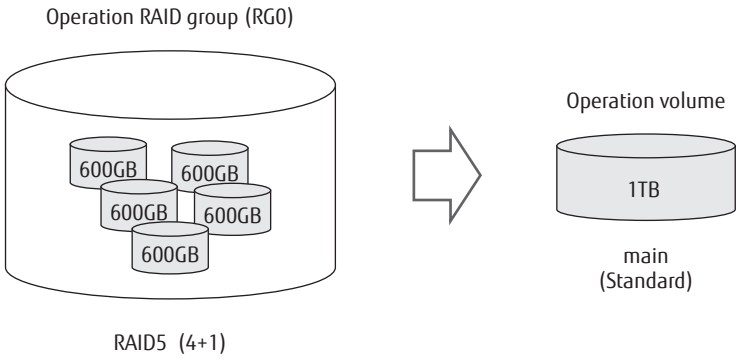


Operation Volume Creation

Create volumes (areas in the drives of a RAID group) in the RAID group.

Create a 1TB Standard volume in the operation RAID group created in "RAID Group Creation" (page 89).

Figure 13 Operation Volume Creation



To perform a backup with SnapOPC+, two types of backup volumes (generation data management area and expansion area where copy data is saved) must be prepared in addition to one for operation. For details about creation of backup volume, refer to "Generation Management Volume (SDV) Creation" (page 94) and "Copy Data Destination Volume (SDPV) Creation" (page 95).

Table 4 Operation Volume Creation

Usage	Item	Capacity	Volume type
Operation volume (copy source)	main	1TB	Standard
Generation management volume	sdv0 - 6	1TB (*1)	Snap Data Volume
Copy data destination volume	sdpv	500GB	Snap Data Pool Volume

***1:** Though the copy source capacity is specified during creation, the capacity allocated to sdv is approximately 0.1% of the copy source capacity.

Note

When creation is finished, the volume is automatically formatted. After volume creation, Standard and SDV become accessible from the host when host affinity setting is completed.

SDPV becomes available when formatting starts after creation.

The procedure to create an operation volume is as follows:

Procedure

1 Click the [Volume] tab on the navigation of the ETERNUS Web GUI screen.
The [Volume] screen appears.

2 In [Action], click [Create].
The [Create Volume] screen appears.

3 Set the required items in the [Create Volume] screen and click the [Create] button.

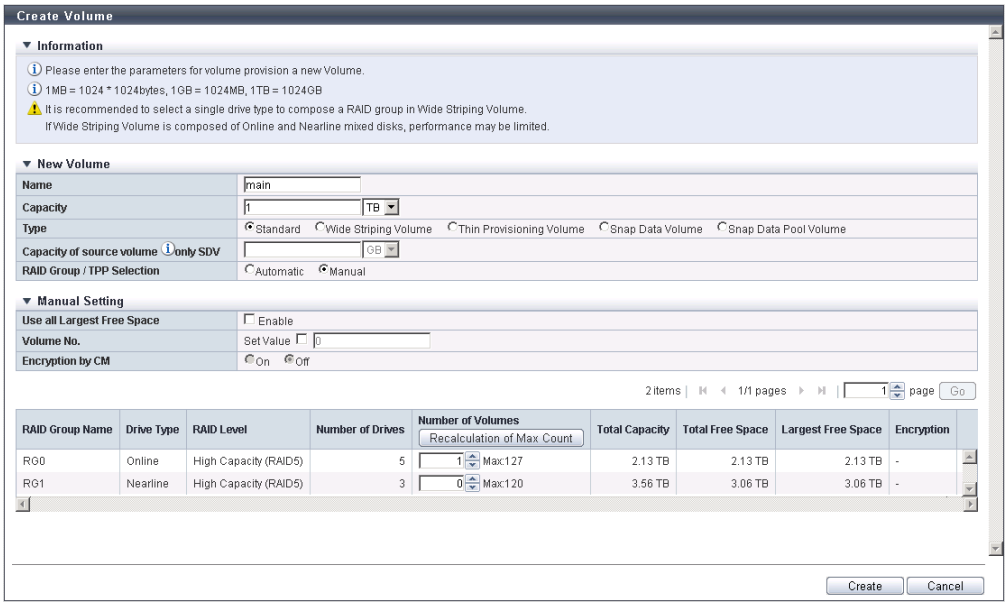
Name: main

Capacity: 1TB

Type: Standard

RAID Group / TPP Selection: Manual

Manual Setting: RG0



A confirmation screen appears.

4 Click the [OK] button.

The volume is created and the registration completion screen appears.

5 Click the [Done] button.

The screen returns to the [Volume] screen.

6 Then, create SDV and SDPV in the backup RAID group (RG1).

For the creation procedure, refer to "Generation Management Volume (SDV) Creation" (page 94) and "Copy Data Destination Volume (SDPV) Creation" (page 95).

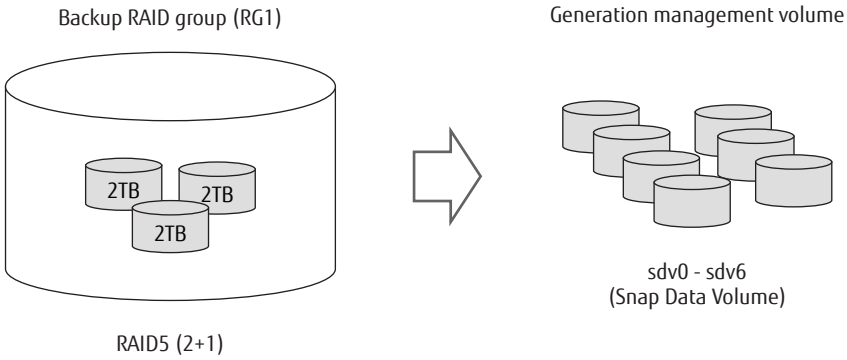
End of procedure

Generation Management Volume (SDV) Creation

Create a generation management volume in the backup RAID group.

Create SDV for seven generations (as a backup area for seven days a week) in the backup RAID group "RG1" created in "RAID Group Creation" (page 89).

Figure 14 Generation Management Volume (SDV) Creation



The procedure to create a generation management volume (SDV) is as follows:

Procedure

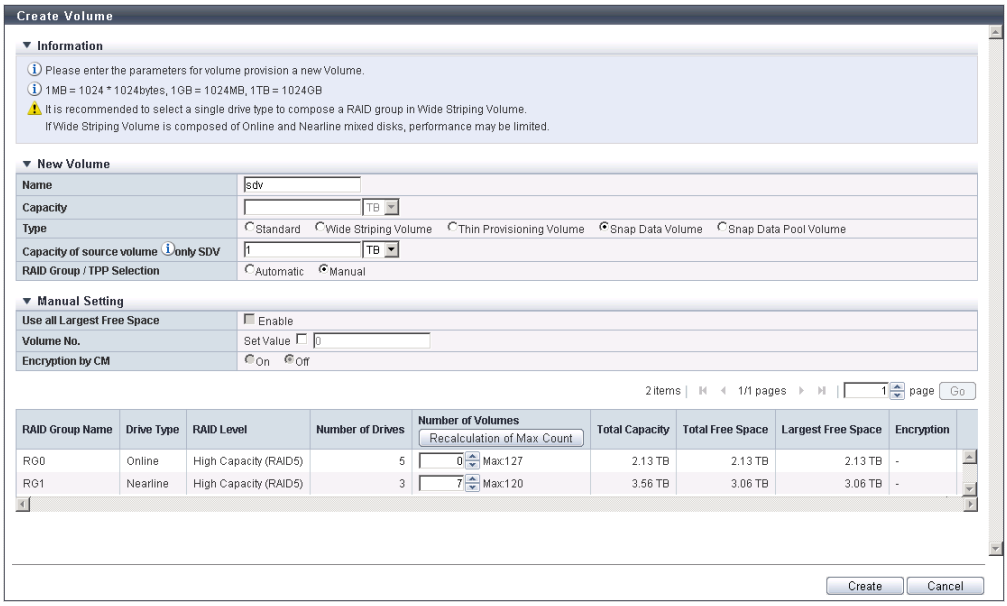
1 Click the [Volume] tab on the navigation of the ETERNUS Web GUI screen.
The [Volume] screen appears.

2 In [Action], click [Create].
The [Create Volume] screen appears.

3 Set the required items in the [Create Volume] screen and click the [Create] button.
Name: sdv
Type: Snap Data Volume
Capacity of source volume: 1TB (*1)
RAID Group / TPP Selection: Manual
Manual Setting: RG1
Number of Volumes: 7 (*2)

***1:** Enter the capacity of the copy source volume during creation of SDV.

***2:** If "7" is specified for the number of volumes, sdv0, sdv1, sdv2, sdv3, sdv4, sdv5, and sdv6 volumes are created.



A confirmation screen appears.

4 Click the [OK] button.

The volume is created and the registration completion screen appears.

5 Click the [Done] button.

The screen returns to the [Volume] screen.

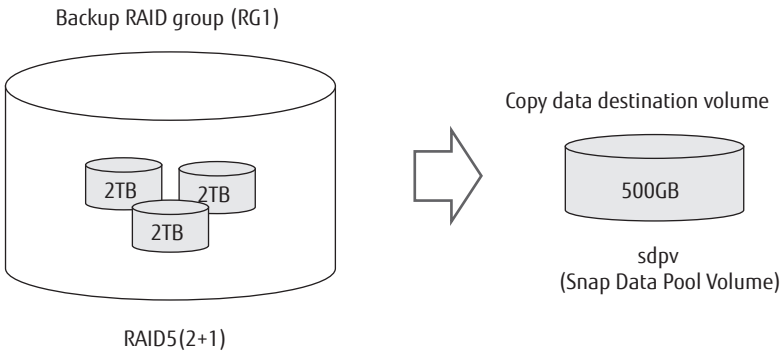
End of procedure

Copy Data Destination Volume (SDPV) Creation

Create a copy data destination volume in the backup RAID group.

Create a volume as an expansion area of SDV in the backup RAID group "RG1" created in "RAID Group Creation" (page 89).

Figure 15 Copy Data Destination Volume (SDPV) Creation



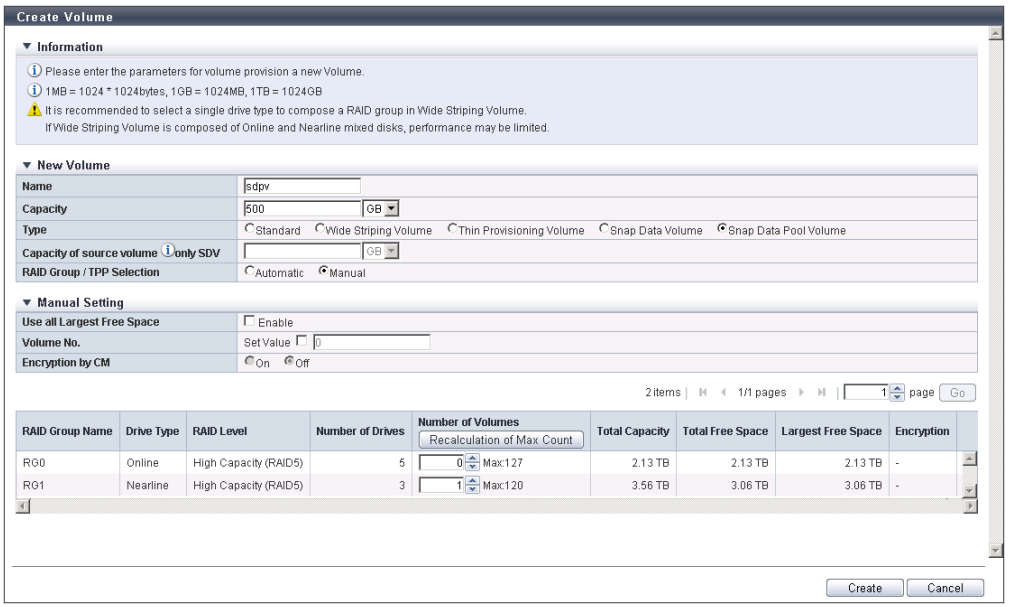
The procedure to create a copy data destination volume (SDPV) is as follows:

Procedure

1 Click the [Volume] tab on the navigation of the ETERNUS Web GUI screen.
The [Volume] screen appears.

2 In [Action], click [Create].
The [Create Volume] screen appears.

3 Set the required items in the [Create Volume] screen and click the [Create] button.
Name: sdpv
Capacity: 500GB
Type: Snap Data Pool Volume
RAID Group / TPP Selection: Manual
Manual Setting: RG1



A confirmation screen appears.

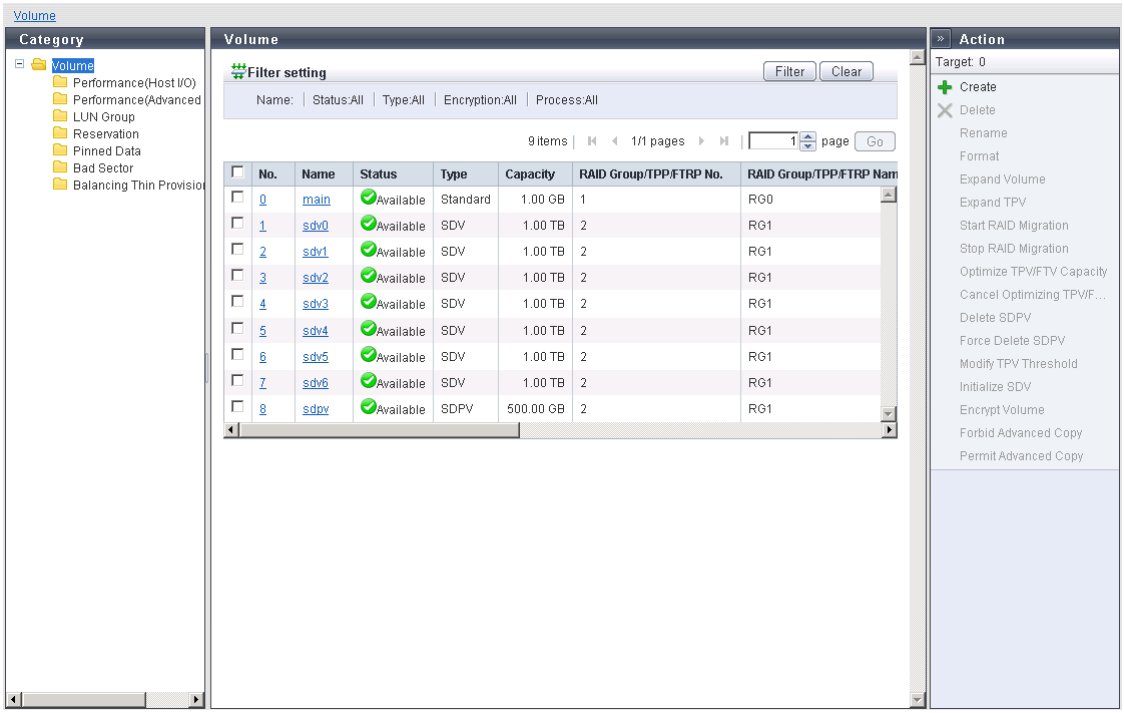
4 Click the [OK] button.
The volume is created and the registration completion screen appears.

5 Click the [Done] button.
The screen returns to the [Volume] screen.

End of procedure

The volume information after the copy data destination volume is created is shown below.

Figure 16 Volume Information after Creation



Hot Spare Registration

Register the hot spare for the failure of a drive.

Note

- Global Hot Spare

  This is available for any RAID group.
- Dedicated Hot Spare

  This is only available to the specified RAID group (one RAID group).
- The following two types of hot spare are available:
  - Global Hot Spare

    This is available for any RAID group.
  - Dedicated Hot Spare

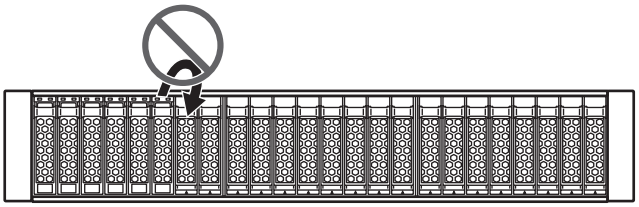
    This is only available to the specified RAID group (one RAID group).
- For a RAID group that contains important data, assign "Dedicated Hot Spare" in order to preferentially use the hot spare.
- When an Advanced Format disk is used as the hot spare, the sector format information that can be confirmed from the server may be changed.

CAUTION

Do Not

- Do not uninstall the drives that are installed by default or move them to any other slot.

  Contact your sales representative or maintenance engineer if drives that are installed by default need to be uninstalled or moved to another slot.



Global Hot Spare Registration

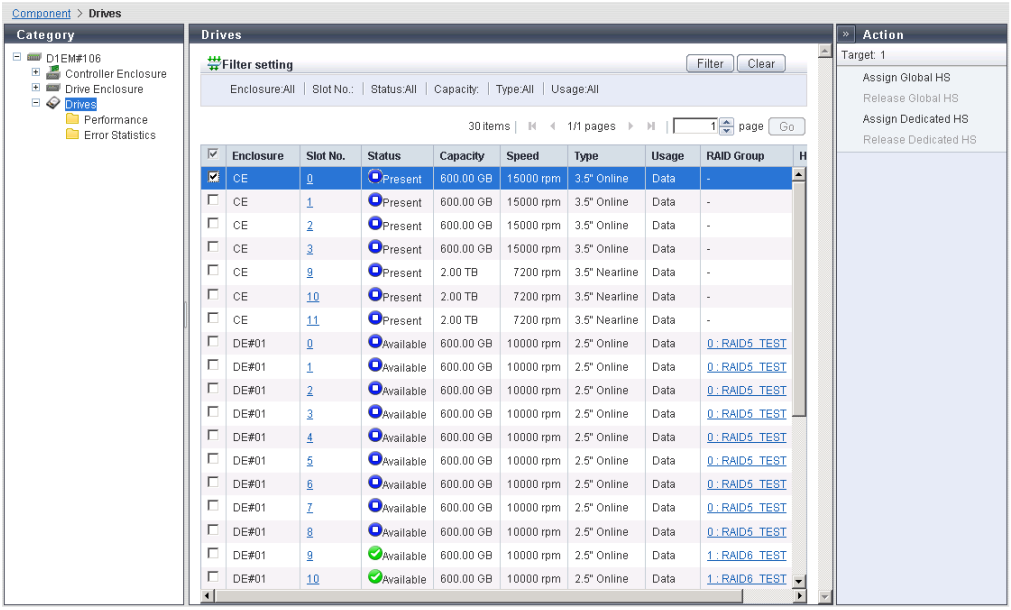
The procedure to register a Global Hot Spare is as follows:

Procedure

1 Click the [Component] tab on the navigation of the ETERNUS Web GUI screen. On the [Component] screen, click [Drives] in [Category].

The [Drives] screen appears.

2 Select the drive that is to be registered as the Global Hot Spare and click [Assign Global HS] in [Action].



A confirmation screen appears.

3 Click the [OK] button.

The Global Hot Spare is registered and the registration completion screen appears.

4 Click the [Done] button.

The screen returns to the [Drives] screen.

End of procedure

■ Dedicated Hot Spare Registration

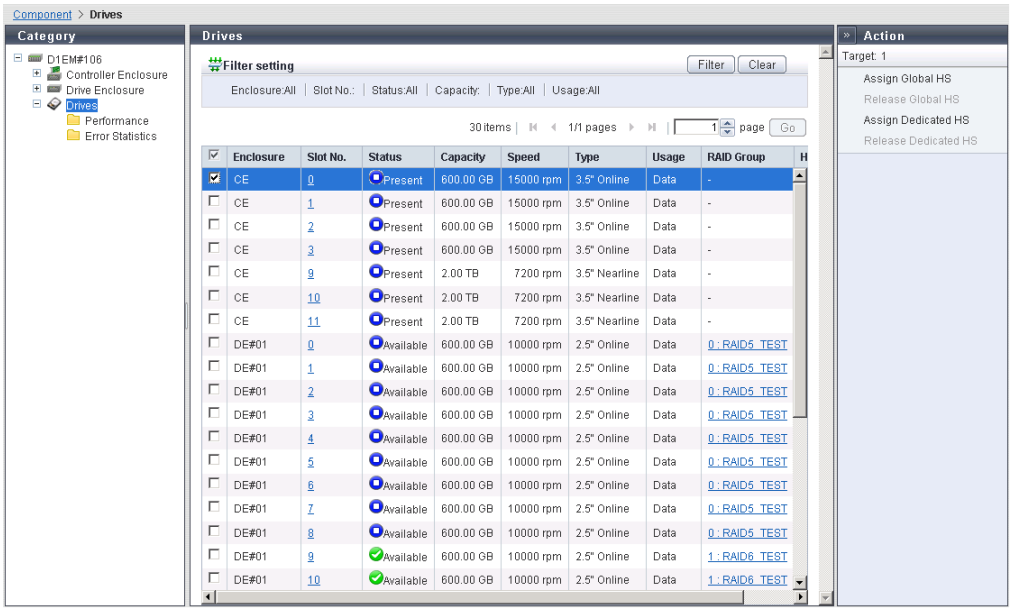
The procedure to register a Dedicated Hot Spare is as follows:

Procedure

1 Click the [Component] tab on the navigation of the ETERNUS Web GUI screen. On the [Component] screen, click [Drives] in [Category].

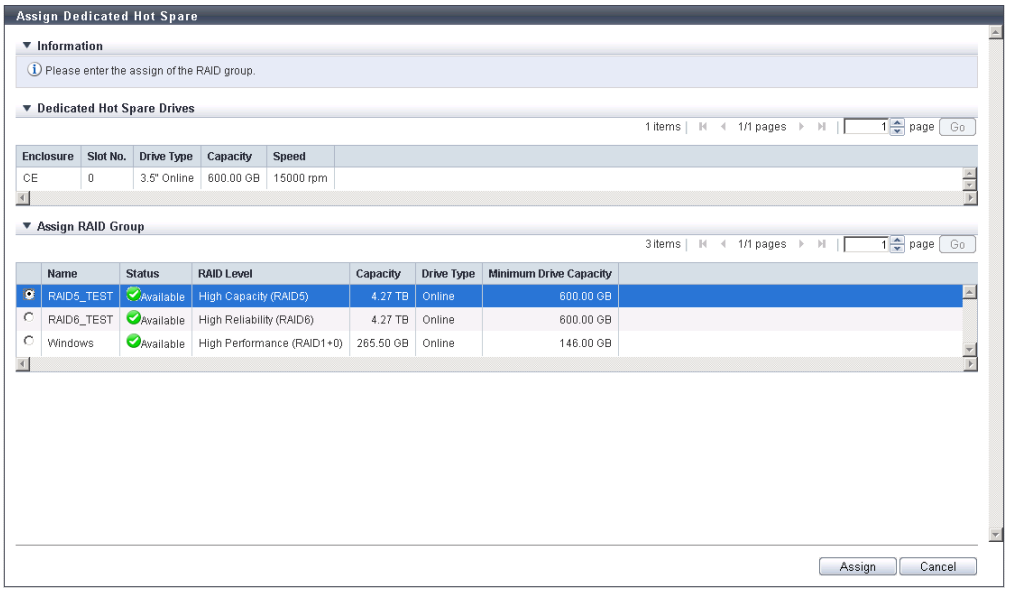
The [Drives] screen appears.

2 Select the drive that is to be registered as the Dedicated Hot Spare and click [Assign Dedicated HS] in [Action].



The [Assign Dedicated Hot Spare] screen appears.

3 Select the RAID group for the drive that was selected in Step 2 as the Dedicated Hot Spare. Click the [Assign] button.



A confirmation screen appears.

4 Click the [OK] button.

The Dedicated Hot Spare is registered and the registration completion screen appears.

5 Click the [Done] button.

The screen returns to the [Drives] screen.

End of procedure

6. Monitoring Settings

Perform the ETERNUS DX monitoring setup if required.

For more details on the setup, refer to "ETERNUS Web GUI User's Guide".

Event Notification Setup

Select whether to report events detected in the ETERNUS DX. There are five methods for event notification: Host Sense Key Code Qualifier, SNMP Trap, E-Mail, syslog, and REMCS.

Caution

If ETERNUS SF Storage Cruiser version 16.4 or later is used and configured to automatically obtain the ETERNUS DX component status, event notifications by SNMP traps for some events are automatically enabled.

The event notification items are as follows:

- Remote Path Error of no Data Transfer
- Recovery module
- Temperature restoration
- FC CA Port Link Status Changed
- iSCSI CA Port Link Status Changed
- Remote Path Recovery
- Events whose notification is enabled by default, but is disabled manually

If the ETERNUS DX is deleted from ETERNUS SF Storage Cruiser, event notifications by SNMP traps return to the default state.

However, if the event notifications by SNMP traps are changed from the ETERNUS DX after they are automatically changed by ETERNUS SF Storage Cruiser, the event notification setting is not returned to the default state even if the ETERNUS DX is deleted from ETERNUS SF Storage Cruiser.

Check that there are no problems with the SNMP trap event notification setting for the ETERNUS DX.

The event notification setting is explained below.

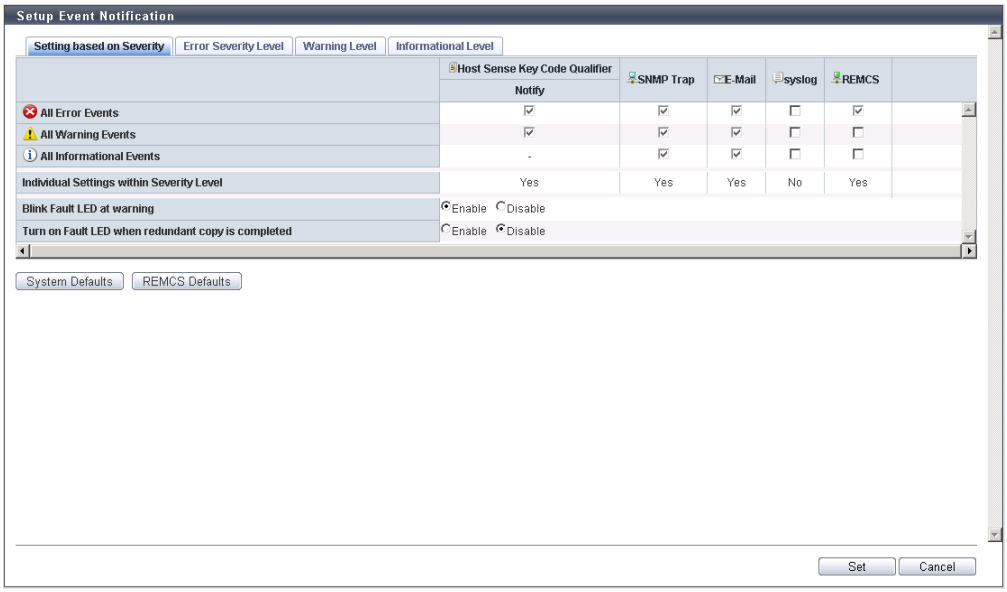
Procedure

1 On the navigation of the ETERNUS Web GUI screen, click [System].
The [System] screen appears.

2 In [Category], click [Event/Dump].
The [Event/Dump] screen appears.

3 In [Action], click [Setup Event Notification].
The [Setting based on Severity] tab screen of the [Setup Event Notification] screen appears.

4 In the [Setting based on Severity] tab screen, select the required items.



5 On the screens that are displayed by clicking each level tab, select the required items.

6 Click the [Set] button to apply the specified settings.
A confirmation screen appears.

7 Click the [OK] button.
The event notification settings are applied.

8 Check the setting completion message and click the [Done] button.
The screen returns to the [Event/Dump] screen.

End of procedure

Various Notification Settings

To monitor an ETERNUS DX, perform the required settings for device error notification.

SNMP Trap Setup

SNMP Trap can be sent to the SNMP Manager (monitoring server) when an event occurs in the ETERNUS DX.

The SNMP Trap setting is explained below.

IMPORTANT

Carefully read this manual and the manuals for the monitoring software (SNMP Manager) that is to be used before monitoring the ETERNUS DX.

■ ETERNUS DX Settings

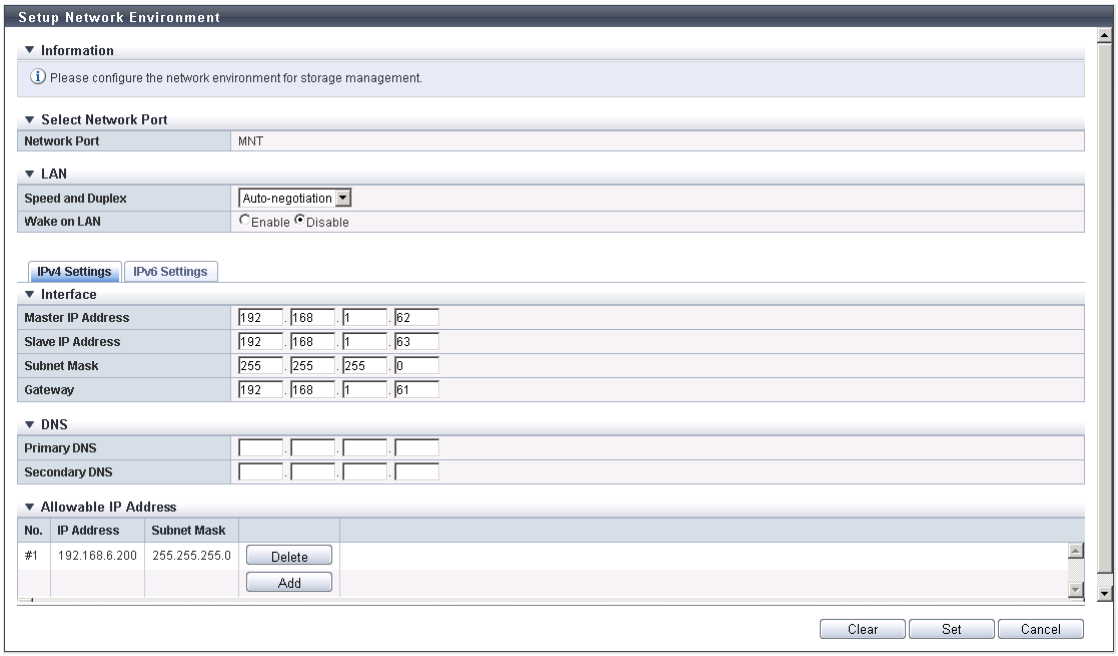
The SNMP Trap test setting is explained below.

Procedure

1 Set up the network environment for the ETERNUS DX.

When the ETERNUS DX and the monitoring server are in different subnet environments, set the Gateway IP address and the Allowable IP address (IP address of the monitoring server or the network address to which the monitoring server belongs) on the [Setup Network Environment] screen of ETERNUS Web GUI.

The following procedure shows an example when selecting the [IPv4 Settings] tab.



2 Set up the SNMP environment.

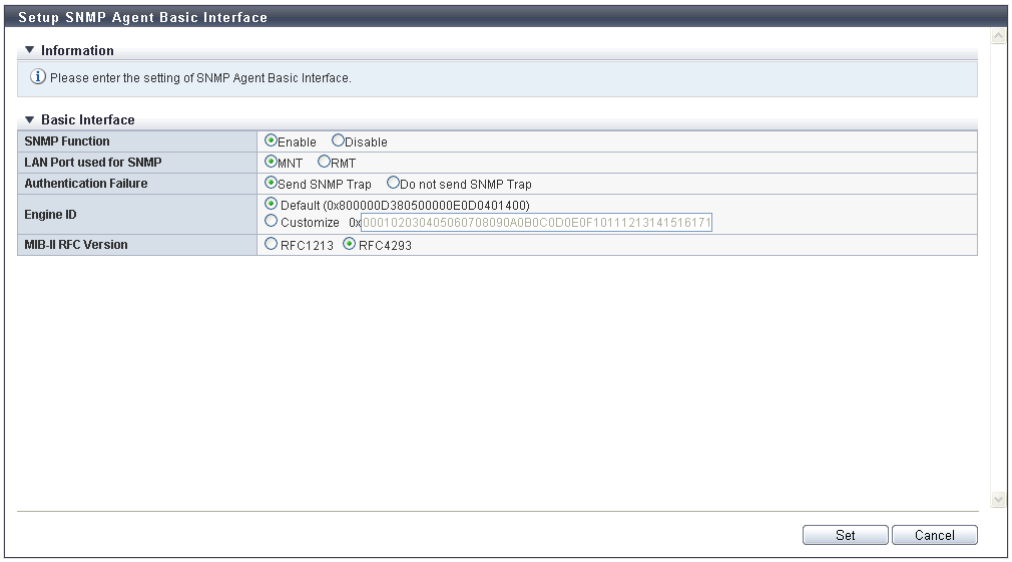
(1) On the navigation of the ETERNUS Web GUI screen, click [System].

The [System] screen appears.

(2) In [Category], click [Network].
The [Network] screen appears.

(3) In [Action], click [Setup SNMP Interface].
The [Setup SNMP Agent Basic Interface] screen appears.

(4) Select [Enable] for [SNMP Function], set the required items, and click the [Set] button.
Select the LAN port that was set up in Step 1 for "LAN Port used for SNMP".



A confirmation screen appears.

(5) Click the [OK] button.
The SNMP Agent basic settings are applied.

(6) Check the setting completion message and click the [Done] button.
The screen returns to the [Network] screen.

3 Set up the SNMP Manager.
Set up the SNMP Manager (monitoring server) that is the destination of the SNMP Trap transmission.

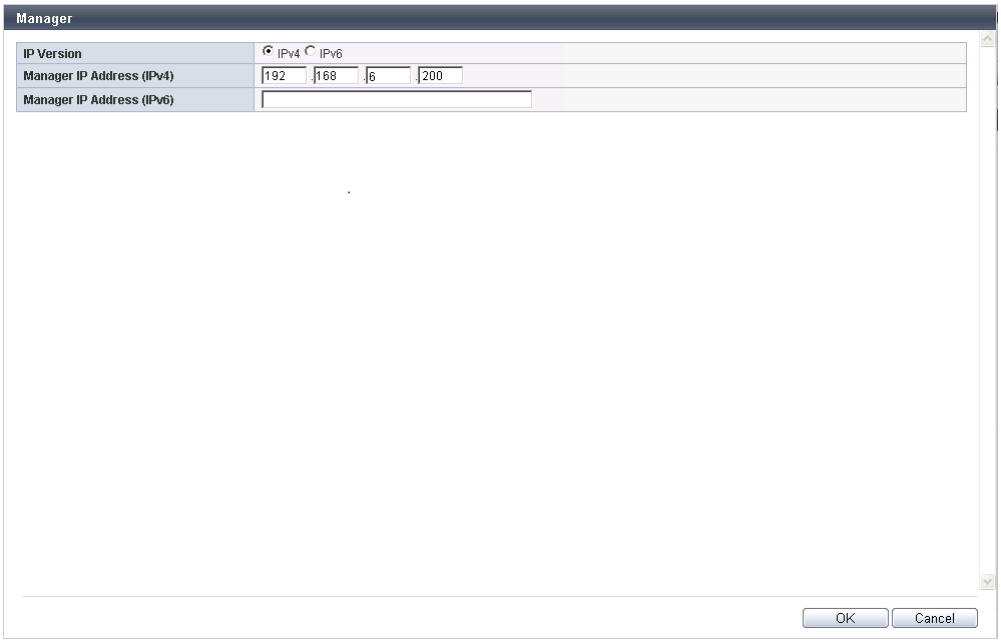
Note

This step is not required when ETERNUS SF Storage Cruiser is used to monitor the ETERNUS DX.

(1) In [Action], click [Setup SNMP Manager].
The [Setup SNMP Manager] screen appears.

(2) In the manager list of the [Setup SNMP Manager] screen, click the [Add] button.
The [Manager] screen appears.

(3) Enter the IP address of SNMP Manager (monitoring server) and click the [OK] button.



The screen returns to the manager list of the [Setup SNMP Manager] screen.

(4) Check the SNMP Manager that was added in Step (3) is displayed in the manager list and click the [Set] button.

A confirmation screen appears.

(5) Click the [OK] button.

The SNMP Manager settings are applied.

(6) Check the setting completion message and click the [Done] button.

The screen returns to the [Network] screen.

4 Set up a community or a user.

Set up the community or the user that is used for SNMP Trap.

Note

- To use SNMPv1 or SNMPv2c, perform the "Setup SNMP Agent Community" settings. To use SNMPv3, perform the "Setup SNMP Agent User" settings.
- To use ETERNUS SF Storage Cruiser for management, perform the "Setup SNMP Agent Community" settings to use SNMPv1.

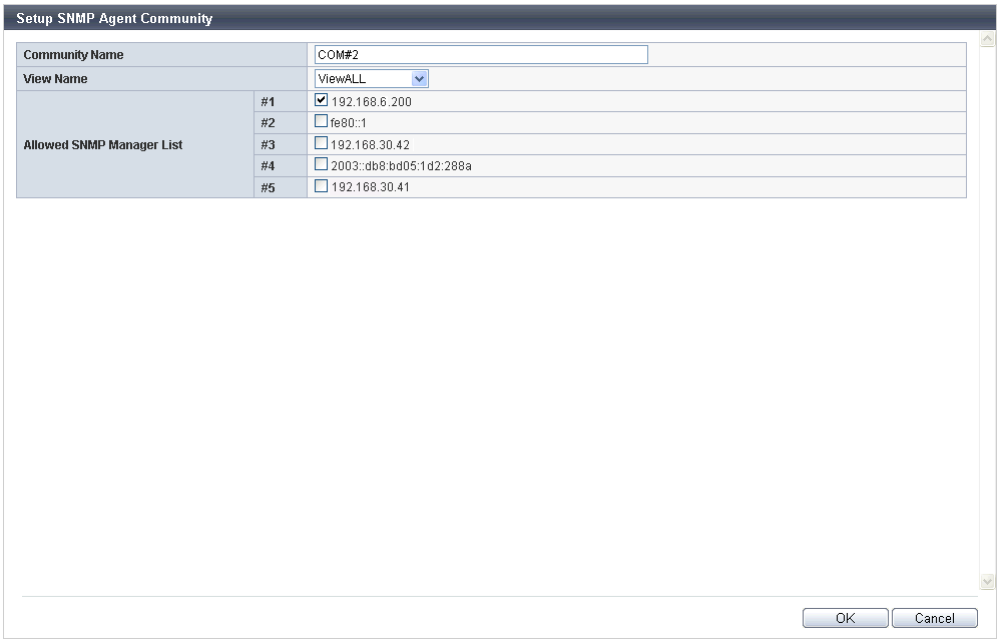
Community setup

(1) In [Action], click [Setup SNMP Community].

The [Setup SNMP Agent Community] screen appears.

(2) In the community list of the [Setup SNMP Agent Community] screen, click the [Add] button.

(3) Enter the community name, set the required items, and click the [OK] button.



The screen returns to the community list of the [Setup SNMP Agent Community] screen.

(4) Check the community name that was set in Step (3) is added in the community list and click the [Set] button.

A confirmation screen appears.

(5) Click the [OK] button.

The SNMP community settings are applied.

(6) Check the setting completion message and click the [Done] button.

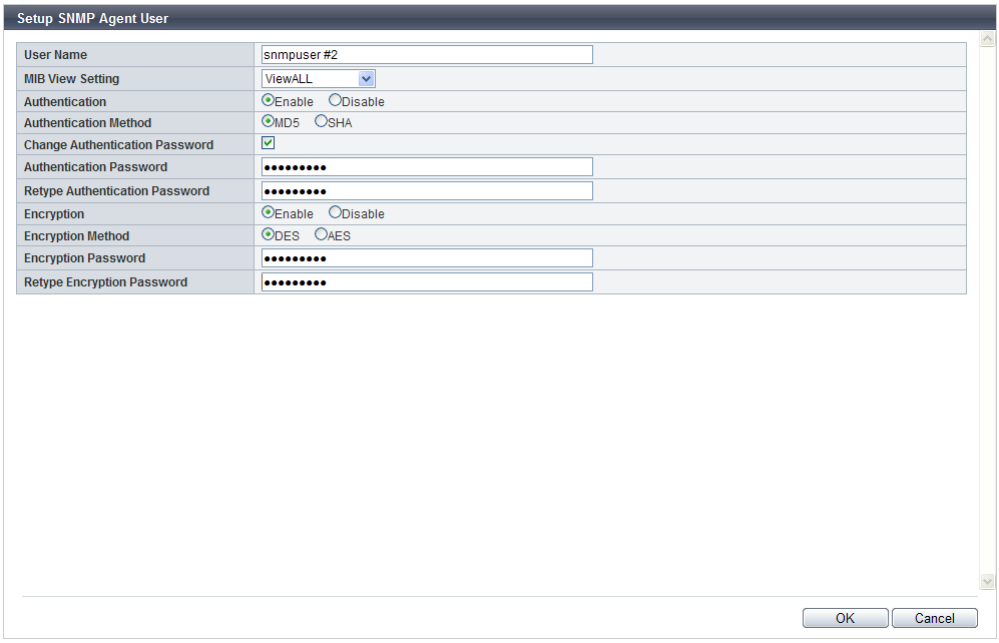
The screen returns to the [Network] screen.

User setup

(1) In [Action], click [Setup SNMP User].
The [Setup SNMP Agent User] screen appears.

(2) In the user list of the [Setup SNMP Agent User] screen, click the [Add] button.

(3) Enter the user name, set the required items, and click the [OK] button.



The screen returns to the user list of the [Setup SNMP Agent User] screen.

(4) Check the user that was set in Step (3) is added in the user list and click the [Set] button.
A confirmation screen appears.

(5) Click the [OK] button.
The SNMP user settings are applied.

(6) Check the setting completion message and click the [Done] button.
The screen returns to the [Network] screen.

5 Trap setup

Set up the destination for sending the SNMP Trap.

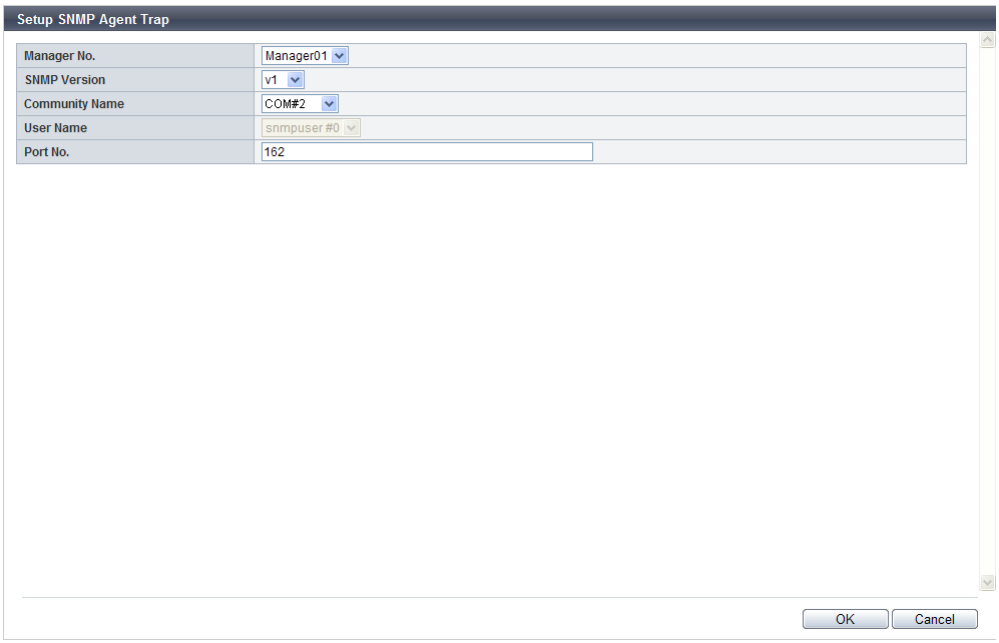
Note

This step is not required when ETERNUS SF Storage Cruiser is used to monitor the ETERNUS DX.

(1) In [Action], click [Setup SNMP Trap].
The [Setup SNMP Agent Trap] screen appears.

(2) In the trap list of the [Setup SNMP Agent Trap] screen, click the [Add] button.

(3) Select the Manager No. that was set in Step 3 for [Manager No.], set the required items, and click the [OK] button.



The screen returns to the trap list of the [Setup SNMP Agent Trap] screen.

(4) Check the trap that was set in Step (3) is added in the trap list and click the [Set] button.
A confirmation screen appears.

(5) Click the [OK] button.
The SNMP Trap settings are applied.

(6) Check the setting completion message and click the [Done] button.
The screen returns to the [Network] screen.

6 Download the MIB file.

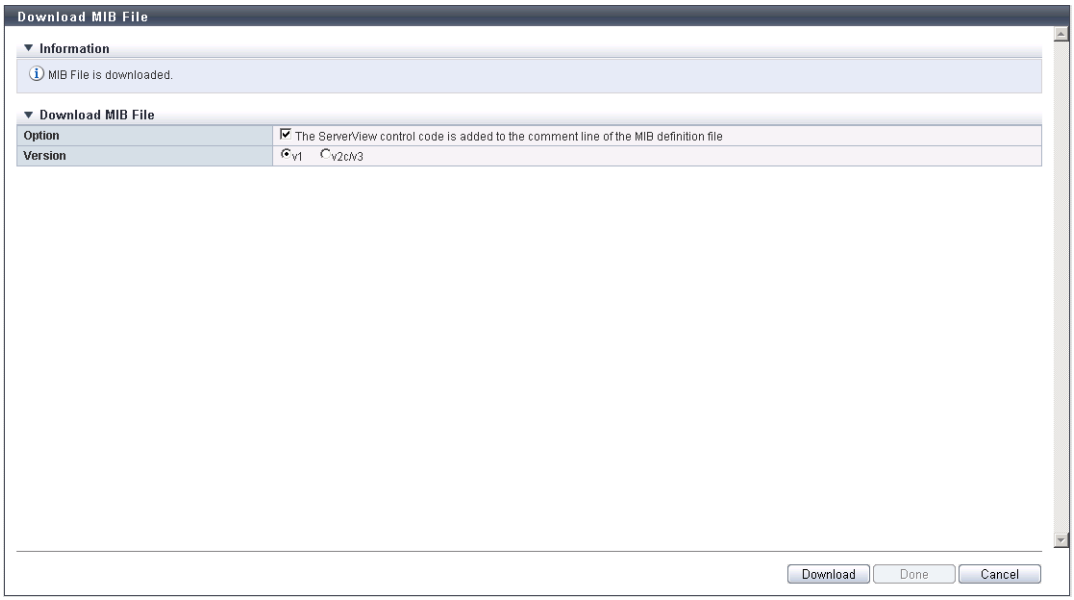
Download the MIB file that is registered in the ETERNUS DX.

(1) In [Action], click [Download MIB File].
The [Download MIB File] screen appears.

(2) In the [Download MIB File] screen, set the required items and click the [Download] button.

Note

Select the "The ServerView control code is added to the comment line of the MIB definition file" checkbox when downloading the MIB file for monitoring the ETERNUS DX by ServerView.



A confirmation screen appears.

(3) Click the [OK] button.
A dialog box to download the file appears.

(4) Click the [Save] button.
The MIB file is saved.

(5) Check the setting completion message and click the [Done] button.
The screen returns to the [Network] screen.

End of procedure

E-mail Setup

If an event occurs in the ETERNUS DX, the event information is reported to the specified e-mail address.

Note

- Up to five e-mail addresses can be set.
- Make sure to check whether the e-mail messages are received correctly after the e-mail notification environment setup is complete.
- E-mail messages are not sent again when a communication error occurs between the ETERNUS DX and the SMTP server.

The e-mail setting is explained below.

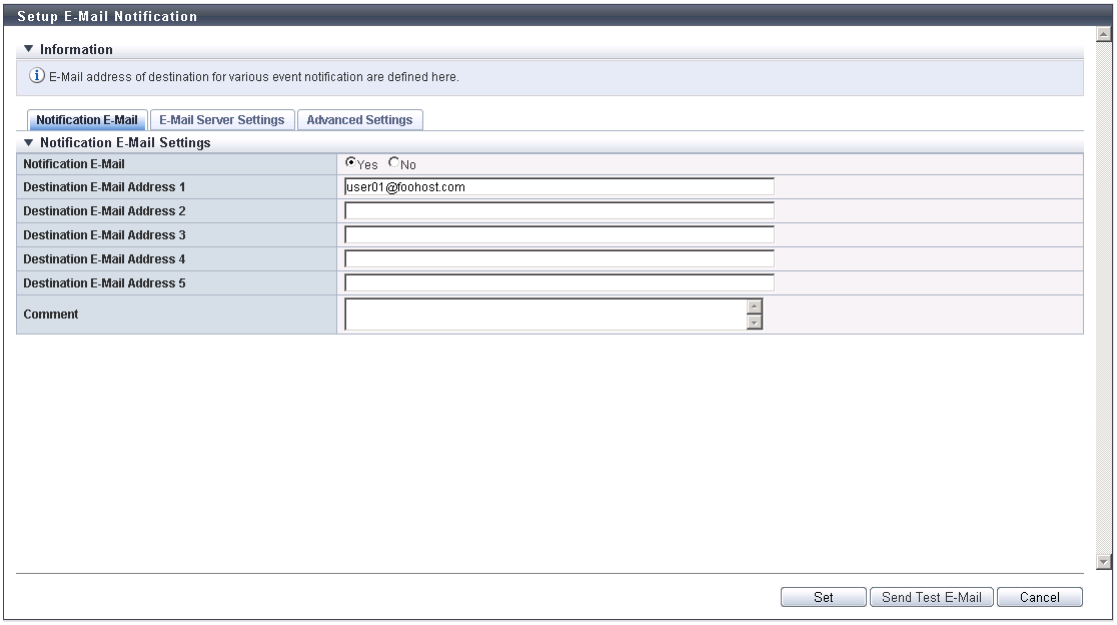
Procedure

1 On the navigation of the ETERNUS Web GUI screen, click [System].
The [System] screen appears.

2 In [Category], click [Network].
The [Network] screen appears.

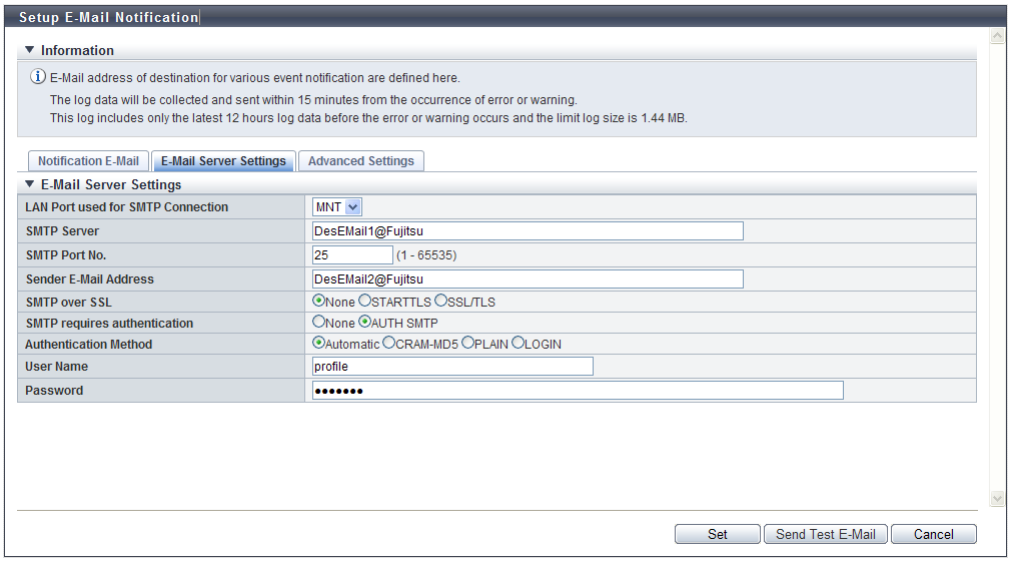
3 In [Action], click [Setup E-Mail Notification].
The [Notification E-Mail] tab screen of the [Setup E-Mail Notification] screen appears.

4 In the [Notification E-Mail] tab screen, set the required items.
- Select "Yes" for "Notification E-Mail".
- Enter the destination e-mail address or addresses for the Destination E-Mail Address fields.



5 Click the [E-Mail Server Settings] tab.
The [E-Mail Server Settings] tab screen appears.

6 In the [E-Mail Server Settings] tab screen, set the required items.

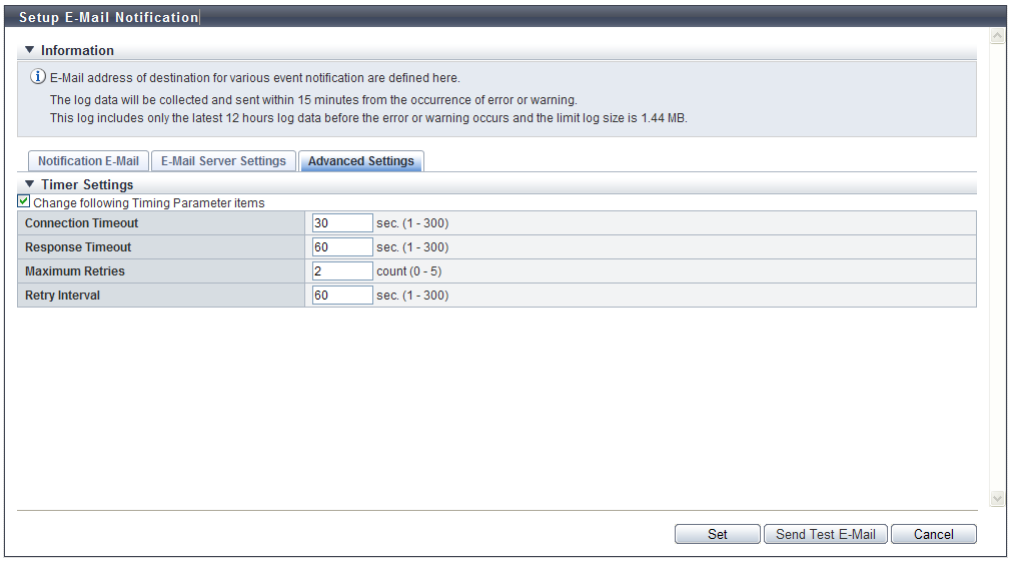


7 Click the [Advanced Settings] tab.
The [Advanced Settings] tab screen appears.

8 In the [Advanced Settings] tab screen, set the required items.

Note

This item does not need to be changed from the default value for normal operation.



9 Click the [Set] button to apply the specified settings.
A confirmation screen appears.

10 Click the [OK] button.
The e-mail notification settings are applied.

11 Check the setting completion message and click the [Done] button.
The screen returns to the [Network] screen.

End of procedure

Syslog Setup

If an event occurs in the ETERNUS DX, logs for the event can be sent to the specified Syslog server (external server).

Note

- Up to two Syslog servers can be set.
- Make sure to check whether the Syslog server receives logs correctly after the Syslog notification environment setup is complete.
- Logs are not sent again when a communication error occurs between the ETERNUS DX and the Syslog server.

The Syslog setting is explained below.

Procedure

1 On the navigation of the ETERNUS Web GUI screen, click [System].
The [System] screen appears.

2 In [Category], click [Network].
The [Network] screen appears.

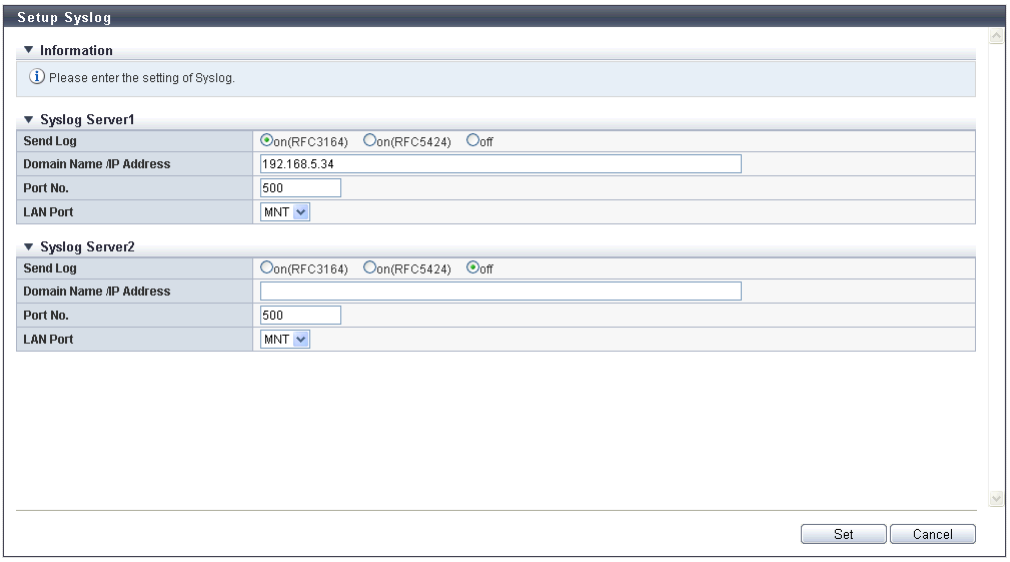
3 In [Action], click [Setup Syslog].
The [Setup Syslog] screen appears.

4 In the [Setup Syslog] screen, set the required items.
- Select "on(RFC3164)" or "on(RFC5424)" for "Send Log".

IMPORTANT

To send messages in RFC5424 format to a target Syslog server that supports RFC5424, select "on(RFC5424)". If this is not the case, select "on(RFC3164)".

- Enter the domain name or IP address of the Syslog server in "Domain Name /IP Address".



5 Click the [Set] button.
A confirmation screen appears.

6 Click the [OK] button.
The Syslog notification settings are applied.

7 Check the setting completion message and click the [Done] button.
The screen returns to the [Network] screen.

End of procedure

Remote Support Setup

When using the remote support, reporting problems in the ETERNUS DX to the remote support center must be set.

Note

Remote support allows prompt detection and resolution of trouble.

Caution

- Service for AIS Connect was discontinued in December 2022.
- Note that AIS Connect and REMCS are not available in some regions. Contact the Support Department for details.
- AIS Connect and REMCS cannot be used at the same time. AIS Connect function can only be used when REMCS is not specified or is stopped. When REMCS is used, suspend the REMCS function, and then enable the AIS Connect function.

Remote Support (by AIS Connect) Setup

When using the remote support function by AIS Connect, perform the environment settings for connecting to the remote server (AIS Connect server) in the remote support center.

Caution

Service for AIS Connect was discontinued in December 2022.

IMPORTANT

- If the REMCS function is being used, temporarily stop the REMCS function.
- In the EMEIA, Central American, and Caribbean regions, the "Log Transmission" setting for the "Set E-Mail Notification" function may be enabled ("Yes" is displayed). If this setting is enabled, disable it (select "No").

Procedure

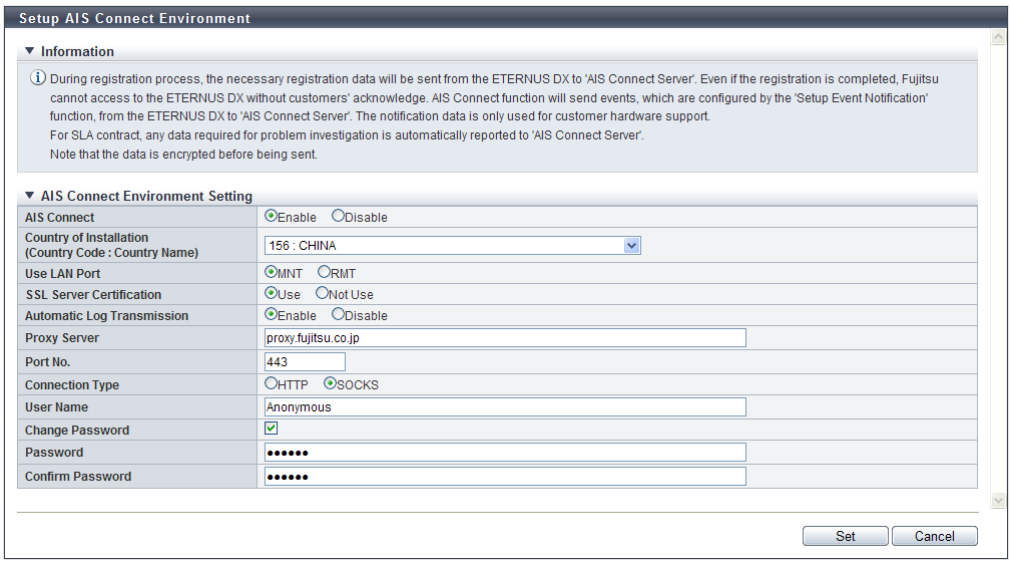
1 On the navigation of the ETERNUS Web GUI screen, click [System].
The [System] screen appears.

2 In [Category], click [AIS Connect] in [Remote Support].
The [Remote Support] screen appears.

3 Perform the environment settings for the AIS Connect function.

(1) In [Action], click [Setup AIS Connect Environment].
The [Setup AIS Connect Environment] screen appears.

(2) Select "Enable" for "AIS Connect" and then "Country code : Country name" for "Country of Installation (Country Code : Country Name)". Perform the other additional settings that are required.



(3) Click the [Set] button.
A confirmation screen appears.

(4) Click the [OK] button.
The AIS Connect settings are applied.

(5) Check the setting completion message and click the [Done] button.
The screen display returns to the remote support screen.

4 Confirm the connection of the ETERNUS DX and the AIS Connect server in the remote support center.

(1) In [Action], click [Test Server Connectivity].
A confirmation screen appears.

(2) Click the [OK] button.
The connection with the server is checked. The result is displayed in the [Test Server Connectivity Result] screen.

(3) Click the [Done] button.
The screen display returns to the remote support screen.

5 Send the test event to confirm that the event is reported to the AIS Connect server.

(1) In [Action], click [Send AIS Connect Test Event].
A confirmation screen appears.

(2) Click the [OK] button.
The test event is sent to the AIS Connect server. The result is displayed in the [Send AIS Connect Test Event Result] screen.

(3) Click the [Done] button.
The screen display returns to the remote support screen.

End of procedure

Remote Support (by REMCS) Setup

When using the remote support function by REMCS, perform the environment settings for connecting to the remote support center, and register the customer information to send to the remote support center.

IMPORTANT

If the AIS Connect function is being used, disable the AIS connect function and then start the remote support (by REMCS) setup.

Procedure

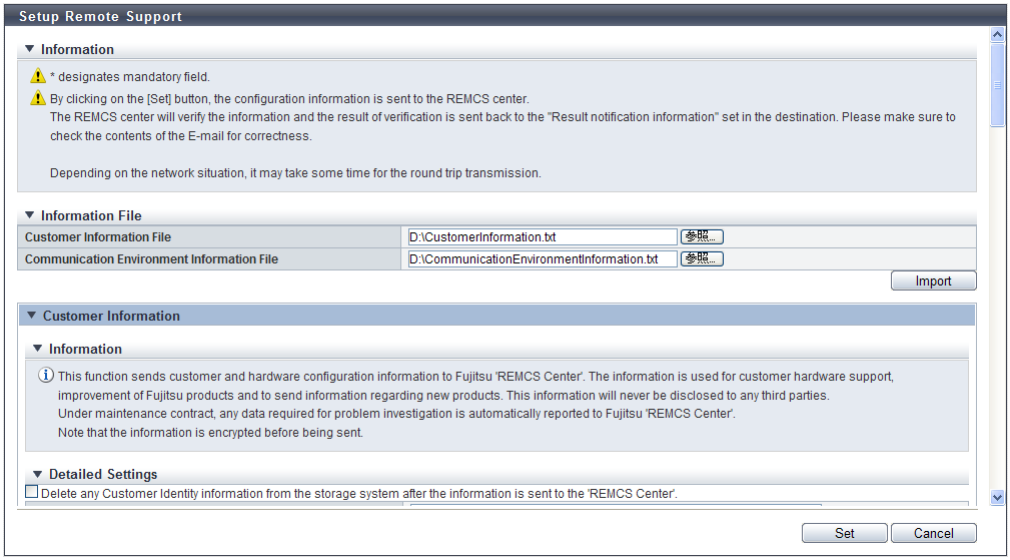
1 On the navigation of the ETERNUS Web GUI screen, click [System].
The [System] screen appears.

2 In [Category], click [REMCS] in [Remote Support].
The [Support Information] tab screen of the [Remote Support] screen appears.

3 In [Action], click [Setup Remote Support].

The [Setup Remote Support] screen appears.

4 In the [Setup Remote Support] screen, set the items in [Customer Information File] and [Communication Environment Information File].



5 Click the [Set] button.

A confirmation screen appears.

6 Click the [OK] button.

The remote support settings are applied.

7 Check the setting completion message and click the [Done] button.

The screen returns to the remote support screen.

The specified information is sent to the remote support center and the connection of the ETERNUS DX and the remote support center is checked.

The connection check result is sent to the e-mail address that is set in "Result notification information".

End of procedure

Audit Log Setup

Audit trail logs (hereinafter referred to as "audit log") that record performed operations by using the ETERNUS DX and the system actions that are associated with these operations can be sent to the specified Syslog server (external server).

Note

- Up to two Syslog servers can be set.
- After the environmental settings for audit logs are complete, confirm that the audit log is successfully received on the Syslog server.
- Even if a communication error occurs between the ETERNUS DX and the Syslog server, the audit log is not sent again.

The audit log setting is explained below.

Procedure

1 On the navigation of the ETERNUS Web GUI screen, click [System].
The [System] screen appears.

2 In [Category], click [Audit Log].
The [Audit Log] screen appears.

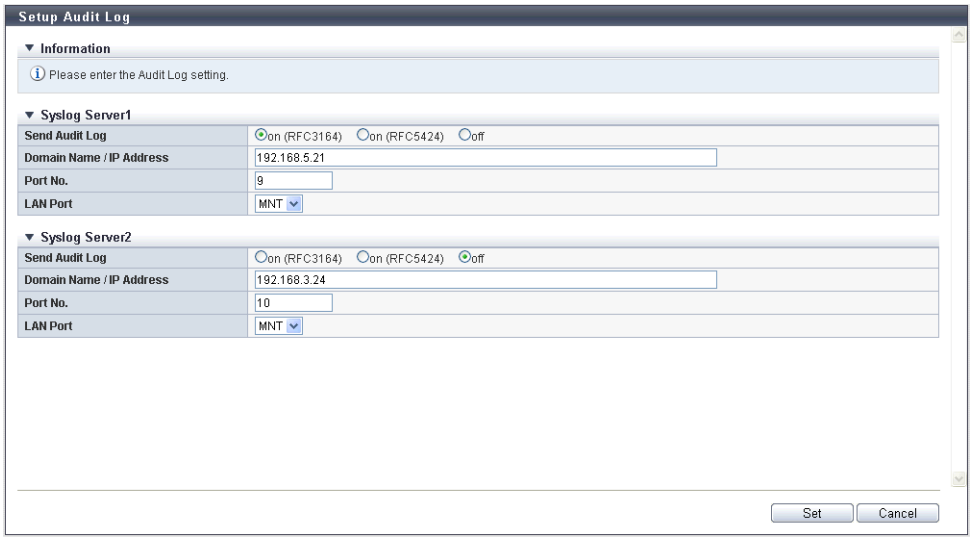
3 If "Disable" is specified for "Audit Log", select "Enable".
(1) Click [Enable Audit Log] in [Action].
A confirmation screen appears.
(2) Click the [OK] button.
Enabling of the audit log starts.
(3) Check the setting completion message and click the [Done] button.
The screen returns to the [Audit Log] screen.

4 Specify the Syslog server to which the audit log is sent.
(1) Click [Setup Audit Log] in [Action].
The [Setup Audit Log] screen appears.
- Select "on (RFC3164)" or "on (RFC5424)" for "Send Audit Log".

IMPORTANT

To send messages in RFC5424 format to a target Syslog server that supports RFC5424, select "on (RFC5424)". If this is not the case, select "on (RFC3164)".

- Enter the domain name or IP address of the Syslog server in "Domain Name /IP Address".



(2) Click the [Set] button.
A confirmation screen appears.

(3) Click the [OK] button.
Setting of the audit log starts.

(4) Check the setting completion message and click the [Done] button.
The screen returns to the [Audit Log] screen.

End of procedure

Monitoring Server (SNMP Manager) Settings

Install and set up the monitoring software on the server side.
Refer to the manual for the monitoring software to install and set the monitoring software.

Note

Register the file that was downloaded in "Download the MIB file" (Step 6) in "SNMP Trap Setup" (page 103) as the MIB definition file for the monitoring software.

Transmission Test Execution

For SNMP Trap notifications or e-mail notifications, perform a transmission test to make sure that event notifications are sent normally.

SNMP Trap Test

Perform the SNMP Trap test to check that the SNMP Trap can be sent from the ETERNUS DX to the SNMP Manager.

The procedure to send a trap test and to check the result is as follows:

Procedure

1 Perform the test transmission of the SNMP Trap.

(1) On the navigation of the ETERNUS Web GUI screen, click [System].

The [System] screen appears.

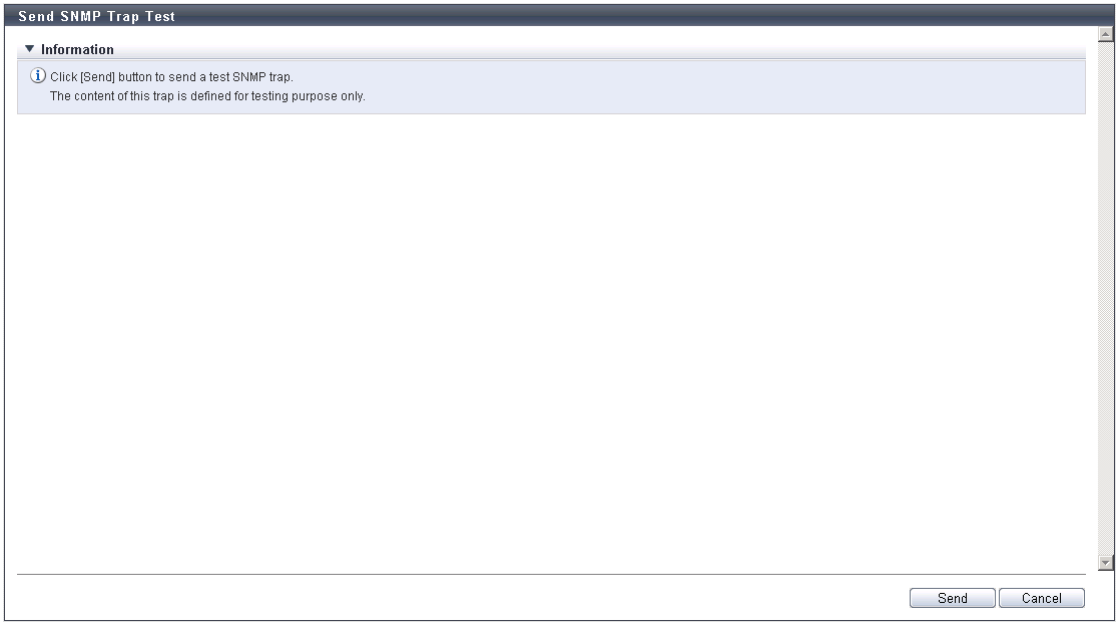
(2) In [Category], click [Network].

The [Network] screen appears.

(3) In [Action], click [Send SNMP Trap].

The [Send SNMP Trap Test] screen appears.

(4) In the [Send SNMP Trap Test] screen, click the [Send] button.



A confirmation screen appears.

(5) Click the [OK] button.

The test transmission of the SNMP Trap is performed.

(6) Check the test transmission completion message and click the [Done] button.

The screen returns to the [Network] screen.

2 Check the result of the test transmission.

Check that the SNMP Trap is notified to the monitoring server.

For details on the messages for test transmission, refer to "Message List".

If the SNMP Manager cannot receive an SNMP test trap, check that the network has no trouble, and the settings for the ETERNUS DX are correct.

- Is the LAN between the monitoring server and ETERNUS DX connected correctly?

  Execute the "ping" command from the monitoring server, and confirm the reply from the ETERNUS DX.

IMPORTANT

When "ICMP" is disabled by the firewall settings for ETERNUS Web GUI, the "ping" command cannot be used for confirmation. Enable "ICMP" before executing the "ping" command.

- Is the monitoring software set correctly to monitor the ETERNUS DX?
- Are the SNMP environment settings and the transmission destination for the SNMP Trap set correctly on the ETERNUS DX?

End of procedure

Send Test E-mail

Perform an e-mail transmission test to check that the e-mail can be sent from the ETERNUS DX to the specified e-mail address.

The procedure to send a test e-mail is as follows:

Procedure

1 On the navigation of the ETERNUS Web GUI screen, click [System].

The [System] screen appears.

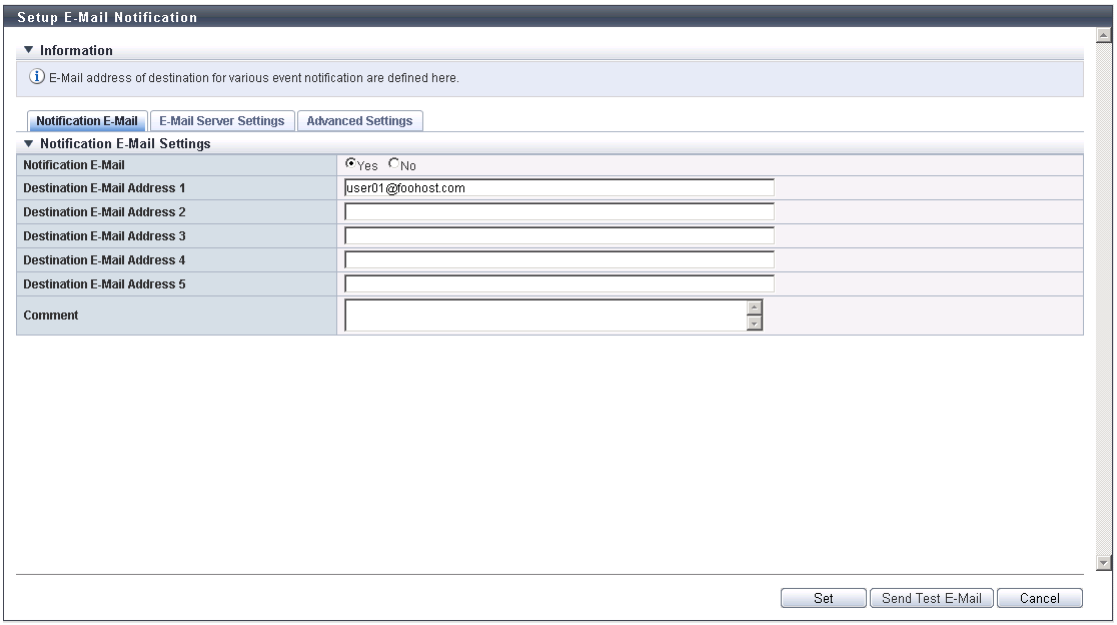
2 In [Category], click [Network].

The [Network] screen appears.

3 In [Action], click [Setup E-Mail Notification].

The [Setup E-Mail Notification] screen appears.

4 Click the [Send Test E-Mail] button.



5 Check that the test e-mail is sent to the e-mail addresses that are set.
For details on the event code and message of the test e-mail, refer to "Message List".

End of procedure

7. Power Control Setup

Perform power control settings as required.

Power control settings must be performed if the Auto Power function (AC automatic linkage mode) is enabled, the Power Resume function (automatic power recovery mode) is enabled, the power synchronized unit is connected, or the Wake On LAN function is used.

For more details on the setup, refer to "ETERNUS Web GUI User's Guide".

Setup of the Auto Power Function and/or the Power Resume Function

To automatically turn on the ETERNUS DX when AC power is supplied or when power is restored after a power failure, use ETERNUS Web GUI to enable the Auto Power function and/or the Power Resume function.

- Auto Power function (AC automatic linkage mode)

  When the Auto Power function is enabled, the ETERNUS DX is automatically turned on when AC power is supplied.

  The Auto Power function is disabled for the factory default setting.

- Power Resume function (automatic power recovery mode)

  When the Power Resume function is enabled, the ETERNUS DX is automatically turned on when the power supply is restored after a power failure.

  The Power Resume function is disabled for the factory default setting.

Table 5 shows how the ETERNUS DX operates when the Auto Power function and the Power Resume function are enabled or disabled.

Table 5 ETERNUS DX Operation according to the Settings of the Auto Power Function and the Power Resume Function

Settings for the power control functions	How the ETERNUS DX operates
Auto Power function is disabled Power Resume function is disabled	The ETERNUS DX is not automatically turned on even when AC power is supplied or when power is restored after a power failure.
Auto Power function is enabled Power Resume function is disabled	The ETERNUS DX is automatically turned on when AC power is supplied. The ETERNUS DX is not turned on even when power is restored after a power failure.
Auto Power function is disabled Power Resume function is enabled	The ETERNUS DX is not turned on automatically even when AC power is supplied. The ETERNUS DX is automatically turned on when power is restored after a power failure.
Auto Power function is enabled Power Resume function is enabled	The ETERNUS DX is automatically turned on when AC power is supplied and when power is restored after a power failure.

The procedure to enable the Auto Power function and the Power Resume function is described below.

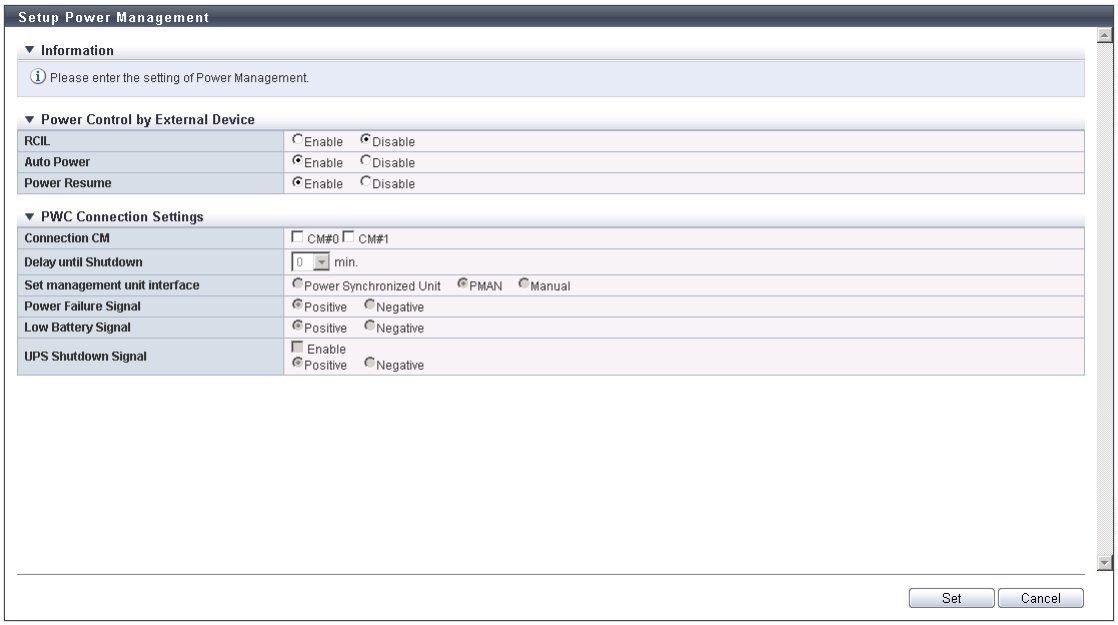
Procedure

1 On the navigation of the ETERNUS Web GUI screen, click [System].
The [System] screen appears.

2 In [Category], click [System Settings].
The [System Settings] screen appears.

3 In [Action], click [Setup Power Management].
The [Setup Power Management] screen appears.

4 In the [Setup Power Management] screen, select [Enable] for [Auto Power], [Power Resume], or both.



5 Click the [Set] button.
A confirmation screen appears.

6 Click the [OK] button.
The Auto Power function and/or the Power Resume function setting is applied.

7 Check the setting completion message and click the [Done] button.
The screen returns to the [System Settings] screen.

End of procedure

Connection Setup for Power Synchronized Units

Refer to "Configuration Guide (Power Synchronized Unit)" for the required settings to use power control by connecting power synchronized units to an ETERNUS DX.

Wake On LAN Settings

A network environment needs to be set to receive magic packets that are used by Wake On LAN for the ETERNUS DX.

The procedure to set Wake On LAN is as follows:

Procedure

1 On the navigation of the ETERNUS Web GUI screen, click [System].

The [System] screen appears.

2 In [Category], click [Network].

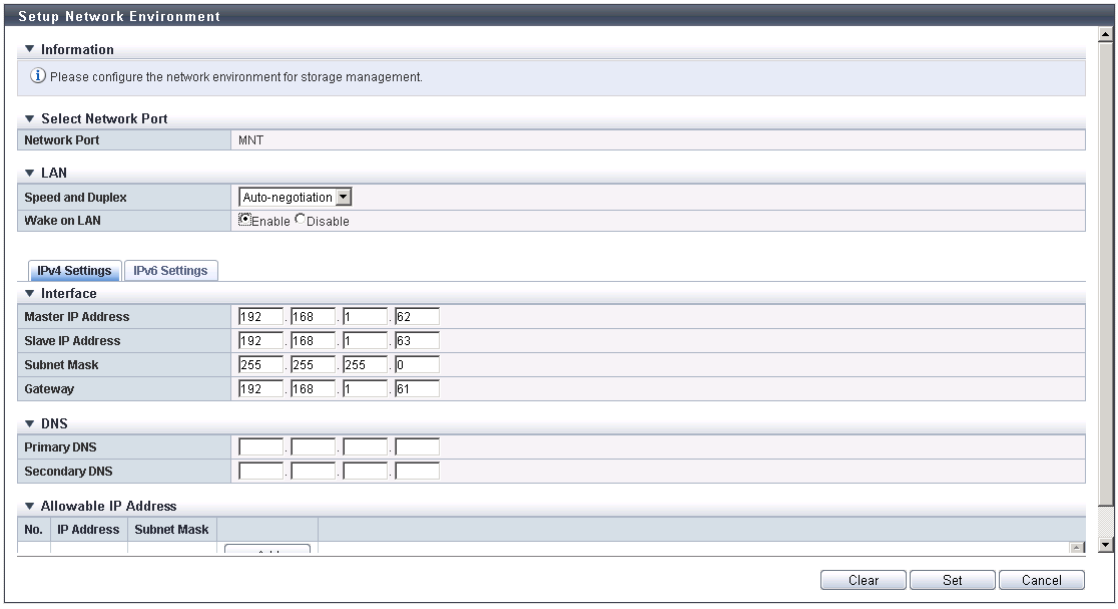
The [Network] screen appears.

3 In [Action], click [Setup Network].

The [Setup Network Environment] screen appears.

4 In the [Setup Network Environment] screen, select [Enable] for [Wake on LAN].

- For operations with cluster connections, set the IP address of the Slave CM for the "Slave IP Address" of the MNT port.
- To control power supply with servers in a network to which the ETERNUS DX does not belong, set "Gateway" and specify the server IP address or the network address in "Allowable IP Address".



5 Click the [Set] button.

A confirmation screen appears.

6 Click the [OK] button.

The network environment settings are applied.

7 Check the setting completion message and click the [Done] button.
The screen returns to the [System Settings] screen.

End of procedure

8. SAN Connection Settings

This chapter explains the required settings to use an ETERNUS DX via a SAN connection.

Connection Settings for the ETERNUS DX

Set up the ETERNUS DX as required to connect to the server.

For a configuration enabled with Thin Provisioning, creation of Thin Provisioning Pools and configuration of host affinity can be simplified using the Smart Setup Wizard.

For details on the settings, refer to "Smart Setup Wizard" (page 134).

Host Response Settings

The host response configures the appropriate operation mode on which the host makes connection. In normal host connection, the recommended patterns prepared for each OS type in advance or the default settings are used.

Table 6 Recommended Patterns of Host Responses

Host response name	Connection environment
Solaris MPxIO	Set this parameter to connect to an Oracle Solaris host and to use the OS standard Multipath Driver (MPxIO).
HP-UX	Set this parameter to connect to an HP-UX host.
AIX	Set this parameter to connect to an AIX host.
AIX VxVM	Set this parameter to connect to an AIX host and to use Veritas Volume Manager (VxVM).
VS850/SVC	Set this parameter to connect to an ETERNUS VS850 Virtualization Storage or an IBM SAN Volume Controller (SVC).
BS2000	Set this parameter to connect to a BS2000 host.
Default	Set this parameter for any host connection environments that are not listed above.

For details about the recommended patterns of host responses, refer to "Add Host Response" in "ETERNUS Web GUI User's Guide".

For details on assigning an appropriate host response, refer to "Configuration Guide -Server Connection-". For details on modifying the host response settings, refer to "Add Host Response" in "ETERNUS Web GUI User's Guide".

Host Affinity Settings

Use ETERNUS Web GUI to set host affinity.

Host affinity settings ensure security when multiple servers are connected by assigning the servers that can access the volumes.

This section provides an example for setting host affinity by associating a host group, a CA port group, and a LUN group when an iSCSI interface is used for connection.

Set host affinity in the following order:

- LUN group addition
- Port parameter settings
- CA port group creation
- Host group addition
- Host affinity creation

For the settings for connection using other interfaces, refer to "Configuration Guide (Web GUI)". Also, refer to "Configuration Guide -Server Connection-" for each OS.

LUN Group Addition

Add a group of volumes that can be recognized by the host (LUN group).

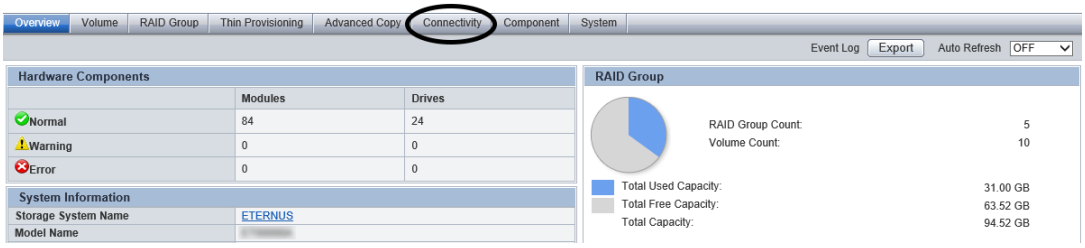
For each LUN group, volume numbers are assigned for the Logical Unit Numbers (LUNs) that are recognized by the host.

The procedure to create a LUN group is as follows:

Procedure

1 On the ETERNUS Web GUI screen, click the [Connectivity] navigation tab on the upper part of the screen.

The following overview screen is displayed after logging in.



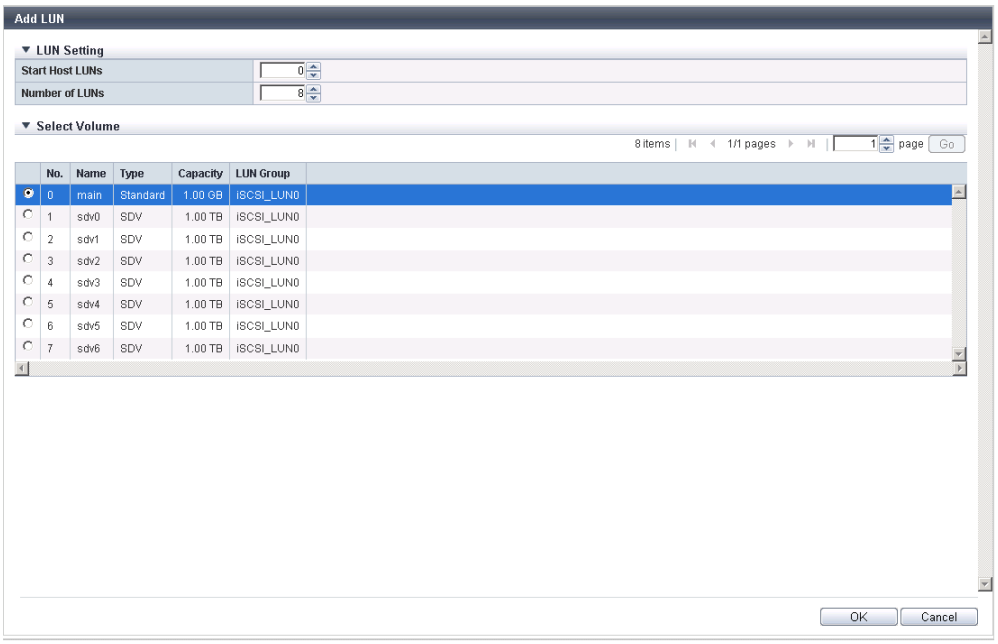
2 Click [LUN Group] in [Category] and click [Add LUN Group] in [Action].

The [Add LUN Group] screen appears.

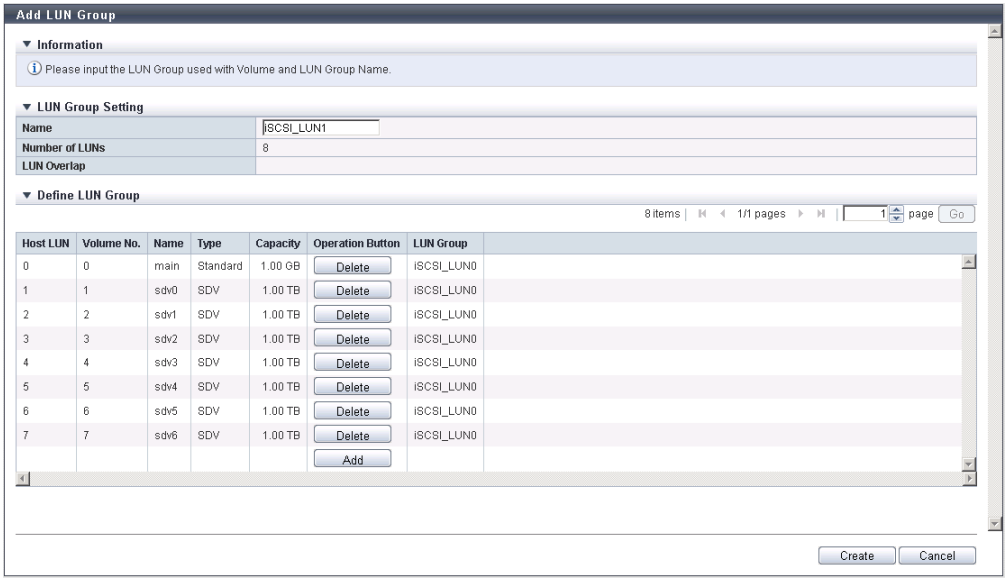
3 Enter the LUN group name in [LUN Group Setting]. Click the [Add] button in [Define LUN Group].

The [Add LUN] screen appears.

4 Enter the number for the first LUN and number of LUNs to allocate to the LUN group in [LUN Setting], select the number for the first volume to be allocated, and click the [OK] button.



The LUNs that are to be registered in the LUN group and the information for the volumes that are allocated to the LUNs are displayed.



5 Click the [Create] button.

A confirmation screen appears.

6 Click the [OK] button.

The LUN group is added and the setting completion screen appears.

7 Click the [Done] button.

The screen returns to the [LUN Group] screen that shows the settings.

End of procedure

iSCSI Port Parameter Settings

Set the connection information between the host interface port and the server.

The procedure to set the port parameters is as follows.

The setting screen that is displayed depends on the host interface port that is being used.

Set the connection information for the iSCSI ports on the ETERNUS DX and the server.

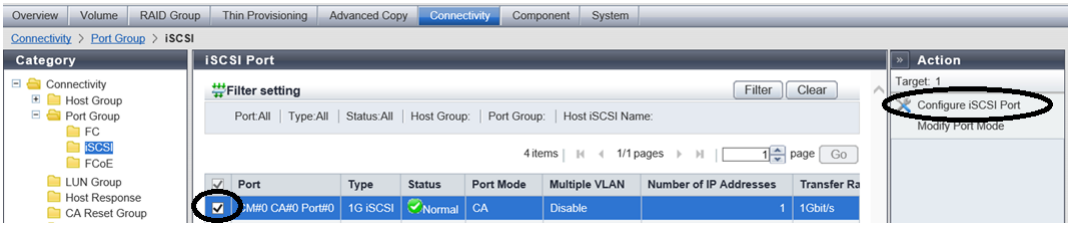
For the port parameter settings for connection using other interfaces, refer to "Configuration Guide (Web GUI)".

Procedure

1 On the navigation of the ETERNUS Web GUI screen, click the [Connectivity] tab.

2 In [Category], click [Port Group].

3 Select which iSCSI port to set the port parameters for and click [Configure iSCSI Port] in [Action].



The [Modify iSCSI Port Parameters] screen appears.

4 Select the target port, specify the items (for TCP/IP settings, iSCSI settings, basic settings, and security settings), and then click the [Set] button.

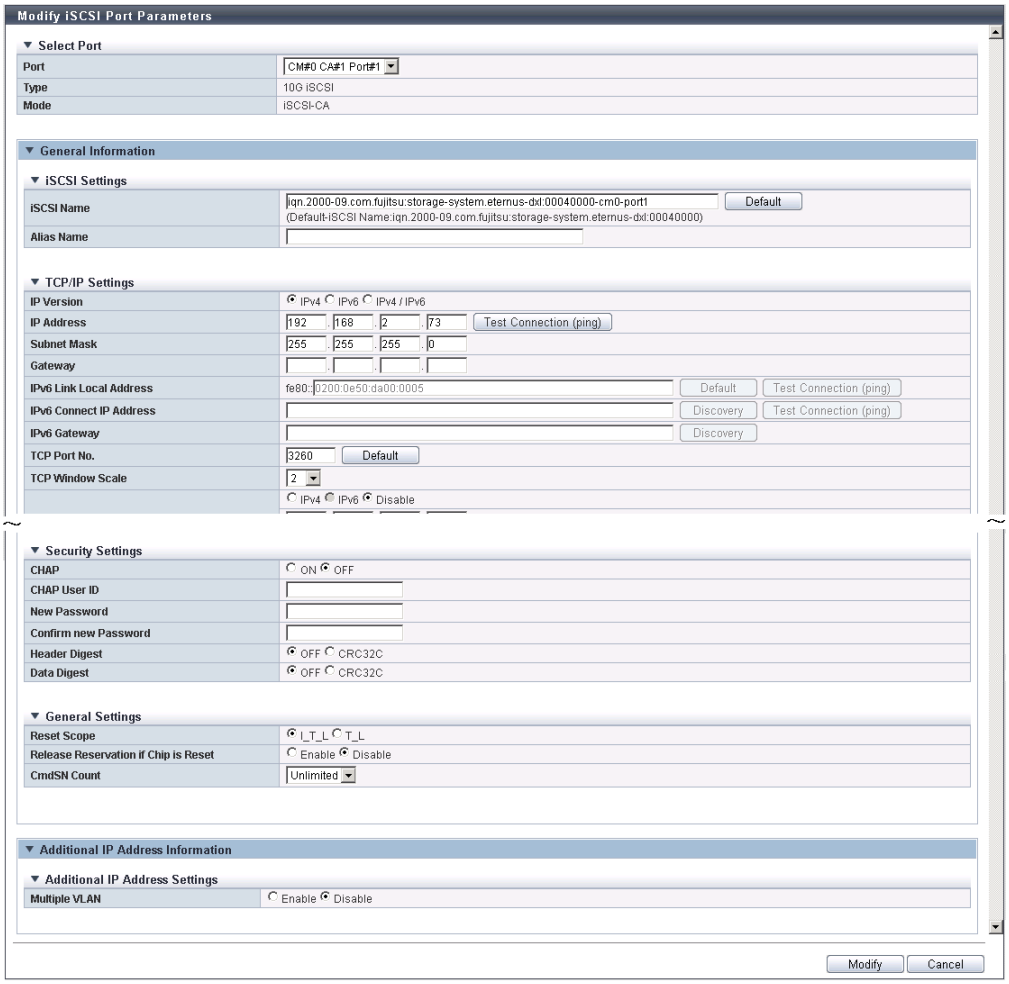
Note

- iSCSI Name can be managed more easily if the port name is added to the end of the default.
- When multiple target ports are selected, the parameters must be set for multiple ports.
  Select the port to be set from the pull-down menu.

The following items are set as shown in this example.

- Port
  CM#0 CA#0 Port#0
- IP Version
  Select an IP address type. IPv4 is used in this example.
- IP Address
  Specify an available IP address for the iSCSI network that is to be connected.
  For IPv4, the subnet mask needs to be specified.
- iSCSI Name
  For multipath connections, each name must be different.
- CHAP
  Specify [ON] to use unidirectional CHAP authentication or bidirectional CHAP authentication for the target port and [OFF] to use neither of them.

To use bidirectional CHAP authentication, the CHAP user name and password must be entered.



A confirmation screen appears.

5 Click the [OK] button.
The port parameter is set and the setting completion screen appears.

6 Click the [Done] button.
The screen returns to the [iSCSI Port Group] screen that shows the settings.

End of procedure

CA Port Group Creation

Create a CA port group for a host to access the ETERNUS DX.

A CA port group is a group of host interface ports that have the same interface and connect to the specific host group.

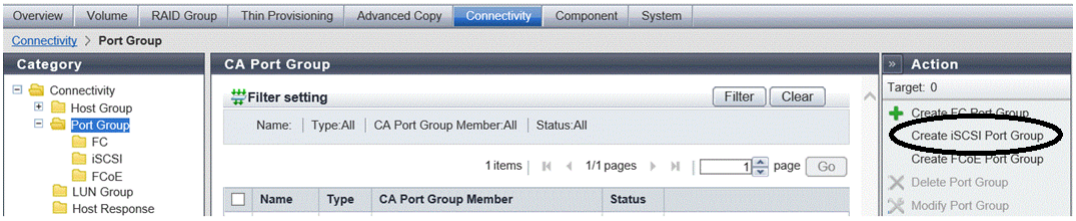
The procedure to create a CA port group is as follows:

Procedure

1 On the navigation of the ETERNUS Web GUI screen, click the [Connectivity] tab.

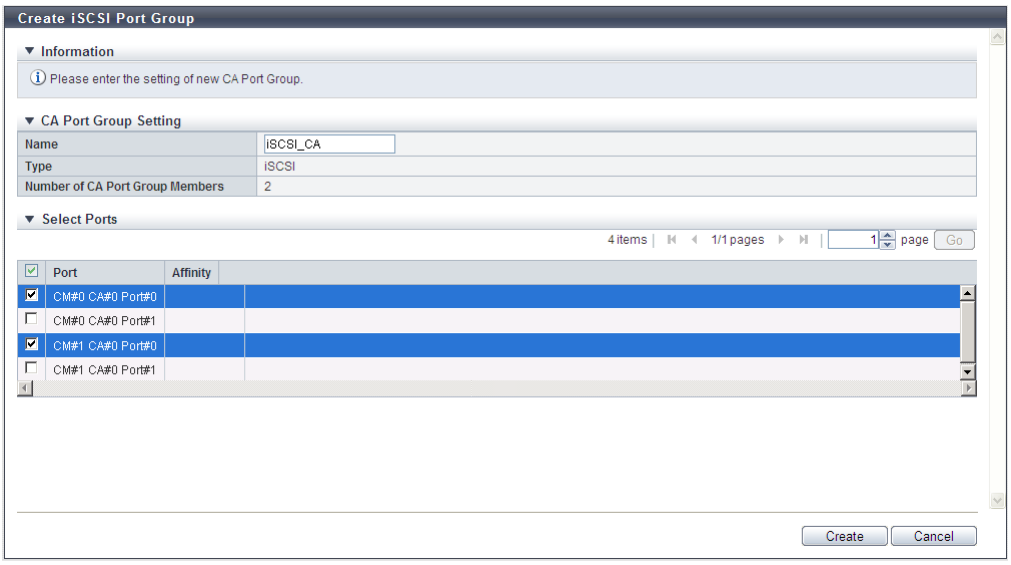
The [CA Port Group] screen appears.

2 Click [Port Group] in [Category] and click [Create iSCSI Port Group] in [Action].



The [Create iSCSI Port Group] screen appears.

3 In the [Create iSCSI Port Group] screen, enter the name of the CA port group that is to be created, select the checkbox for the ports that are to be registered in the CA port group, and click the [Create] button.



A confirmation screen appears.

4 Click the [OK] button.

The CA port group is created and the setting completion screen appears.

5 Click the [Done] button.

The screen returns to the [CA Port Group] screen that shows the settings.

End of procedure

iSCSI Host Group Addition

Add the information on the hosts (servers) that access the ETERNUS DX via the host interface port. Create a host group when adding a host.

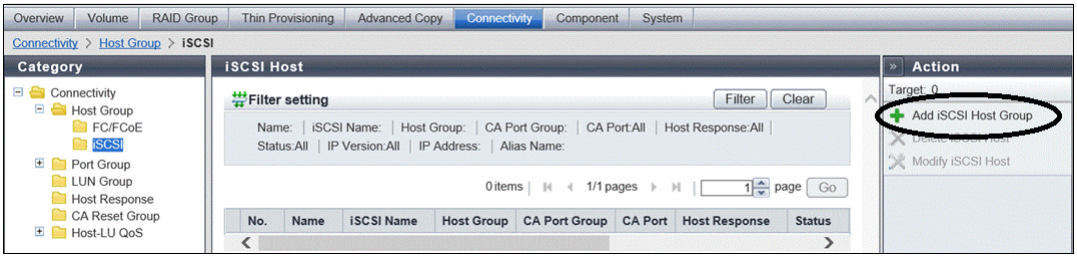
A host group is a group of HBAs that have the same host interface and access the same LUN groups.

The procedure to register a host group is as follows:

Procedure

1 On the navigation of the ETERNUS Web GUI screen, click the [Connectivity] tab.

2 Click [Host Group] in [Category] and click [Add iSCSI Host Group] in [Action].

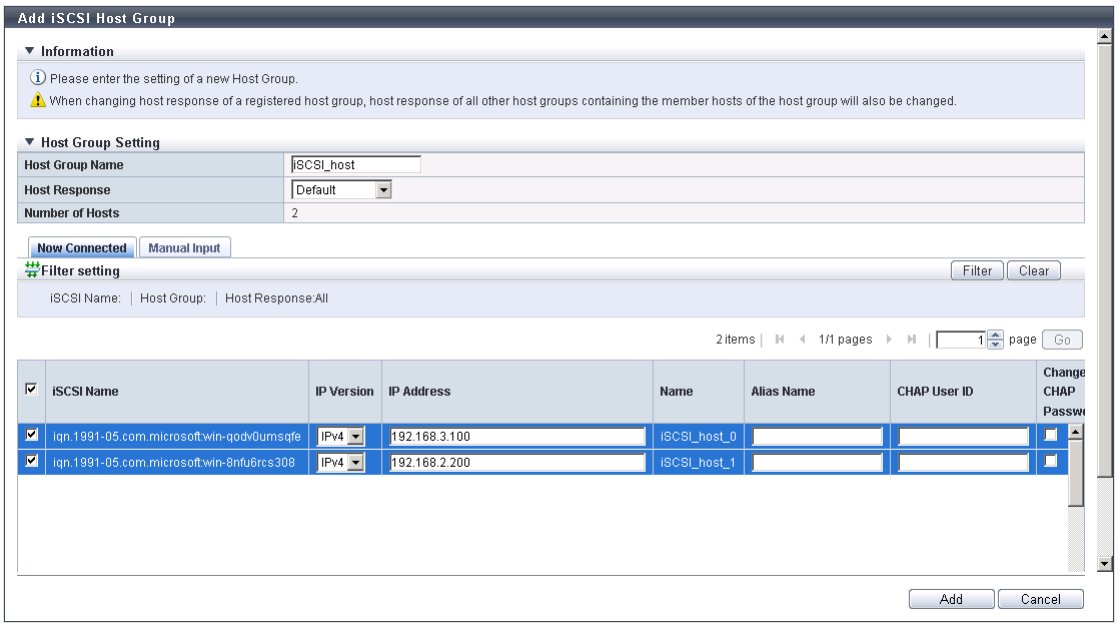


The [Add iSCSI Host Group] screen appears.

3 Specify a host group name to be created, and select a host response to be assigned to the host group.

4 Register an iSCSI host in a host group and click the [Add] button.

The following screen shot shows registration of a host by clicking the [Now Connected] tab.



A confirmation screen appears.

5 Click the [OK] button.

The iSCSI host group is added and the registration completion screen appears.

6 Click the [Done] button.
The screen returns to the [Host Group] screen that shows the settings.

End of procedure

Host Affinity Creation

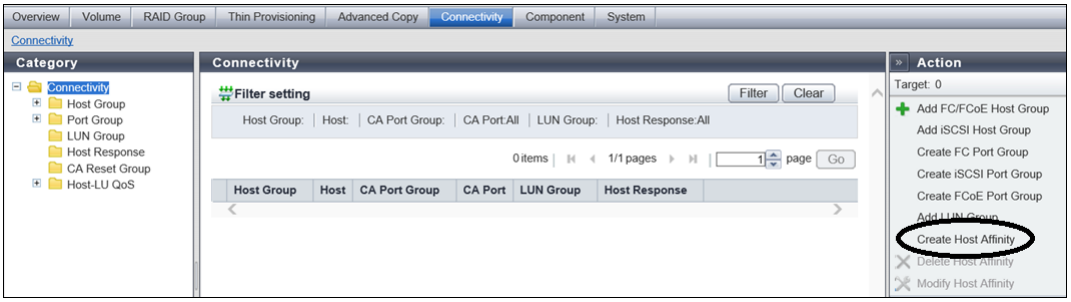
Create an association between a host group, a CA port group, and a LUN group to enable the host to recognize a LUN group.

The procedure to create a host affinity is as follows:

Procedure

1 On the navigation of the ETERNUS Web GUI screen, click the [Connectivity] tab.

2 In [Action], click [Create Host Affinity].



The [Create Host Affinity] screen appears.

3 Select "Host Group - CA Port Group" in "Target Connection".

4 Select the "Host Group", the "CA Port Group", and the "LUN Group" that are to be associated.

(1) Click the [Browse] button in [Host Group].
A screen to select the host group appears.

(2) Select "Host Group" or "All" in "Target Connection".

Note

To allow all of the hosts to recognize the LUN group, select "All".

- When "Host Group" is selected
  Select a host group that is to be associated, and click the [OK] button.
- When "All" is selected
  Select a host response, and then click the [OK] button.

(3) Click the [Browse] button in [CA Port Group].
A screen to select the CA port group appears.

(4) Select the CA port group that is to be associated and click the [OK] button.
The name of the selected CA port group is displayed in "CA Port Group".

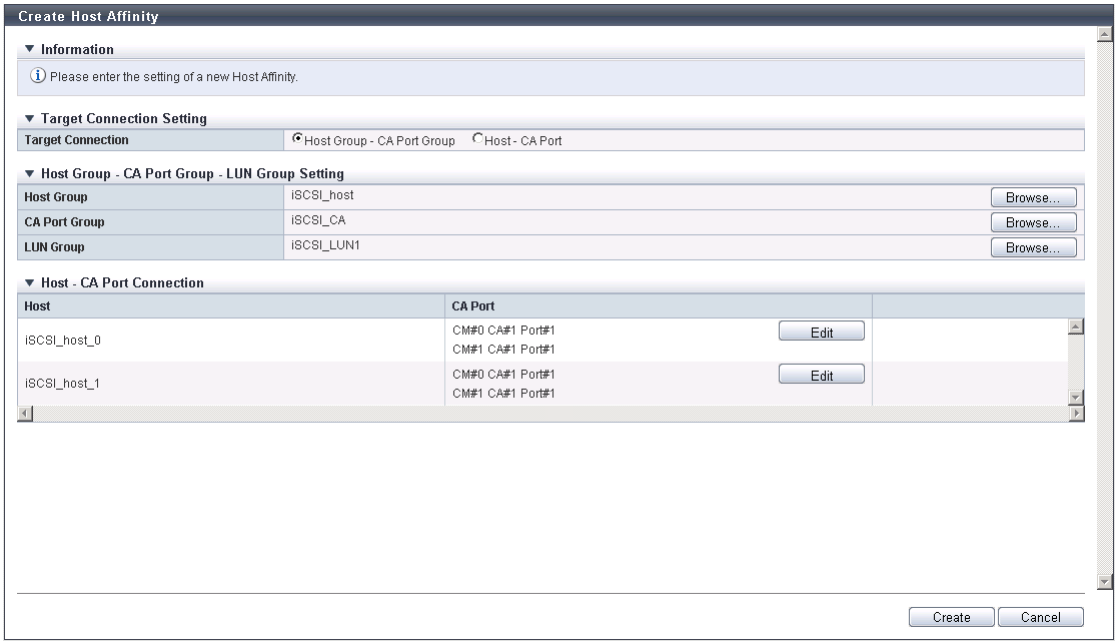
(5) Click the [Browse] button in [LUN Group].

A screen to select the LUN group appears.

(6) Select the LUN group that is to be associated and click the [OK] button.

The name of the selected LUN group is displayed in "LUN Group".

5 Check the path between the host and the host interface port on the ETERNUS DX in [Host - CA Port Connection], and click the [Create] button.



A confirmation screen appears.

6 Click the [OK] button.

The host affinity is created and the registration completion screen appears.

7 Click the [Done] button.

The screen returns to the [Connectivity] screen that shows the settings.

End of procedure

Smart Setup Wizard

With the Smart Setup Wizard, configure the settings that are required for access from the host (server) to Thin Provisioning Volumes.

To assign volumes other than Thin Provisioning Volumes to a host, refer to "Host Response Settings" (page 126) and "Host Affinity Settings" (page 127).

Caution

- The Smart Setup Wizard cannot be started for the following conditions.
  - The Thin Provisioning function is disabled.
  - An FC/iSCSI/SAS CA is not activated.
  - A Thin Provisioning Pool has not been created and the drive used to create the Thin Provisioning Pool has not been installed.
- If the host connection is iSCSI, log in to the iSCSI port of the ETERNUS DX from the host before using the Smart Setup Wizard.

  If the login operation for the iSCSI port is not performed from the host, the hosts that are connected via iSCSI are not displayed.

  For details, refer to "Configuration Guide -Server Connection- for iSCSI" for each OS.

Note

- If a Thin Provisioning Pool has not been created, the Smart Setup Wizard automatically determines the Thin Provisioning Pool configuration.
  - The priority for selecting drive types is as follows.

    SSD > SSD SED > Online > Online SED > Nearline > Nearline SED

    If multiple drive types exist, the drive type with the highest priority is selected to create a Thin Provisioning Pool.

    To create another Thin Provisioning Pool with the unselected drive types, this wizard cannot be used. Use the dedicated function provided by this storage system to create a Thin Provisioning Pool.
  - The RAID levels and the number of drives for RAID groups that configure the Thin Provisioning Pool are as follows.

Drive type	RAID level	Number of drives
SSD / SSD SED	RAID5	5 to 48
Online / Online SED / Nearline / Nearline SED	RAID6	7 to 48

  - A Global Hot Spare is registered for each Thin Provisioning Pool.
  - The same Deduplication/Compression setting as the Deduplication/Compression mode of the ETERNUS DX is applied to the Thin Provisioning Pool.
- When this wizard is used, host affinity is automatically set by using the following hosts, ports, and LUN groups.
  - All hosts selected in the [Select Host] screen
  - All the CA ports registered in the ETERNUS DX whose port mode is "CA" or "CA/RA" (if multiple types of CAs are installed in the ETERNUS DX, the selected type of CA is used)
  - The LUN groups to which all the volumes selected in the [Select Volume] screen belongs

The Smart Setup Wizard is started with one of the following ways.

- After the completion of the Initial Setup 2 wizard, the [Smart Setup Wizard] screen appears.
- Click the [System] tab and then click [Smart Setup Wizard] in [Action].

This section explains the procedure in which the Smart Setup Wizard is started from [Action] in the [System] tab and "FC" is selected for the CA type. The procedure is similar for cases where "SAS" is selected.

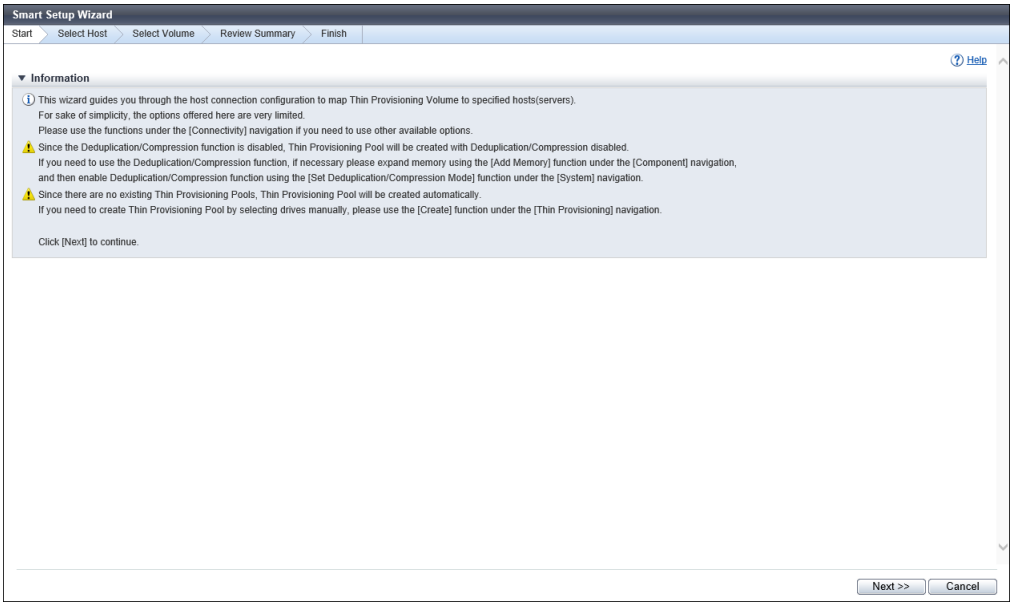
Refer to "ETERNUS Web GUI User's Guide" for the procedure if the CA type is "iSCSI".

Procedure

1 Click the [System] tab on the navigation of the ETERNUS Web GUI screen.

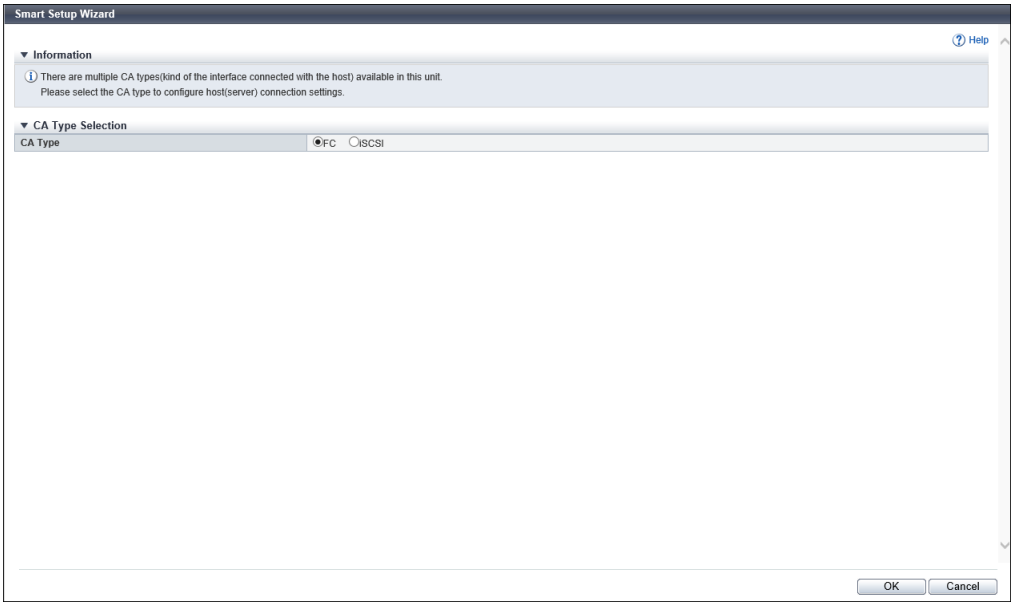
2 In [Action], click [Smart Setup Wizard].
The [Start] screen of the Smart Setup Wizard appears.

3 Click the [Next >>] button.



If multiple CA types are installed, the configuration screen for the CA type selection (Step 4) appears.
If only FC type CAs are installed, the configuration screen for the port setting (Step 5) appears.

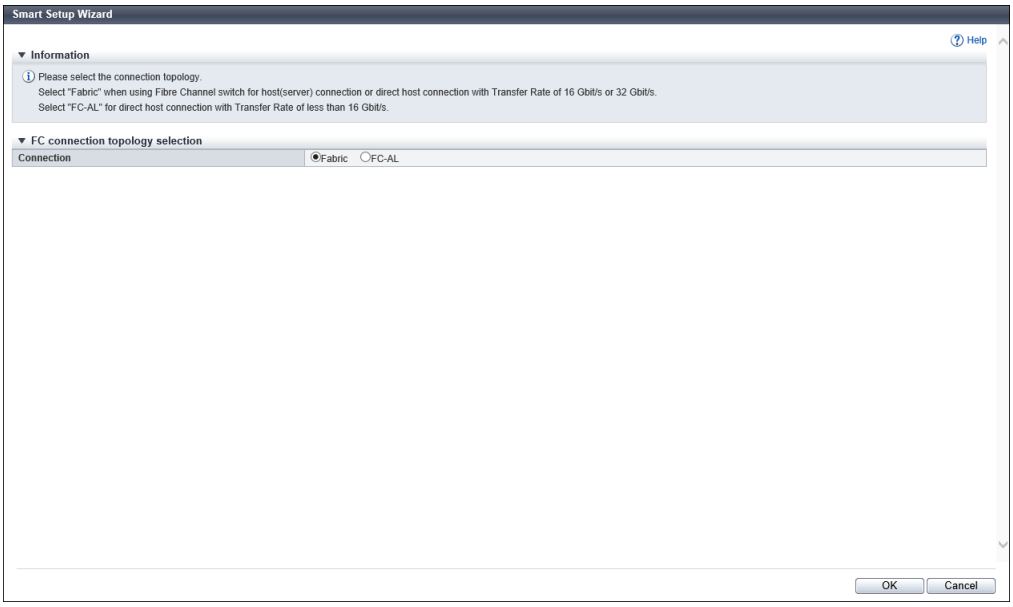
4 CA type selection
Select a CA type to connect with the host and then click the [Next >>] button.
The following shows an example in which [CA Type] is set as [FC].



5 Port setting

Select a connection topology and then click the [OK] button.

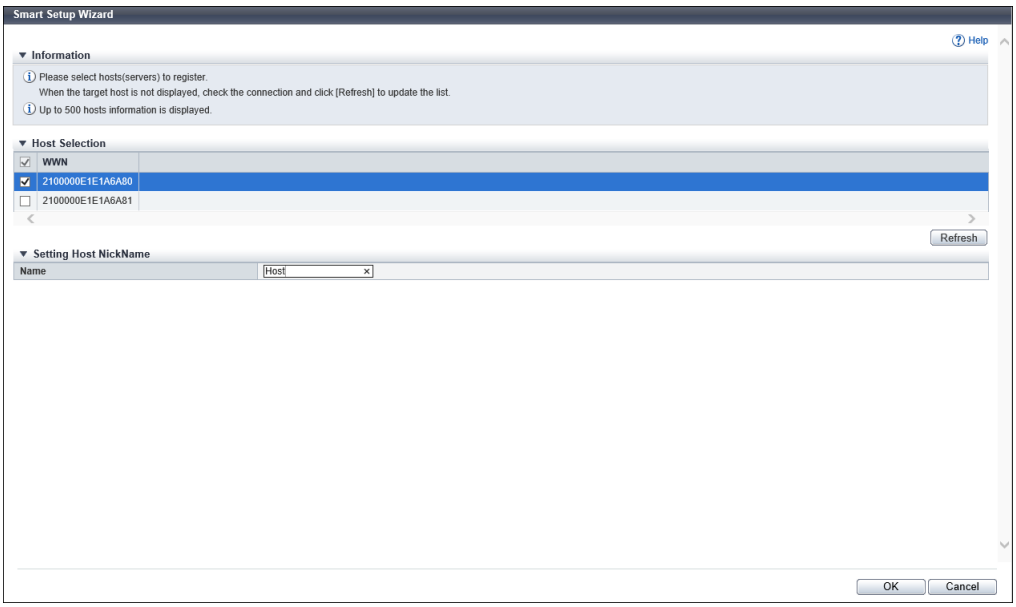
The following shows an example in which the FC port connection topology is set as [Fabric].



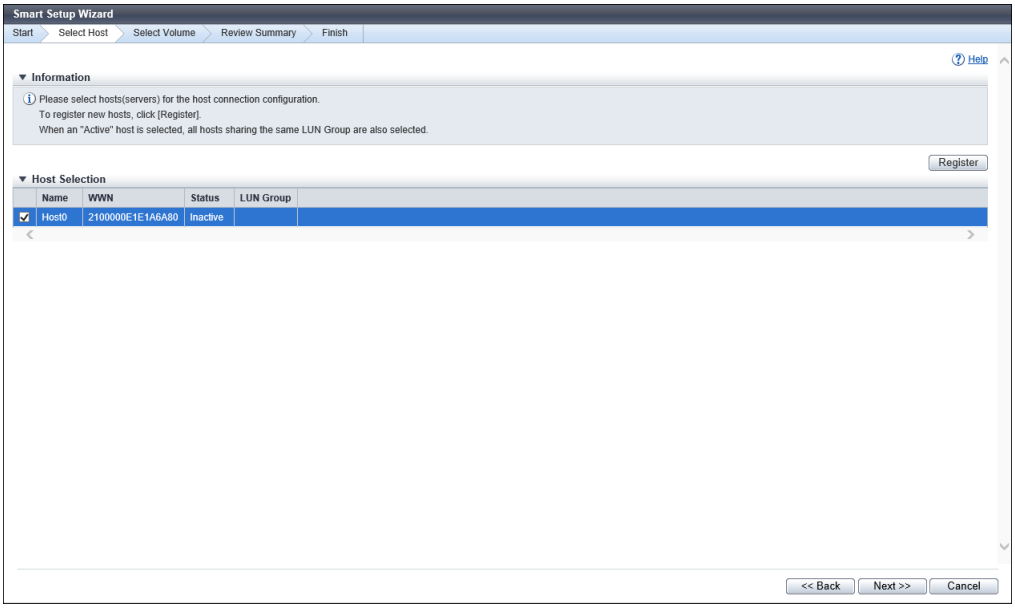
6 Host selection

(1) Click the [Register] button.

(2) Select a host to register in the ETERNUS DX from the host selection list, enter a nickname, and then click the [OK] button.



(3) Select a host to assign volumes from the host selection list and then click the [Next >>] button.



The screen for automatically creating Thin Provisioning Pool configurations (Step 7) appears.

If a Thin Provisioning Pool has been created, but no volumes are created, the configuration screen for the creation of new volumes (Step 8) appears.

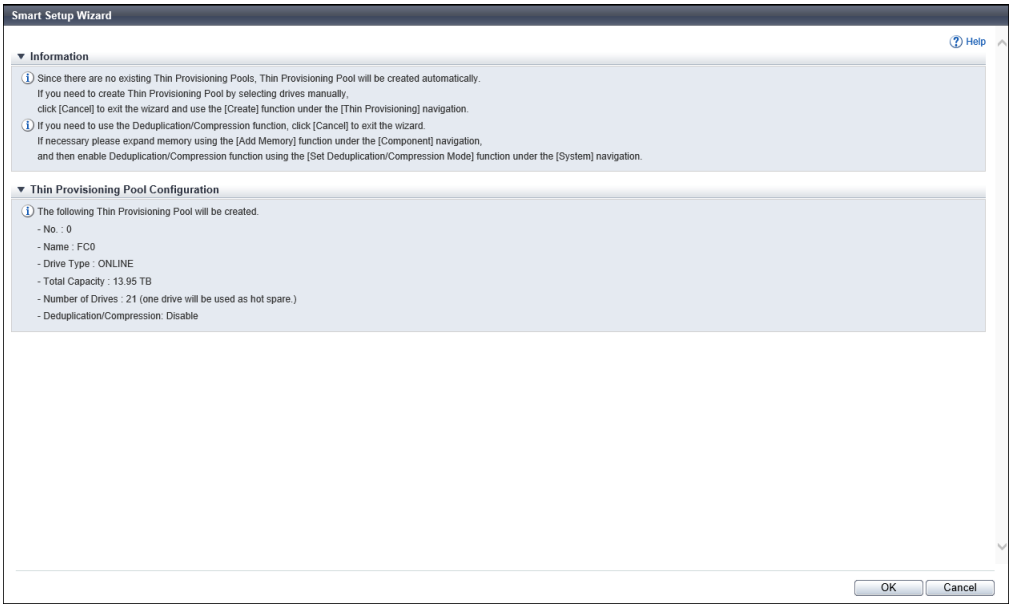
If a Thin Provisioning Pool has been created and volumes are created, [Select Volume] (Step 9) appears.

7 Automatic creation of a Thin Provisioning Pool configuration

Configuration of the Thin Provisioning pool that is automatically created is displayed.

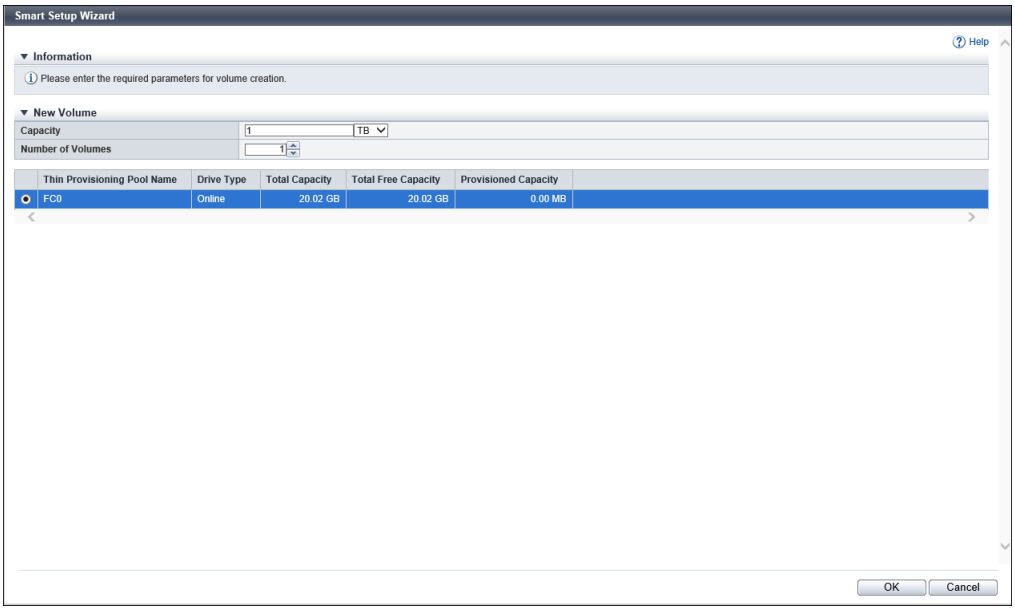
Check the configuration and click the [OK] button.

To create a Thin Provisioning Pool with a different configuration, click the [Cancel] button and exit the Smart Setup Wizard.



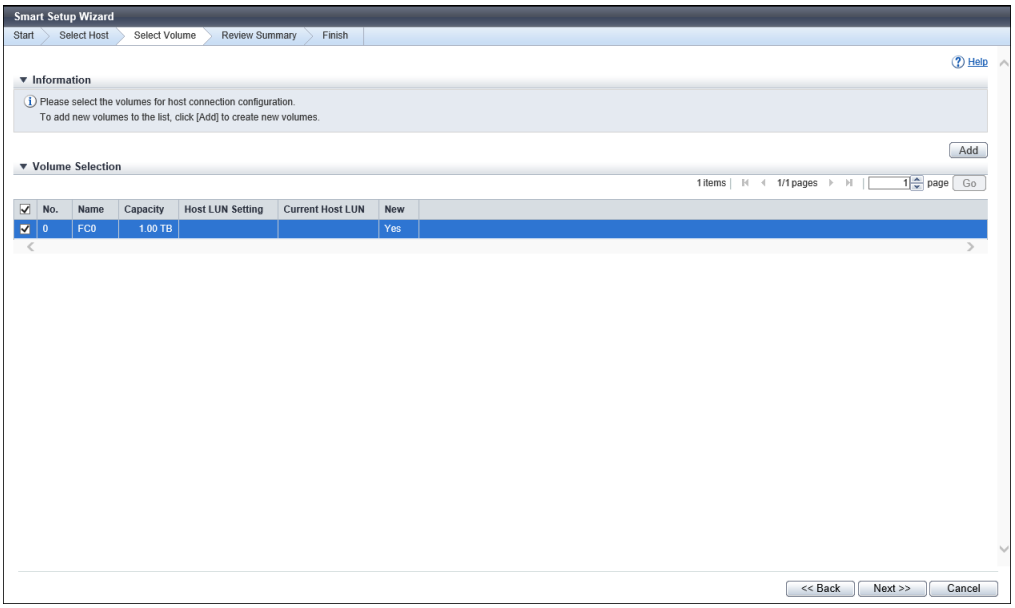
8 New volume creation

Set the capacity and number of new volumes, select the Thin Provisioning Pool where the volumes are to be created, and then click the [OK] button.



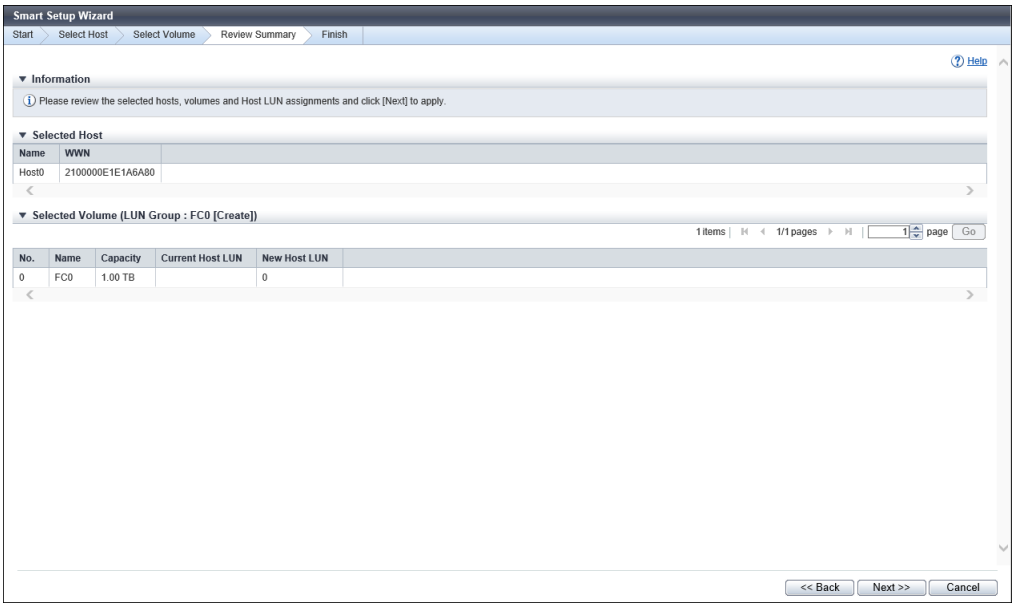
9 Volume selection

Select a volume to assign to the host and then click the [Next >>] button.



10 Configuration confirmation

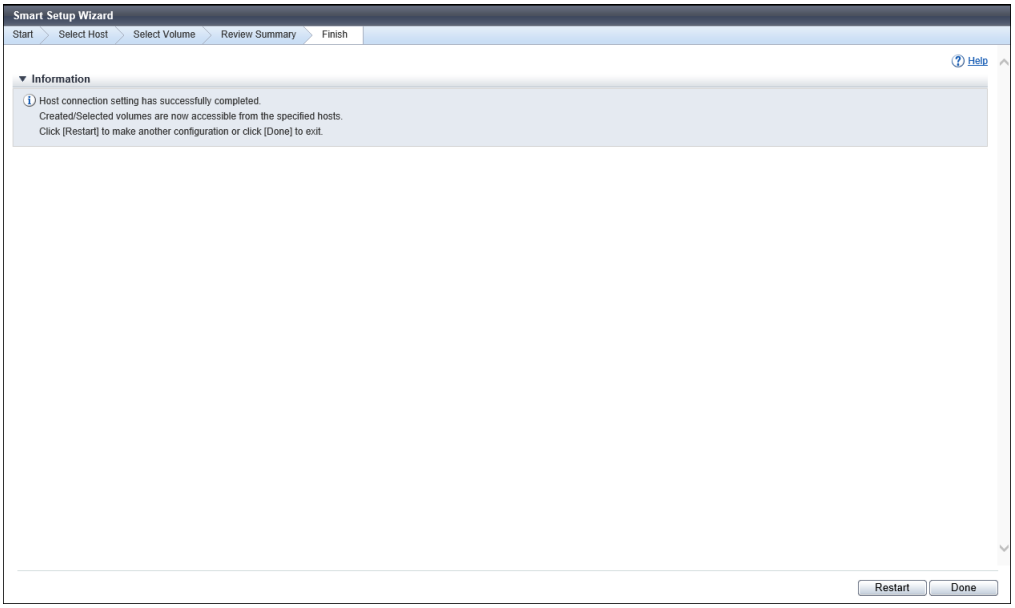
Check the displayed information and then click the [Next >>] button.



11 A confirmation screen appears. Click the [OK] button.

The configuration of the host connection and host affinity starts.

12 A configuration completion screen appears. Click the [Done] button.



End of procedure

CA Reset Group Settings

All the ports are configured to be members of one CA reset group in the initial setting.

In consideration of the range affected by inaccessible port, this function can be used to create CA reset group on only a specific port and change the member ports of an existing CA reset group.

For normal operations, the setting does not need to be changed. For the servers that require CA reset group to be set, refer to "Configuration Guide -Server Connection-" for each OS.

Procedure

1 Click the [Connectivity] tab on the navigation of the ETERNUS Web GUI screen. On the [Connectivity] screen, click [CA Reset Group] in [Category].

2 Select the CA reset group to be set. In [Action], click [Set Reset Group].
All the ports are configured in one reset group in the initial setting.

3 Set the CA reset group member ports and click the [Modify] button.

4 In the confirmation screen, click the [OK] button.

5 Click the [Done] button to return to the [CA Reset Group] screen.

End of procedure

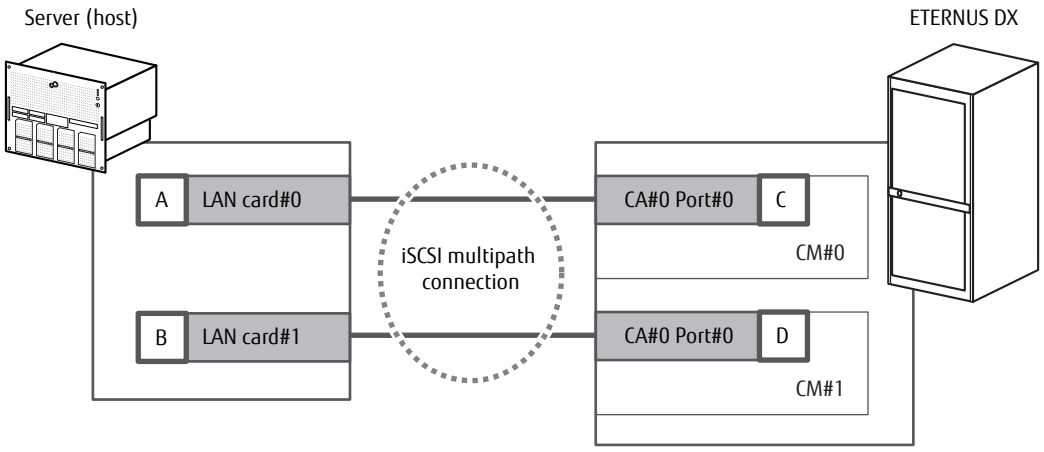
Server Connection Setup

Set up the server as required to connect to the ETERNUS DX.

The IP address to connect to the iSCSI network must be set on the server before the ETERNUS DX is connected.

After the server connection setup is completed, confirm that the volumes in the ETERNUS DX can be recognized by the server.

Figure 17 Connection Configuration with Servers



iSCSI Initiator Parameter Settings (Connection Information Settings)

Use the iSCSI Software Initiator to set the iSCSI initiator parameters.

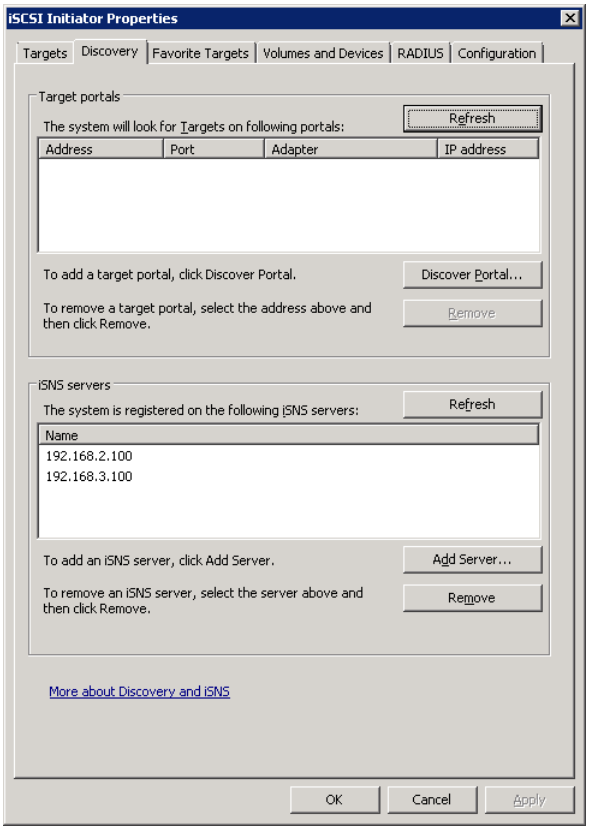
After performing the settings, check the connection to the ETERNUS DX.

Turn on the ETERNUS DX while its iSCSI port is connected to the LAN port for iSCSI connection on the server with the host interface cable. After confirming that the ETERNUS DX is in READY status, turn on the server.

Procedure

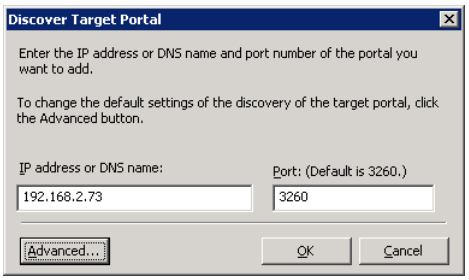
1 On the [iSCSI Initiator Properties] screen, click the [Discovery] tab.

2 In [Target portals], click the [Discover Portal] button.



3 In [IP address or DNS name] on the [Discover Target Portal] screen, specify the IP address of "CM#0 CA#0 Port#0" of the ETERNUS DX (C in Figure 17).

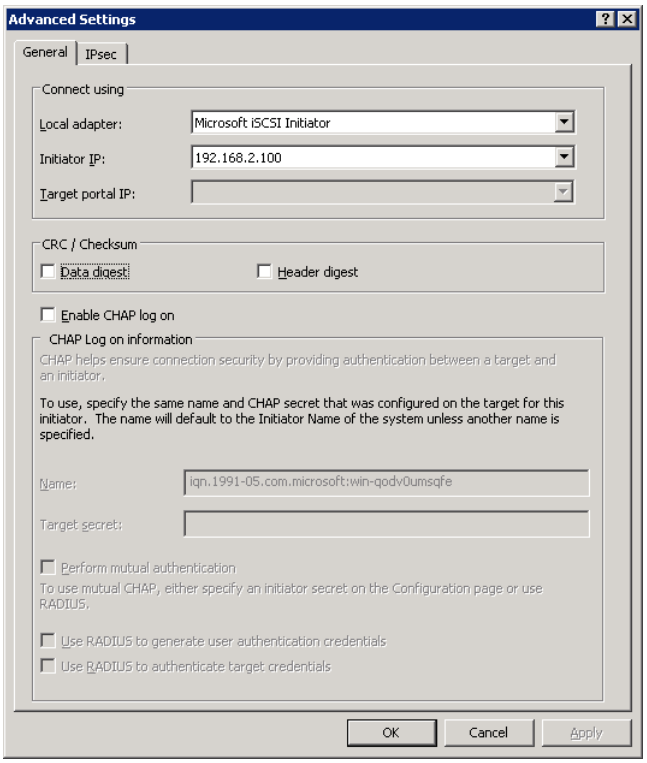
When the port number on the ETERNUS DX is changed, the value set in [Port] must be changed.



4 Click the [Advanced] button.

5 On the [Advanced Settings] screen, click the [General] tab.

6 Specify the following items under [Connect using].
Local adapter: Microsoft iSCSI Initiator
Initiator IP: IP address of the server (A in Figure 17)
When setting access restrictions, the settings related to CHAP authentication is required.
For details on CHAP authentication, refer to "Configuration Guide -Server Connection-".
To enable mutual authentication, select [Perform mutual authentication].

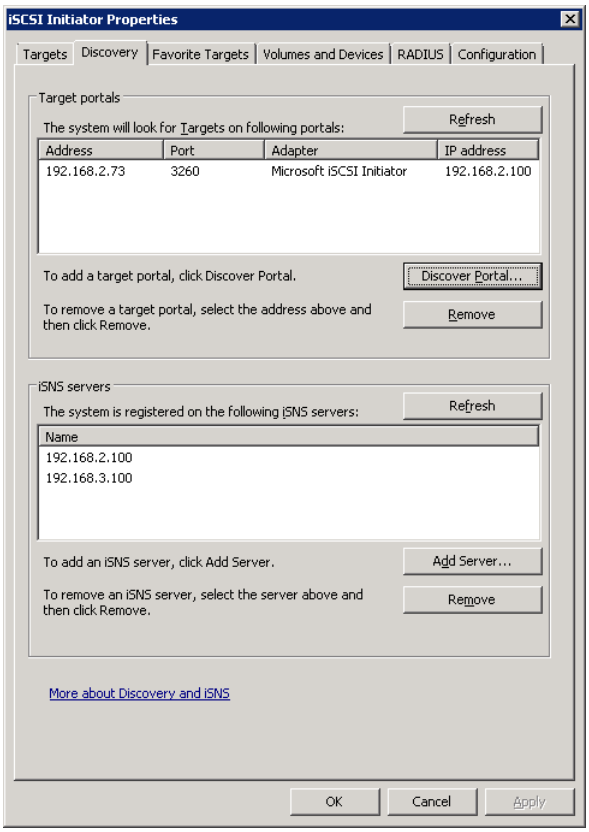


7 Click the [OK] button.
The screen returns to the [Discover Target Portal] screen.

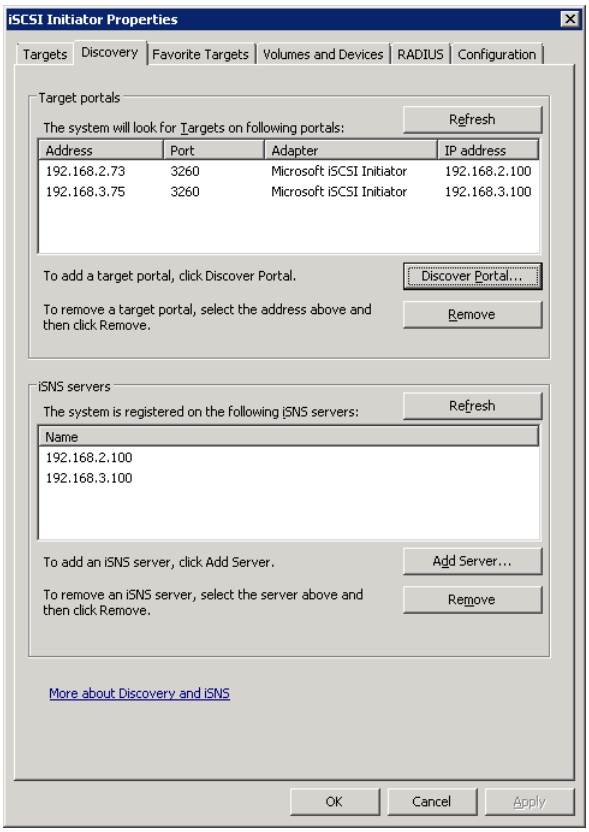
8 Click the [OK] button.

9 On the [iSCSI Initiator Properties] screen, click the [Discovery] tab.

Confirm that the specified settings are correctly reflected to [The system will look for Targets on following portals].



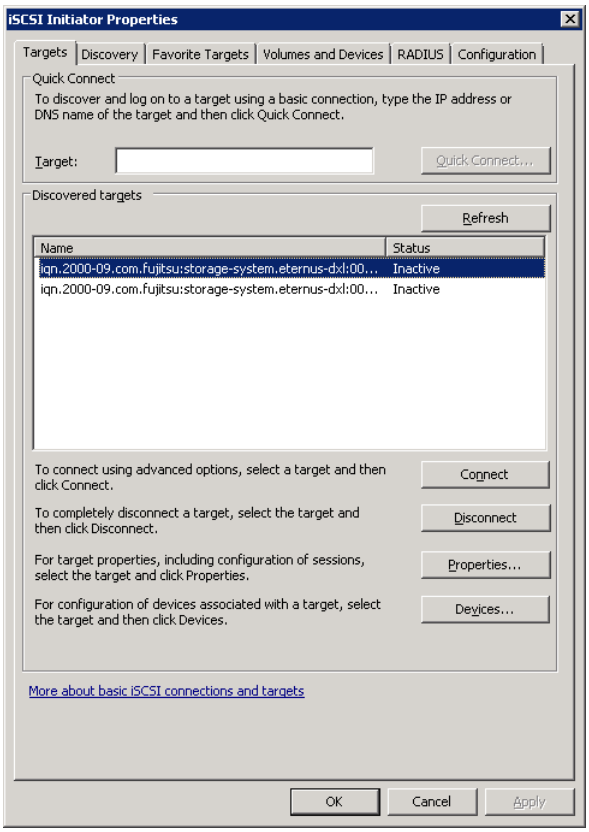
10 In the same way, repeat Step 3 through Step 9 to specify the IP address of the other LAN card (B in Figure 17) on the server and the IP address of "CM#1 CA#0 Port#0" (D in Figure 17) for the ETERNUS DX.



11 On the [iSCSI Initiator Properties] screen, click the [Targets] tab.

Confirm whether the specified contents in [The system will look for Targets on following portals] have been applied correctly before checking connection.

12 Confirm that the ETERNUS DX iSCSI name is displayed in [Discovered targets] and that the [Status] is [Inactive].

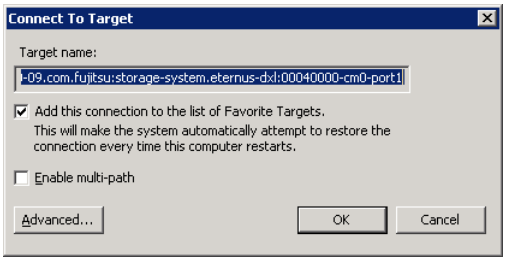


13 Select the iSCSI name that is to be the connection target, and click the [Connect] button.

In this example, "CM#0 CA#0 Port#0" with an iSCSI name that is specified in "iSCSI Port Parameter Settings" (page 129) is the target.

[Connect To Target] appears.

14 Confirm the controller number at the end of the target name and click the [Advanced] button.

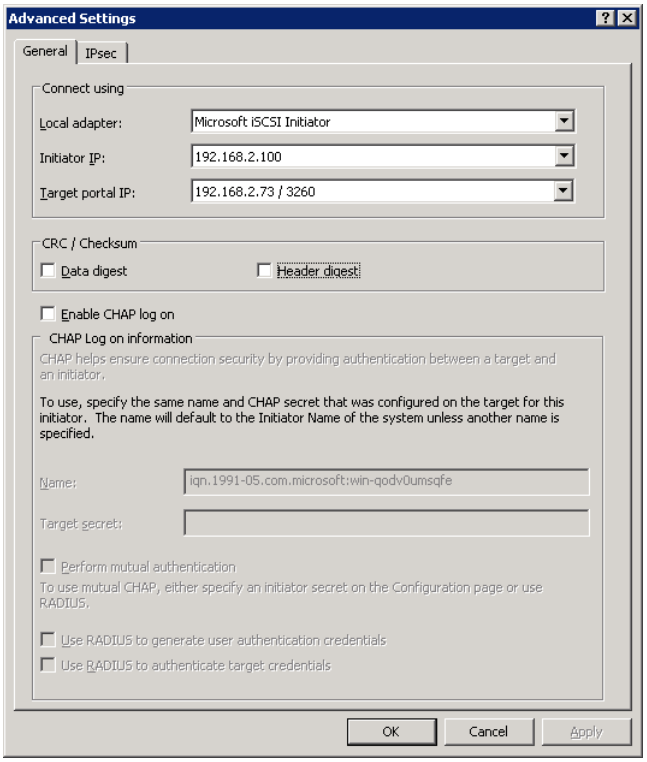


15 On the [Advanced Settings] screen, specify the following items under [Connect using] and click the [OK] button.

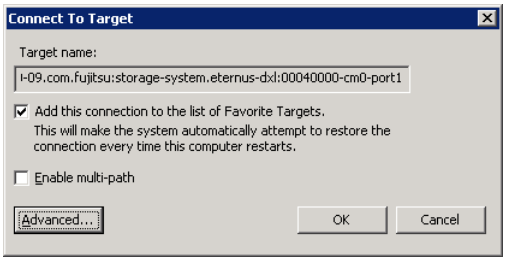
Local adapter: Microsoft iSCSI Initiator

Initiator IP: IP address of the server (A in Figure 17)

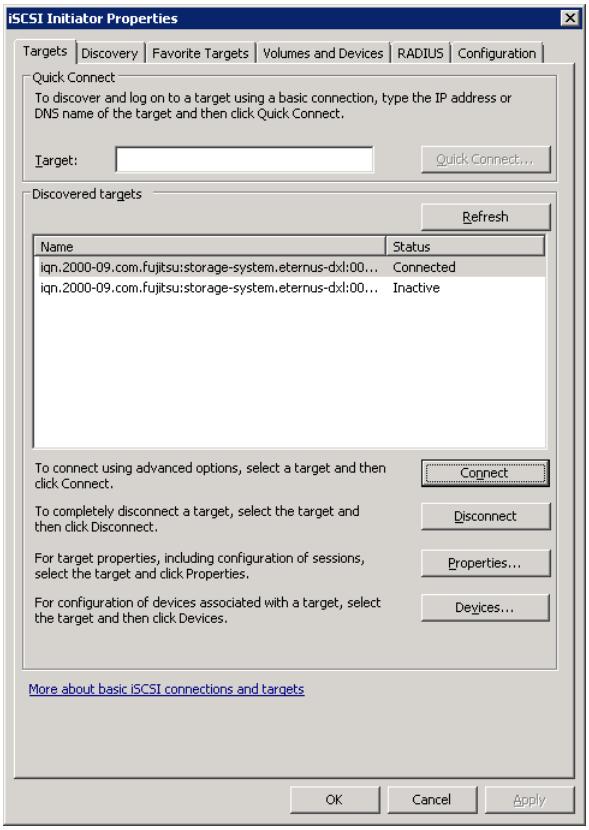
Target portal IP: IP address of the ETERNUS DX (C in Figure 17)



16 Confirm that the [Add this connection to the list of Favorite Targets.] checkbox is selected and click the [OK] button.

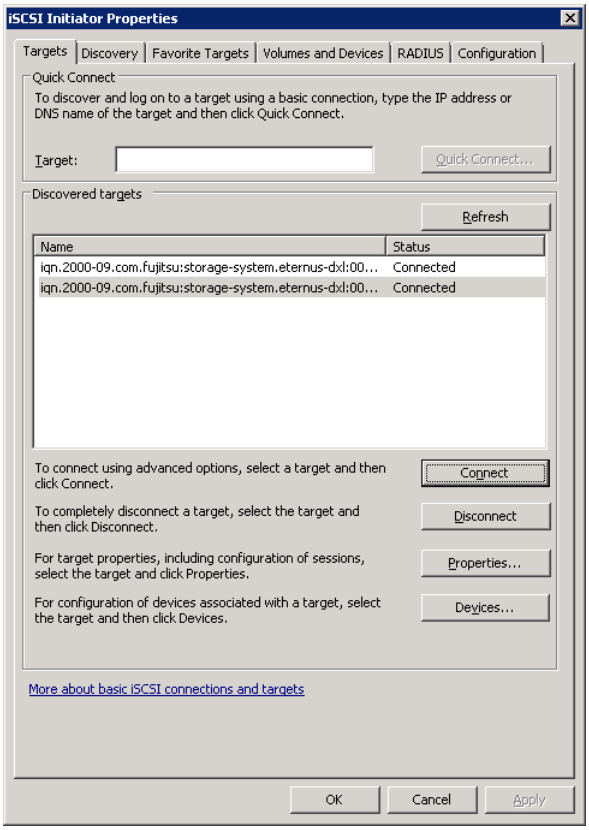


17 On the [iSCSI Initiator Properties] screen, confirm that [Status] has changed to [Connected].



18 In the same way, repeat Step 11 and later steps for the other target.
Initiator IP: IP address of the server (B in Figure 17)
Target portal IP: IP address of the ETERNUS DX (D in Figure 17)

19 Confirm that [Status] of the two targets has changed to [Connected] and click the [OK] button.



End of procedure

LUN Recognition Check

When connection is completed, confirm that the server recognizes the LUN set to the ETERNUS DX.

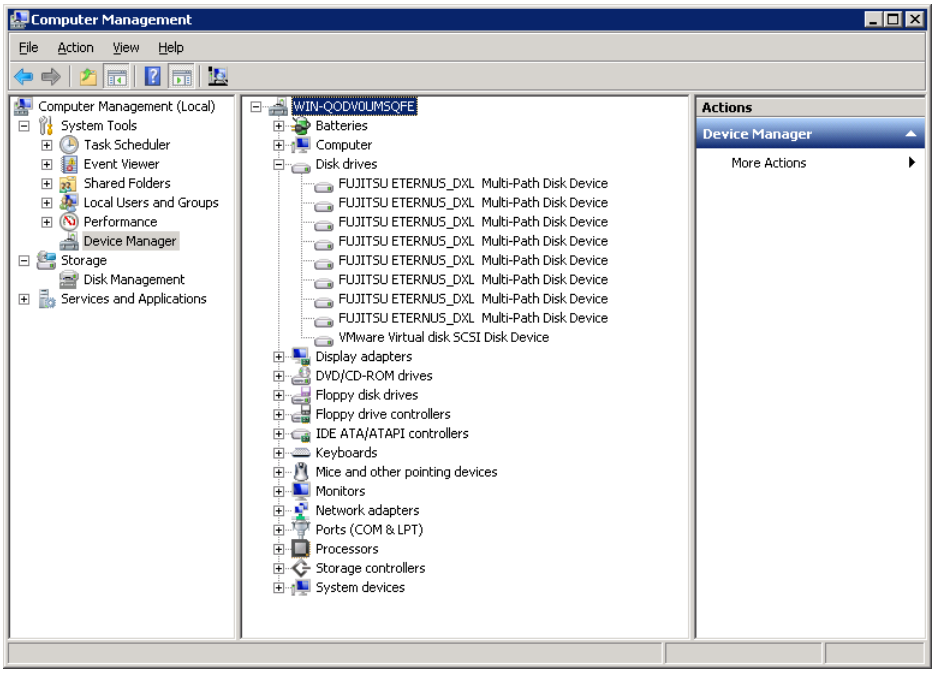
When Checking Using the Windows Device Manager

The following procedure explains how to check LUN using the Windows Device Manager.

Procedure

1 Open [Device Manager] and expand [Disk drives].

2 Confirm that the same number of "FUJITSU..." items are displayed as the number of LUNs that are set.



If the example is used, eight "FUJITSU..." items are displayed.

End of procedure

When Checking Using the ETERNUS Multipath Driver

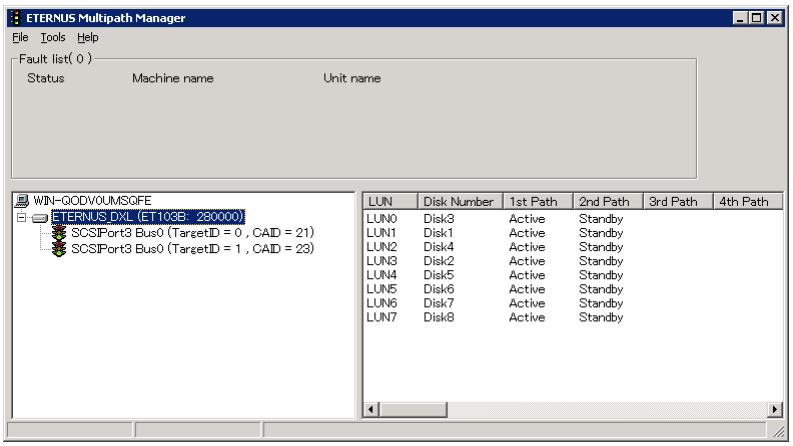
The following procedure explains how to check LUNs with the ETERNUS Multipath Driver.

Procedure

1 Click the [Start] button, expand [ETERNUS Multipath Driver] from [All Programs], and open [ETERNUS Multipath Manager].

2 Confirm that the same number of LUNs are displayed as the number of LUNs that are set.

If the LUNs for the ETERNUS DX storage systems are recognized by the server, the devices (LUNs) in the ETERNUS DX storage systems are displayed under LUN and Disk Number.



Note

The host interface (CA) numbers of the ETERNUS DX are displayed on ETERNUS Multipath Driver as shown below.

CM#0 CA#0 Port#0 → CAID = 00	CM#1 CA#0 Port#0 → CAID = 02
CM#0 CA#0 Port#1 → CAID = 01	CM#1 CA#0 Port#1 → CAID = 03
CM#0 CA#1 Port#0 → CAID = 20	CM#1 CA#1 Port#0 → CAID = 22
CM#0 CA#1 Port#1 → CAID = 21	CM#1 CA#1 Port#1 → CAID = 23

End of procedure

Disk Partition Settings

Set up disk partitions to use the specified LUNs for the ETERNUS DX.

The volumes are recognized as disks in order, starting from the volume that is set for LUN0.

For example, if LUN0 is recognized as Disk 1, LUN1 is recognized as Disk 2 and LUN2 as Disk 3.

Perform the settings as shown below.

Drive	File system that is to be created	LUN	Volume No.	Volume name	Type	Capacity (*1)
F	NTFS	0	0	main	Standard	1TB
G	RAW	1	1	sdv0	SDV	(1TB)
H	RAW	2	2	sdv1	SDV	(1TB)
I	RAW	3	3	sdv2	SDV	(1TB)
J	RAW	4	4	sdv3	SDV	(1TB)
K	RAW	5	5	sdv4	SDV	(1TB)
L	RAW	6	6	sdv5	SDV	(1TB)
M	RAW	7	7	sdv6	SDV	(1TB)

***1:** The capacity that is displayed in "( )" is the copy source capacity.

For the operation volume (Standard), perform "■ Operation Disk Settings" (page 156) in "Disk Settings" (page 156).

For the volume for generation copy (Snap Data Volume), perform "■ SnapOPC+ Destination Settings" (page 159) in "Disk Settings" (page 156).

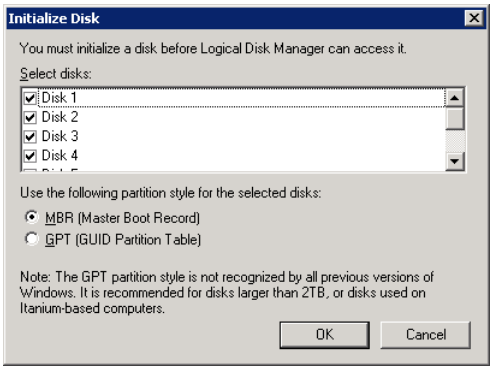
Disk Recognition

The following procedure explains how to create a disk partition.

Procedure

1 Select [Disk Management] from [Computer Management].

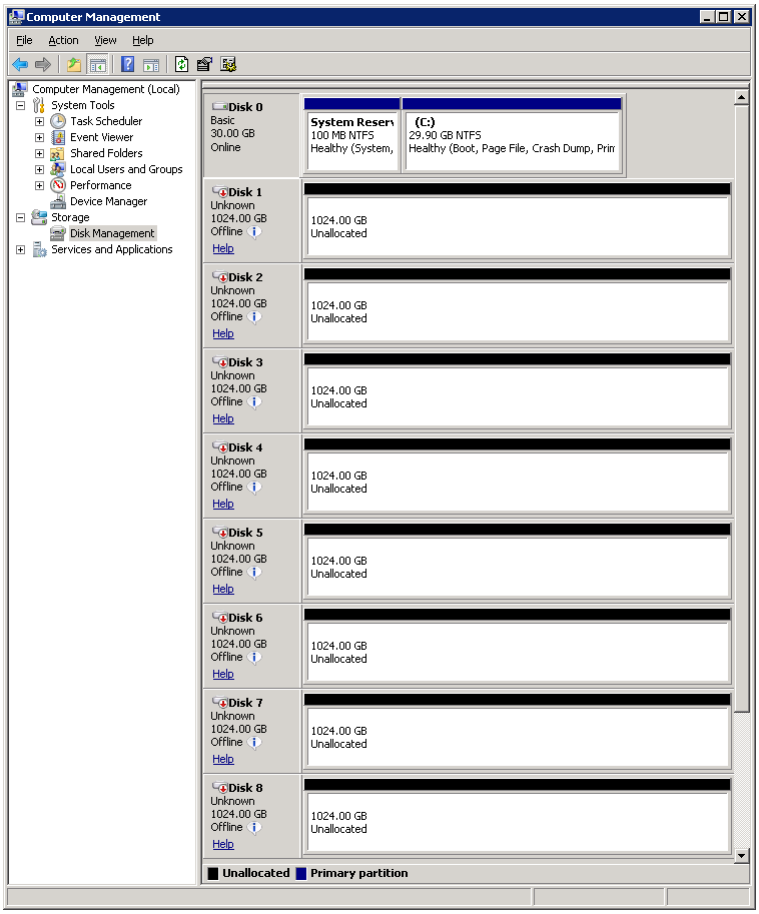
2 If the [Initialize Disk] screen appears, confirm that all the disks are selected and click the [OK] button. Then proceed to Step 6.



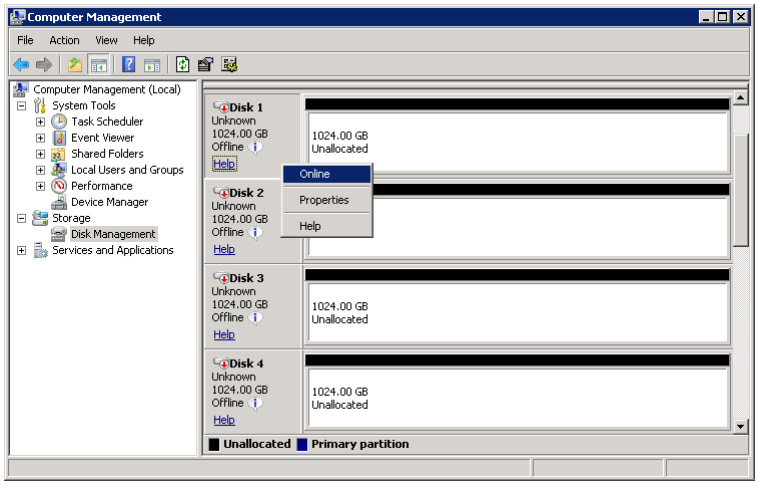
Select the checkbox for eight disks in this example.

When Windows Server 2008 Enterprise is used, [Initialize Disk] does not appear. Perform the steps from Step 3 onwards.

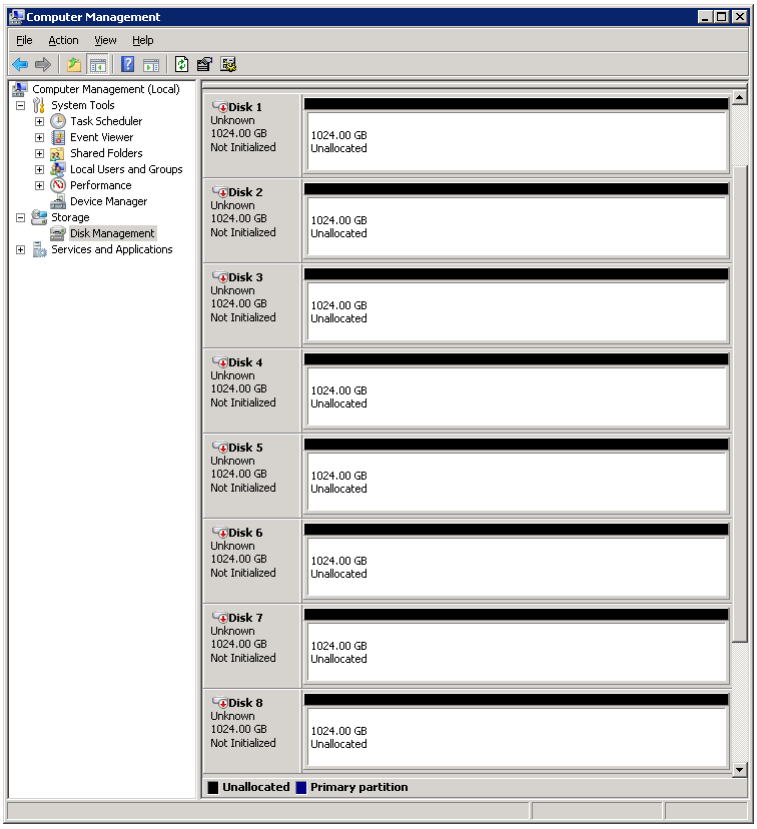
The LUNs that are set with the ETERNUS DX are recognized as [Offline].



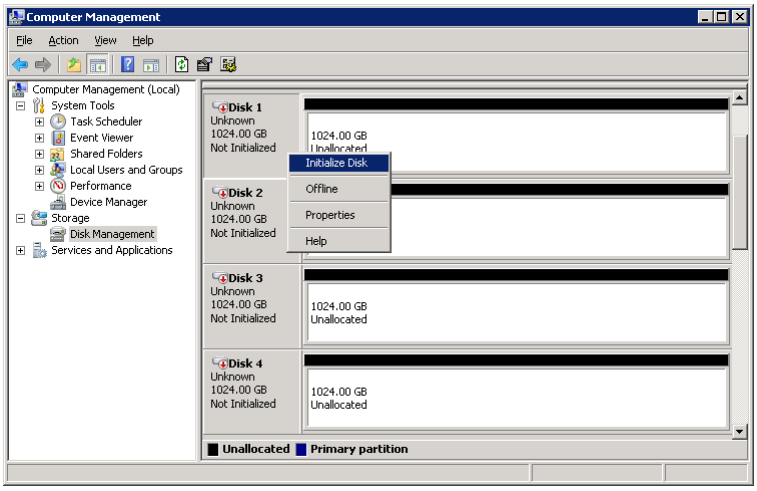
3 Right-click all the disks displayed as offline, and select [Online].



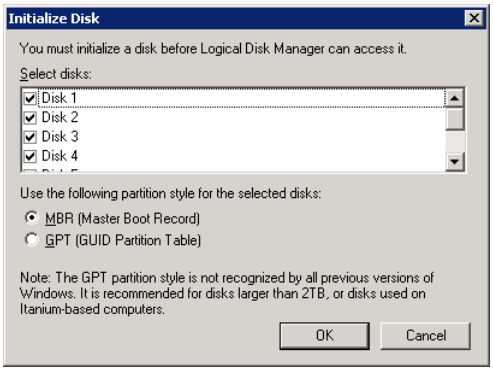
[Offline] changes to [Not Initialized].



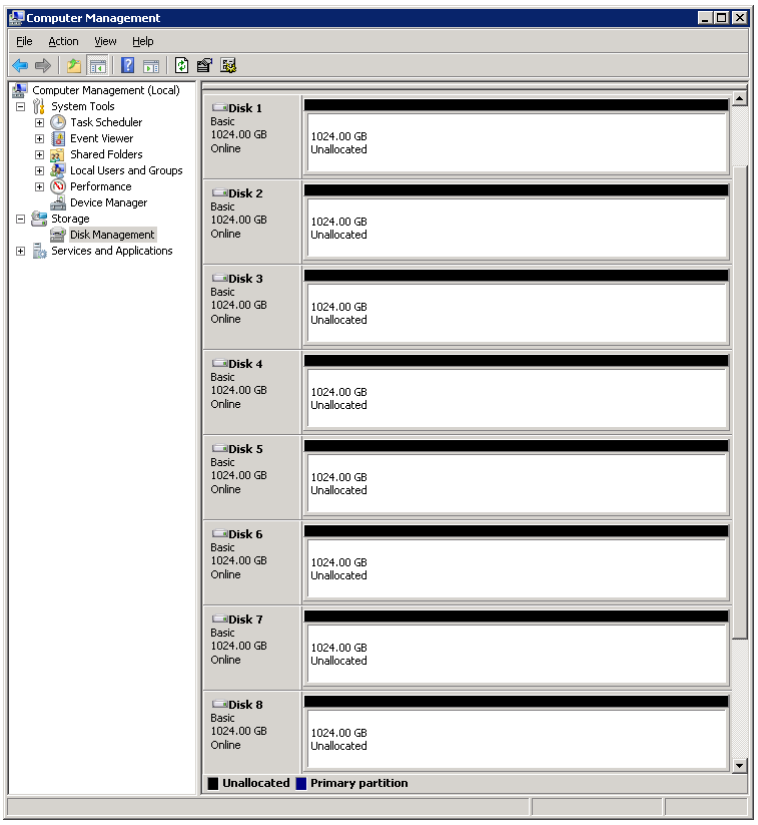
4 Right-click all the disks to be changed to online, and select [Initialize Disk].



5 When the [Initialize Disk] screen appears, confirm that all the disks are selected and click the [OK] button.



6 Confirm that the initialized disks are displayed as [Online].



End of procedure

Disk Settings

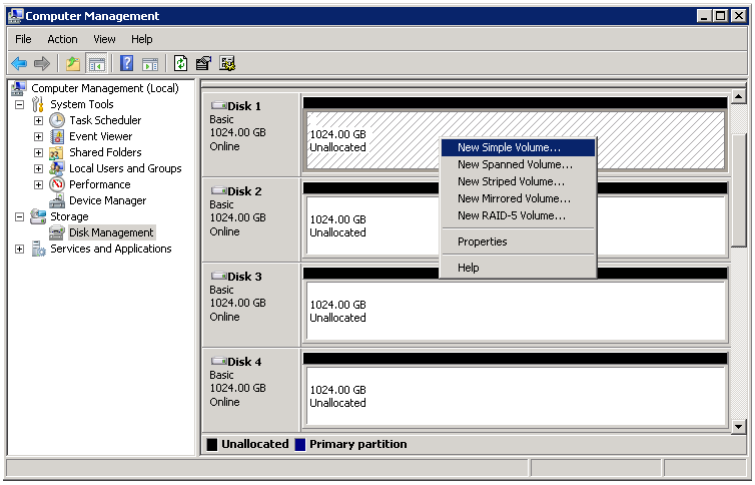
After initialization is complete, create a file system in a disk with offline status.

■ Operation Disk Settings

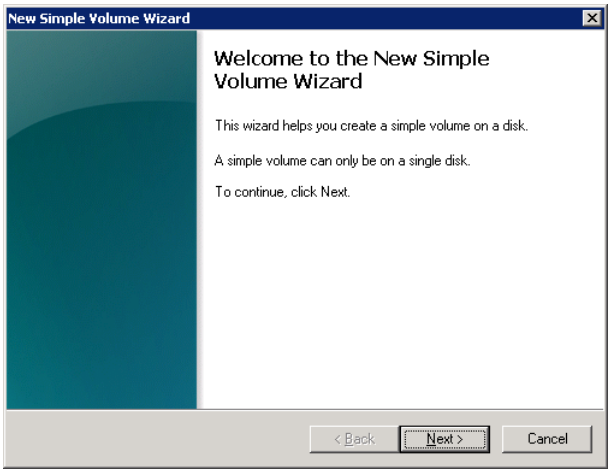
The following procedure explains how to set up the operation disk.

Procedure

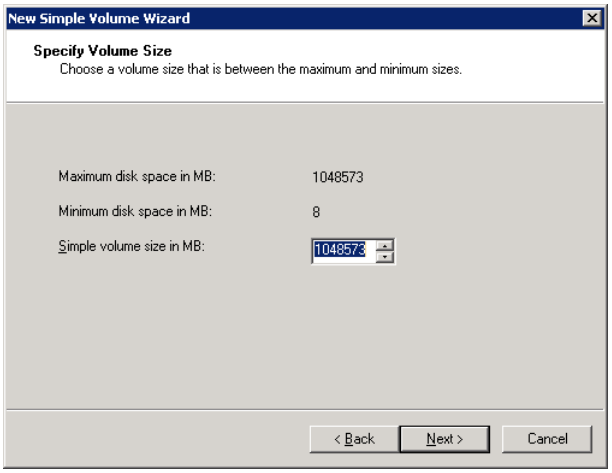
1 Select [Disk Management] from [Computer Management].



2 On the [New Simple Volume Wizard] screen, click the [Next] button.



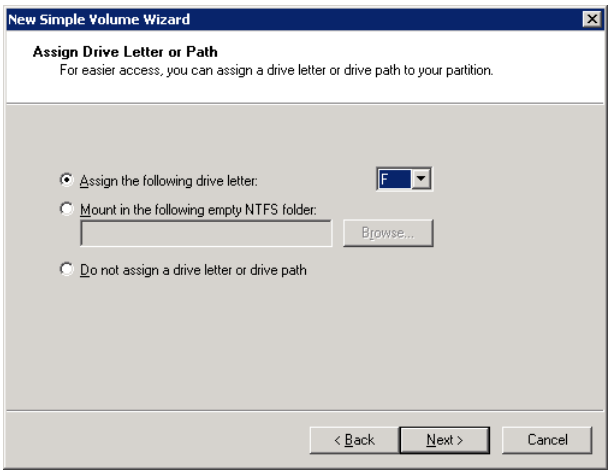
3 Specify the capacity in [Specify Volume Size], and click the [Next] button.



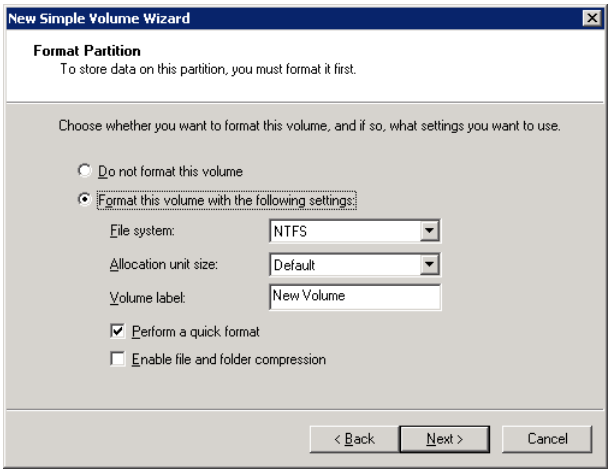
Set the capacity assuming "LUN size = drive size" for this example.

4 When [Assign Drive Letter or Path] appears, assign a drive letter and click the [Next] button.
Perform the settings as shown below.

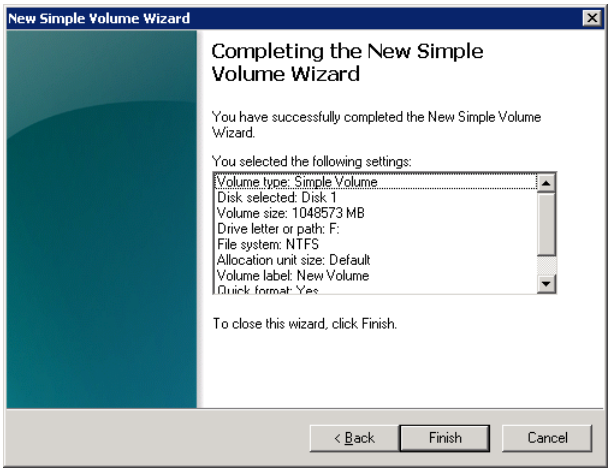
Drive	File system that is to be created	LUN	Volume No.	Volume name	Type	Capacity
F	NTFS	0	0	main	Standard	1TB



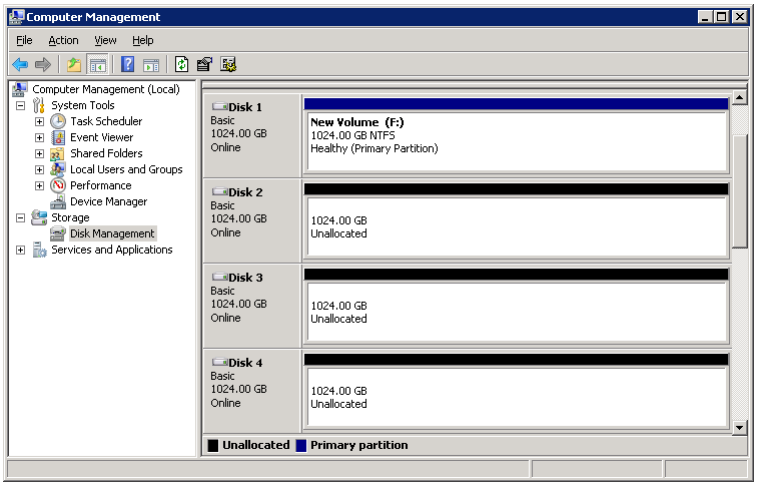
5 [Format Partition] appears. Click the [Next] button.



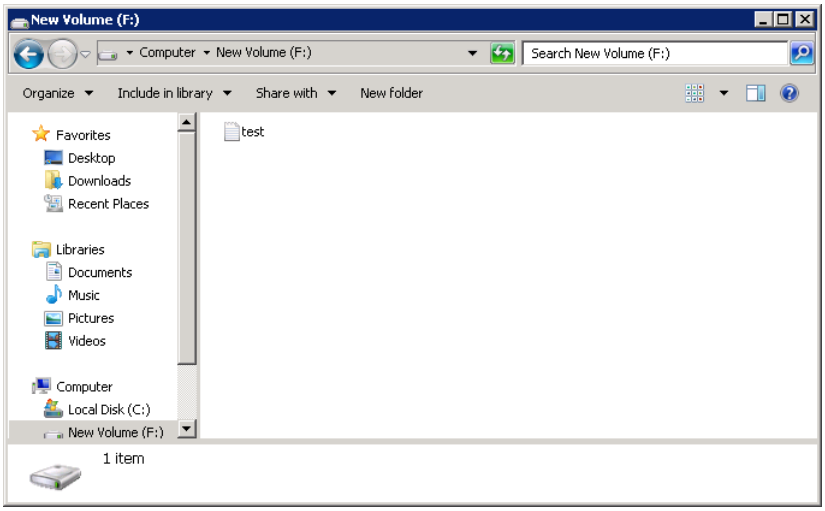
6 [Completing the New Simple Volume Wizard] appears. Click the [Finish] button.



7 Check that the specified settings are displayed correctly.



8 Check whether a file or other item can be created in the created drive.



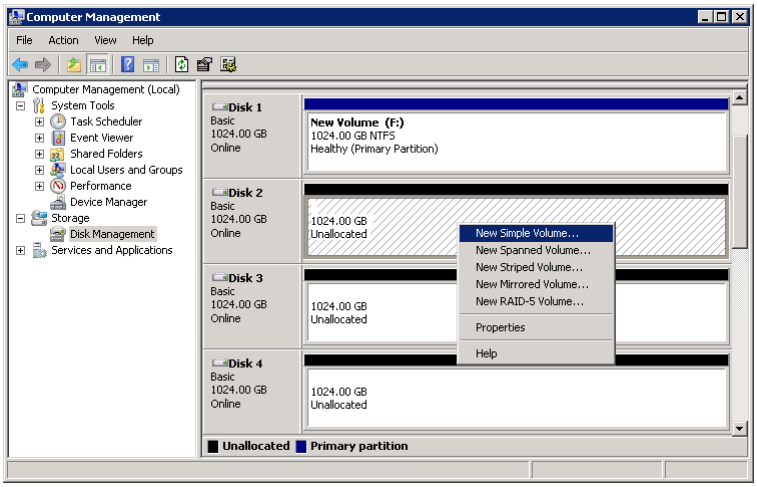
End of procedure

■ SnapOPC+ Destination Settings

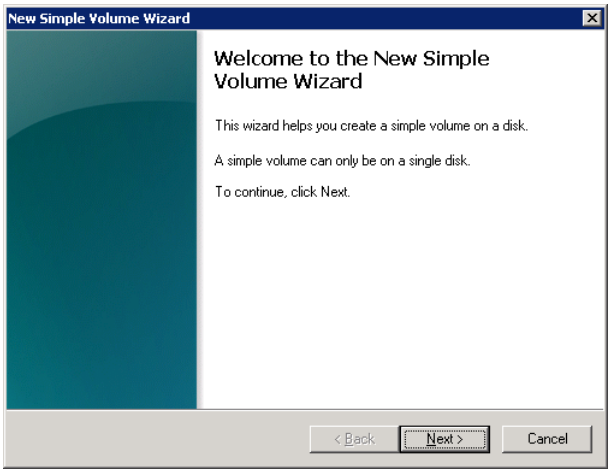
Set up the disk created in [Snap Data Volume].

Procedure

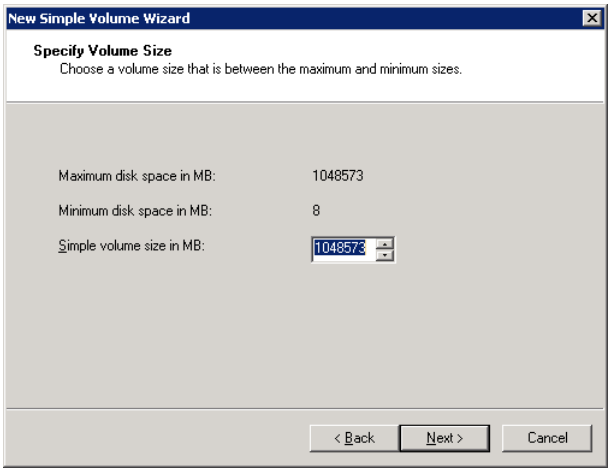
1 During volume creation, right-click the disk created in [Snap Data Volume] and select [New Simple Volume].



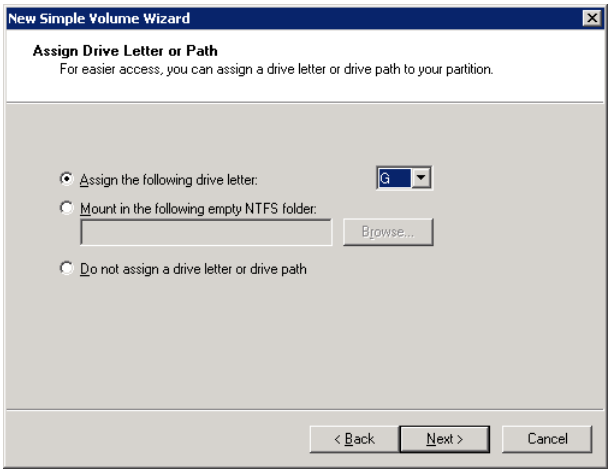
2 [New Simple Volume Wizard] appears. Click the [Next] button.



3 Without changing the default settings of [Specify Volume Size], click the [Next] button.



4 Assign a drive letter in [Assign Drive Letter or Path] and click the [Next] button.

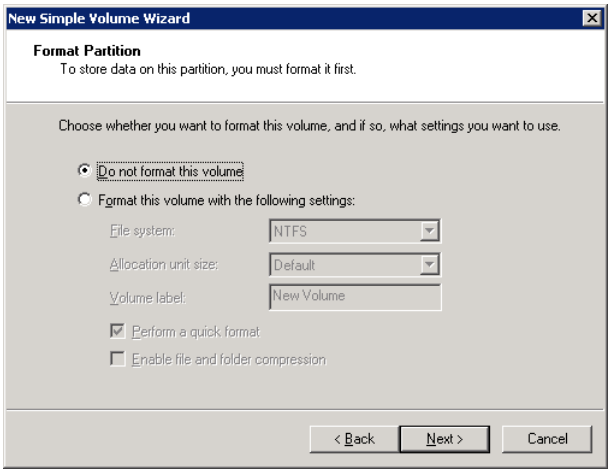


Perform the settings as shown below.

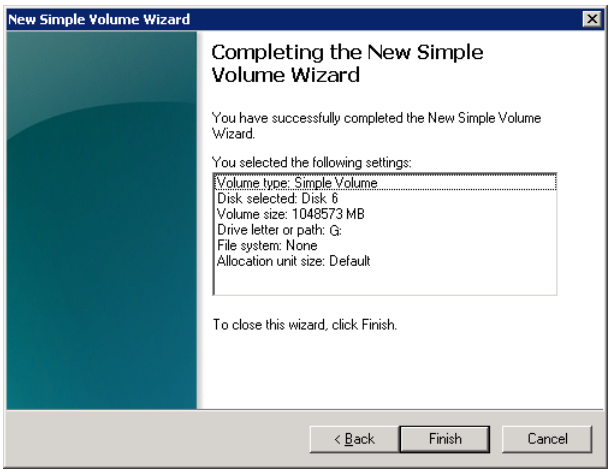
Drive	File system that is to be created	LUN	Volume No.	Volume name	Type	Capacity (*1)
G	RAW	1	1	sdv0	SDV	(1TB)
H	RAW	2	2	sdv1	SDV	(1TB)
I	RAW	3	3	sdv2	SDV	(1TB)
J	RAW	4	4	sdv3	SDV	(1TB)
K	RAW	5	5	sdv4	SDV	(1TB)
L	RAW	6	6	sdv5	SDV	(1TB)
M	RAW	7	7	sdv6	SDV	(1TB)

***1:** The capacity that is displayed in "( )" is the copy source capacity.

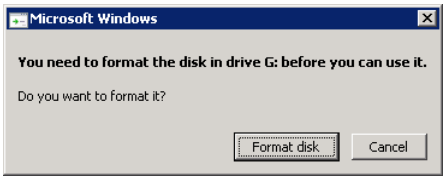
5 Select [Do not format this volume], and click the [Next] button.



6 [Completing the New Simple Volume Wizard] appears. Click the [Finish] button.



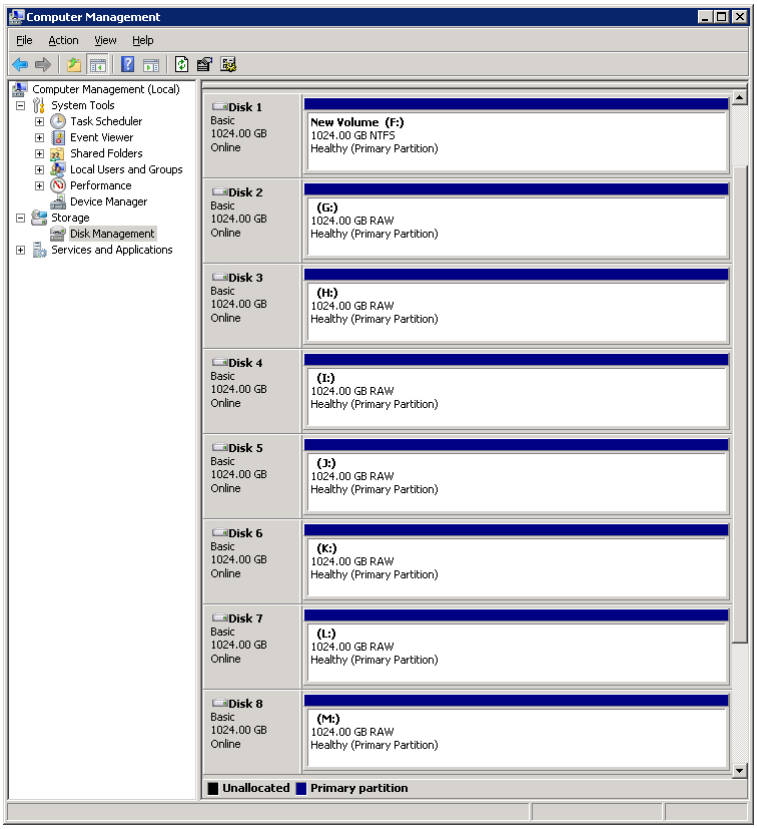
7 The next dialog box appears. Click the [Cancel] button.



Caution

Do not click the [Format disk] button.

8 Repeat the procedure in Step 1 through Step 7 for all the disks created in [Snap Data Volume].



In this case, seven disks are created as [Drive Letter: Assigned, RAW].

End of procedure

9. Advanced Copy Settings

This chapter explains the required setting to perform Advanced Copy. This chapter also provides a procedure on how to perform Advanced Copy.

Advanced Copy Basic Settings

This section describes the basic settings to use Advanced Copy.

Copy Priority Settings

Specify the copy priority when using the EC (*1) and OPC (*2) functions.

To set the copy priority, the host I/O load and the copy processing load must be taken into consideration. The specified copy priority is applied not only to the next session, but also to the existing session.

***1:** An EC includes ECs and RECs with direct connections.

***2:** An OPC includes OPC, QuickOPC, SnapOPC, and SnapOPC+.

Procedure

1 Click the [Advanced Copy] tab on the navigation of the ETERNUS Web GUI screen. Then, click [Settings] in [Category].

2 In [Action] on the [Settings] screen, click [Modify EC/OPC Priority].

3 Select the EC/OPC priority and click the [Set] button.

- Automatic Priority

  This mode changes the EC/OPC priority automatically in response to the operating load status.

- High Priority

  This mode operates by making maximum use of internal resources.

  This mode greatly affects host access performance, thus should not be used during normal operation. Use when the operation load is low.

- Middle Priority

  This mode operates slightly slower than the High Priority mode.

  Select this mode when performance is greatly affected by the High Priority mode, but the copy speed is too slow with the Low Priority mode.

- Low Priority

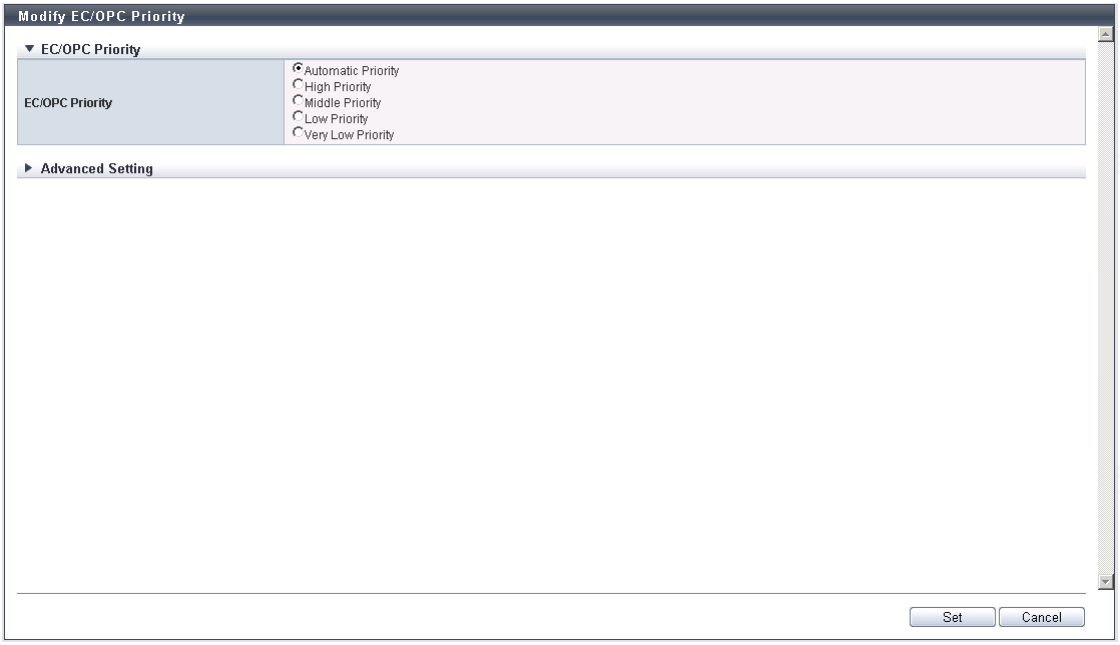
  This mode reduces the effect on host access.

  Select this mode when using EC and/or OPC during operation.

- Very Low Priority

  This mode operates slower than the Low Priority mode.

Select this mode when performance is affected (such as when the performance of host response is reduced) by the Automatic Priority or Low Priority mode.



4 In the confirmation screen, click the [OK] button.
EC/OPC priority setting starts.

5 In the setting completion screen, click the [Done] button.
The screen returns to the [Setting (Advanced Copy)] screen.

End of procedure

Copy Table Size Settings

On the controller cache memory, set the copy table size used by the firmware.

This copy table is used as the area for copy progress management when the EC (EC, REC) or OPC (OPC, QuickOPC, SnapOPC+) functions are executed.

Caution

- When the copy table size is 0MB, the copy function cannot be used.
- Before reducing the copy table size, stop copy sessions.
- The maximum capacity of copy table size is 512MB.
- Set the same resolution to the REC source and REC destination ETERNUS DX storage systems.
- Changes in the resolution is applied when the next copy session starts. If a copy session is already running, copy is continued with the resolution set at the beginning of the copy session. Restore OPC operates with the same resolution as the target session. Restore OPC for copy sessions that have been running even before the resolution is changed operates with the same resolution as the copy sessions that are running. To apply the changed resolution to a running copy session, cancel the target copy session and then start the session again.
- It is recommended to set the maximum resolution if the amount of data increase in the copy target area cannot be estimated.

Procedure

1 Click the [Advanced Copy] tab on the navigation of the ETERNUS Web GUI screen. Then, click [Settings] in [Category].

2 In [Action] on the [Settings] screen, click [Modify Copy Table Size].

3 Set the required items and click the [Set] button.

- Resolution

  Select the resolution. Specify "×64" in this example.

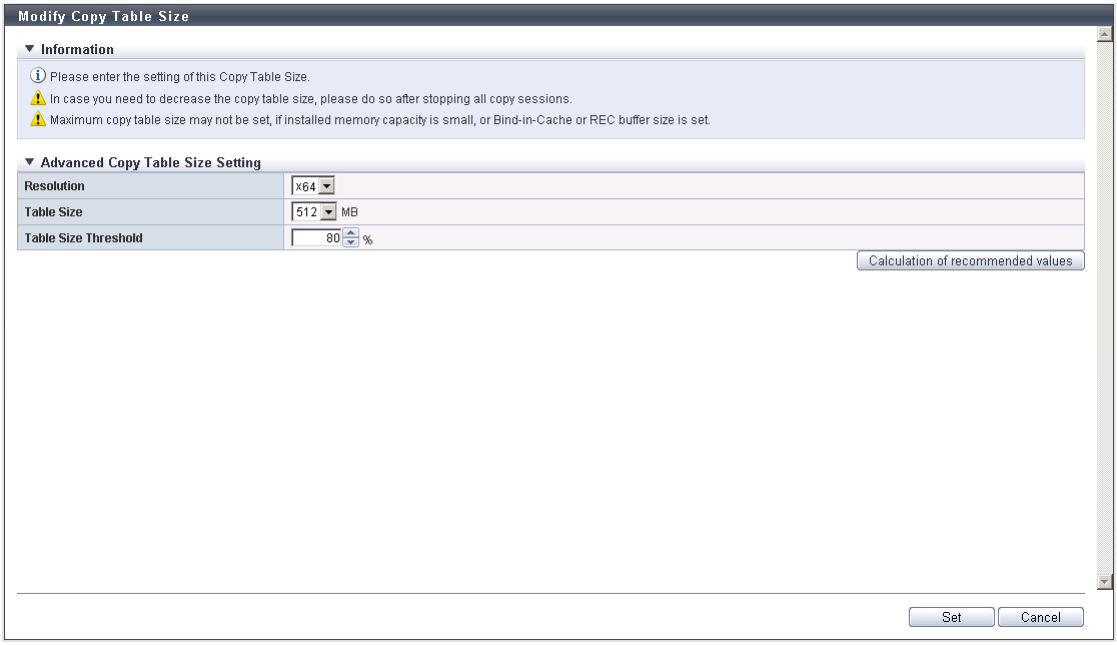
- Table Size (MB)

  Specify the copy table size. Specify "512 (MB)" in this example.

- Table Size Threshold

  Select the threshold for the table size usage rate.

To send notification automatically when the usage rate exceeds the threshold, enable notification in "Event Notification Setup" (page 101) and specify the notification method (email, SNMP, trap, or Syslog).



4 In the confirmation screen, click the [OK] button.
Copy table size setting starts.

5 In the setting completion screen, click the [Done] button.
The screen returns to the [Setting (Advanced Copy)] screen.

End of procedure

Copy Parameter Settings

Set the parameter and the area allocation unit (SDPE) to execute notification automatically when the SDP capacity becomes insufficient while SnapOPC+ is running.

The following four types of notification methods are available: E-mail, SNMP, Trap, and Syslog. The method that is specified in "Event Notification Setup" (page 101) is used as the notification to the user. Specify whether to enable notification and the notification method when enabled in advance.

Caution

If the data to be copied exceeds the physical capacity of the copy destination (if no SDP with free space exists), the copy session and the copy sessions of earlier generations cause an error.

Notification occurs only once for each policy level. No notification is sent even if the threshold is reached within 24 hours from the previous notification. Notification is sent after 24 hours have passed.

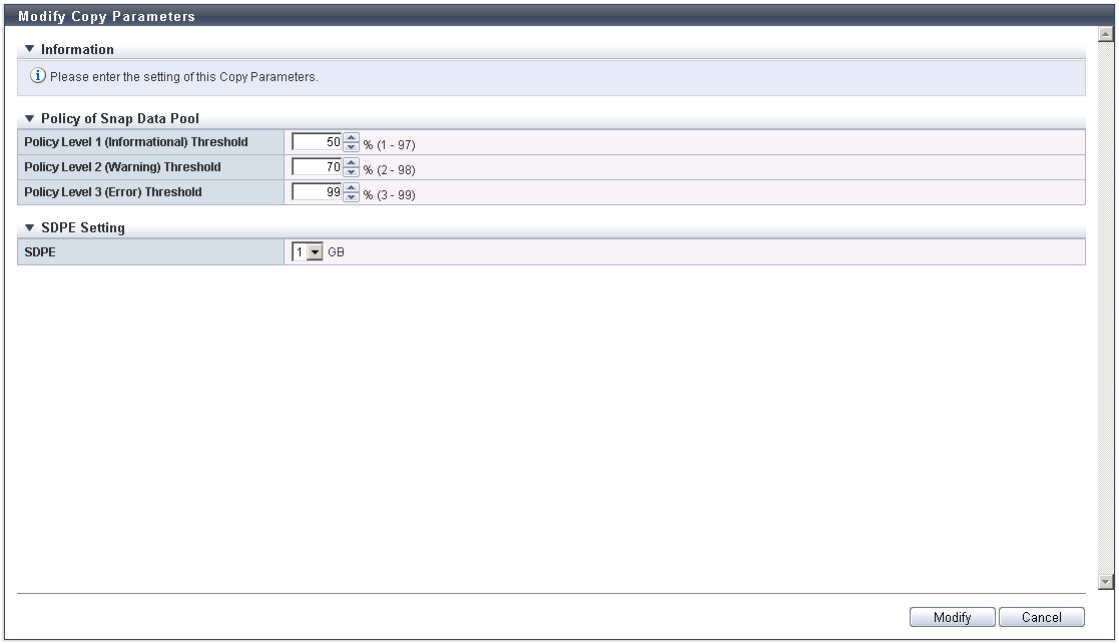
When the thresholds of multiple levels are reached at the same time, the highest level of notification is sent.

Procedure

1 Click the [Advanced Copy] tab on the navigation of the ETERNUS Web GUI screen. Then, click [Snap Data Pool] in [Category].

2 In [Action] on the [Setting] screen, click [Modify Copy Parameters].

3 Set the required items and click the [Modify] button.



4 In the confirmation screen, click the [OK] button.

Copy table size setting starts.

5 In the setting completion screen, click the [Done] button.

The screen returns to the [Snap Data Pool] screen.

End of procedure

Performing a Copy (SnapOPC+)

SnapOPC+ is a function to copy the data of the operation volume before update (previous data) to the duplicate volume.

Though SnapOPC+ can be executed both from ETERNUS Web GUI and ETERNUS CLI, operation using batch files is recommended in consideration of daily operations.

To use SnapOPC+, the same number of volumes as there are generations is required for the copy destination. Create any of the following volumes types in advance.

- SDV (SDPVs must be created as expansion areas)
- TPV
- FTV

If the volume type of the copy destination is SDV, SDVs must be used for all generations.

If the volume type of the copy destination is TPV or FTV, a mixture of TPVs and FTVs is available. Use TPV or FTV for each generation.

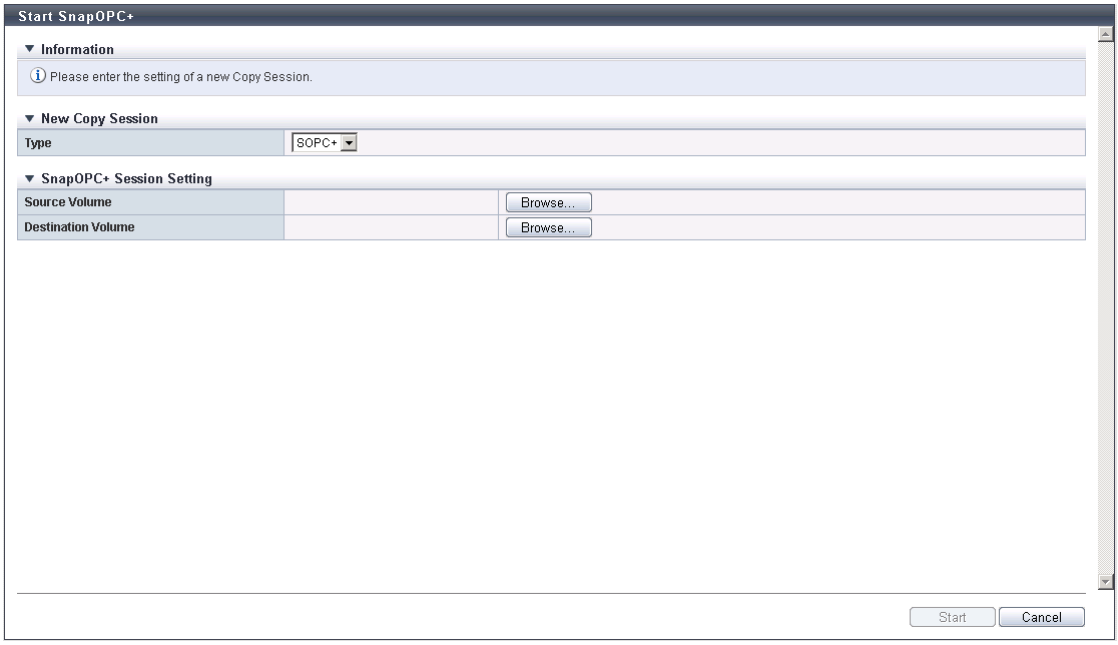
The procedure to perform SnapOPC+ is as follows:

Procedure

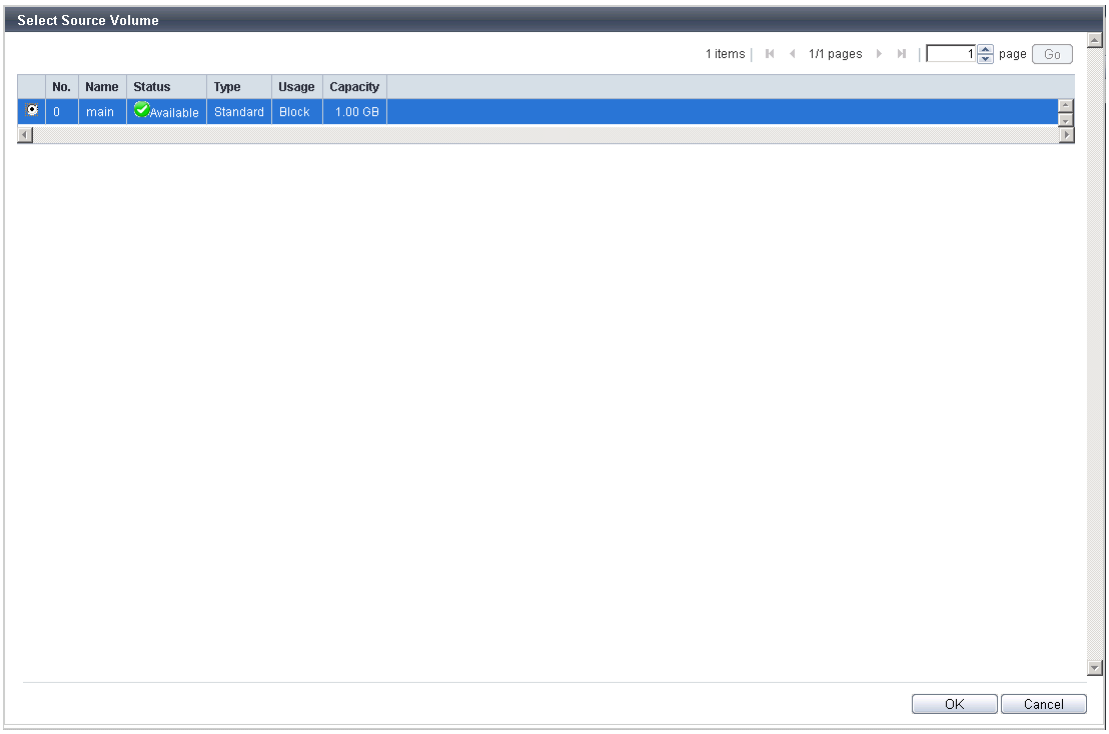
1 On the navigation of the ETERNUS Web GUI screen, click the [Advanced Copy] tab.

2 In [Action], click [Start SnapOPC+].

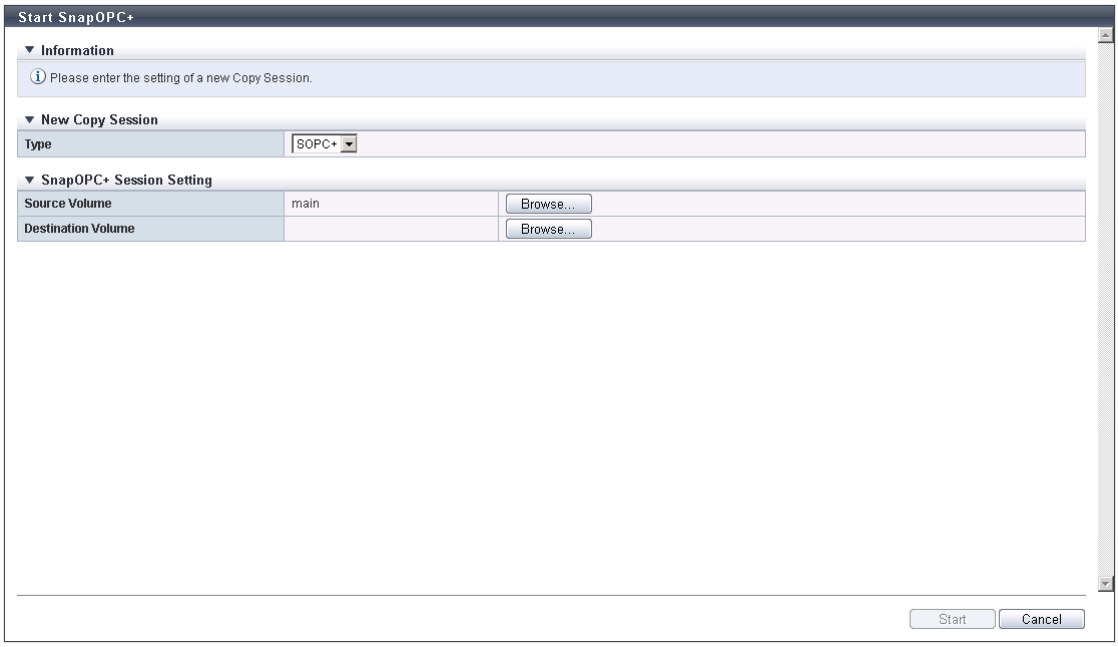
3 Click the [Browse] button of the copy source volume.



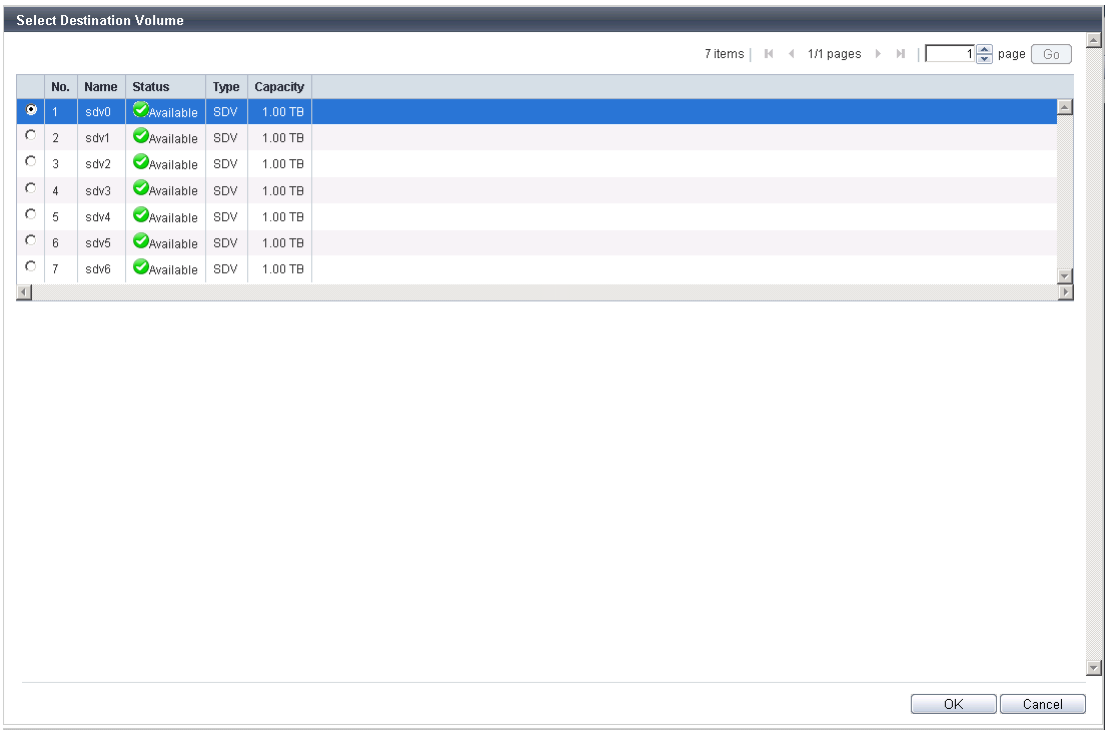
4 Select the radio button of the volume that is to be used, and then click the [OK] button.
Select the "No.: 0, Name: main" volume.



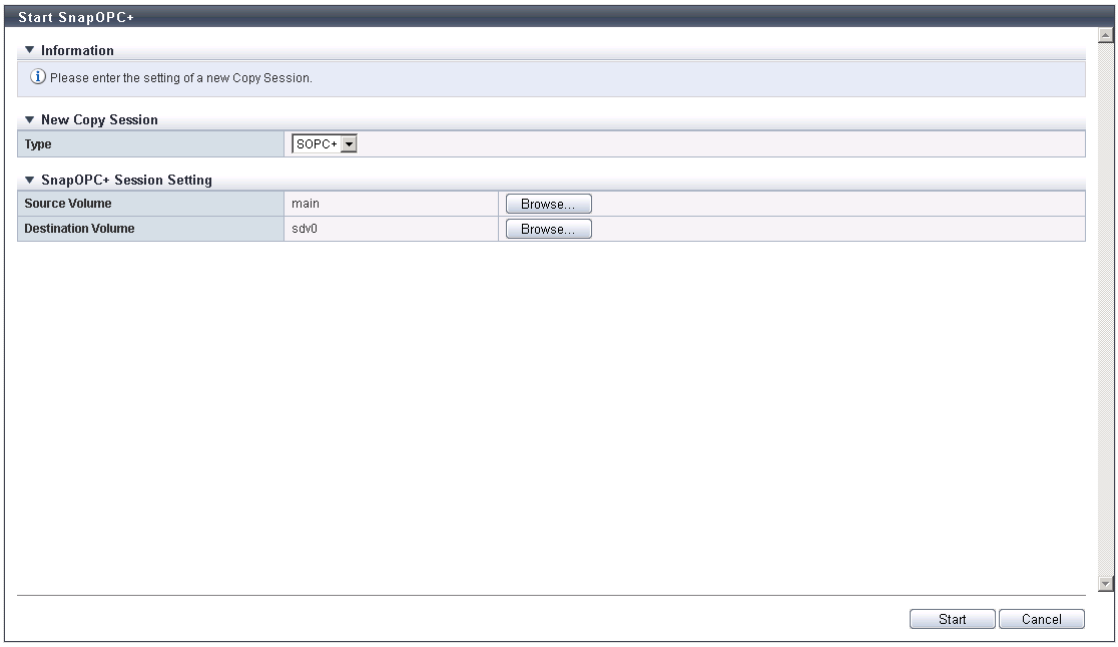
5 In the same way as the copy source volume, click the [Browse] button of the copy destination volume.



6 Select the radio button of the volume that is to be used, and then click the [OK] button.
Select the "No.: 1, Name: sdv0" volume.



7 Check the displayed information, and then click the [Start] button.



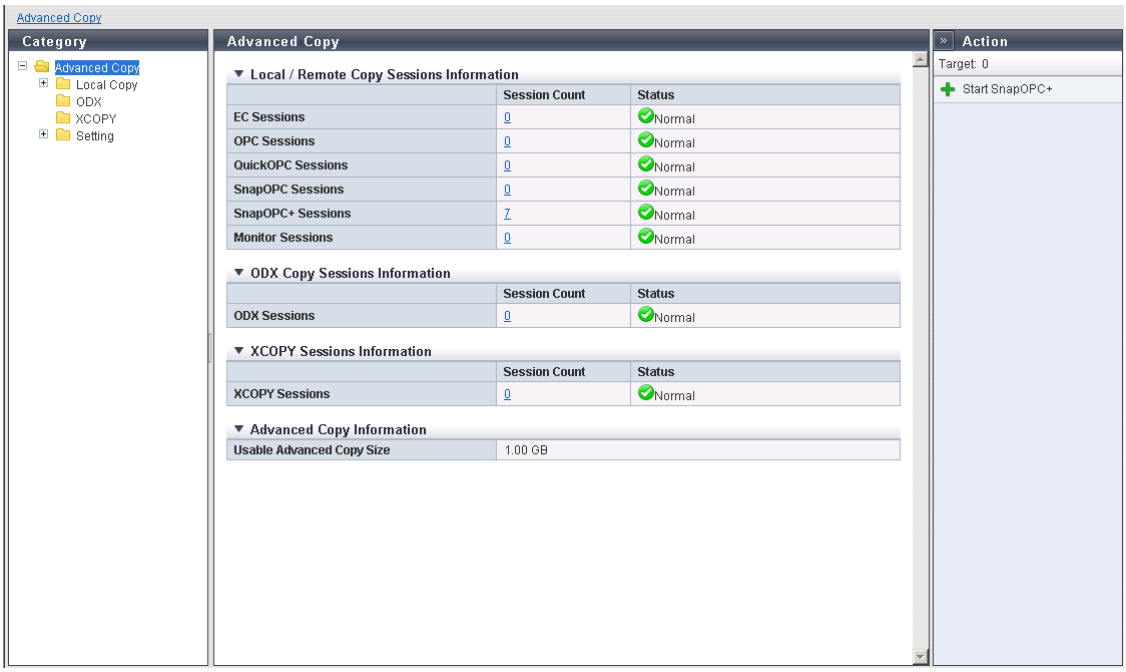
8 In the confirmation screen, click the [OK] button.
The SnapOPC+ session starts.

9 Click the [Done] button to return to the [Advanced Copy] screen.

10 Use the same method to create sessions for the remaining six generations.

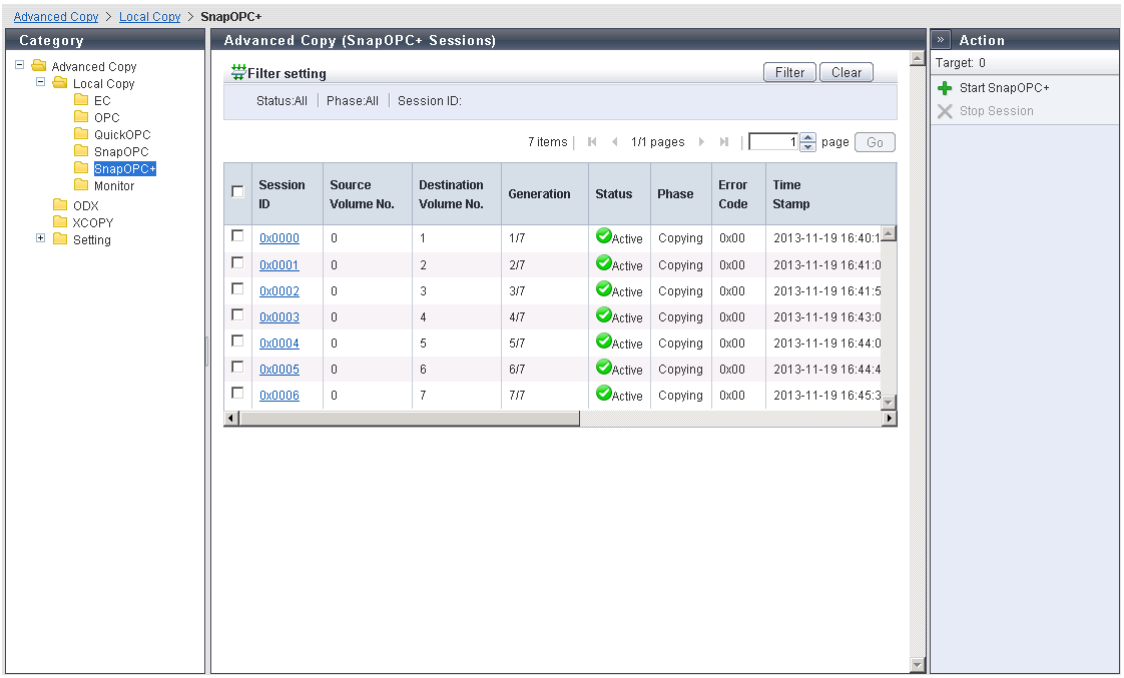
Specify from "No.: 3, Name: sdv1" through to "No.: 8, Name: sdv6" for the copy destination volumes.

11 After all of the sessions are created, click the number of sessions in [SnapOPC+ Sessions].



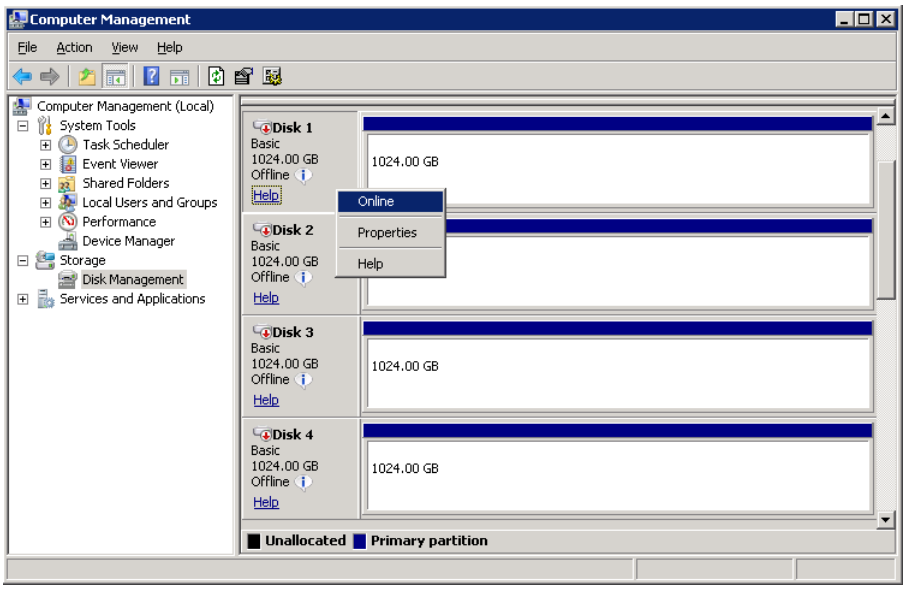
12 Check the status of the copy source volume and the copy destination volume.

In this case, the copy source volume number is "0" and the copy destination volume numbers are from "1" through to "7".



13 Open [Disk Management] from [Computer Management].

14 Change the status of all the disks with [Offline] to [Online]. In this case, change the status of Disk 1 through to Disk 8 to [Online].

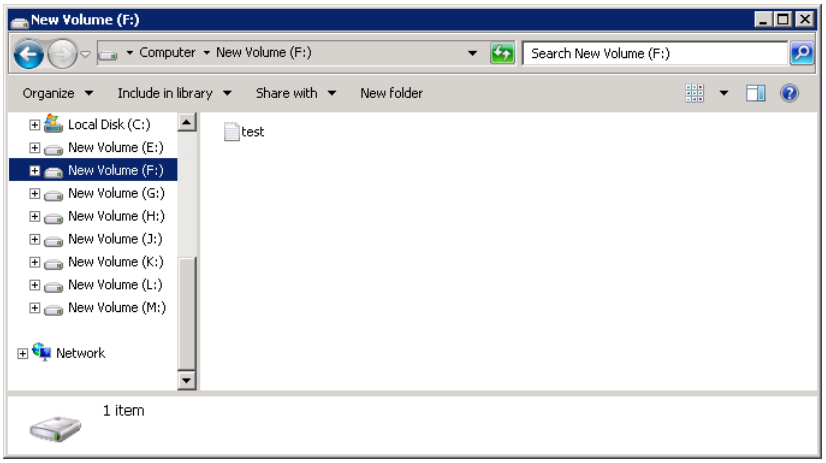


After the status of the disks is changed to [Online], file systems and drive letters are assigned.

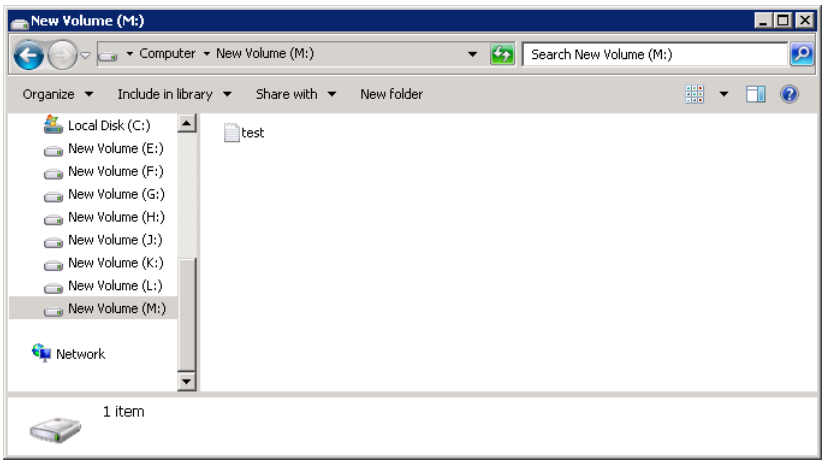
Note

If any drive letter is unused, the unused drive letter is assigned in ascending order of the drive letters, which results in discontinuous drive letters. Change the automatically assigned drive letter if necessary.

15 Check if the file that was created in Step 8 in "■ Operation Disk Settings" (page 156) in "Disk Settings" (page 156) is displayed for the copy source drive.



16 Use the same method to open the remaining seven copy destination drives to check if those files that were created in Step 15 are displayed.



End of procedure

Old data can be restored by simply copying and pasting the data files that are to be restored from the server.

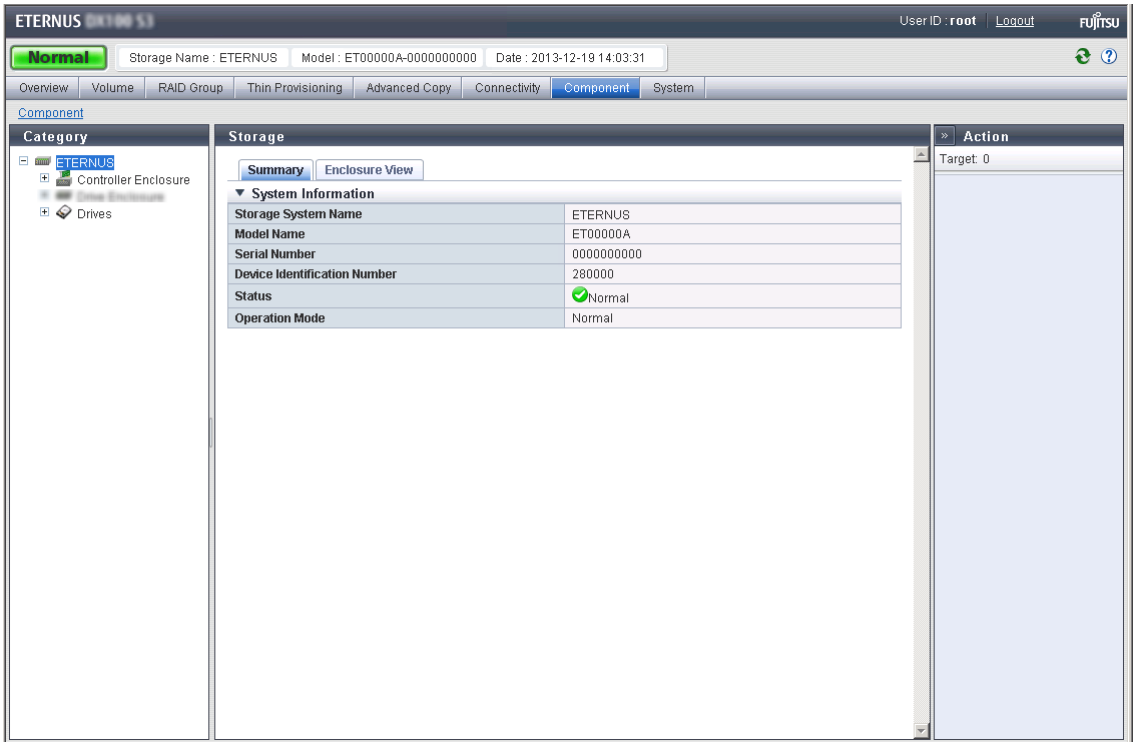
10. System Status Check

Check the status of the ETERNUS DX on the ETERNUS Web GUI screen or ETERNUS CLI.

Checking the Component Status

The status of the ETERNUS DX can be checked by general status in the upper left of the ETERNUS Web GUI screen.

When the general status image is "Normal", the ETERNUS DX is in normal status. When the general status image is other than "Normal" ("Error", "Warning", etc.), an abnormality has been detected in the ETERNUS DX. Check the status of each component on the [Storage] screen.

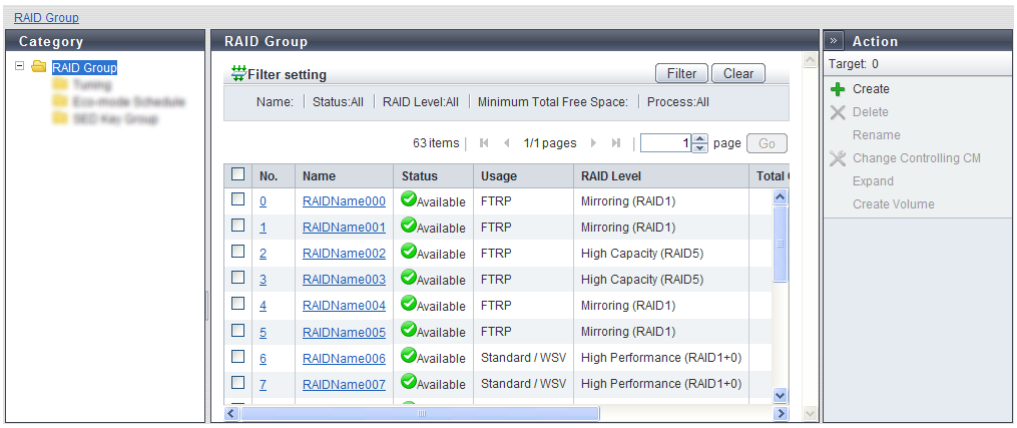


If there is a component in Warning or Error status, contact your sales representative or maintenance engineer.

Checking the RAID Groups

On the [RAID Group Details] screen of ETERNUS Web GUI, the status of RAID groups that you have created is displayed. Check if RAID configuration is set correctly.

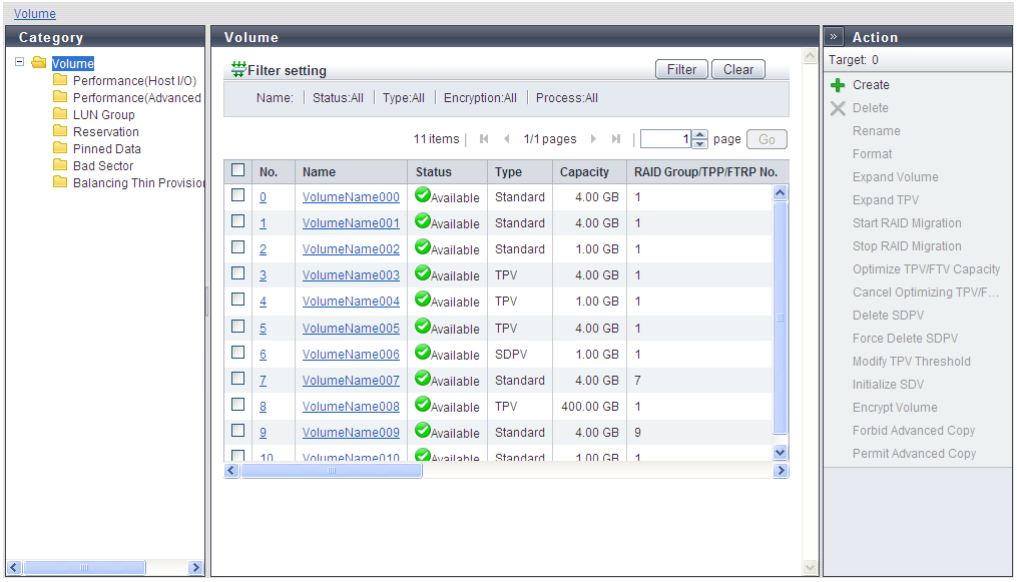
To display the [RAID Group Details] screen, click the [RAID Group] tab on the navigation of the ETERNUS Web GUI screen. In the [RAID Group (Basic Information)] screen that appears, select which RAID group to check the information for and click the No. or name of this RAID group.



Checking the Volumes

On the [Volume Details] screen of ETERNUS Web GUI, the status of volumes that you have created is displayed. Check if volumes are set correctly.

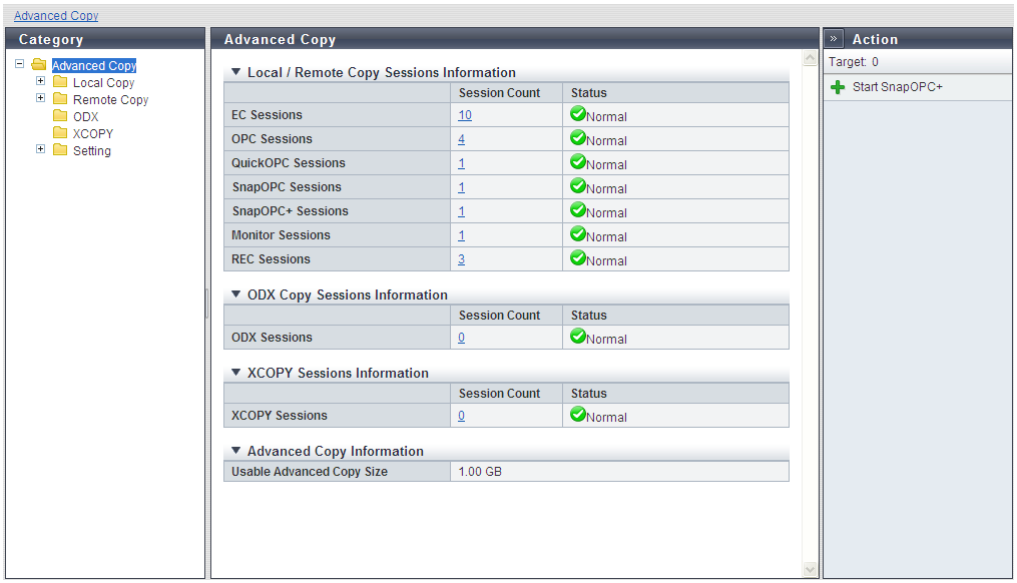
To display the [Volume Details] screen, click the [Volume] tab on the navigation of the ETERNUS Web GUI screen. In the [Volume (Basic Information)] screen that appears, select which volume to check the information for and click the No. or name of this volume.



Checking the Copy Sessions

On the [Advanced Copy] screen, the status of the copy sessions that are set is displayed. Check if the copy session status is normal.

To display the [Advanced Copy] screen, click the [Advanced Copy] tab on the navigation of the ETERNUS Web GUI screen and click the number of sessions in [SnapOPC+ Sessions].

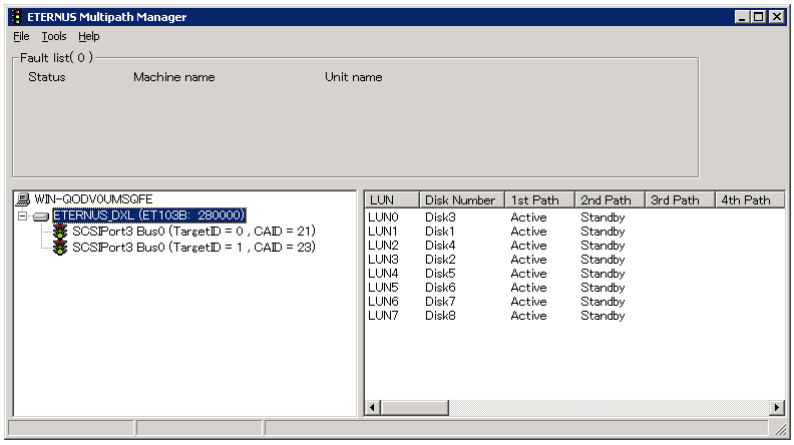


Checking the LUNs

Check the LUN status from the server.

This section describes the check procedure using the ETERNUS Multipath Driver.

Click the [Start] button for Windows, expand [ETERNUS Multipath Driver] from [All Programs], and open [ETERNUS Multipath Manager]. Check that the LUN status is normal (that the signal icon is blue).



Powering Off

To turn off the ETERNUS DX, perform one of the procedures below.

- Via the power switch

  Press the Power switch to turn off the ETERNUS DX.

- Via ETERNUS Web GUI or ETERNUS CLI

  Use ETERNUS Web GUI or ETERNUS CLI to turn off the ETERNUS DX.

The following methods can be used to turn off the power by linking with the server.

- Via the power synchronized unit

  Use the power synchronized unit to turn off the ETERNUS DX.

IMPORTANT

- When turning off the ETERNUS DX, the power shuts off after the data in the cache memory is written to the drives. As a result, it may take approximately five minutes (or approximately 10 minutes in a Unified configuration and 20 minutes in a VLAN/Bonding maximum configuration) or a maximum of 10 minutes (or approximately 40 minutes in a Unified configuration and 50 minutes in a VLAN/Bonding maximum configuration) for the power supply to be completely turned off.
- Do not turn off the power of the ETERNUS DX and the network devices that connect the ETERNUS DX to a server while the server is operating. This may result in the loss of data or prevent data from being saved in the ETERNUS DX.
- When using a power synchronized unit for power control, turn off the power of the ETERNUS DX via the power synchronized unit. When a power synchronized unit is connected, the power of the ETERNUS DX is automatically turned on because the power synchronization function is activated.
- To turn off the ETERNUS DX100 S4/DX200 S4, use the Power switch, a power synchronized unit, ETERNUS Web GUI, or ETERNUS CLI. If any other method is used to turn off the ETERNUS DX, the replacement time for the battery is sped up significantly because the battery continues to charge and discharge.

This section explains how to use the Power switch and the power synchronization unit to turn off the ETERNUS DX.

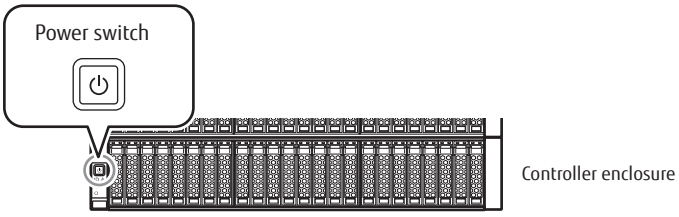
For other procedures, refer to the related manuals.

When Controlling by the Power Switch

This section explains how to use the Power switch to turn off the ETERNUS DX.

Procedure

1 Press and hold the Power switch of the controller enclosure for four seconds or more.



The READY LED ( ) on the controller enclosure is turned off.

IMPORTANT

- After power-off, wait for about one minute before turning power on again.
- If the Power switch is pressed again between the time of the READY LED ( ) turning off and the POWER LED ( ) turning off, the ETERNUS DX power may turn on.

2 The power of the ETERNUS DX is disconnected.

When the power is disconnected, the POWER LED ( ) of the controller enclosure and the POWER LEDs ( ) of the drive enclosures are turned off.

End of procedure

When a Power Synchronized Unit Is Used

If the server is turned off, the ETERNUS DX is also turned off.

11. Solution Configuration

This chapter describes the optimum solutions provided by the ETERNUS DX linking with software programs.

Continuous Business

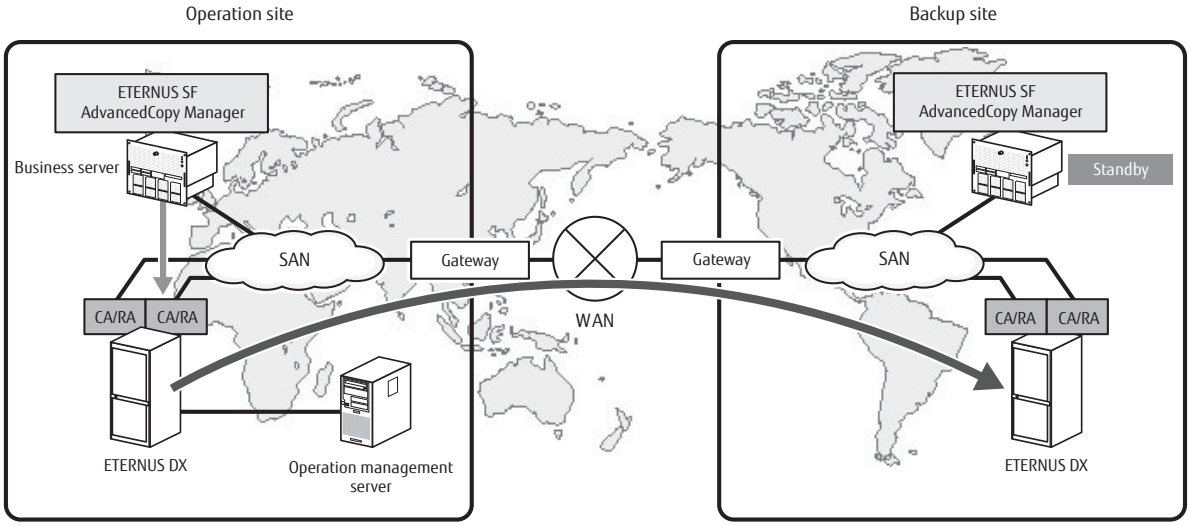
Remote Copy Operations for the Storage System (Copies between ETERNUS DX Storage Systems)

■ Solution Overview

The ETERNUS DX can perform real time data transfers from the operation site to a remote site. Even if an error occurs in the operation site, operations can continue by switching operation from the operation site to the back-up site. Data transfers to a remote site occur only between storage systems, not through servers, which reduces the load on the server.

Support for multiple transfer methods also enables flexible backup systems to be configured according to the operation environment.

Figure 18 Solution – Continuous Business (Copy between ETERNUS DX Storage Systems)



■ Configuration Procedure

Configure the system to perform Remote Advanced Copying (REC) by using ETERNUS SF AdvancedCopy Manager (ACM).

Operations are performed from the business server as an ETERNUS SF AdvancedCopy Manager agent and from the operation management server as an ETERNUS SF AdvancedCopy Manager manager.

Register the business server (ETERNUS SF AdvancedCopy Manager agent) and the business volumes that are to be backed up in the operation management server (ETERNUS SF AdvancedCopy Manager manager).

REC related settings and connection path settings must be performed in the ETERNUS DX.

Required Environment

ETERNUS SF AdvancedCopy Manager agent and a gateway device (that connects the storage systems) must be installed in each operation site and backup site. ETERNUS SF AdvancedCopy Manager manager must be installed in either of the sites (one ETERNUS SF AdvancedCopy Manager manager can manage the ETERNUS SF AdvancedCopy Manager agents of both sites).

Configuration Procedure

- Settings for the ETERNUS DX

  Register the following information with ETERNUS Web GUI.

  - Host interface settings

    Set the port mode of the host interface to RA or CA/RA.

  - Copy table size settings

    Set a memory area to manage the REC progress.

  - Copy path settings

    Set the information of the copy paths between the storage systems to perform an REC. Confirm that the storage systems can communicate with each other after setting of the copy paths is complete.

  - REC Buffer settings

    This setting is required when an REC is performed in the Consistency mode. The Consistency mode guarantees the order of data transfers to the connection destination storage system for all of the specified REC sessions.

  - REC Disk Buffer registration

    Set the REC Disk Buffer when REC Buffer capacity is to be expanded.

- Settings for ETERNUS SF AdvancedCopy Manager

  Register the following information in the operation management server (ETERNUS SF AdvancedCopy Manager).

  - Registration of the ETERNUS SF AdvancedCopy Manger license

    Register a license key via the ETERNUS SF Web Console or ETERNUS SF CLI.

  - Business server registration

    Register the server in which the ETERNUS SF AdvancedCopy Manager agent is running as the business server in the operation management server.

  - Registration of the device information in the server that is the management target

    Register the device information in the server that is the management target to the operation management server.

  - Settings for replication

    Register the replication source volumes and the replication destination volumes.

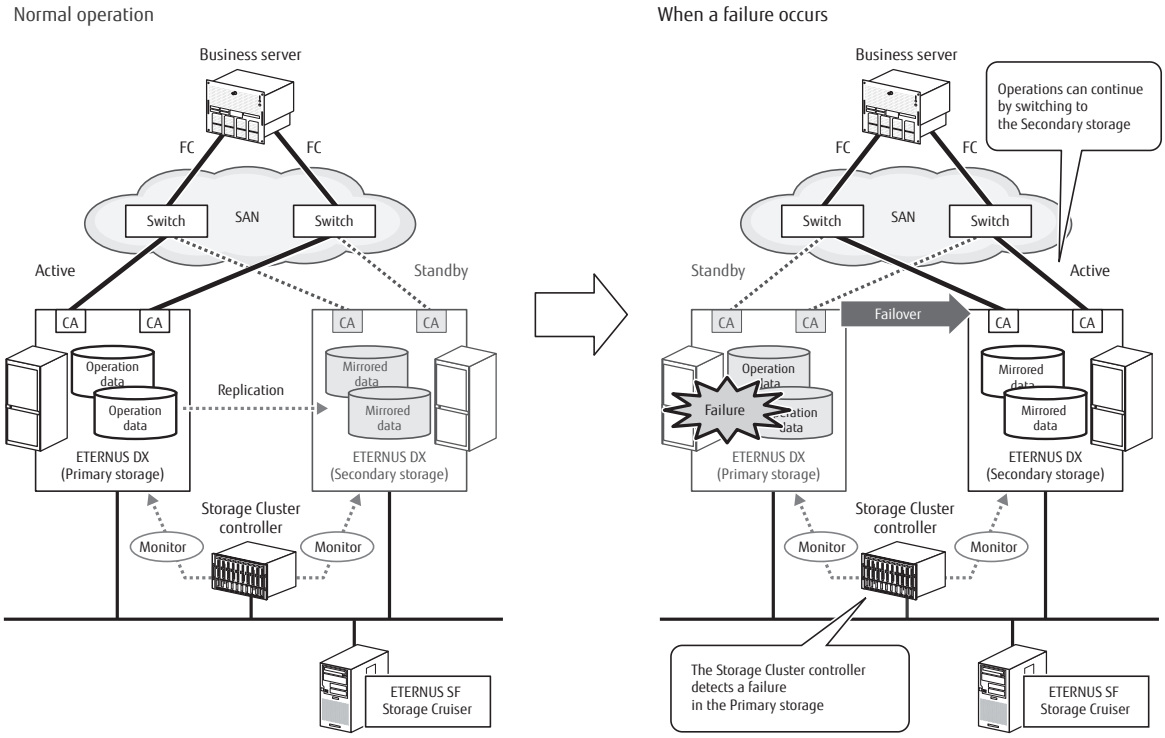
For more details on the settings for ETERNUS SF AdvancedCopy Manager, refer to "ETERNUS SF AdvancedCopy Manager Operation Guide".

Automatic Switching Operation of the Storage Systems (Storage Cluster)

■ Solution Overview

Since data equivalence is maintained between two ETERNUS DX storage systems, even when one of the ETERNUS DX storage systems fails, operation can continue by switching the I/O access destination to the other ETERNUS DX either manually or automatically (automatic failover).

Figure 19 Solution – Continuous Business (Storage Cluster)



■ Configuration Procedure

Connect business servers to the ETERNUS DX storage systems (Primary and Secondary storage systems) via switches, and then connect the management server (ETERNUS SF Storage Cruiser) to the ETERNUS DX storage systems via LANs.

To perform automatic failover, connect the Storage Cluster controller to ETERNUS DX storage systems (Primary and Secondary storage systems) via the LAN in order to detect trouble in the ETERNUS DX storage systems.

To configure Storage Cluster, perform the settings with ETERNUS SF Storage Cruiser.

● Required Environment

Two ETERNUS DX storage systems are required.

To use Storage Cluster, the ETERNUS SF Storage Cruiser Storage Cluster option is necessary.

A Storage Cluster controller is required to perform automatic failover.

● Configuration Procedure

Use ETERNUS SF Storage Cruiser to perform the following settings.

- Registration of the ETERNUS DX
- License Registration

- Registration and configuration for servers and FC switches
- Storage Cluster configuration settings
- Operation volume preparation
- Access path settings
- Storage Cluster controller settings (when performing automatic failover)

For more details on the settings for ETERNUS SF Storage Cruiser, refer to "ETERNUS SF Storage Cruiser Operation Guide".

Storage Optimization

Automated Storage Tiering

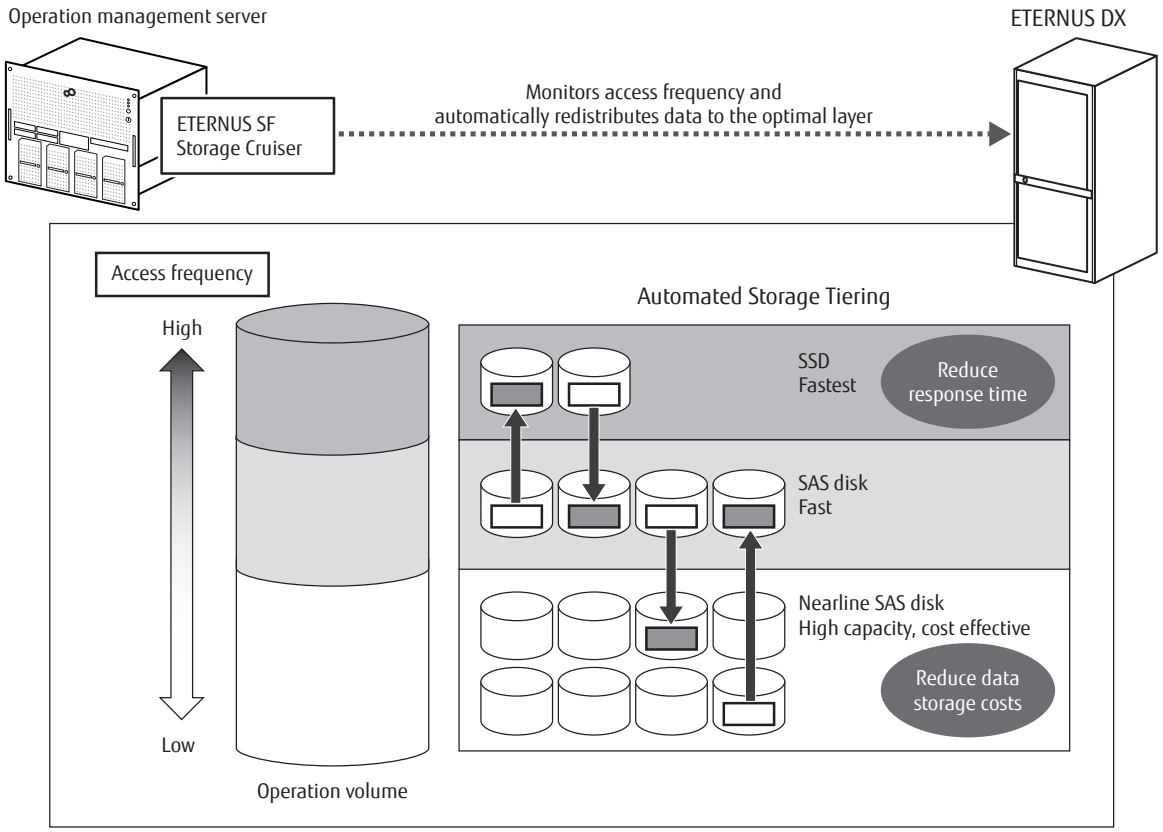
■ Solution Overview

Automated Storage Tiering is a function that detects frequently accessed data by monitoring data access to the storage, and redistributes data between drives of various types according to the policy that is set.

By storing the less frequently accessed data to cost effective Nearline SAS disks with a large capacity, storage cost can be reduced. By storing the frequently accessed data to high performance SSDs, response time are reduced and performance is improved.

In addition, by automating operation, data management hours and management costs can be reduced.

Figure 20 Solution – Automated Storage Tiering



■ Configuration Procedure

Automated Storage Tiering can be achieved by using the Flexible Tier function of the ETERNUS DX and the function of ETERNUS SF Storage Cruiser.

● Required Environment

For single tier pools, ETERNUS SF Storage Cruiser must be installed. For two or three tier pools, the ETERNUS SF Storage Cruiser Optimization option must be installed.

● Configuration Procedure

Set the tiering policy and the virtual storage pool in the operation management server (ETERNUS SF Storage Cruiser).

For details on the settings, refer to "ETERNUS SF Storage Cruiser Operation Guide for Optimization Option".

Performance/Tuning

■ Solution Overview

The performance of existing systems may be affected when the number of servers that access the ETERNUS DX increases due to increased operations. The process performance that the user sets as the target value can be automatically adjusted by using ETERNUS SF Storage Cruiser to automate Quality of Service (QoS). This guarantees the bandwidth for a server according to the operation priority to reduce the effect on one server from another server, which results in the performance of a server with high priority and important operations to be guaranteed.

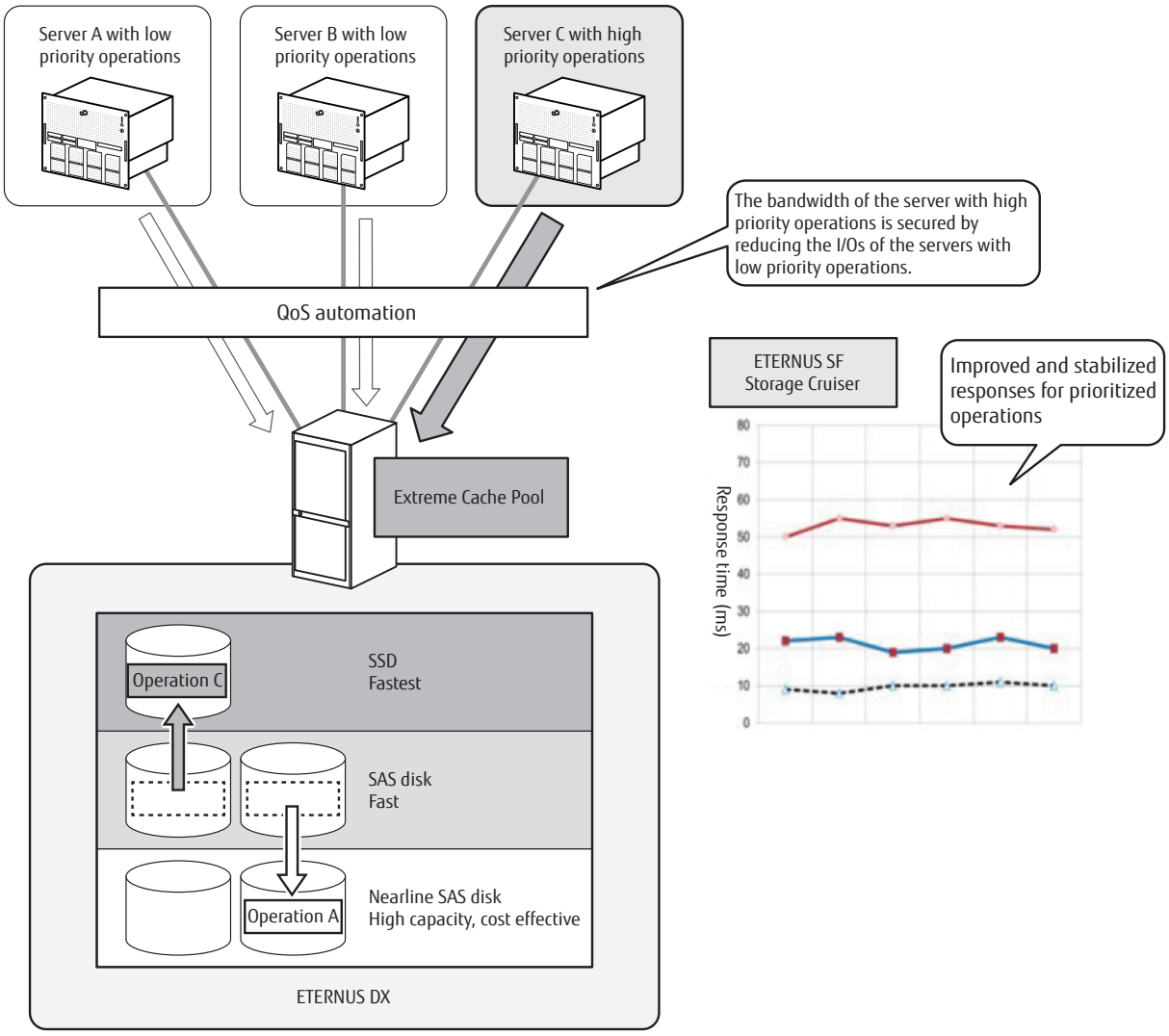
In addition, with Automated Storage Tiering, resources can be used efficiently and storage costs can be optimized.

By automating the link between bandwidth adjustment and data redistribution with QoS, complicated storage resource management can be simplified.

By allocating Extreme Cache Pool to SSDs, cache hit ratio for read access can be improved significantly. Extreme Cache Pool can be enabled or disabled for each volume.

Efficient operation can be achieved when the response performance of different operations are guaranteed in different time periods. Examples of this include when the Exchange server and backup applications exist together, and the Exchange environment is given priority during daytime and backup application operations are given priority during nighttime.

Figure 21 Solution – Performance/Tuning



■ Configuration Procedure

Automated Storage Tiering

Automated Storage Tiering can be achieved by using the Flexible Tier function of the ETERNUS DX and the function of ETERNUS SF Storage Cruiser.

QoS automation

To automate QoS, install ETERNUS SF Storage Cruiser and the ETERNUS SF Storage Cruiser QoS Management option on the operation management server.

Extreme Cache Pool

To enable the Extreme Cache Pool function, install SSDs in the ETERNUS DX and define them as Extreme Cache Pool.

Required Environment

Automated Storage Tiering

For single tier pools, ETERNUS SF Storage Cruiser must be installed. For two or three tier pools, the ETERNUS SF Storage Cruiser Optimization option must be installed.

QoS automation

To automate QoS, the ETERNUS SF Storage Cruiser QoS Management option must be installed.

Extreme Cache Pool

To enable the Extreme Cache Pool function, install SSDs with the required capacity in the ETERNUS DX.

Configuration Procedure

Automated Storage Tiering

Set the tiering policy and the virtual storage pool in the operation management server (ETERNUS SF Storage Cruiser).

For details on the settings, refer to "ETERNUS SF Storage Cruiser Operation Guide for Optimization Option".

QoS automation

Specify the target performance value for each volume in the operation management server (ETERNUS SF Storage Cruiser).

For more details on the settings for ETERNUS SF Storage Cruiser, refer to "ETERNUS SF Storage Cruiser Operation Guide".

Extreme Cache Pool

Register the volumes to enable Extreme Cache Pool from ETERNUS Web GUI or ETERNUS CLI.

Green

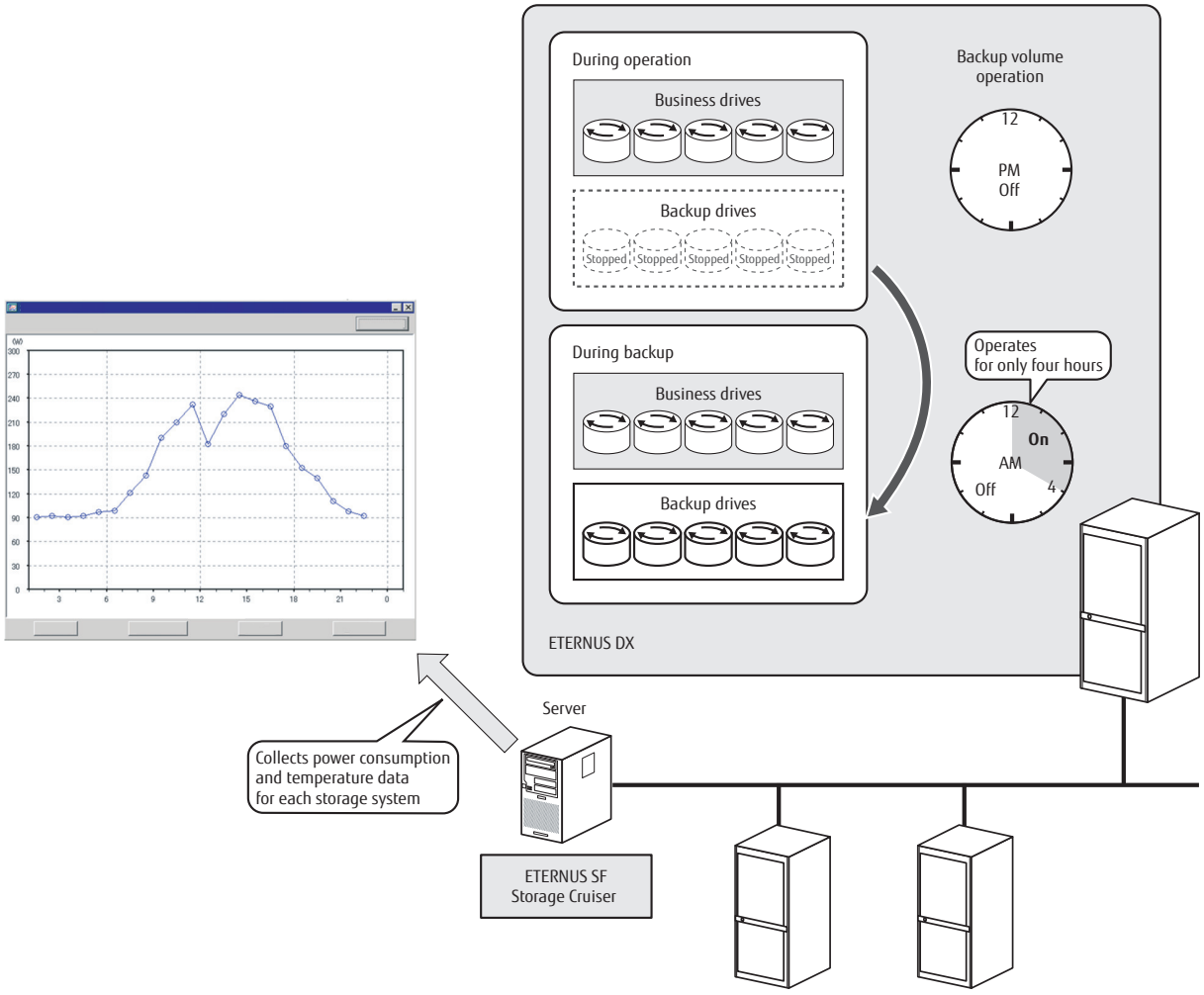
Solution Overview

Power consumption can be reduced by stopping disk motors when they are not being used. Making power consumption more efficient reduces the cost of electricity, noise emissions, and CO_2 emissions.

If the backup time period is predetermined, power saving operations can be implemented effectively by setting the Eco-mode schedule for backing up disk drives to only activate the disks when required. The disks motor or the disks power can be turned on and off according to the backup operation state using ETERNUS SF Advanced Copy Manager.

The graphical display when ETERNUS SF Storage Cruiser is used makes it easy to understand changes in power consumption and in temperature as well as check the effect of power saving operations and the effect of air conditioning around the ETERNUS DX. This statistical data can be output to a file so that it can be used when planning which power supply equipment and air conditioning equipment should be used by monitoring the degree of changes in power consumption and temperature.

Figure 22 Solution – Green



■ Configuration Procedure

Perform the required settings for Eco-mode. These settings can be performed with either ETERNUS SF Storage Cruiser or ETERNUS Web GUI.

To set the visualization of power consumption and temperature, use ETERNUS SF Storage Cruiser. ETERNUS SF Storage Cruiser obtains power consumption of the ETERNUS DX for "power consumption" and ambient temperature (intake air temperature for the fans) for "temperature".

● Required Environment

ETERNUS SF Storage Cruiser is required to visualize (graphically display) the power consumption and temperature.

● Configuration Procedure

Eco-mode

Perform the following settings with the operation management server (ETERNUS SF Storage Cruiser) or ETERNUS Web GUI:

- Eco-mode setup

  Enable the Eco-mode for the ETERNUS DX.

- Eco-mode schedule setup

  Set the schedule to apply Eco-mode. Register the time period to turn on the disk motors or turn on the disk power for backups as well as the RAID group that contains these target disks.

Visualization of the power consumption and the temperature

Register the ETERNUS DX storage systems that are the targets for performance management in the operation management server (ETERNUS SF Storage Cruiser).

For more details on the settings for ETERNUS SF Storage Cruiser, refer to "ETERNUS SF Storage Cruiser Operation Guide".

Virtualization Platform

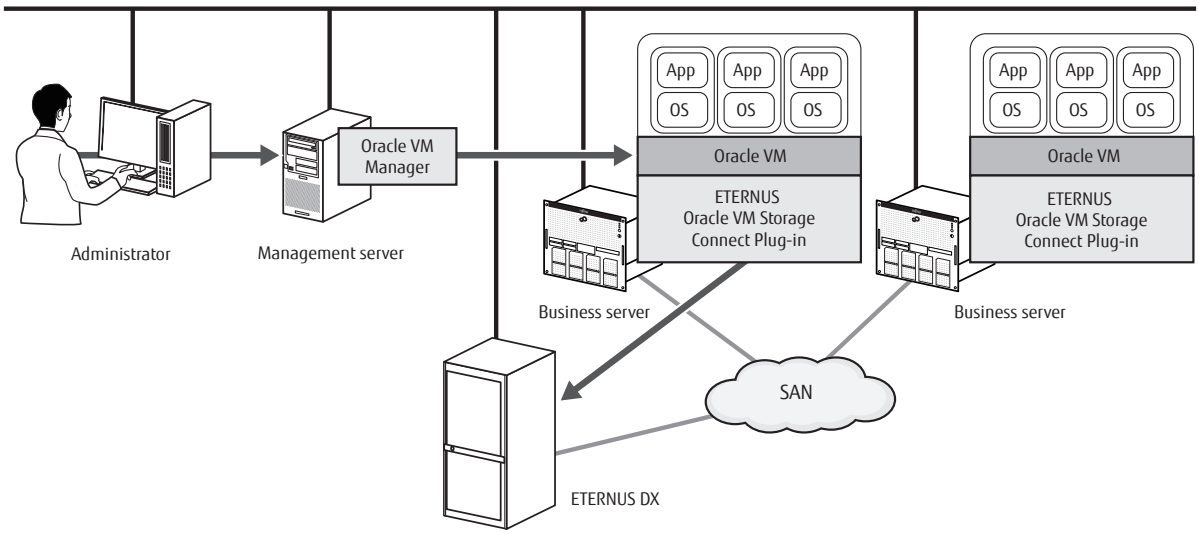
By linking virtualization software, the entire status of a system that has an ETERNUS DX can be understood by using the management tool for the server virtualization environment. This central administrative control of the virtual environment enables operations to be improved and optimized.

Oracle VM Linkage

■ Solution Overview

The Oracle VM Storage Connect framework supports creation, deletion, and expansion of Logical Unit Number (LUN) and snapshot native storage service, so that Oracle VM Manager can directly use the resources and functions of the storage system existing in the Oracle VM environment.

Figure 23 Solution – Virtualization Platform (Oracle VM Linkage)



■ Configuration Procedure

Install any plug-ins that are required for Oracle VM linkage and perform the necessary settings.

● Required Environment

For linkage with Oracle VM Manager, ETERNUS Oracle VM Storage Connect Plug-in is required. An Advanced Copy Feature license is also required.

● Configuration Procedure

Install ETERNUS Oracle VM Storage Connect Plug-in in the Oracle VM Server. For details on ETERNUS Oracle VM Storage Connect Plug-in installation, refer to "ETERNUS Oracle VM Storage Connect Plug-in User's Guide".

- Settings for the ETERNUS DX

  Use ETERNUS Web GUI or ETERNUS CLI to perform the following preliminary settings.

  - Registration of a user account with the Software role
  - RAID group and Thin Provisioning Pool creation
  - Settings of a LAN for operation management (such as the firewall settings and the SSH connection settings)

- SAN connection

  Perform FC switch zoning settings to connect the Oracle VM Server and the ETERNUS DX with FC switches.

- Registration of the ETERNUS DX

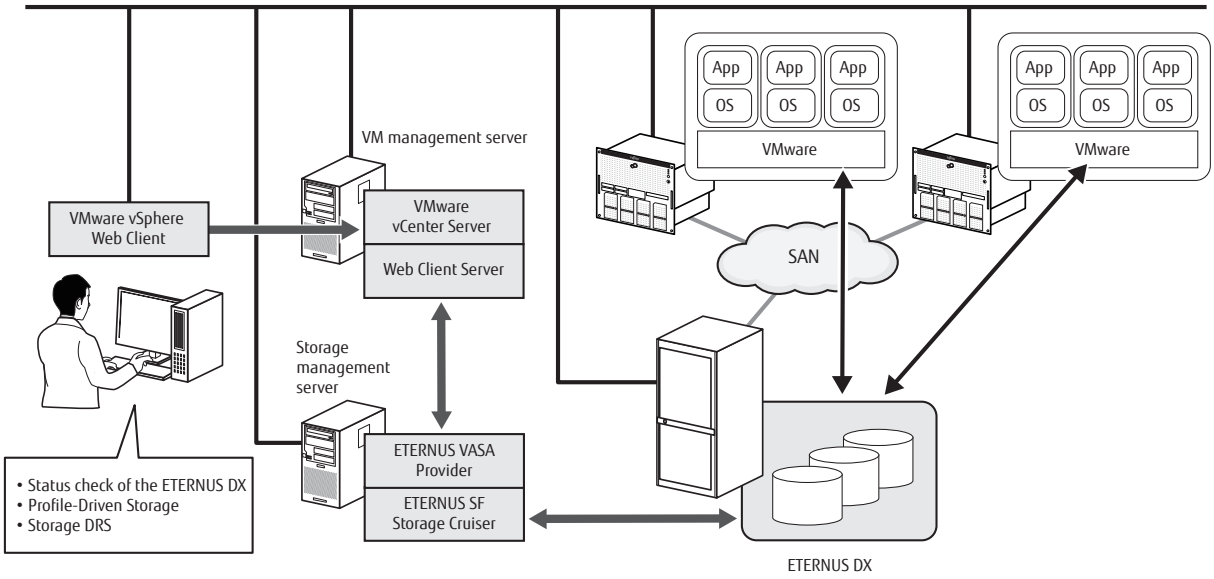
  Discover a SAN server with Oracle VM Manager and register the ETERNUS DX. For details on operating Oracle VM Manager, refer to "Oracle VM User's Guide".

VMware Linkage

■ Solution Overview

Information on the ETERNUS DX can be checked from the vSphere Web Client by expanding the user interface for VMware vSphere Web Client. The VMware administrator can grasp the physical and virtual mapping related to virtual machine, datastore, and host system, allowing integrated management of the infrastructure under a virtual environment. In addition, installation of vSphere Storage APIs for Storage Awareness (VASA) can enhance the VMware storage management function.

Figure 24 Solution – Virtualization Platform (VMware Linkage)



■ Configuration Procedure

Install any plug-ins that are required for VMware linkage and perform the necessary settings.

● Required Environment

For linkage with vSphere Web Client, ETERNUS vCenter Plug-in is required.

For linkage with VASA, ETERNUS SF Storage Cruiser and ETERNUS VASA Provider are required.

● Configuration Procedure

vCenter

Install ETERNUS vCenter Plug-in in a Windows server where VMware Web Client Server is installed.

- Server-side settings

  Install ETERNUS vCenter Plug-in and then register the ETERNUS DX as a management target device.

- Settings for the ETERNUS DX

  Enable SSH connections in the firewall settings of the network settings in ETERNUS Web GUI.

For mode details on the settings for ETERNUS vCenter Plug-in, refer to "ETERNUS vCenter Plug-in User's Guide".

VASA Provider

Install ETERNUS VASA Provider in the storage management server in which ETERNUS SF Storage Cruiser is operating.

- Settings for ETERNUS VASA Provider

  Install ETERNUS VASA Provider in the storage management server.

  Perform the settings that are related to ETERNUS VASA Provider in the vCenter Server after installation.

- Settings for ETERNUS SF Storage Cruiser

  Before starting the ETERNUS VASA Provider service, register ESXi Server and the ETERNUS DX that is to be monitored in ETERNUS SF Storage Cruiser.

  Update the configuration file and enable linkage with the device event information to apply the ETERNUS VASA Provider settings.

For more details on the settings for ETERNUS VASA Provider, refer to "ETERNUS VASA Provider User's Guide".

For more details on the settings for ETERNUS SF Storage Cruiser, refer to "ETERNUS SF Web Console Manual" and "ETERNUS SF Storage Cruiser Operation Guide".

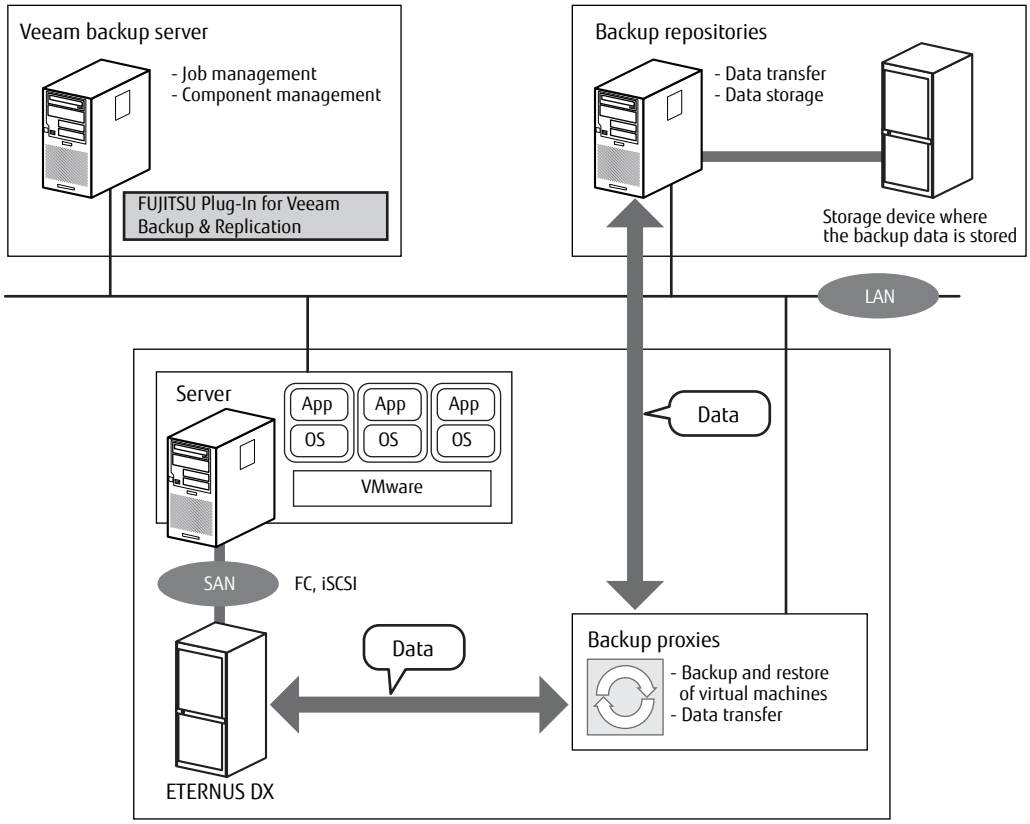
Veeam Storage Integration

Veeam Storage Integration is available for the ETERNUS DX100 S4/DX200 S4.

■ Solution Overview

The operability and efficiency of Virtual Machine backups in virtual environments (VMware) are improved by using the ETERNUS DX storage snapshot integration with Veeam Backup & Replication provided by Veeam Software.

Figure 25 Solution – Virtualization Platform (Veeam Storage Integration)



■ Configuration Procedure

For Veeam Storage Integration, register the license, install the required FUJITSU Plug-In for Veeam Backup & Replication, and perform the necessary settings.

● Required Environment

The controller firmware version of the ETERNUS DX must be V10L86 or later.

An Advanced Copy Feature license is required to use Veeam Storage Integration.

Configuration Procedure

Caution

- To use Veeam Storage Integration, set Advanced Copy in advance.

  For the procedure to set Advanced Copy, refer to "9. Advanced Copy Settings" (page 163).
- iSCSI and FC host interfaces are supported in Veeam Storage Integration for the connection between backup proxies and the ETERNUS DX.
- SnapOPC+ is used for Veeam Storage Integration.

  Thin Provisioning Volumes (TPVs) or Flexible Tier Volumes (FTVs) are used as SnapOPC+ copy destination volumes.

  Configure an appropriate maximum pool capacity for the Thin Provisioning function by taking the total capacity of volumes used for Veeam Storage Integration and the number of snapshot generations into consideration.

  For more details about the maximum pool capacity setting, refer to "Thin Provisioning Pool Management" in "ETERNUS Web GUI User's Guide".

  Guidelines for the maximum pool capacity for the Thin Provisioning function:

  Maximum pool capacity ≥ total capacity of TPVs and FTVs + total capacity of volumes for Veeam Storage Integration × (number of snapshot generations + 1)
- To connect a Backup Proxy with the ETERNUS DX via an FC, the host affinity settings must be configured for the Backup Proxy using ETERNUS CLI. For more details, refer to "ETERNUS CLI User's Guide".
- For a restore process using a host that does not have any LUNs attached, host affinity settings for the host must be configured in advance. For more details, refer to "ETERNUS CLI User's Guide".

Note

- Veeam Storage Integration supports the following volumes.

  Table 7 Volume Types That Can Be Used with Veeam Storage Integration

Volume type	Copy source	Copy destination
Standard	○	×
WSV	○	×
TPV	○ (*1)	○ (*1)
FTV	○	○
SDV	×	×
SDPV	×	×

  ○: Supported ×: Not supported

  ***1 :** Deduplication/Compression Volumes (TPVs) are not supported.

- Copy destination TPVs/FTVs are automatically created when snapshots are created with Veeam Backup & Replication (*2).

  ***2 :** Copy destination TPVs/FTVs are automatically created in the following TPPs/FTRPs.

  - If the copy source volume is a Standard volume or a WSV, the TPP with the smallest number in the ETERNUS DX or if no TPP exists, the FTRP with the smallest number in the ETERNUS DX
  - If the copy source volume is a TPV/FTV, the same TPP/FTRP as the copy source

  Copy destination TPVs/FTVs can also be created in any TPP/FTRP using ETERNUS CLI.

- Configuration of Veeam Storage Integration environment

  Connect the ETERNUS DX, the backup proxies, the Veeam backup server, and the backup repositories properly.

  For details, refer to the Veeam Backup & Replication manual that is provided by Veeam Software.

- Settings for the ETERNUS DX

  Obtain and register a Veeam Storage Integration license.

  - A Veeam Storage Integration license and FUJITSU Plug-In for Veeam Backup & Replication (*1) can be obtained from the following website.

    ***1:** FUJITSU Plug-In for Veeam Backup & Replication is used with the Veeam backup server settings.

    https://www.fujitsu.com/global/support/products/computing/storage/download/veeam/

    Note

    The serial number of the storage system is required to obtain a Veeam Storage Integration license and FUJITSU Plug-In for Veeam Backup & Replication.

  - Register the Veeam Storage Integration license.

    Refer to "License Registration" in "Operation Guide (Basic)" for details.

  - If the backup proxy is connected to the ETERNUS DX via an FC, configure the host affinity settings for the backup proxy using ETERNUS CLI.

    For the host affinity settings of the backup proxy, refer to "ETERNUS CLI User's Guide".

- Installation of FUJITSU Plug-In for Veeam Backup & Replication

  Install FUJITSU Plug-In for Veeam Backup & Replication to Veeam Backup & Replication.

For details about how to install FUJITSU Plug-In for Veeam Backup & Replication and use Veeam Backup & Replication, refer to the Veeam Backup & Replication manual that is provided by Veeam Software.

Caution

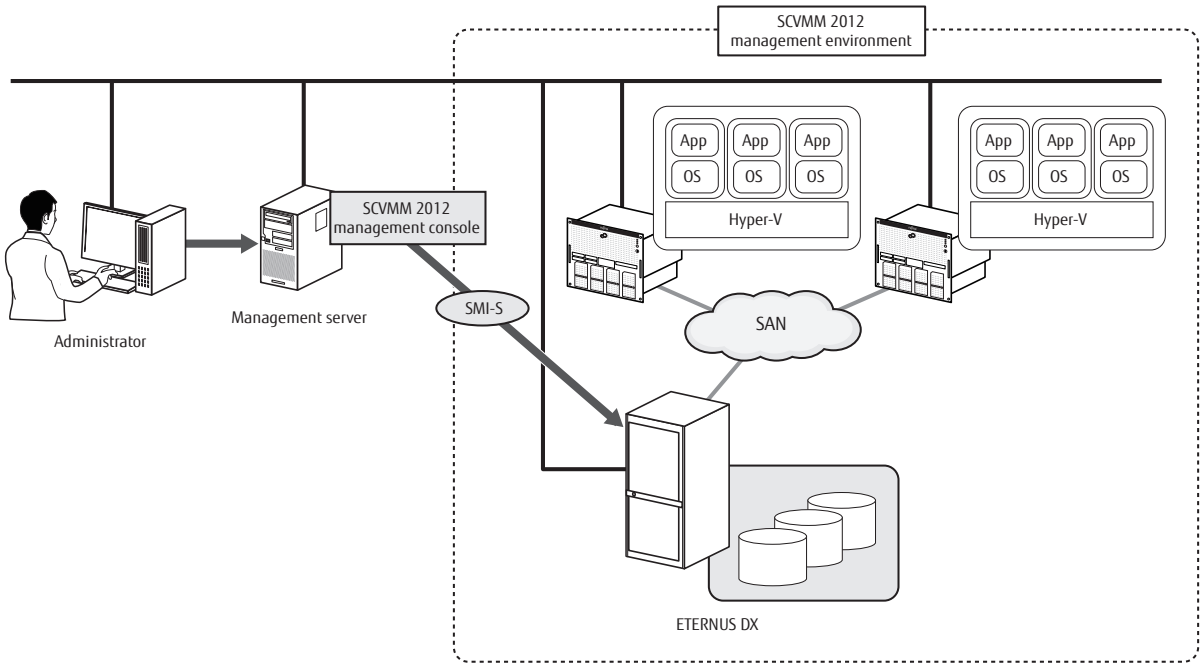
- If a volume has several snapshot generations and these snapshots have been created with different resolutions, only the oldest snapshot generation can be deleted.
- The following volumes cannot be managed or operated by Veeam Backup & Replication:
  - Volumes used for the Storage Cluster function
  - Virtual Volumes (VVOLs)
  - Volumes with Advanced Copy sessions except SnapOPC+ sessions
  - Volumes with SnapOPC+ sessions created by ETERNUS SF AdvancedCopy Manager
- Veeam Backup & Replication jobs or operations may fail during a firmware upgrade, a RAID migration, a Thin Provisioning Volume balancing, or a Flexible Tier Pool balancing.
- It is not recommended to use multiple Veeam Backup & Replication for managing a single ETERNUS DX. In such configuration, an error might occur at the jobs that are in conflict with each other when being executed from multiple Veeam Backup & Replication.

Microsoft Linkage

■ Solution Overview

By linking with Microsoft System Center Virtual Machine Manager (SCVMM), the resources and functions of the ETERNUS DX can be controlled directly from the management console of System Center 2012 or later.

Figure 26 Solution – Virtualization Platform (Microsoft Linkage)



■ Configuration Procedure

Install any plug-ins that are required for function linkage and perform the necessary settings.

● Required Environment

For linkage with System Center 2012, no plug-ins are required.

● Configuration Procedure

SCVMM2012

Use ETERNUS Web GUI to enable the SMI-S settings in the ETERNUS DX.

If the management console for SCVMM2012 uses a different subnet, add the subnet to [Allowed IP List] in [Set Network Environment].

When Windows Server 2012 or later is installed in the Hyper-V server, the ODX function is available for data copying. Create ODX volumes after enabling the ODX settings for the Advanced Copy function in the ETERNUS DX with ETERNUS Web GUI.

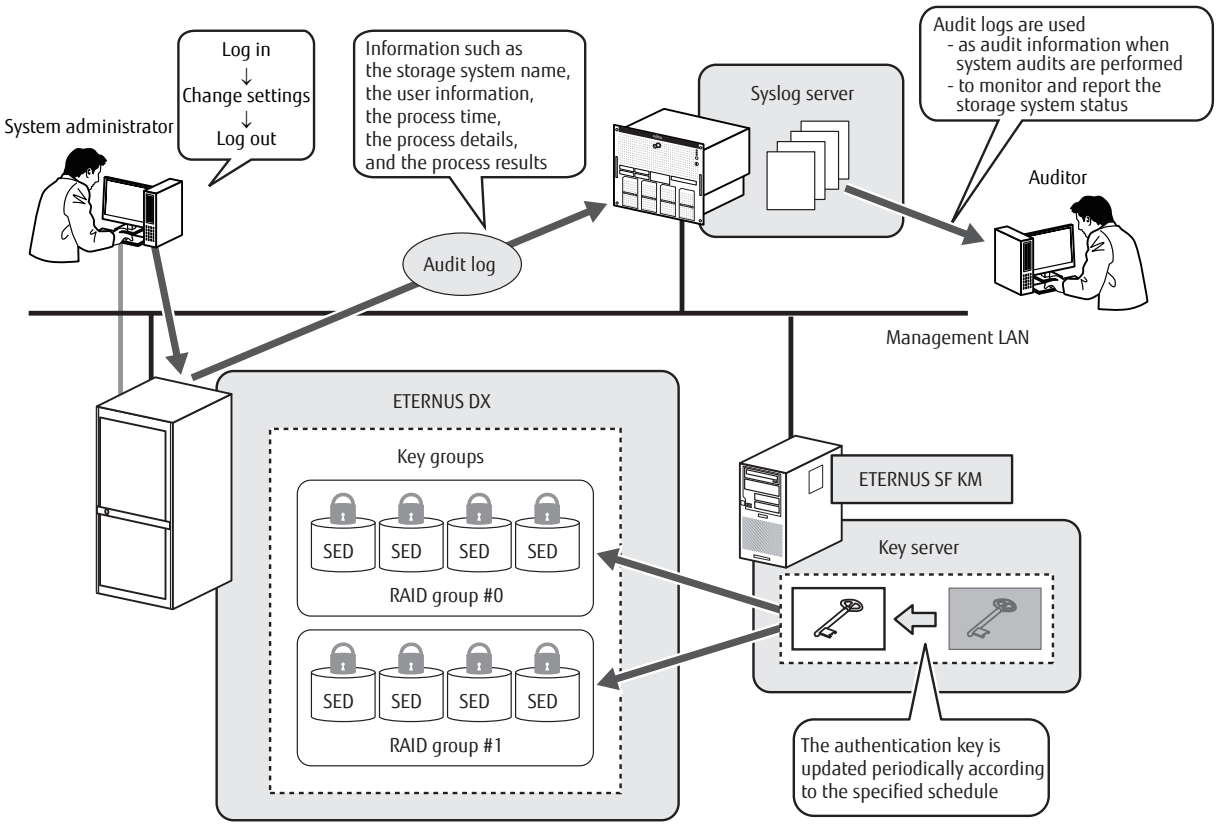
For details on the SCVMM2012 settings, refer to the manual of the SCVMM2012.

Security

Solution Overview

Unauthorized access can be monitored by using the ETERNUS DX's audit log collection and transfer function. Use acquired audit log information as audit trail information to monitor and track suspicious operations and access.

Centralized administrative control of SED authentication keys in an external server can be performed by linking with the key server. Even if a data drive in the ETERNUS DX is stolen, data leakage can be prevented by safely storing the authentication key. Automatic updating of the authentication key on a periodic basis also enhances the security of the entire system.



Configuration Procedure

Use the ETERNUS DX to enable the audit log transmission function and to register the Syslog server as the destination to which audit logs are sent.

When key management server linkage is used, set up SED key management in the operation management server (ETERNUS SF KM). Use the ETERNUS DX to create a key group and to register the key server. Keys are created in the operation management server. The ETERNUS DX requests the key to be extracted from the operation management server or requests the key to be updated when required.

Required Environment

A Syslog server is required for the destination for the transmission of the audit log that is collected.

Note that ETERNUS SF KM is required when linking with the key management server.

Configuration Procedure

Audit log transmission

Perform the following settings with the ETERNUS DX:

- Audit log setup

  Use ETERNUS Web GUI to specify the message format of audit logs that are sent and specify the domain name or the IP address for the Syslog server that receives these logs.

For details on the settings for a Syslog server that receives audit logs, refer to the manuals of the Syslog management software.

Key management server linkage

- Settings for the ETERNUS DX

  Register the following information with ETERNUS Web GUI.

  - SED authentication key registration

    Register the key that is managed in the ETERNUS DX (common key).

  - Self-signed SSL certificate creation

    Create a self-signed SSL certificate as the SSL certificate of the ETERNUS DX to establish communication between the ETERNUS DX and the key server.

  - Key management device name setup

    Specify the name (machine ID) of the ETERNUS DX that is used for key management.

  - Key server setup

    Specify the FQDN or the IP address of the key server that is linked.

  - Key group creation

    Create a key group to register the RAID groups that use the same key.

  - SSL/KMIP server certificate import

    Register the SSL/KMIP server-side certificate that is exported from the key server in the ETERNUS DX.

  - SED authentication key update

    Obtain the key that is set to the key group from the server.

  - Creating the key group

    Register the RAID groups that use the same key in the key group.

- Settings for ETERNUS SF KM

  Register the following information in the key server (ETERNUS SF KM):

  - SSL certification registration

    Perform the setting to use the self-signed SSL certificate of the ETERNUS DX in order to provide the key.

  - Network setting

    Add the IP address and the host name of the ETERNUS DX in the hosts file.

  - Specifying the ETERNUS DX that is the target for management

    Specify the group name that is registered in the ETERNUS DX and the name (machine ID) of the ETERNUS DX that is set for key management.

To complete the settings for the ETERNUS DX and ETERNUS SF KM, the certificate for the ETERNUS DX must be registered in ETERNUS SF KM. The certificate for ETERNUS SF KM must also be registered in the ETERNUS DX. For details on the setting procedures and setting items, refer to "ETERNUS SF KM Installation Guide".

A. Component Names

This appendix provides the component names of the ETERNUS DX.

Controller Enclosures

An operation panel and drives are installed in the front of the controller enclosure. Controllers and power supply units are installed in the rear.

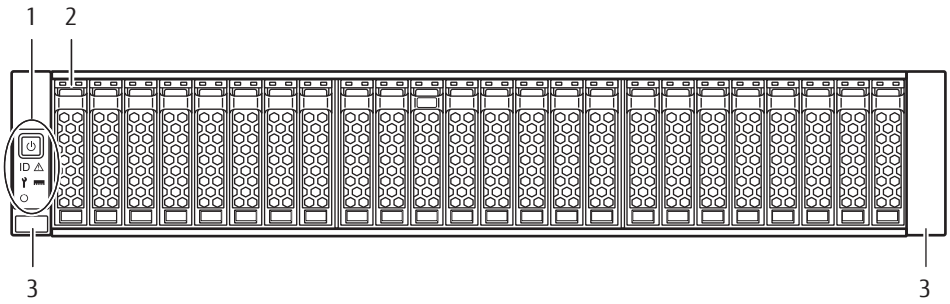
Note that the shape of the controllers is different in the ETERNUS DX100 S4/DX200 S4 and the ETERNUS DX100 S3/DX200 S3.

Front

This section provides the names of the components on the front of a controller enclosure.

■ 2.5" Type

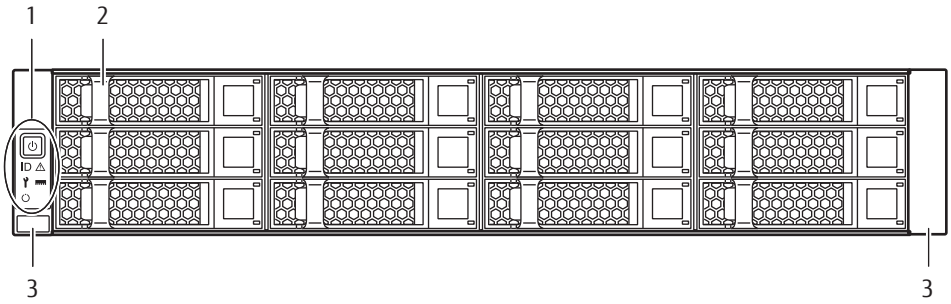
Figure 27 Front View of a 2.5" Type Controller Enclosure



1. Operation panel
2. 2.5" drive
3. Flange cover

■ 3.5" Type

Figure 28 Front View of a 3.5" Type Controller Enclosure



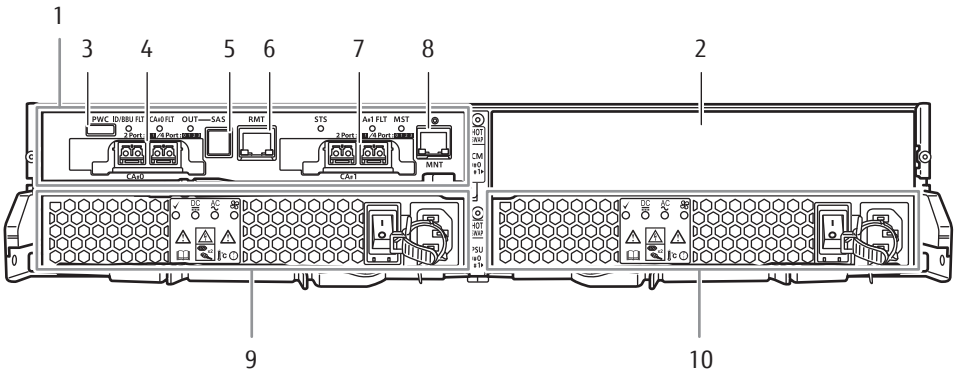
1. Operation panel
2. 3.5" drive
3. Flange cover

Rear

This section provides the names of the components on the rear of a controller enclosure.

- When only one controller is installed

  Figure 29 Rear View of a Controller Enclosure (When Only One Controller Is Installed)

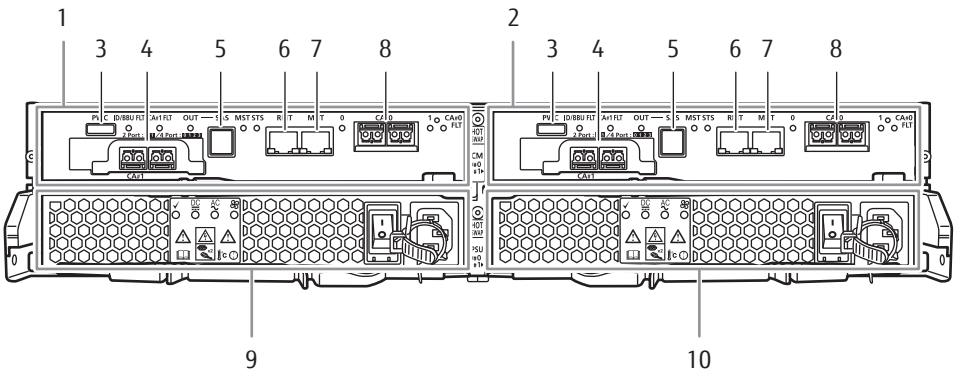


1. Controller (CM#0)
2. Cover
3. PWC port
4. Host interface (CA#0)
5. Drive interface (OUT) port
6. RMT (LAN) port
7. Host interface (CA#1)
8. MNT (LAN) port
9. Power supply unit (PSU#0)
10. Power supply unit (PSU#1)

- When two controllers are installed

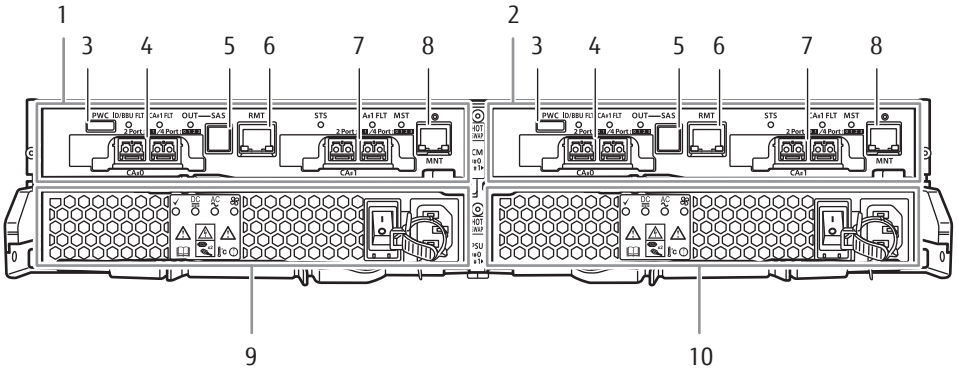
  There are two types of configurations that correspond to the combination of host interfaces.

  Figure 30 Rear Views of a Controller Enclosure (When Two Controllers Are Installed)



1. Controller (CM#0)
2. Controller (CM#1)
3. PWC port
4. Host interface (CA#1)

5. Drive interface (OUT) port
6. RMT (LAN) port
7. MNT (LAN) port
8. Host interface (CA#0)
9. Power supply unit (PSU#0)
10. Power supply unit (PSU#1)



1. Controller (CM#0)
2. Controller (CM#1)
3. PWC port
4. Host interface (CA#0)
5. Drive interface (OUT) port
6. RMT (LAN) port
7. Host interface (CA#1)
8. MNT (LAN) port
9. Power supply unit (PSU#0)
10. Power supply unit (PSU#1)

Drive Enclosures

Drives and an operation panel are installed in the front of the drive enclosure. I/O modules and power supply units are installed in the rear.

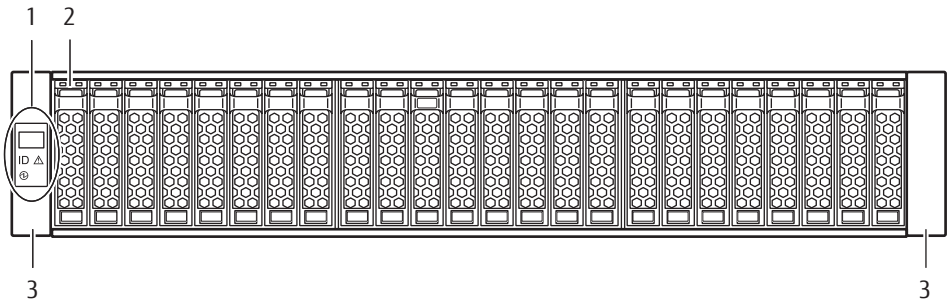
Three types of drive enclosures are available; a 2.5" type, a 3.5" type, and a high-density type.

Front

This section provides the names of the components on the front of a drive enclosure.

■ 2.5" Type

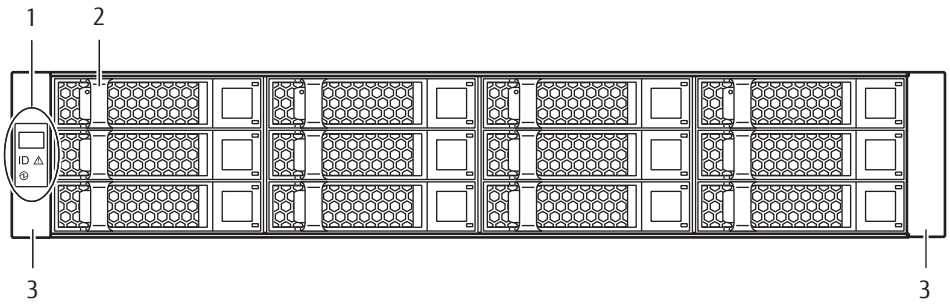
Figure 31 Front View of a 2.5" Type Drive Enclosure



1. Operation panel
2. 2.5" drive
3. Flange cover

■ 3.5" Type

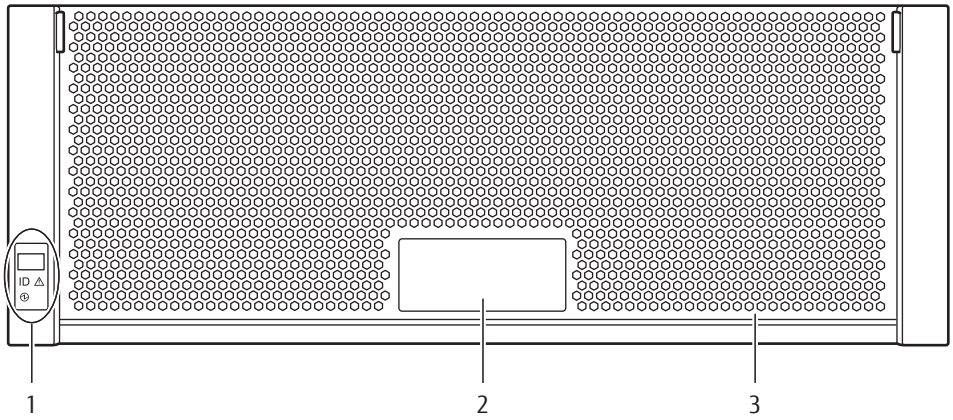
Figure 32 Front View of a 3.5" Type Drive Enclosure



1. Operation panel
2. 3.5" drive
3. Flange cover

■ High-Density Drive Enclosure

Figure 33 Front View of a High-Density Drive Enclosure



1. Operation panel
2. Disk Activity Panel (DAP)
3. Front cover

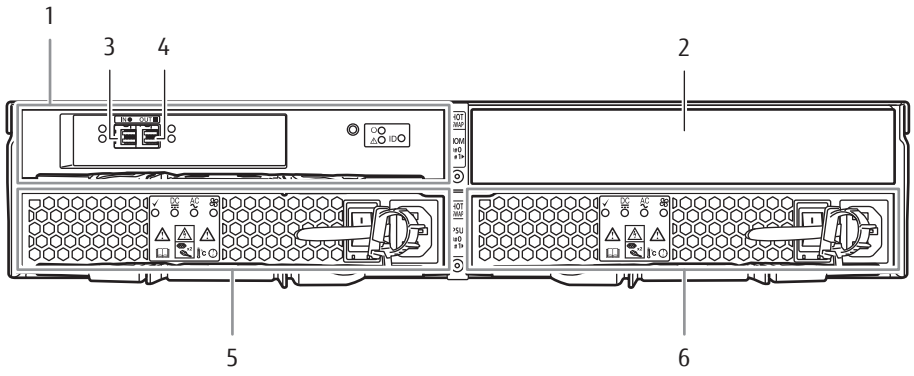
Rear

This section provides the names of the components on the rear of a drive enclosure.

■ 2.5" Type / 3.5" Type

- When only one I/O module is installed

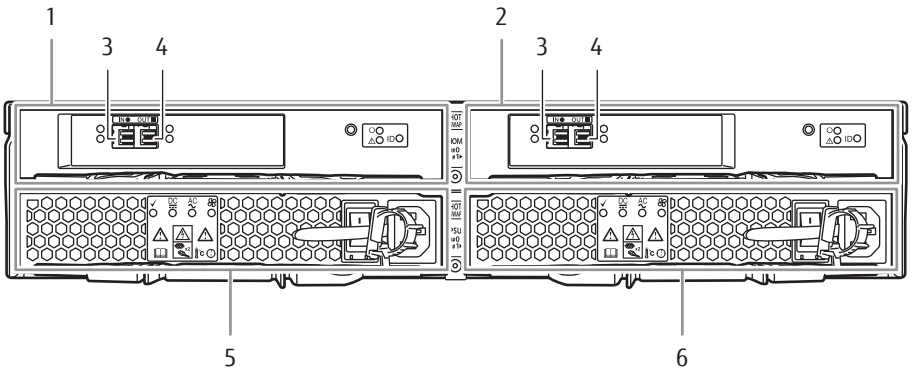
Figure 34 Rear View of a Drive Enclosure (When Only One I/O Module Is Installed)



1. I/O module (IOM#0)
2. Cover
3. Drive interface (IN) port
4. Drive interface (OUT) port
5. Power supply unit (PSU#0)
6. Power supply unit (PSU#1)

- When two I/O modules are installed

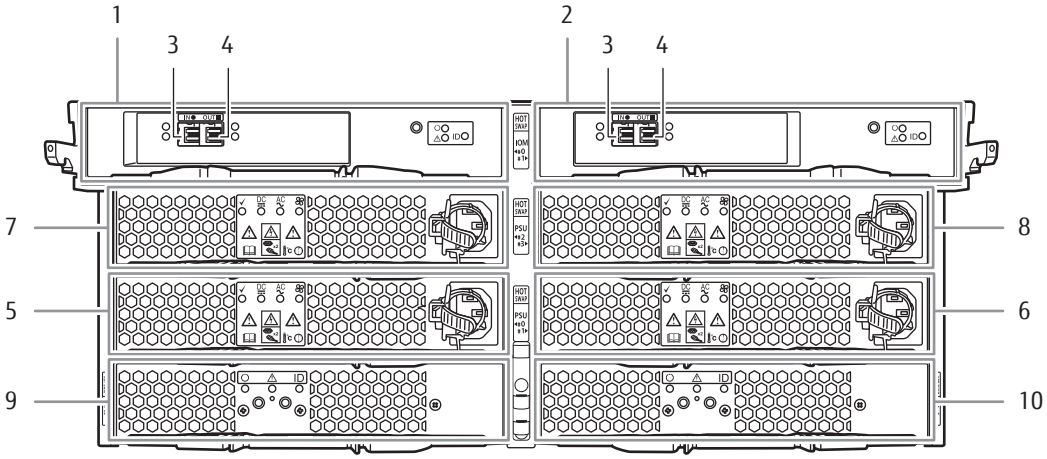
Figure 35 Rear View of a Drive Enclosure (When Two I/O Modules Are Installed)



1. I/O module (IOM#0)
2. I/O module (IOM#1)
3. Drive interface (IN) port
4. Drive interface (OUT) port
5. Power supply unit (PSU#0)
6. Power supply unit (PSU#1)

■ High-Density Drive Enclosures

Figure 36 Rear View of a High-Density Drive Enclosure



1. I/O module (IOM#0)
2. I/O module (IOM#1)
3. Drive interface (IN) port
4. Drive interface (OUT) port
5. Power supply unit (PSU#0)
6. Power supply unit (PSU#1)
7. Power supply unit (PSU#2)
8. Power supply unit (PSU#3)
9. Fan expander module (FEM#0)

10. Fan expander module (FEM#1)

Power Distribution Units (for Regions other than the EMEIA, Central American, and Caribbean Regions)

There are two sizes for power distribution units: 1U and 2U.

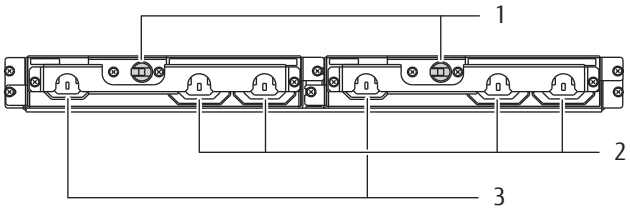
Power Distribution Units (1U)

The 1U power distribution unit has four outlets and two inlets.

Power Distribution Unit (AC200-240V, 1U, 4 Outlets)

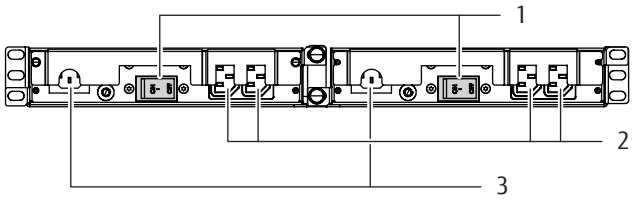
For power distribution units (AC200-240V, 1U, 4 Outlets), there are two different types of exteriors.

Figure 37 Power Distribution Unit (AC200-240V, 1U, 4 Outlets)



1. Main line switch
2. Outlet (OUTPUT)
3. Inlet (INPUT)

Figure 38 Power Distribution Unit (AC200-240V, 1U, 4 Outlets)



1. Main line switch
2. Outlet (OUTPUT)
3. Inlet (INPUT)

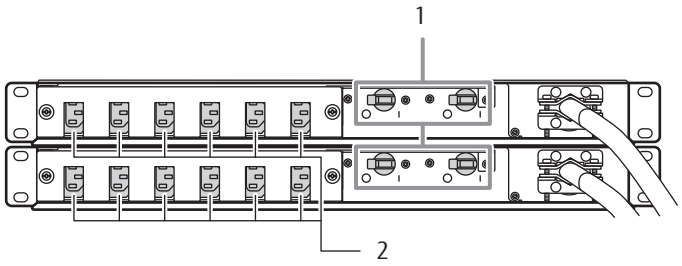
Power Distribution Units (2U)

2U power distribution units are available in two types: a 12 outlet type and a 16 outlet type.

Power Distribution Unit (AC200-240V, 2U, 12 Outlets)

There are 12 outlets.

Figure 39 Power Distribution Unit (AC200-240V, 2U, 12 Outlets)



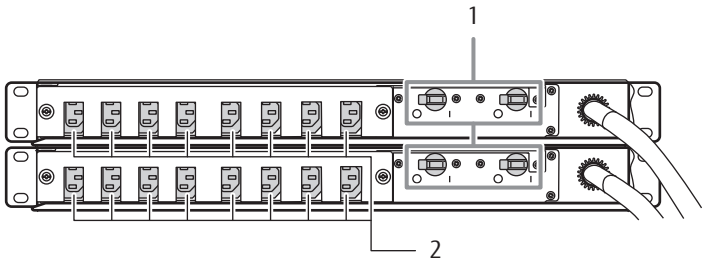
1. Main line switch
2. Outlet (OUTPUT)

Power Distribution Unit (AC200-240V, 2U, 16 Outlets)

For power distribution units (AC200-240V, 2U, 16 Outlets), there are two different types of exteriors.

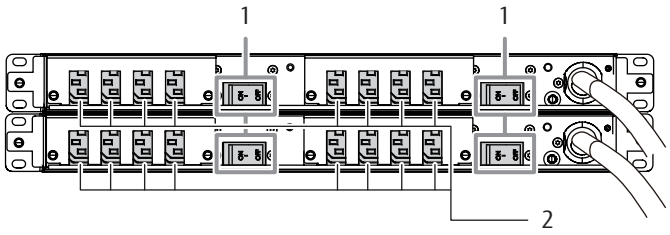
There are 16 outlets.

Figure 40 Power Distribution Unit (AC200-240V, 2U, 16 Outlets)



1. Main line switch
2. Outlet (OUTPUT)

Figure 41 Power Distribution Unit (AC200-240V, 2U, 16 Outlets)



1. Main line switch
2. Outlet (OUTPUT)

FUJITSU Storage ETERNUS DX100 S4/DX200 S4, ETERNUS DX100 S3/DX200 S3 Hybrid Storage Systems
Configuration Guide (Basic)

P3AM-7652-17ENZ0

Date of issuance: January 2023
Issuance responsibility: FUJITSU LIMITED