



FUJITSU Storage ETERNUS SF Storage Cruiser V16.0

Operation Guide

B1FW-6007-01ENZ0(04)
August 2014

Preface

Purpose

This manual describes the FUJITSU Storage ETERNUS SF Storage Cruiser used by the following FUJITSU Storage ETERNUS SF products:

- FUJITSU Storage ETERNUS SF Express (hereafter referred to as "Express")
- FUJITSU Storage ETERNUS SF Storage Cruiser (hereafter referred to as "Storage Cruiser")
- FUJITSU Storage ETERNUS SF AdvancedCopy Manager (hereafter referred to as "AdvancedCopy Manager")

Intended Readers

The manual is intended for operations managers who use ETERNUS SF Storage Cruiser for storage management.

The procedure used for actual system configuration assumes that the reader knows the basic configuration procedure for the installation target server, storage units, and their network.

Organization

This manual is composed as follows:

[Chapter 1 Overview](#)

Explains the ETERNUS SF Storage Cruiser.

[Chapter 2 Fault Monitoring](#)

Explains how to detect errors occurring in the devices making up a storage system, the screen displayed for them, and how to respond to them.

[Chapter 3 Operation Design](#)

Explains LAN connections.

[Chapter 4 Environment Configuration](#)

Provides the settings and notes required for devices to be managed.

[Chapter 5 Startup and Setting](#)

Provides device definitions and operation flowcharts required for operating this product software.

[Chapter 6 Operation](#)

Explains how to use each view of the resource view and Correlation window.

[Chapter 7 Performance Management](#)

Explains performance management functions.

[Chapter 8 Reporting Function](#)

Explains reporting functions.

[Chapter 9 Maintenance of Devices to be Managed](#)

Explains the screen displayed at the occurrence of a device error and how to respond to it.

[Chapter 10 Maintenance of the Administrative Environment](#)

Explains how to maintain databases and the troubleshooting required if a problem occurs.

[Chapter 11 Linkage to Other Software](#)

Explains how to link with other software.

[Chapter 12 Command References](#)

Explains how to use each command.

[Appendix A Customization](#)

Explains how to customize definition files.

[Appendix B Troubleshooting](#)

Explains basic troubleshooting and also provides information on where to find further help.

[Appendix C How to check product version](#)

Explains how to check version of installed ETERNUS SF Storage Cruiser.

Notation

The names, abbreviations, and symbols shown below are used in this manual.

Operating Systems

Product Name	Notation	
Microsoft(R) Windows Server(R) 2003, Standard Edition Microsoft(R) Windows Server(R) 2003, Standard x64 Edition Microsoft(R) Windows Server(R) 2003, Enterprise Edition Microsoft(R) Windows Server(R) 2003, Enterprise x64 Edition Microsoft(R) Windows Server(R) 2003 R2, Standard Edition Microsoft(R) Windows Server(R) 2003 R2, Standard x64 Edition Microsoft(R) Windows Server(R) 2003 R2, Enterprise Edition Microsoft(R) Windows Server(R) 2003 R2, Enterprise x64 Edition	Windows Server 2003	Windows
Microsoft(R) Windows Server(R) 2008 Standard (32-bit)(64-bit) Microsoft(R) Windows Server(R) 2008 Standard without Hyper-V(TM) (32-bit) (64-bit) Microsoft(R) Windows Server(R) 2008 Enterprise (32-bit)(64-bit) Microsoft(R) Windows Server(R) 2008 Enterprise without Hyper-V(TM) (32-bit) (64-bit) Microsoft(R) Windows Server(R) 2008 Datacenter (32-bit)(64-bit) Microsoft(R) Windows Server(R) 2008 Datacenter without Hyper-V(TM) (32-bit) (64-bit)	Windows Server 2008	
Microsoft(R) Windows Server(R) 2008 R2 Foundation Microsoft(R) Windows Server(R) 2008 R2 Standard Microsoft(R) Windows Server(R) 2008 R2 Enterprise Microsoft(R) Windows Server(R) 2008 R2 Datacenter	Windows Server 2008 R2	
Microsoft(R) Windows Server(R) 2012 Standard Microsoft(R) Windows Server(R) 2012 Datacenter	Windows Server 2012	
Microsoft(R) Windows Server(R) 2012 R2 Standard Microsoft(R) Windows Server(R) 2012 R2 Datacenter	Windows Server 2012 R2	
Windows Vista(R) Home Basic Windows Vista(R) Home Premium Windows Vista(R) Business Windows Vista(R) Enterprise Windows Vista(R) Ultimate	Windows Vista	
Windows(R) 7 Home Basic Windows(R) 7 Home Premium Windows(R) 7 Professional Windows(R) 7 Enterprise Windows(R) 7 Ultimate	Windows 7	

Product Name	Notation		
Windows(R) 8 Windows(R) 8 Pro	Windows 8		
Windows(R) 8.1 Windows(R) 8.1 Pro	Windows 8.1		
Solaris(TM) 9 Operating system	Solaris 9	Solaris or Solaris OS	
Oracle Solaris 10	Solaris 10		
Oracle Solaris 11	Solaris 11		
Red Hat(R) Enterprise Linux(R) AS (v.4 for x86) Red Hat(R) Enterprise Linux(R) AS (v.4 for EM64T)	RHEL-AS4	Linux	
Red Hat(R) Enterprise Linux(R) ES (v.4 for x86) Red Hat(R) Enterprise Linux(R) ES (v.4 for EM64T)	RHEL-ES4		
Red Hat(R) Enterprise Linux(R) 5 (for x86) Red Hat(R) Enterprise Linux(R) 5 (for Intel64)	RHEL5		
Red Hat(R) Enterprise Linux(R) 6 (for x86) Red Hat(R) Enterprise Linux(R) 6 (for Intel64)	RHEL6		
SUSE(R) Linux Enterprise Server 11 for x86 SUSE(R) Linux Enterprise Server 11 for EM64T	SUSE Linux Enterprise Server 11		
HP-UX 11i v1 HP-UX 11i v2 HP-UX 11i v3	HP-UX		
AIX(R) V6.1 AIX(R) V7.1	AIX		
VMware vSphere(R) 4 Essentials Kit VMware vSphere(R) 4 Essentials Plus Kit VMware vSphere(R) 4 Standard Edition(TM) VMware vSphere(R) 4 Standard Plus Data Recovery VMware vSphere(R) 4 Advanced Edition(TM) VMware vSphere(R) 4 Enterprise Edition(TM) VMware vSphere(R) 4 Enterprise Plus Edition(TM)	VMware vSphere 4	VMware	
VMware vSphere(R) 5 Essentials Kit VMware vSphere(R) 5 Essentials Plus Kit VMware vSphere(R) 5 Standard Edition(TM) VMware vSphere(R) 5 Standard Plus Data Recovery VMware vSphere(R) 5 Enterprise Edition(TM) VMware vSphere(R) 5 Enterprise Plus Edition(TM)	VMware vSphere 5		

Oracle Solaris might be described as Solaris, Solaris Operating System, or Solaris OS.

FUJITSU Storage ETERNUS

Formal Name	Abbreviation	
FUJITSU Storage ETERNUS DX60/DX60 S2 FUJITSU Storage ETERNUS DX80/DX80 S2 FUJITSU Storage ETERNUS DX90/DX90 S2	-	
FUJITSU Storage ETERNUS DX100 S3 FUJITSU Storage ETERNUS DX200 S3		
FUJITSU Storage ETERNUS DX410 FUJITSU Storage ETERNUS DX440	ETERNUS DX400 series	ETERNUS DX400/ DX400 S2 series
FUJITSU Storage ETERNUS DX410 S2 FUJITSU Storage ETERNUS DX440 S2	ETERNUS DX400 S2 series	

Formal Name	Abbreviation	
FUJITSU Storage ETERNUS DX500 S3 FUJITSU Storage ETERNUS DX600 S3	-	
FUJITSU Storage ETERNUS DX8100 FUJITSU Storage ETERNUS DX8400 FUJITSU Storage ETERNUS DX8700	ETERNUS DX8000 series	ETERNUS DX8000/ DX8000 S2 series
FUJITSU Storage ETERNUS DX8100 S2 FUJITSU Storage ETERNUS DX8700 S2	ETERNUS DX8000 S2 series	
FUJITSU Storage ETERNUS DX200F	-	
FUJITSU Storage ETERNUS LT20/LT20 S2 FUJITSU Storage ETERNUS LT40/LT40 S2 FUJITSU Storage ETERNUS LT60/LT60 S2 FUJITSU Storage ETERNUS LT200 FUJITSU Storage ETERNUS LT210 FUJITSU Storage ETERNUS LT220 FUJITSU Storage ETERNUS LT230 FUJITSU Storage ETERNUS LT250 FUJITSU Storage ETERNUS LT270/LT270 S2	ETERNUS tape library	
FUJITSU Storage ETERNUS Multipath Driver	ETERNUS Multipath Driver	

Each individual device name in this document is listed with "FUJITSU Storage" omitted from it.

Software Products

Formal Name	Abbreviation
Microsoft(R) Internet Explorer(R)	Internet Explorer
Mozilla(R) Firefox(R)	Firefox
Microsoft(R) Cluster Service	MSCS
Microsoft(R) Windows Server(R) Failover Clustering	WSFC
Microsoft(R) Exchange Server	Exchange Server
Microsoft(R) SQL Server(R)	SQL Server
VMware(R) ESX(R)	VMware ESX
VMware(R) ESXi(TM)	VMware ESXi
VMware(R) vCenter(TM) Server	VMware vCenter Server or vCenter Server
FUJITSU Software PRIMECLUSTER Global Disk Services	GDS
FUJITSU Software PRIMECLUSTER Global File Services	GFS

Manuals

Formal Name	Abbreviation
FUJITSU Storage ETERNUS SF Express / ETERNUS SF Storage Cruiser / ETERNUS SF AdvancedCopy Manager Quick Reference	ETERNUS SF Quick Reference
FUJITSU Storage ETERNUS SF Express / ETERNUS SF Storage Cruiser / ETERNUS SF AdvancedCopy Manager Release Notes	ETERNUS SF Release Notes
FUJITSU Storage ETERNUS SF Express / ETERNUS SF Storage Cruiser / ETERNUS SF AdvancedCopy Manager Installation and Setup Guide	ETERNUS SF Installation and Setup Guide
FUJITSU Storage ETERNUS SF Express / ETERNUS SF Storage Cruiser / ETERNUS SF AdvancedCopy Manager Migration Guide	ETERNUS SF Migration Guide

Formal Name	Abbreviation
FUJITSU Storage ETERNUS SF Express / ETERNUS SF Storage Cruiser / ETERNUS SF AdvancedCopy Manager Web Console Guide	ETERNUS SF Web Console Guide
FUJITSU Storage ETERNUS SF Storage Cruiser / ETERNUS SF AdvancedCopy Manager Cluster Environment Setup Guide	ETERNUS SF Cluster Environment Setup Guide
FUJITSU Storage ETERNUS SF Express / ETERNUS SF Storage Cruiser / ETERNUS SF AdvancedCopy Manager Messages	ETERNUS SF Messages
FUJITSU Storage ETERNUS SF Express / ETERNUS SF Storage Cruiser Event Guide	ETERNUS SF Event Guide
FUJITSU Storage ETERNUS SF Express / ETERNUS SF Storage Cruiser / ETERNUS SF AdvancedCopy Manager Glossary	ETERNUS SF Glossary

Besides the above-mentioned, each individual manual name in this document is listed with "FUJITSU Storage" omitted from it.

Others

- "Fibre Channel switch" includes "Converged Switch".
- ETERNUS SF Web Console is abbreviated as "Web Console".
- Quality of Service is abbreviated as "QoS".
- It is described when showing bringing the following products together as "Windows Server 2012".
 - Windows Server 2012
 - Windows Server 2012 R2
- In this document, unless there is a special explanatory note, ETERNUS DX200 S3 indicates ETERNUS DX200 S3 and ETERNUS DX200F. In addition, ETERNUS Disk storage system includes ETERNUS DX200F All Flash Arrays. However, the following functions are not supported in ETERNUS DX200F:
 - Energy saving operation for storage device
 - NAS operation for storage device
 - Automated Storage Tiering operation at multiple tiers (two or more)

Export Controls

Exportation/release of this document may require necessary procedures in accordance with the regulations of your resident country and/or US export control laws.

Trademarks

- Microsoft, Windows, Windows Server, Windows Vista and Internet Explorer are trademarks or registered trademarks of Microsoft Corporation in the United States and other countries.
- UNIX is a registered trademark of The Open Group in the United States and other countries.
- Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.
- Linux is a registered trademark of Linus Torvalds.
- Red Hat and RPM are registered trademarks of Red Hat, Inc. in the U.S. and other countries.
- SUSE is a registered trademark of Novell, Inc., in the United States and other countries.
- HP-UX is a trademark of Hewlett-Packard Company in the United States and other countries.
- AIX is a trademark or a registered trademark of International Business Machines Corporation in the United States and other countries.

- VMware, VMware logo, Virtual SMP, and vMotion are the registered trademarks or trademarks of VMware, Inc. in the United States and other countries.
- All other brand and product names are trademarks or registered trademarks of their respective owners.

Shipment Date and Revision History

Shipment Date	Revision	Document Part Number	
		PDF	HTML
December 2013	1	B1FW-6007-01ENZ0(00)	B1FW-6007-01ENZ2(00)
March 2014	1.1	B1FW-6007-01ENZ0(01)	B1FW-6007-01ENZ2(01)
April 2014	1.2	B1FW-6007-01ENZ0(02)	B1FW-6007-01ENZ2(02)
May 2014	1.3	B1FW-6007-01ENZ0(03)	B1FW-6007-01ENZ2(03)
August 2014	1.4	B1FW-6007-01ENZ0(04)	B1FW-6007-01ENZ2(04)

Notes

- No part of this manual may be reproduced without permission.
- This manual is subject to change without advance notice.

Copyright

Copyright 2013-2014 FUJITSU LIMITED

Update History

Content of Update	Updated Section	Revision
Notes when creating a NAS interface were added.	6.6.3.2	1.1
Notes when setting up an authentication server were added.	6.6.3.3	
The access method by CIFS protocol was changed.	6.6.4	
Operating environment was changed.	6.6.1.3	1.2
The information related to ETERNUS DX200F was described.	"Others" in Preface, 1.2.5, 6.6, 6.6.1.3, 7.1.1, 12.1.1.6, 12.1.2	1.3
Backup/restore procedure of Manager for Windows/Solaris in cluster environment is changed.	10.1.1.2.2, 10.1.1.2.6, 10.1.1.3.2, 10.1.1.3.6	1.4

Manual Organization and Reading Suggestions

Manual Organization

The following table describes the Manual organization of Express, Storage Cruiser and AdvancedCopy Manager.

When to Read	Related Manuals (Abbreviated)	Related Products (*1)			Explanation
		EXP	SC	ACM	
Before installation	Quick Reference	Yes	Yes	Yes	This manual is common for all products.
	Release Notes	Yes	Yes	Yes	This manual is common for all products.
	Overview	-	-	Yes	This manual is unique for the product.
During installation	Installation and Setup Guide	Yes	Yes	Yes	This manual is common for all products.
	Cluster Environment Setup Guide	-	Yes	Yes	This manual is common for Storage Cruiser and AdvancedCopy Manager.
	Migration Guide	Yes	Yes	Yes	This manual is common for all products.
During operation	Operation Guide	Yes	Yes	Yes	This manual is unique for each product. The following manuals are available: <ul style="list-style-type: none"> - Express Operation Guide - Storage Cruiser Operation Guide - Storage Cruiser Operation Guide for Optimization Function - AdvancedCopy Manager Operation Guide (for Windows) - AdvancedCopy Manager Operation Guide (for Solaris) - AdvancedCopy Manager Operation Guide (for Linux) - AdvancedCopy Manager Operation Guide (for HP-UX) - AdvancedCopy Manager Operation Guide (for AIX) - AdvancedCopy Manager Operation Guide for Copy Control Module
	Web Console Guide	Yes	Yes	Yes	This manual is common for all products.
Anytime	Event Guide	Yes	Yes	-	This manual is common for Express and Storage Cruiser.
	Messages	Yes	Yes	Yes	This manual is common for all products.
	Glossary	Yes	Yes	Yes	This manual is common for all products.

*1: "EXP" indicates Express, "SC" indicates Storage Cruiser and "ACM" indicates AdvancedCopy Manager.

How to Read Manuals

Please use the following table to find the most useful information in the Express, Storage Cruiser and AdvancedCopy Manager manuals to answer your inquiry.

Purpose	Manual	Main Contents	How to Read
Acquiring a product overview and	Quick Reference	<ul style="list-style-type: none"> - Product overview - Installation decision 	Please read if you want to acquire a fundamental knowledge of the product and

Purpose	Manual	Main Contents	How to Read
basic operation knowledge		<ul style="list-style-type: none"> - Overview of the necessary tasks from installation to first use 	its operation in order to decide to install it or not.
	AdvancedCopy Manager Overview	<ul style="list-style-type: none"> - Main functions - Linkable applications - Procedure overview for Advanced Copy of ETERNUS Disk storage system 	
Confirming the updated contents	Release Notes	<ul style="list-style-type: none"> - New function overview - Incompatibilities with previous version - Fixed bugs 	Please read if you want to know the updated contents from a previous version and if you perform the upgrade.
Deciding if a version upgrade is required	Migration Guide	<ul style="list-style-type: none"> - Notes and cautions about version upgrade - Version upgrade procedure 	Please read if you want to upgrade from a previous version.
Installing and correctly operating the product Setting up operating environment depending on purpose	Installation and Setup Guide	<ul style="list-style-type: none"> - Operating environment - Installation procedure - Setup procedure - Uninstallation procedure 	Please read if you want to install and setup the product.
	Cluster Environment Setup Guide	<ul style="list-style-type: none"> - Supported cluster software - Installation procedure for a clustered system - Setup procedure for a clustered system - Uninstallation procedure for a clustered system 	Please read if you want to install and setup the product on a clustered system.
Administration and operation of the installed system	Express Operation Guide	<ul style="list-style-type: none"> - Starting and stopping the software - Device monitoring - Data copy inside the storage system - Necessary tasks after an architectural modification of the system as well as product maintenance 	Please read if you want to start or shutdown the system, monitor the operation status, do backup/restore operations, etc.
	Storage Cruiser Operation Guide	<ul style="list-style-type: none"> - Starting and stopping the software - Device monitoring - Necessary tasks after an architectural modification of the system as well as product maintenance - Command reference 	

Purpose	Manual	Main Contents	How to Read
	Storage Cruiser Operation Guide for Optimization Function	<ul style="list-style-type: none"> - Operating environment construction - Operating status monitoring - Necessary tasks after an architectural modification of the system as well as product maintenance - Command reference 	
	AdvancedCopy Manager Operation Guide (for Windows)	<ul style="list-style-type: none"> - Starting and stopping the software 	
	AdvancedCopy Manager Operation Guide (for Solaris)	<ul style="list-style-type: none"> - Data backup/restore inside the storage system 	
	AdvancedCopy Manager Operation Guide (for Linux)	<ul style="list-style-type: none"> - Necessary tasks after an architectural modification of the system as well as product maintenance 	
	AdvancedCopy Manager Operation Guide (for HP-UX)	<ul style="list-style-type: none"> - Command reference 	
	AdvancedCopy Manager Operation Guide (for AIX)		
	AdvancedCopy Manager Operation Guide for Copy Control Module		
	Web Console Guide	<ul style="list-style-type: none"> - Operating environment - Screen layout description 	Please read if you want to understand the ETERNUS SF Web Console.
Dealing with messages issued by the software	Messages	<ul style="list-style-type: none"> - Messages and their explanations - Parameter (variable information) description - System action - Countermeasures 	Please read if you want a practical way of investigating and dealing with messages issued by the software.
Dealing with events issued by the software	Event Guide	<ul style="list-style-type: none"> - Phenomenon of event - Countermeasures 	Please read if you need to find a practical way of investigating and dealing with events.
Researching the meaning of specific terms related to the products and other important terms	Glossary	<ul style="list-style-type: none"> - Product specific terminology explanation - Explanation of important terminology appearing in the manual - Synonyms and related terms - Proper form of abbreviated terms 	Please read if you want to learn the meaning of important terms, product specific terms or abbreviations used in the manuals.

Contents

Chapter 1 Overview.....	1
1.1 Product Features.....	1
1.2 Summary of Each Function.....	1
1.2.1 Configuration management.....	2
1.2.2 Fault management.....	2
1.2.3 Performance management.....	3
1.2.4 Reporting Function.....	4
1.2.5 Energy-saving operation for storage device.....	7
1.2.6 Storage capacity virtualization operation.....	8
1.2.7 Support levels.....	9
1.3 Storage Cruiser Configuration.....	11
Chapter 2 Fault Monitoring.....	13
2.1 Receiving SNMP Traps.....	13
2.2 Analyzing SNMP Traps.....	14
2.3 Device Polling.....	15
2.4 Setting Event Levels.....	16
Chapter 3 Operation Design.....	17
3.1 LAN Connections.....	17
3.1.1 Network requirements.....	17
3.1.2 SNMP Community.....	18
3.2 Server node middleware for which management is possible.....	19
Chapter 4 Environment Configuration.....	21
4.1 Server Node.....	21
4.1.1 Solaris OS server node.....	21
4.1.1.1 SNIA HBA API library settings.....	21
4.1.1.2 N-port settings.....	21
4.1.2 Windows server node.....	22
4.1.2.1 SNIA HBA API library settings.....	22
4.1.2.2 N-port settings.....	22
4.1.3 Linux server node.....	23
4.1.3.1 SNIA HBA API library settings.....	23
4.1.3.2 Using the udev device.....	24
4.1.4 HP-UX server node.....	25
4.1.5 AIX server node.....	25
4.1.6 Other server nodes (Supported OS or Solaris OS/Windows/Linux/HP-UX/AIX without Agent).....	26
4.1.7 VMware server node.....	26
4.1.7.1 VMware vSphere 4 or later.....	26
4.2 Fibre Channel switch.....	28
4.2.1 SN200 (Brocade) Fibre Channel switch.....	28
4.2.1.1 Setting.....	28
4.2.1.2 Zoning.....	30
4.2.1.3 Problem-handling (FAQ).....	31
4.2.2 PRIMERGY Fibre Channel switch blade.....	34
4.2.3 Brocade VDX series.....	34
4.2.3.1 Setting.....	34
4.2.3.2 Zoning.....	35
4.2.3.3 Problem-handling (FAQ).....	36
4.2.4 PRIMERGY BX Ethernet Fabric Switch.....	38
4.3 Disk Array.....	38
4.3.1 Disk array ETERNUS DX series.....	38
4.3.1.1 Setting.....	38
4.3.1.2 Problem-handling (FAQ).....	41

4.4 NetApp FAS Series and V-Series Network Disk Storage system.....	41
4.5 ETERNUS VS850 Virtualization Storage.....	42
4.6 ETERNUS CS800 De-dupe Appliance.....	42
4.7 Tape Library Device.....	43
4.7.1 Tape library device ETERNUS LT250/LT270.....	43
4.7.2 Tape library device ETERNUS LT20/LT20 S2/LT40/LT40 S2/LT60/LT60 S2/LT200/LT210/LT220/LT230/LT270 S2.....	43
4.7.3 Virtual Tape Appliance ETERNUS CS2000.....	44
Chapter 5 Startup and Setting.....	45
5.1 Opening and Closing.....	45
5.2 Registering device.....	45
5.2.1 Device search.....	45
5.2.2 Registering a Device.....	47
5.2.3 Deletion.....	48
5.2.4 Function for setting event notification destinations.....	49
5.2.5 SNMP Trap transmission place automatic setting function.....	49
5.2.6 Registering a Manually Embedded Device.....	50
5.3 Checking Management Status.....	50
Chapter 6 Operation.....	53
6.1 Resource Management.....	53
6.1.1 RAID Group Management.....	53
6.1.2 Volume Management.....	53
6.1.3 Thin Provisioning Management.....	53
6.1.4 Advanced Copy Management.....	54
6.1.5 Connectivity Management.....	54
6.1.6 How to control the Eco-mode.....	55
6.1.7 End to End list display.....	56
6.1.8 Extreme Cache Management.....	58
6.2 Access Path Management.....	59
6.2.1 What is an access path?.....	59
6.2.2 Access path display (display of the logical relationship between a server node and storage systems).....	59
6.2.2.1 Access path status display.....	60
6.2.3 Access path setting.....	62
6.2.3.1 Preparations.....	64
6.2.3.2 Setting.....	64
6.2.4 Deleting an access path.....	67
6.2.4.1 Preparations.....	67
6.2.4.2 Setting.....	68
6.2.5 Access path inheritance.....	69
6.2.6 To manage Fibre Channel switch that has already set in port zoning.....	70
6.3 Event Display and Linkage.....	70
6.4 Thin Provisioning Management.....	73
6.4.1 Threshold Monitoring.....	73
6.4.2 Capacity Management.....	74
6.4.2.1 Capacity Graph Window Types.....	74
6.5 Automated Storage Tiering Management.....	75
6.5.1 Configure One Layer Tier Pool.....	75
6.5.1.1 Create One Layer Tier Pool.....	76
6.5.1.2 Change Single Layer Tier Pool.....	76
6.5.1.3 Delete One Layer Tier Pool.....	77
6.5.1.4 Expand Sub-Pool Capacity in One Layer Tier Pool.....	77
6.5.2 Configure FTV.....	78
6.5.2.1 Create FTV.....	78
6.5.2.2 Change FTV.....	78
6.5.2.3 Format FTV.....	78
6.5.2.4 Delete FTV.....	78
6.5.3 Measures to be taken when Tier pool configuration has been changed with managed devices.....	79

6.5.4 Change to Multiple Layer Tier Pool.....	79
6.6 NAS Management.....	79
6.6.1 Overview of Functions.....	79
6.6.1.1 About NAS Management.....	79
6.6.1.1.1 Basic System Configuration.....	80
6.6.1.1.2 Support Features.....	80
6.6.1.1.3 Configuration Items of the NAS File System.....	81
6.6.1.2 Backup of the NAS Environment.....	83
6.6.1.2.1 Backup/Restoration of NAS Volume.....	83
6.6.1.2.2 Mounting/Unmounting the NAS Backup Volume.....	84
6.6.1.3 Operating Environment.....	85
6.6.2 Required Setup Configuration.....	86
6.6.2.1 ETERNUS Disk Storage System Configuration.....	86
6.6.2.2 Authentication Server Setup.....	86
6.6.2.3 Prior Configurations for this Product.....	87
6.6.3 Installation Steps.....	88
6.6.3.1 Creating Shared Folder.....	88
6.6.3.2 Creating NAS Interface.....	91
6.6.3.3 Configuration of Authentication Server.....	92
6.6.4 Operation Method.....	93
6.6.4.1 Changing the Shared Folder.....	94
6.6.4.2 Changing the NAS Interface.....	95
6.6.4.3 Changing the Authentication Server.....	95
6.6.4.4 Activating Sharing.....	95
6.6.4.5 Stopping Sharing.....	96
6.6.4.6 Creating the NAS Backup Volume.....	96
6.6.4.7 Performance Management of NAS Volume.....	97
6.6.4.8 Capacity Management of Thin Provisioning Pool.....	97
6.6.4.9 Expansion of NAS File System.....	97
6.6.4.10 Deleting of the NAS Environment.....	98
Chapter 7 Performance Management.....	101
7.1 Overview.....	101
7.1.1 Performance Information Types.....	101
7.1.2 Performance Graph Window Types.....	104
7.1.3 Threshold Monitoring Types.....	104
7.2 Flow of Performance Management.....	105
7.2.1 Checking disk space on the Management Server.....	105
7.2.2 Instruction for performance management.....	105
7.2.3 Setting monitoring intervals.....	106
7.2.4 Displaying performance information of the selected device.....	108
7.2.5 Displaying Fibre Channel switch performance information.....	108
7.2.6 Displaying storage performance information.....	108
7.2.6.1 Displaying LogicalVolume and RAIDGroup performance information.....	108
7.2.6.2 Displaying disk (physical drive) performance information.....	108
7.2.6.3 Displaying CM performance information.....	108
7.2.6.4 Displaying CA and CMPort performance information.....	108
7.2.6.5 Displaying the number of active disks, power consumption, and temperature performance information.....	108
7.2.7 Examples of use of performance management.....	109
7.2.8 Instruction for stopping performance management.....	109
7.2.9 Updating configuration information.....	109
7.2.10 Performance data.....	110
7.3 Flow of Threshold Monitoring.....	110
7.3.1 Checking disk space on the Management Server.....	111
7.3.2 Instruction for threshold management.....	111
7.3.3 Setting the threshold monitoring hours.....	111
7.3.4 Setting the threshold monitoring information.....	111

7.3.5 Instruction for stopping threshold monitoring.....	111
7.4 Evaluation Criteria for Thresholds in Threshold Monitoring.....	111
7.5 Definition File.....	112
7.6 Examples of Threshold Monitoring.....	113
Chapter 8 Reporting Function.....	117
8.1 Overview.....	117
8.1.1 Set Policy.....	118
8.1.2 Collect Report Information.....	118
8.1.3 Create Report.....	119
8.2 Supported Device.....	121
8.3 Operation.....	121
8.3.1 Design.....	122
8.3.1.1 Define Charging Method.....	122
8.3.1.2 Concept of Volume Allocation Period.....	123
8.3.1.3 Define Report Information Retention Period.....	125
8.3.2 Setup.....	126
8.3.2.1 Obtain and Setup License.....	126
8.3.2.2 Setup Policy.....	126
8.3.2.3 Setup Periodic Command Execution.....	126
8.3.2.4 Create Accounting Application.....	127
8.3.3 Operation.....	128
8.3.3.1 Create Invoice.....	128
8.3.4 Maintain.....	128
8.3.4.1 Backup/Restore of Report Related Files.....	128
8.3.4.2 Error When Running Report Information Collection Command.....	129
8.3.4.3 Error When Running Report Creation Command.....	129
8.4 Configuration of Report File.....	129
Chapter 9 Maintenance of Devices to be Managed.....	136
9.1 Windows displayed in the event of a fault and troubleshooting.....	136
9.2 Replacing supported device.....	138
9.2.1 Replacing a server node.....	138
9.2.2 Replacing ETERNUS Disk storage system.....	139
9.2.3 Replacing ETERNUS LT250/LT270.....	141
9.2.4 Replacing Fibre Channel switch.....	142
9.2.5 Replacing manually embedded device.....	144
9.3 Replacing supported device components.....	145
9.3.1 Replacing server node components.....	146
9.3.1.1 Host bus adapter (HBA) replacement of server node.....	147
9.3.1.1.1 [For Solaris OS server node] Host bus adapter (HBA) replacement.....	147
9.3.1.1.2 [For operating systems other than the Solaris OS] Host bus adapter (HBA) replacement.....	148
9.3.1.2 Access path inheritance after HBA replacement.....	149
9.3.1.2.1 Post-replaced HBA state is "Changed".....	149
9.3.1.2.2 Post-replaced HBA state is "Unknown".....	149
9.3.2 Replacing faulty components of ETERNUS Disk storage systems, ETERNUS LT250/LT270.....	150
9.3.3 Replacing faulty components of a manually embedded device.....	150
9.4 Adding supported device components.....	153
9.4.1 Adding ETERNUS LT270 S2 extended cabinet.....	153
Chapter 10 Maintenance of the Administrative Environment.....	155
10.1 Maintenance of Manager.....	155
10.1.1 Maintenance of manager.....	155
10.1.1.1 Collecting data for troubleshooting.....	155
10.1.1.2 Backup of Manager.....	155
10.1.1.2.1 Backup of Solaris OS Manager.....	155
10.1.1.2.2 Backup of Solaris OS Manager (cluster environment).....	158
10.1.1.2.3 Backup of Linux Manager.....	159

10.1.1.2.4 Back up of Linux Manager (cluster environment).....	159
10.1.1.2.5 Backup of Windows Manager.....	159
10.1.1.2.6 Backup of Windows Manager (cluster environment).....	163
10.1.1.3 Restoring Manager.....	164
10.1.1.3.1 Restoring Solaris OS Manager.....	164
10.1.1.3.2 Restoring Solaris OS Manager (cluster environment).....	167
10.1.1.3.3 Restoring Linux Manager.....	167
10.1.1.3.4 Restoring Linux Manager (cluster environment).....	167
10.1.1.3.5 Restoring Windows Manager.....	167
10.1.1.3.6 Restoring Windows Manager (cluster environment).....	172
10.1.2 Changing the operating environment.....	172
10.1.2.1 Changing the IP address of the Management Server.....	172
10.1.2.2 Changing the IP address of a server node (host).....	172
10.1.2.3 Changing the server name of the Management Server.....	173
10.1.2.4 Changing the name of a server node (host).....	173
10.1.2.5 Changing the IP address or the SNMP Community name of a supported device.....	174
10.1.2.6 Changing the operation management of the clustered system (node name takeover).....	174
10.1.2.7 Changing the configuration of supported devices.....	174
10.1.2.8 Changing the password of supported devices.....	175
10.2 [Solaris OS Version] Maintenance of Agent.....	175
10.2.1 Action to take for troubleshooting.....	175
10.2.2 Collecting data for troubleshooting.....	175
10.2.3 Changing the administrative environment.....	176
10.2.3.1 Changing the IP address of a server node (host).....	176
10.3 [Windows Version] Maintenance of Agent.....	176
10.3.1 Action to take for troubleshooting.....	176
10.3.2 Collecting data for troubleshooting.....	176
10.3.3 Changing the administrative environment.....	176
10.3.3.1 Changing the IP address of a server node (host).....	177
10.4 [Linux Version] Maintenance of Agent.....	177
10.4.1 Collecting data for troubleshooting.....	177
10.4.2 Changing the administrative environment.....	177
10.4.2.1 Changing the IP address of a server node (host).....	177
10.5 [HP-UX Version] Maintenance of Agent.....	177
10.5.1 Collecting data for troubleshooting.....	177
10.5.2 Changing the administrative environment.....	177
10.5.2.1 Changing the IP address of a server node (host).....	177
10.6 [AIX Version] Maintenance of Agent.....	177
10.6.1 Collecting data for troubleshooting.....	177
10.6.2 Changing the administrative environment.....	177
10.6.2.1 Changing the IP address of a server node (host).....	178
Chapter 11 Linkage to Other Software.....	179
11.1 Linkage with Systemwalker Centric Manager.....	179
11.1.1 Linkage function with Systemwalker Centric Manager.....	179
11.1.2 Required versions.....	180
11.1.3 Preparations.....	180
11.1.4 Setup procedure.....	180
11.1.4.1 Setup on Systemwalker Centric Manager administrative client.....	180
11.1.4.2 Action to be taken if Systemwalker Centric Manager administrative server and this software Management Server are the same server.....	182
11.1.4.3 Setting confirmation test.....	185
11.2 Linking with Systemwalker Service Quality Coordinator.....	186
11.3 Linkage with Other Administrative Software.....	187
Chapter 12 Command References.....	188
12.1 Manager Commands.....	188
12.1.1 Commands for operating environment management.....	188

12.1.1.1 sanadmsh chtraprcvip (SNMP Trap transmission place IP address change command).....	188
12.1.1.2 swtraptest (SNMP Trap test for Fibre Channel switch).....	190
12.1.1.3 grtraptest (SNMP Trap test for ETERNUS Disk storage system).....	191
12.1.1.4 storageadm zone (Host affinity and zoning operation command).....	192
12.1.1.5 storageadm iscsizone (Host affinity operation command).....	197
12.1.1.6 storageadm perfdata (Performance information operation command).....	202
12.1.1.7 storageadm spindle (Disk control command).....	209
12.1.1.8 storageadm remcs (REMCS notification command).....	215
12.1.1.9 esfsnap (Troubleshooting information collection of Manager).....	215
12.1.2 Commands for storage management.....	217
12.1.2.1 storageadm disk (Disk management command).....	217
12.1.2.2 storageadm raid (RAID management command).....	218
12.1.2.3 storageadm volume (Volume management command).....	223
12.1.2.4 storageadm affinity (AffinityGroup management command).....	228
12.1.2.5 storageadm ecomode (Eco-mode management command).....	233
12.1.2.6 storageadm port (Port management command).....	234
12.1.2.7 storageadm iscsiport (iSCSI port management command).....	236
12.1.2.8 storageadm progress (Progress display command).....	241
12.1.2.9 storageadm perfctl (Performance monitoring command).....	243
12.1.2.10 storageadm device (Device management command).....	245
12.2 Agent Commands.....	246
12.2.1 setagtip (Agent information change command).....	246
12.2.2 traptest (SNMP Trap test for server node agent).....	248
12.2.3 agentsnap (Troubleshooting information collection of Agent).....	249
12.3 Starting and Stopping the Manager.....	250
12.3.1 Starting and stopping services (Windows environment).....	250
12.3.1.1 Starting and stopping the SNMP Trap monitoring service.....	250
12.3.1.2 Starting and stopping the service.....	251
12.3.2 Starting and stopping daemons (Solaris environment).....	252
12.3.2.1 Starting and stopping the SNMP Trap monitoring daemon.....	252
12.3.2.2 Starting and stopping the daemons at specific times.....	252
12.3.3 Starting and stopping daemons (Linux environment).....	253
12.3.3.1 Starting and stopping the SNMP Trap monitoring daemon.....	253
12.3.3.2 Starting and stopping the daemon.....	254
12.4 Starting and Stopping the Agent.....	254
12.4.1 Starting and stopping services (Windows environment).....	254
12.4.2 Starting and stopping daemons (Solaris, Linux, HP-UX, or AIX environment).....	255
12.5 Commands for Reporting Function.....	255
12.5.1 esfadm report collect (Report information collection command).....	255
12.5.2 esfadm report create (Report creation command).....	257
Appendix A Customization.....	260
A.1 Overview.....	260
A.2 sanma.conf Parameter.....	260
A.3 ssmgr.conf Parameter.....	261
A.4 perf.conf Parameter.....	262
A.5 SNMP Trap XML Definition File.....	264
A.6 Correlation.ini Parameter.....	271
A.7 Device Polling Setting File.....	272
A.8 Polling Service Setting File.....	276
A.9 Explanation of the Configuration Settings File.....	278
A.10 snmptrapd.conf Configuration File.....	280
A.11 policy.conf Parameter.....	282
Appendix B Troubleshooting.....	283
B.1 Collecting the troubleshooting information.....	283
B.2 Information for initial investigation.....	283
B.2.1 Collecting information from the Management Server (Solaris OS).....	284

B.2.2 Collecting information from the Management Server (Linux).....	284
B.2.3 Collecting information from the Management Server (Windows).....	284
B.2.4 Collecting information on the Managed Server node (Solaris OS).....	285
B.2.5 Collecting information on the Managed Server node (Windows).....	285
B.2.6 Collecting information on the Managed Server node (Linux).....	285
B.2.7 Collecting information on the Managed Server node (HP-UX).....	285
B.2.8 Collecting information on the Managed Server node (AIX).....	286
B.3 Information for further investigation.....	286
B.3.1 Collecting information from the Management Server (Solaris OS).....	286
B.3.2 Collecting information from the Management Server (Linux).....	287
B.3.3 Collecting information from the Management Server (Windows).....	287
B.3.4 Collecting information on the Managed Server node (Solaris OS).....	288
B.3.5 Collecting information on the Managed Server node (Windows).....	288
B.3.6 Collecting information on the Managed Server node (Linux).....	288
B.3.7 Collecting information on the Managed Server node (HP-UX).....	288
B.3.8 Collecting information on the Managed Server node (AIX).....	288
Appendix C How to check product version.....	289
C.1 To check the product version in Windows operating system.....	289
C.2 To check the product version in Solaris OS.....	290
C.3 To check the product version in Linux.....	290
C.4 To check the product version in HP-UX.....	290
C.5 To check the product version in AIX.....	291
Index.....	292

Chapter 1 Overview

1.1 Product Features

This software stands behind the stable operation of a multi-vendor storage system environment such as a SAN, a DAS, and a NAS using the configuration that provide integrated management of storage-related resources and functions of connection, fault and performance management, and reporting function.

Configuration management realizing total management of devices in an entire system

This function displays the status of each device in a current entire storage system and the status of physical connection between devices graphically on the Web Console. You can drill down from an icon of each device to the detail window to get detail information which part of the device (for example, a Fibre Channel switch port) is connected to which part.

Correlation management realizing total management of small-sized resources of all devices

This function not only manages detailed configurations within the storage devices but also automatically obtains the physical paths from disks and related server node configuration information, and then displays information correlating to this data on a single window.

It used to be very hard to recognize the correlation between entities because those entities were supported by their own management tools and were displayed in various formats respectively. In this software, the correlation of entities can be displayed in a common display format on a single window, and consequently the entire configuration can simply be grasped and an error can be detected if any configuration error should exist.

Fault management function for facilitating to locate of failed parts and affected areas

Failures that occur on devices are properly displayed in an understandable way.

Error information can be automatically reported to Systemwalker, integrated administrative software, and other vendors' Management Software, and centralized management of the system becomes available.

Optimal environment delivery via performance information management

Performance information of managed devices can be managed and displayed. Performance information of devices are stored on the Management Server, past performance information can be accessed as well as real-time performance information. Additionally, because performance information can be viewed in a graphic format, you can simply see the picture of the performance statuses and load statuses of devices.

In addition, threshold values can be set on devices so that alarms are reported when those threshold values are exceeded. The bottleneck causes and locations can be identified, and as a result, the configuration of devices is improved and the operation in the optimal environment is delivered.

Performance information can be viewed from the Report window of Systemwalker Service Quality Coordinator.

Reporting Function

This function collects capacity and usage time information for volumes connected to servers. This provides the required information for you to charge fees based on volume utilization.

1.2 Summary of Each Function

This section explains the function that this software provides for storage systems.

1.2.1 Configuration management

Connection status management

This function displays on the Web Console the status of physical connections between devices. This makes it possible to get a grasp of the access points for the parts of each device (for example, the Fibre Channel switch ports).

Also, since this function displays on the Web Console information correlating with the connections within the storage device and with the servers, it is possible to get a grasp of the entire configuration by looking at one screen.

The Web Console utilizes a web browser for operation and is used for the Storage Cruiser.

Access path management

This function manages and sets access paths automatically by performing integrated management of security functions provided from the server node side, Fibre Channel switch side, and storage side.

An access path can be automatically recognized and displayed from the binding/zoning information that has already been set in a device. Access paths are managed based on the security information from all registered devices. Even if a physical Fibre Channel cable or a SAN route that forms an access path is disconnected, the access path will be displayed with Error status.

For access paths managed by this software, the configuration definition of a device can be changed manually as well as automatically from this software. In such cases, it can check whether the manual configuration changes were performed correctly.



Point

.....

Devices subject to storage management must be registered with this software. To register a device, the IP address of the device is required. In addition, a user ID and password for management are required for the Fibre Channel switch.

.....

1.2.2 Fault management

The fault management function of this software has the three features described below.

The fault management function starts monitoring through the registration of the target device to the manager and continues monitoring processing during start up of the manager.



Note

.....

Fault monitoring is performed via LAN. As such, it is not possible to perform fault monitoring for devices which cannot be connected by LAN.

.....

Asynchronous fault event monitoring using event notification from devices

This software processes an SNMP Trap from a device and monitoring information from Agent, properly decodes them, and displays them as an asynchronous event.

Since the displayed contents of the event are more detailed and easier to understand than decodes generated by a normal SNMP MIB compiler, they support smooth operation.

The display format (show, hide) for events can be customized in detail by using an XML file. Therefore, operation can be made suitable for the environment used. In addition, fault management of a device not supported by this software is dynamically enabled by adding and editing the XML file.

Since events can be linked to the Systemwalker Centric Manager linkage and Shell files that can be edited as desired by users, operation can be made suitable for the environment used.



.....
Refer to "[A.5 SNMP Trap XML Definition File](#)" for details of customization.
.....

Fault monitoring using the device polling function (automatic operation by Manager)

The device polling function is a function for this software to observe regularly the state of all devices connected with LAN by using SNMP, ping or unique protocol. When the SNMP Trap from the device cannot be received, the change in the state of the device can be detected and the network error between each device and the Management Server of this software can be detected by this function.

The state change is reflected in the event log and the icon color.

This function is effective to the manual embedded device.

Fault monitoring by checking the current status of devices (manual operation performed by users)

The icon color of a device changes depending on the current status of the device by acquiring latest information.

If a problem occurs, a device status changes the display corresponding to its status.

1.2.3 Performance management

When the performance information reservation command is issued from the Main View, Domain view or SAN view for devices from which performance information is to be obtained, the performance management part of this software uses SNMP to obtain performance information from the devices and saves the obtained information on the Management Server. The information can be displayed and managed in the Web Console.

Performance control functionality supports the Fibre Channel switch and ETERNUS Disk storage systems. This function can be used to obtain the detailed operational status and load status of a device. Additionally, by knowing the number of active disks, it is possible to verify the Eco-mode status of the ETERNUS Disk storage system.

In addition, a threshold can be set for particular information. The function can detect a potential bottleneck and be used to address the problem.

The performance information can be referenced using Systemwalker Service Quality Coordinator. For details, refer to the Systemwalker Service Quality Coordinator manual.



.....
Refer to "[1.2.7 Support levels](#)" for details about supported devices.
.....

Information available for performance management

The information managed by the performance control is different for the fibre channel switch and ETERNUS Disk storage systems. Refer to "[7.1.1 Performance Information Types](#)" for details.

Information available for threshold monitoring

The information managed by the threshold monitoring is different for the fibre channel switch and ETERNUS Disk storage systems. Refer to "[7.1.3 Threshold Monitoring Types](#)" for details.

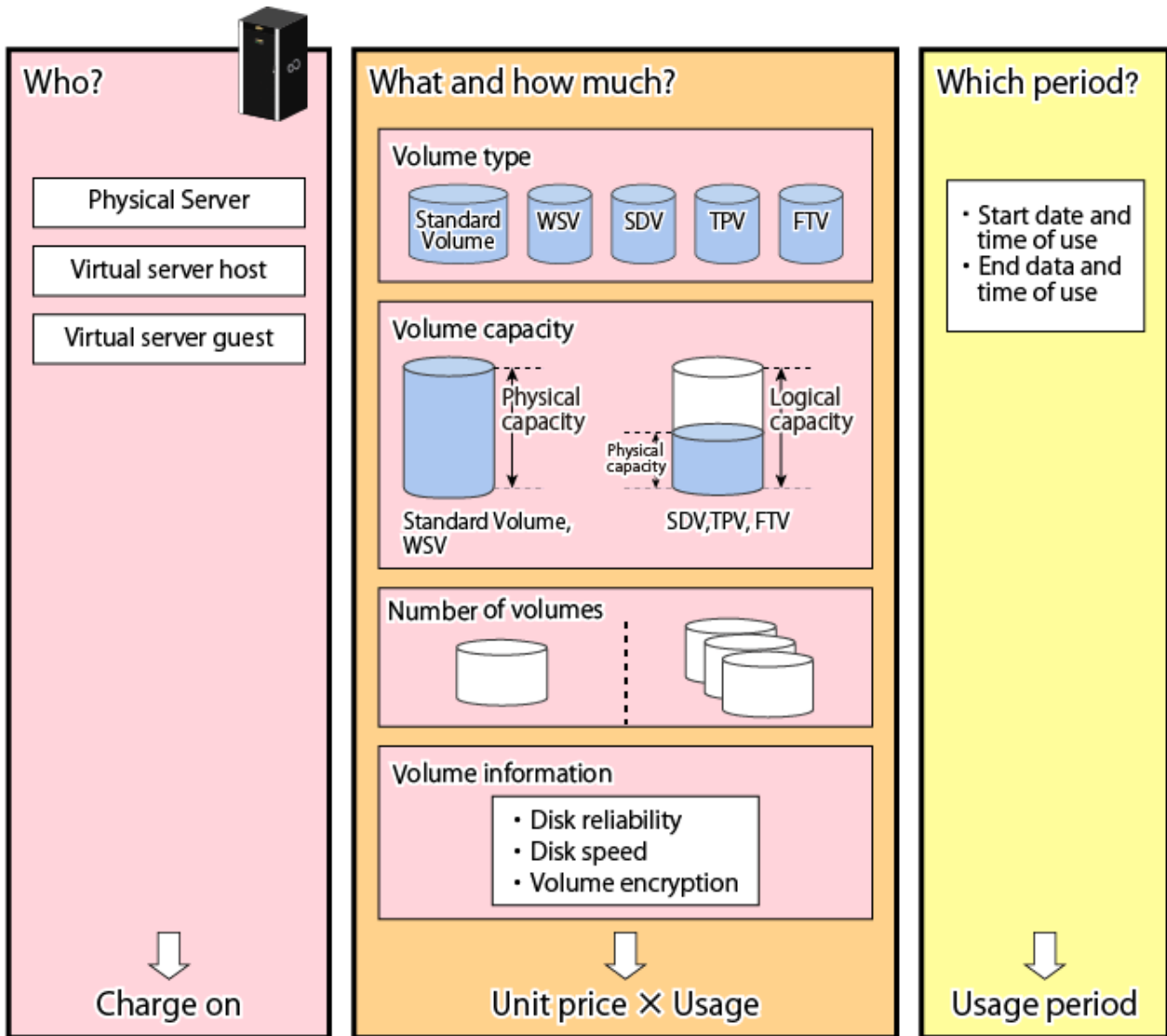
1.2.4 Reporting Function

The Reporting function collects the information associated with volumes connected to servers and outputs the information required for charging such as capacity information and usage time.

What is information required for charging?

To collect information required for charging, the following points should be made clear:

- Who used it?
- What and how much was used?
- In which period was it used?



Information collectable by the Reporting function

The information collectable by the Reporting function is as follows:

Table 1.1 Information collectable by the Reporting function

Information Collectable by the Reporting Function	
Unit of counting servers	Physical server
	Virtual server host

Information Collectable by the Reporting Function	
Volume type and capacity	Physical capacity of Standard Volume
	Physical capacity of WSV
	Logical capacity of SDV
	Logical capacity of TPV
	Logical capacity of FTV
Usage period	Start date and time of use
	End date and time of use
Volume information	RAID level
	Disk type: SAS, SSD, SED-SAS
	Volume encryption

Information

The following information cannot be collected by the Reporting function:

- Virtual server guest
- Physical capacity of SDV
- Physical capacity of TPV
- Physical capacity of FTV

Required operation for charging

For the center administrator to make an invoice, the following operation is required:



Center Administrator

Prepare

- Determine a policy for charging.
- Create an accounting application.
(Set Charged items and unit price)

Range of Reporting Function

Collect Report Information

- Collect report information (required for charging) per minimum unit of charged period.
(e.g.: When charging by the day, collect information once a day.)

Create Report File

- Tally up report information within charged period to create a report file per charged period.
(e.g.: If charged period is one month, create a report file once a month)

Make Invoice

- Input report file and make an invoice from accounting application.



Center User

1. Prepare
Determine charged items, unit price, charged period and minimum unit of charged period.
2. Collect Report Information
Collect the information required for charging.

3. Create Report File
Collected information is totaled.
4. Make Invoice
Make an invoice through an accounting application from the report file.

 **Point**

.....

The center administrator can create an accounting application with customized charged items and unit prices from a report file. This allows the center administrator to respond to various charging requirements.

.....

1.2.5 Energy-saving operation for storage device

ETERNUS Disk storage systems have an Eco-mode which controls the ON/OFF status for a disk drive spindle rotation based on Massive Arrays of Idle Disks (MAID) technology.

By stopping the spindle rotation at times when there is no disk drive access, it is possible to cut power consumption and provide an even more eco-friendly environment.

In this software, the following functionality is provided for ETERNUS Disk storage systems.

 **Note**

.....

This function cannot be used for ETERNUS DX200F.

.....

Controlling the Eco-mode

The Eco-mode can be controlled via the Web Console or by executing the storageadm command in the Management Server.

 **See**

.....

Refer to "[6.1.6 How to control the Eco-mode](#)" for details.

.....

Displaying the performance information for the number of active disks

Among all disks loaded in the ETERNUS Disk storage system, the disks that "Motor Status" is not "Idle" are displayed as the "number of active disks".

By using the performance information for the number of active disks, the effects of energy-saving operations can be easily verified.

 **See**

.....

Refer to "[7.2.6.5 Displaying the number of active disks, power consumption, and temperature performance information](#)" for details.

.....

Displaying power consumption and temperature performance information (ETERNUS DX60/DX60 S2/DX80/DX80 S2/DX90/DX90 S2/DX100 S3/DX200 S3, DX400 S2 series, DX500 S3/DX600 S3 and DX8000 S2 series only)

The amount of power used by an ETERNUS Disk storage system device as a whole is displayed as "Power consumption".

The peripheral temperature (fan intake temperature) of an ETERNUS Disk storage system is displayed as "Temperature".

By using the performance information for power consumption, the effects of energy-saving operations can be easily verified.

By using the performance information for temperature, the air-conditioning effects at the device periphery can be easily verified.



See

Refer to "[7.2.6.5 Displaying the number of active disks, power consumption, and temperature performance information](#)" for details.

Concerns in storage system operation when using Eco-mode

There are following concerns when using Eco-mode in storage system operation.

Unit of the Eco-mode control

The Eco-mode can be controlled for each RAID group. Therefore, when different transactions (type, online time, etc.) use a RAID group, the disk drives of its RAID group may not be able to be stopped depending on the operating policy of the transaction. Consider the relation between RAID group and transactions in the design of the storage system operation using Eco-mode.

Uncontrollable RAID groups

The Eco-mode is not available for the following RAID groups.

- A RAID group for which the system disk is included
- A RAID group for which it is set in the NAS area
- A RAID group for which the mainframe volumes, MVV volumes or MVV Concatenation volumes are registered
- A RAID group for which no volumes are registered
- A RAID group that includes an SSD
- A RAID group used by Thin Provisioning function
- A RAID group used by Flexible Tier
- A RAID group belonging to a REC disk buffer
- Temporary RAID group created while executing the Logical Device Expansion

Stopping disk drives

The ETERNUS Disk storage system stops a disk drive after confirming that its disk drive is not accessed within a certain period of time (30 minutes). Therefore, time more than its period is needed until the disk drive stops actually even if the "stop request" in this software is executed.

The ETERNUS Disk storage system does not stop a disk drive while the configuration of the RAID group or volume is changed and the Advanced Copy to access to its disk drive is done. Therefore, the disk drives may not be stopped even if the "stop request" in this software is executed. The disk drives will stop when the procedure is completed in the ETERNUS Disk storage system.

Starting disk drives

When it is accessed to the stopped disk drive, the ETERNUS Disk storage system starts its disk drive rotation. However, a few minutes (about three minutes) is needed until the disk drive becomes the accessible status.

Continuous disk drive rotation

When the number of the starting disk drive rotation exceeds the number of certain times (three times), the ETERNUS Disk storage system judges that its disk drive is used with high frequency and does not stop its disk drive rotation. Therefore, even if the "stop request" in this software is executed, after the disk drive status changes from "Idle" to "Active" and there is no access to its disk drive, its disk drive status may not change to "Idle".

The number of the starting disk drive rotation per one day is cleared to zero when time of ETERNUS Disk storage system becomes 00:00.

1.2.6 Storage capacity virtualization operation

The ETERNUS Disk storage systems below are equipped with a storage capacity virtualization function that uses Thin Provisioning technology.

Storage Device Name	Firmware Version
ETERNUS DX80 S2/DX90 S2 ETERNUS DX100 S3/DX200 S3 ETERNUS DX400/DX400 S2 series ETERNUS DX500 S3/DX600 S3 ETERNUS DX8000/DX8000 S2 series	All versions

Thin provisioning technology virtualizes and allocates storage resources, thus enabling the physical capacity of the storage to be reduced. Environments where thin provisioning have been installed manage physical disks as a common disk pool, and allocations to servers are treated as allocations to a virtual volume. When writing to a virtual volume, physical disks are allocated from the disk pool in accordance with the size of the data being written. Physical disks can be extended in accordance with the disk pool busy rate without affecting the servers. This enables users to start operation using only a small physical disk capacity to make large capacity virtual disk allocations to servers, thus keeping the initial investment low (small start).

In this software, the following functionality is provided for the above ETERNUS Disk storage systems with Thin Provisioning.

Configuration management

This function makes the associations between virtual volumes and physical disks visible. The Web Console displays the associations between the configuration that is virtualized by means of thin provisioning (disk pool and virtual volumes) and the physical configuration (RAID groups and physical disks). This function makes it easy to check the affected location when a physical disk fault or other problem occurs.

Threshold monitoring

This function monitors the disk pool threshold values and performs capacity management. Threshold values are established for the physical disk pool and these values are monitored so that consumption of the physical capacity does not cause disk pool shortages. When the disk busy rate reaches the threshold value, an alarm notifies the user, thus preventing operation stoppages.



See

.....
Refer to "6.4 Thin Provisioning Management" for details.
.....

Notes on storage capacity virtualization operation

There are following concerns when managing storage capacity virtualization operations.

Operations that are not possible

This product cannot perform the following operations related to thin provisioning and Flexible Tier:

- Performance monitoring of disk pools

1.2.7 Support levels

The scope of the storage management functions of this software that can be used varies with the storage device model being used. For this software, the scope of available functions is represented as support levels, which are used as settings of the fault monitoring function and for other purposes. The table below lists the support levels that can be selected.

Support Level	Typical Device Name	Device Detection	Fault Management			Management Window Linkage	Performance Management
			SNMP Trap Monitoring	Device Polling Monitoring (*1)	Acquisition of Device State		
A	ETERNUS DX series ETERNUS SN200 (except model 250M) ETERNUS PRIMERGY	Automatic (*2)	Y1	Y1	Y1	Y1	Y1 (*6)

Support Level	Typical Device Name	Device Detection	Fault Management			Management Window Linkage	Performance Management
			SNMP Trap Monitoring	Device Polling Monitoring (*1)	Acquisition of Device State		
	BX600 Fibre Channel switch blade Brocade series Brocade VDX series (*5) (*8) PRIMERGY BX Ethernet Fabric Switch (*5)(*8)						
B	Solaris OS, Windows, Linux, HP-UX, AIX server node on which Storage Cruiser's agent is already installed ETERNUS LT250/LT270 (*5)	Automatic (*2)	Y1	Y1	Y1	Y1	-
C	VMware vSphere 4 or later	Automatic (*2)	-	Y1	Y1	-	-
D	NetApp FAS Series NetApp V-Series	Manual	Y1 (*5)	Y1	-	Manual setting	Y1 (*7 For data collection only)
E	ETERNUS LT20/LT20 S2 ETERNUS LT40/LT40 S2 ETERNUS LT60/LT60 S2 ETERNUS LT200 ETERNUS LT210 ETERNUS LT220 ETERNUS LT230 ETERNUS LT270 S2 ETERNUS VS850	Manual	Y1 (*5)	Y1	-	Manual setting	-
	ETERNUS CS800 ETERNUS CS2000	Manual	Y1 (*5)	Y1	-	-	-
H	ETERNUS SN200 model 250M	Manual	Y1 (*5)	Y1	-	Manual setting	-
I	Other devices that are manually embedded	Manual	- (*3)	- (*4)	-	Manual setting	-

Y1: Detail information on device internal elements can be displayed.

Y2: Information on the device and FC port can be displayed.

*1: The protocols using in the device polling are as follows.

Typical device name	Protocol Name
ETERNUS DX series ETERNUS SN200 (except model 250M) PRIMERGY BX600 Fibre Channel switch blade	SNMP

Typical device name	Protocol Name
Brocade series Brocade VDX series PRIMERGY BX Ethernet Fabric Switch	
Server node on which Storage Cruiser's agent is already installed	unique protocol
VMware vSphere 4 or later	VMware dedicated protocol
Other than listed above	ping

*2: The "Detect device in subnet" function is not supported by the devices below. Specify and register the IP addresses.

- The following devices that firmware version is V20L20 or later:
ETERNUS DX400 series and ETERNUS DX8000 series
- Solaris OS, Windows, Linux, HP-UX, AIX server node on which Storage Cruiser's agent is already installed
- VMware server node
- ETERNUS LT250,LT270
- The following switches may not be able to be detected in subnet depending on the firmware version, etc.
ETERNUS SN200 series, Brocade series, PRIMERGY BX600 Fibre Channel switch blade, Brocade VDX series, PRIMERGY BX Ethernet Fabric Switch

*3: For devices supporting SNMP Traps, this function is enabled by creating a SNMP Trap XML definition file.

*4: For devices supporting LAN, ping monitoring is enabled by specifying an IP address at manual embedding.

*5: SNMP Trap transmission must be set for each device. (This software does not automatically make said setting.)

*6: There are concerns in performance information. Refer to the Note in "[7.1.1 Performance Information Types](#)".

*7: For NetApp FAS Series. To refer to the performance information that is collected on the NetApp FAS Series, must be linkage with Systemwalker Service Quality Coordinator. Contact Fujitsu Technical Support for details on performance information.

*8: Only as for devices whose firmware version number is 3.0.1 or later, the performance management function is supported.

1.3 Storage Cruiser Configuration

Storage Cruiser consists of the following programs: Manager function and Agent function.

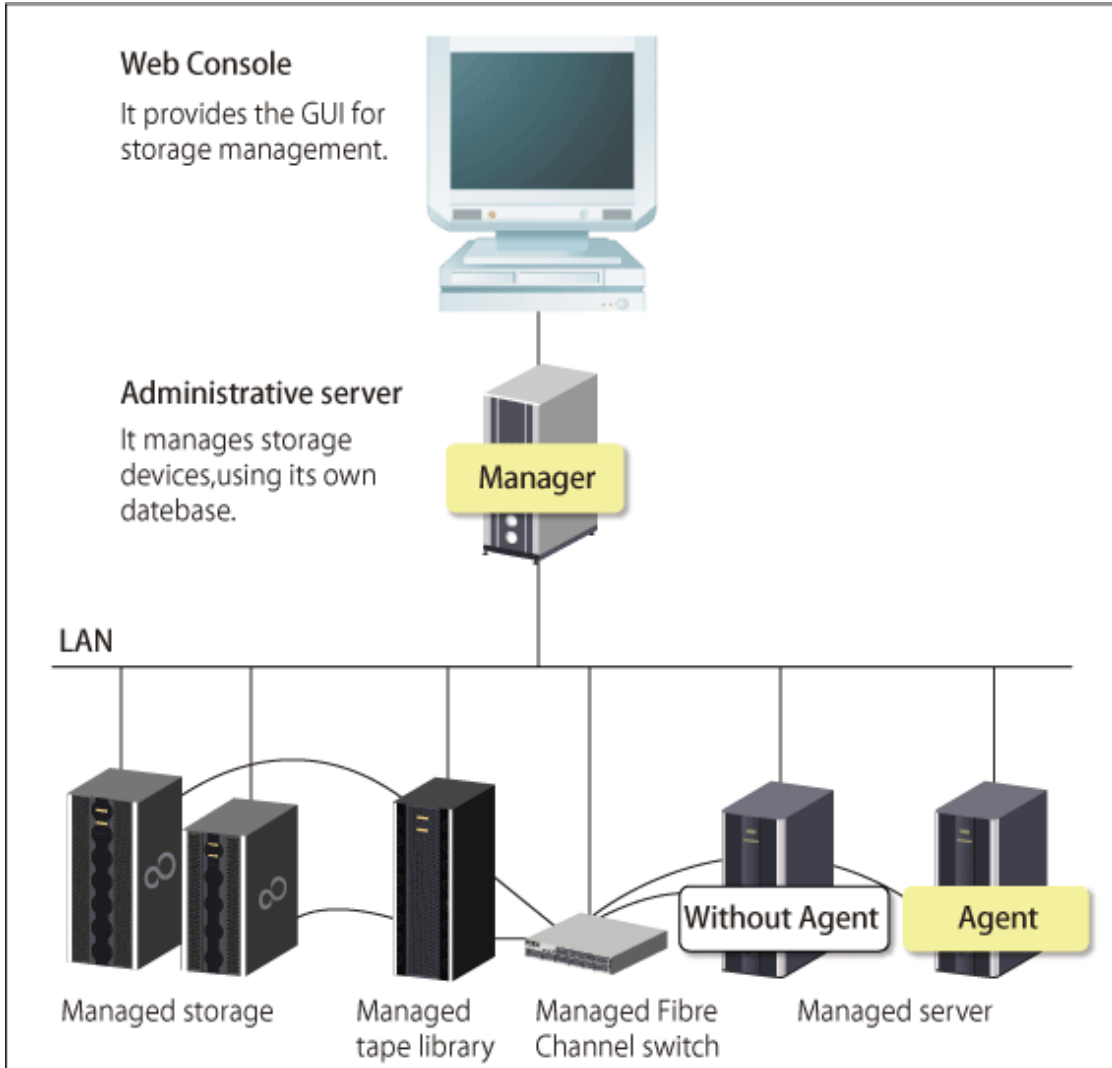
This guide refers to devices on which respective programs were installed as the Management Server and the server node. These programs can be installed on a single device and operated as well. In that manner, there is no restriction on the order of installation of these programs.

Manager function (Management Server) is the central management part of Storage Cruiser that obtains and sets information about devices involved in the storage system on the LAN. Important data among those used for controls are stored in the database.

Agent function (server node) controls information about home software such as an HBA and a multipath driver on the server node using the storage and communicates with Manager function. When there are several server nodes, it must be installed on each of them.

The Manager function is accessed using the Web Console. It is possible to connect to one ESC Manager from the multiple Web Consoles.

Figure 1.1 Storage Cruiser Configuration



Chapter 2 Fault Monitoring

This chapter describes how this software monitors for faults in devices consisting of a storage system and explains the fault information displayed and actions to be taken if an error occurs.

See

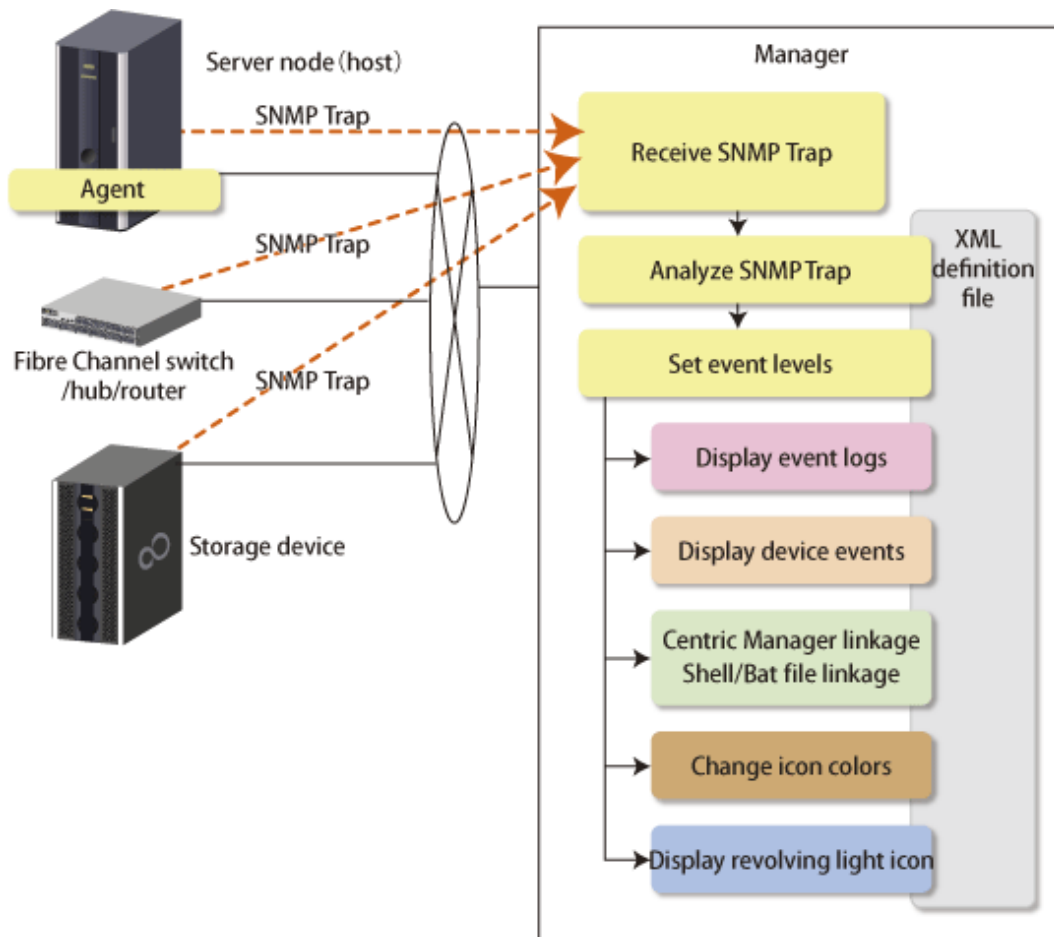
Refer to "1.2.2 Fault management" for details on fault monitoring.

Refer to the *ETERNUS SF Event Guide* for details on events.

Refer to "1.2.7 Support levels" for details on the support levels mentioned in this chapter.

This software performs the fault monitoring operation as explained below by processing events that are asynchronously reported by monitoring information from Agent and an SNMP Trap from each device. The SNMP Trap must be correctly set in the device that supports that SNMP Trap.

The Manager's event processing function is a resident function that is always when Manager is started (when the Management Server is started up). Therefore, a Web Console does not need to be started when a fault is only reported by Systemwalker Centric Manager linkage or Shell/bat linkage.



Manager processes event monitoring information from Agent in the same manner as for an SNMP Trap.

2.1 Receiving SNMP Traps

First, set up an environment in which devices can send SNMP Traps.

Server node

SNMP Trap transmission place addresses are automatically set for the server node agent when this software registers devices.

If Manager operates across multiple networks, however, this software may not be able to set correct settings for the server node agent. In this event, check whether SNMP Trap transmission place addresses are correctly set for the server node agent. The files indicated below for the server nodes specify the SNMP Trap transmission place addresses of the server node agent. Check the addresses, and edit any address that must be corrected. To operate according to the contents of the file the restart of Agent is needed.

Server Node OS	Place of File
Windows	\$TMP_DIR\ESC\Agent\var\sanm.ip (\$TMP_DIR means "Work Directory" specified at the Agent installation.)
Solaris OS, Linux, HP-UX, AIX	/var/opt/FJSVssage/sanm.ip

Note

The SNMP Trap fault monitoring function is not supported for VMware vSphere 4 or later.

Support levels A, B

When this software registers devices, SNMP Trap transmission place addresses are automatically set for devices to be managed.

However, if Manager operates across multiple networks, this software may not be able to set the correct setting for each device to be managed. In this case, check whether SNMP Trap transmission target addresses are correctly set for the managed devices.

In addition, if SNMP Trap transmission place addresses are automatically set, the SNMP Trap transmission send destination community name is fixed to "public".

Support levels E, I (for devices supporting SNMP Traps)

The SNMP Trap transmission place address is set on a device to the Management Server. For details of this setting, refer to the operation manual of the device.

Support level I (for devices not supporting SNMP Traps)

Fault monitoring by the mechanism is disabled since said devices do not support the SNMP Trap function.

Other server nodes (including Solaris OS and Windows server nodes without an agent) do not support fault management.

Note

Check whether the SNMP Trap monitoring service is running. If not, start it. For details about checking and starting the service, refer to the following sections:

- For Windows environment
"[12.3.1.1 Starting and stopping the SNMP Trap monitoring service](#)"
- For Solaris environment
"[12.3.2.1 Starting and stopping the SNMP Trap monitoring daemon](#)"
- For Linux environment
"[12.3.3.1 Starting and stopping the SNMP Trap monitoring daemon](#)"

2.2 Analyzing SNMP Traps

The Management Server processes SNMP Traps according to the support levels of the mechanism for devices, as described below.

- Server node agent

SNMP Traps are decoded.

- Support levels A, B and E

SNMP Traps are decoded. Incidentally, the only SNMP Traps decoded are those for which event display and linkage are required.

- Support level I (for devices supporting SNMP Traps)

Device-specific SNMP Traps are not decoded.

Note that SNMP Traps not supported by this software can be decoded, however, by creating a SNMP Trap XML definition file. For details, see "[A.5 SNMP Trap XML Definition File](#)".

Information

Methods of decoding SNMP Traps can be customized. Refer to "[A.5 SNMP Trap XML Definition File](#)" for details.

Note

If an Error or Warning level event is reported, update the corresponding storage system element status manually.

When the status of the storage system is recovered, also update the corresponding storage system element status manually.

The global status of the system containing the element is updated automatically.

Refer to "Reload ETERNUS Disk Storage System Configuration Information" in the *ETERNUS SF Web Console Guide* for details on the operation procedures.

2.3 Device Polling

The Manager checks the statuses of registered devices by using SNMP, ping or unique protocol at intervals of 60 seconds (default). It is as follows which polling method.

Polling Method	Protocol	Devices
Device status	SNMP	ETERNUS Disk storage system NetApp FAS Series and V-Series
Communication status	SNMP	ETERNUS SN200 series Fibre Channel switch PRIMERGY Fibre Channel switch blade Brocade Fibre Channel switch Brocade VDX series PRIMERGY BX Ethernet Fabric Switch
	unique protocol	server nodes for which Agent is installed
	private protocol	VMware vSphere 4 or later
	ping	Devices supporting automatic detection, other than the above devices. Manually embedded devices for which IP addresses are set.

- Device status polling method

For devices using SNMP, the system obtains status information using the respective vendor's private MIB. If the status has been changed compared with that stored by Manager, an event is displayed depends on the change.

- Communication status polling method

Changes in device status cannot be detected. However, if an abnormality occurs in the device or in a network between the device and the Manager and there is no response to a communication (non-communicating state), then an event is displayed and the icon color changes to gray. The next time there is a response to polling, the previous state (the one before the non-communicating state) is restored.

For VMware vSphere 4 or later, this software uses a private protocol of VMware. The communication status polling method does not detect changes in the device status, but does detect the non-communicating status. The polling is performed only for VM hosts; VM guests are not polled. When the non-communicating state is detected for a VM host, this software judges that the VM host and all the VM guests included in it are in the non-communicating state.

With either SNMP or ping, Systemwalker Centric Manager linkage and Shell/bat linkage are enabled by default. The swsag code reported to Centric Manager is 4822. The linkage behavior can be modified. For information see "[A.7 Device Polling Setting File](#)".

Users can customize polling intervals, the time at which operation stops, the specification of devices to be excluded from polling operation, and other device polling functions. For details, see "[A.7 Device Polling Setting File](#)".

Note

- When the device polling detects a change in network or device status, any event of "Device Polling Event" in the *ETERNUS SF Event Guide* is displayed. However, when the state change of device is detected by executing [Reload Conf.] operation, the following events are not displayed. Confirm the state from a Web Console.
- In a large-scale environment in which hundreds of devices targeted for polling are registered, not all the devices may be checked within 60 seconds (default). In that case, on the next polling cycle, the devices whose statuses were not checked on the last polling cycle are given priority. The polling interval can be changed. Refer to "[A.7 Device Polling Setting File](#)" for details.

2.4 Setting Event Levels

If Manager receives an SNMP Trap from a device, the device's status display on the Web Console is displayed as described below depending on the support level of the mechanism for the device.

There are three event levels: Error, Warning, and Information.

- Server node agent

The device status may or may not be changed.

For HBA faults and faults detected in the multipath driver, the device status will be changed to a status that is the same as the event level.

For faults detected in middleware besides the multipath driver, the device status is not reflected in the event-only display.

- Support levels A, B and E

The device status is changed to a status which is the same as the event level.

If you have performed "Reload Conf." after this, the device status for support levels A and B will be changed to the statuses read from the device.

- Support level I (for devices supporting SNMP Traps)

Status is not changed.

Information

The event level for individual SNMP Traps can be customized. Refer to "[A.5 SNMP Trap XML Definition File](#)" for details.

Chapter 3 Operation Design

3.1 LAN Connections

Manager manages devices, using the LAN I/Fs of a device subject to management.

Connect the LAN for management to all devices subject to management.

In this case, transactions affected by management can be minimized by separating the LAN for management from that for transaction.

3.1.1 Network requirements

When a firewall is placed between Manager and a device subject to management, set the following port numbers to be able to pass the firewall.

Communication with the manager

Transmission Destination Device	Port/Protocol	Transmission Start Direction	Function
Server node (Agent)	4917/tcp	Manager -> device	Configuration management, Polling monitoring
	162/udp	Device -> Manager	Fault management
Windows Server 2008 R2 (Hyper-V function installation environment) Windows Server 2012 (Hyper-V function installation environment)	5985/tcp	Manager -> device	Configuration management
VMware vSphere 4 or later VMware vCenter Server 4 or later	443/tcp	Manager -> device	Configuration management, Polling monitoring
Fibre Channel switch ETERNUS SN200 series Brocade Fibre Channel switch PRIMERGY Fibre Channel switch blade	161/udp	Manager -> device	Configuration management, Performance management, Polling monitoring
	23/tcp	Manager -> device	Configuration management
	162/udp	Device -> Manager	Fault management
Brocade VDX series PRIMERGY BX Ethernet Fabric Switch	161/udp	Manager -> device	Configuration management, Performance management, Polling monitoring
	830/tcp	Manager -> device	Configuration management
	162/udp	Device -> Manager	Fault management
Disk Storage System ETERNUS DX80 S2/DX90 S2 ETERNUS DX100 S3/DX200 S3 ETERNUS DX400 S2 series ETERNUS DX500 S3/DX600 S3 ETDRNUS DX8000 S2 series	161/udp	Manager -> device	Configuration management, Performance management, Polling monitoring
	22/tcp	Manager -> device	Configuration management, Performance management
	23/tcp	Manager -> device	Configuration management
	1999/tcp (*1)	Manager -> device	Configuration management

Transmission Destination Device	Port/Protocol	Transmission Start Direction	Function
	1372/tcp (*2)	Manager -> device	Configuration management, Performance management
	162/udp	Device -> Manager	Fault management
Disk Storage System ETERNUS DX60/DX60 S2/DX80/DX90 ETERNUS DX400 series ETERNUS DX8000 series	161/udp	Manager -> device	Configuration management, Performance management, Polling monitoring
	1999/tcp (*1)	Manager -> device	Configuration management
	23/tcp	Manager -> device	Configuration management (For ETERNUS DX60/DX60 S2/DX80/DX90)
	162/udp	Device -> Manager	Fault management
Disk Storage System other than listed above	161/udp	Manager -> device	Configuration management, Polling monitoring
	80/tcp	Manager -> device	Configuration management
	1999/tcp (*1)	Manager -> device	Configuration management
	162/udp	Device -> Manager	Fault management
Tape library ETERNUS LY250/LT270	161/udp	Manager -> device	Configuration management
	162/udp	Device -> Manager	Fault management
	ping/icmp	Manager -> device	Polling monitoring
Network disk array NetApp FAS Series and V-Series	162/udp	Device -> Manager	Fault management
	161/udp	Manager -> device	Polling monitoring
Manual embedding, and others	162/udp	Device -> Manager	Fault management
	ping/icmp	Manager -> device	Polling monitoring

*1: For Maintenance connection

*2: For Maintenance-Secure connection

3.1.2 SNMP Community

The SNMP Community names which the Manager uses for the managed devices and their SNMP transmissions are specified during device registration. The defaults for the managed device's SNMP Community names are as follows:

Transmission Destination Device	Default	Access	Method of Settings
Fibre Channel switch ETERNUS SN200 series Brocade Fibre Channel switch PRIMERGY Fibre Channel switch blade	public	read	Refer to "4.2.1.1 Setting" for detailed settings.
	private	read/write	
Brocade VDX series PRIMERGY BX Ethernet Fabric Switch	public	read	Refer to "4.2.3.1 Setting" for detailed settings.
Disk Storage System ETERNUS DX series	public	read	Refer to "4.3.1.1 Setting" for detailed settings.

The SNMP Community name can be changed with the Web Console.

3.2 Server node middleware for which management is possible

The server node middleware for which management is possible are as follows. Inquire for the latest support information.

OS Platform	Type of Middleware	Product Name	Version No.	Fault Monitoring
Solaris 9	Multipath driver	ETERNUS Multipath driver	2.0.1 or later	A
	Mirror disk driver	PRIMECLUSTER Global Disk Services	All versions	A
	File system	UFS	-	N/A
Solaris 10 (*2, *3)	Multipath driver	ETERNUS Multipath driver	2.0.1 or later	A
		MPxIO	-	A
	Mirror disk driver	PRIMECLUSTER Global Disk Services	4.1A40 or later	A
	File system	UFS	-	N/A
		ZFS	-	N/A
		QFS	-	N/A
Solaris 11 (*2, *4)	Multipath driver	MPxIO	-	A
	Mirror disk driver	PRIMECLUSTER Global Disk Services	4.3A10 or later	A
	File system	UFS	-	N/A
		ZFS	-	N/A
Windows Server 2003 (x86)	Multipath driver	ETERNUS Multipath driver	V2.0L10 or later	A
	File system	NTFS	-	N/A
Windows Server 2003 (x64)	Multipath driver	ETERNUS Multipath driver	V2.0L11 or later	A
	File system	NTFS	-	N/A
Windows Server 2008	Multipath driver	ETERNUS Multipath driver	V2.0L14 or later	A
		msdsm (*5)	6.0 or later	A
	File system	NTFS	-	N/A
Windows Server 2012	Multipath driver	ETERNUS Multipath driver	V2.0L19 or later	A
		msdsm (*5)	6.2 or later	A
	File system	NTFS, ReFS	-	N/A
RHEL-AS4 RHEL-ES4	Multipath driver	ETERNUS Multipath driver	V2.0L02 or later (*1)	A
	File system	ext2, ext3	-	N/A
RHEL5 RHEL6	Multipath driver	ETERNUS Multipath driver	V2.0L11 or later	A
		Device-Mapper Multipath	-	A
	File system	ext2, ext3	-	N/A
SUSE Linux Enterprise Server 11	Multipath driver	ETERNUS Multipath driver	V2.0L11 or later	A
		Device-Mapper Multipath	-	A
	File system	ext2, ext3, reiserfs	-	N/A

OS Platform	Type of Middleware	Product Name	Version No.	Fault Monitoring
HP-UX 11i v1	Multipath driver	PV-LINK (LVM function) (*6)	-	A
HP-UX 11i v2	Mirror disk	LVM	-	N/A
HP-UX 11i v3	Multipath driver	PV-LINK (LVM function) (*6)	-	A
		Native multipath function (*6)	-	A
	Mirror disk	LVM	-	N/A
AIX	Multipath driver	MPIO	-	A
	File system	JFS, JFS2	-	N/A

*1: For V2.0L02, it is necessary to implement the patch (ETERNUS Multipath driver V2.0L02 patch01).

*2: If using a zone with Solaris 10 or Solaris 11, the non-global zone is not supported for fault monitoring.

*3: If using a SUN-made HBA, only the file system (UFS, ZFS, and QFS) and the multipath driver (MPxIO) are supported.

*4: If using a SUN-made HBA, only the file system (UFS and ZFS) and the multipath driver (MPxIO) are supported.

*5: This is a multipath driver embedded as a standard in the Windows Server 2008 and later Windows operating systems.

*6: The [Mount Point] in the [End to End View] displays a hyphen ("-").

Chapter 4 Environment Configuration

This chapter provides settings and notes required for devices to be managed.

Flow of All Operations

Whether building a new storage system or using this software for an existing storage system, start the environment setup and operation according to the procedure indicated in the figure shown below. Software can be installed and set up on individual devices in any sequence.

Note that once this software is installed and devices to be managed are registered, regardless of the connection status from the Web Console, while the Management Server is starting up, the processing for when there is a fault/fault monitoring will be performed to the registered device. Also, for the device for which performance management is being performed, performance information will continue to be stored.

4.1 Server Node

4.1.1 Solaris OS server node

Two methods are used for managing Solaris OS server nodes: one method installs Agent on the host, and the other does not.

There is a difference in functionality depending on whether the agent was installed or whether it was not installed (with registration performed by manual embedding).



Refer to "3.2 Server node middleware for which management is possible" for information about products that can be monitored by Agent.



The limitations when Solaris OS server nodes are managed using the Agent:

- If device files of more than one controller number are generated

If more than one device driver type is used to access storage of a different type from a single HBA, device files for at least 2 controller numbers may be generated for the single HBA. This software does not support this status.

If there is a problem with information gathering or display, manage the server nodes using the manual embedding function. Refer to "5.2.6 Registering a Manually Embedded Device" for details on the manual embedding function.

4.1.1.1 SNIA HBA API library settings

To manage the HBAs that are installed at Solaris OS server nodes, the SNIA HBA API library that an HBA vendor distributes must be installed.

Refer to the *SNIA HBA API Library Installation Guide* at the following URL for details on how to install the HBA API library:

<http://www.fujitsu.com/global/services/computing/storage/eternus/documentation/>

4.1.1.2 N-port settings

N port setting is needed on the side of HBA when connecting with the Fibre Channel switch. The method of setting the port of HBA as N port depends on the HBA type. Each method for setting is shown below.

For Solaris OS default emlxs driver (target HBA : XSEFC401AF, XSEFC402AF, SG-XPCIE2FC-EM4, SG-XPCIE2FC-EM8, and so on.)

Specify "2" for the emlxsX-topology parameter in the /kernel/drv/emlxs.conf file.

```
#
# +++ Fibre Channel specific parameters +++
#
# topology: link topology for initializing the Fibre Channel connection.
#
#         0 = attempt loop mode, if it fails attempt point-to-point mode
#         2 = attempt point-to-point mode only
#         4 = attempt loop mode only
#         6 = attempt point-to-point mode, if it fails attempt loop mode
#
# Set point-to-point mode if you want to run as an N_Port.
# Set loop mode if you want to run as an NL_Port.
#
# Range: Min:0 Max:6 Default:0
#
emlxs0-topology=2;
emlxs1-topology=2;
```

For Solaris OS default qlc driver (target HBA : SE0X7F21F, SE0X7F22F, SG-XPCI1FC-QF2, SG-XPCI2FC-QF2, SG-XPCI1FC-QL2, SG-XPCI2FC-QF2-Z, SG-XPCI1FC-QF4, SG-XPCIE2FC-QF8, and so on.)

N port settings are not required.

4.1.2 Windows server node

This software provides two methods for managing Windows hosts: one method installs Agent on the host, and the other does not.

There is a difference in functionality depending on whether the agent was installed or whether it was not installed (with registration performed by manual embedding).



See

Refer to "3.2 Server node middleware for which management is possible" for information about the products that can be observed by Agent.

4.1.2.1 SNIA HBA API library settings

To manage the HBAs that are installed in Windows server nodes, the SNIA HBA API library that an HBA vendor distributes must be installed.

Refer to the *SNIA HBA API Library Installation Guide* at the following URL for details on how to install the HBA API library:

<http://www.fujitsu.com/global/services/computing/storage/eternus/documentation/>

4.1.2.2 N-port settings

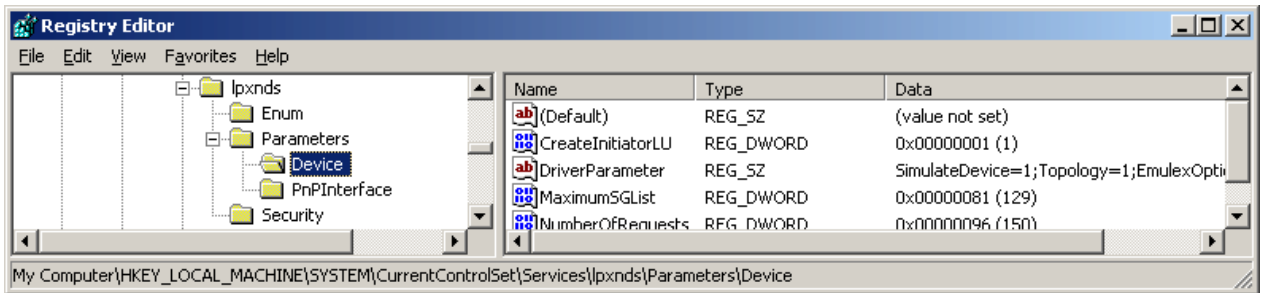
To connect Emulex Corporation LP7000, 8000, 9000, 9002L, 9802, 1050, 1050Ex, to a Fibre Channel switch, N-port settings are required on the HBA side.

To make up a SAN by connecting Emulex Corporation LP7000, 8000, 9000, 9002L, 9802, 1050, 1050Ex to the fibre channel switch, use the driver parameter in the registry to indicate explicitly that the topology is an N-port. The following indicates the procedure for setting the topology in the driver parameter:

1. Open the registry editor.
Select [Start] - [Run...] from the task bar, and then execute the following:
regedit.exe

2. Open the keyword of the following registry key, and then set the Topology value to 1:

```
HKEY_LOCAL_MACHINE\
System\
  CurrentControlSet\
    Services\
      lpxnds\
        Parameters\
          Device\
            "DriverParameter"      Topology=1
```



- The DriverParameter value depends on the version of the driver used. The Topology word may not exist depending on the driver version. In this event, the Topology word must be added. For details, refer to the readme file supplied with the driver or contact the HBA vendor.
- If the system accommodates more than one Emulex HBA and you want to connect them to Fibre Channel using different topologies, follow the above procedure for each HBA. For details, refer to the readme file supplied with the driver or contact the HBA vendor.
- The procedure involves changing the registry contents. Take particular care when carrying out the procedure because, if any part of the registry becomes corrupted as a result of an operation mistake or an operation that is not in the procedure, restarting the Windows system may not be possible.

4.1.3 Linux server node

This software provides Linux server nodes with two management methods. In one method Agent is installed and in the other method Agent is not installed.

There is a difference in functionality depending on whether the agent was installed or whether it was not installed (with registration performed by manual embedding).



Refer to "3.2 Server node middleware for which management is possible" for information about the products that can be observed by Agent.

4.1.3.1 SNIA HBA API library settings

It is necessary to install the HBA API library that the HBA vender distributes to manage HBA installed in the Linux server node.

Refer to the *SNIA HBA API Library Installation Guide* at the following URL for details on how to install the HBA API library:

4.1.3.2 Using the udev device

Information

- The udev device is a Linux function that always assigns a fixed device name, even if the hardware configuration is changed.

It assigns a device name that starts with "/dev/disk", unlike for existing device names, such as "/dev/sda".

"/dev/disk/by-path/xxxxxxx" xxxxxxxx is information generated from the disk location information

"/dev/disk/by-id/yyyyyyy" yyyyyyyy is information generated from the disk ID information

In the following explanations, device names that start with "/dev/disk/by-path" are shown as "by-path", and device names that start with "/dev/disk/by-id" are shown as "by-id". Existing device names, such as "/dev/sda", are shown as compatible device names.

If the Linux udev function is used for devices monitored using Storage Cruiser, use "by-id".

"by-id" is a symbolic link to "/dev/sd?name", therefore the relationship for "by-id" and the compatible device name displayed in this software can be checked by using the "ls -l /dev/disk/by-id" command.

Example

The method shown below checks "by-id" for "/dev/sdb"

```
# ls -l /dev/disk/by-id/  
Total 0  
lrwxrwxrwx 1 root root 9 April 3 21:28 scsi-1FUJITSU_300000690000 -> ../../sdb  
lrwxrwxrwx 1 root root 10 April 3 21:28 scsi-1FUJITSU_300000690000-part1 -> ../../sdb1  
lrwxrwxrwx 1 root root 10 April 3 21:28 scsi-1FUJITSU_300000690000-part2 -> ../../sdb2  
lrwxrwxrwx 1 root root 10 April 3 21:28 scsi-1FUJITSU_300000690000-part3 -> ../../sdb3  
lrwxrwxrwx 1 root root 10 April 3 21:28 scsi-1FUJITSU_300000690000-part7 -> ../../sdb7  
lrwxrwxrwx 1 root root 9 April 3 21:28 scsi-1FUJITSU_300000690001 -> ../../sdc  
lrwxrwxrwx 1 root root 10 April 3 21:28 scsi-1FUJITSU_300000690001-part1 -> ../../sdc1  
lrwxrwxrwx 1 root root 10 April 3 21:28 scsi-1FUJITSU_300000690001-part2 -> ../../sdc2  
lrwxrwxrwx 1 root root 10 April 3 21:28 scsi-1FUJITSU_300000690001-part3 -> ../../sdc3  
lrwxrwxrwx 1 root root 10 April 3 21:28 scsi-1FUJITSU_300000690001-part7 -> ../../sdc7  
lrwxrwxrwx 1 root root 9 April 3 21:28 scsi-1FUJITSU_300000690002 -> ../../sdd  
lrwxrwxrwx 1 root root 10 April 3 21:28 scsi-1FUJITSU_300000690002-part1 -> ../../sdd1  
lrwxrwxrwx 1 root root 10 April 3 21:28 scsi-1FUJITSU_300000690002-part2 -> ../../sdd2  
lrwxrwxrwx 1 root root 10 April 3 21:28 scsi-1FUJITSU_300000690002-part3 -> ../../sdd3  
lrwxrwxrwx 1 root root 10 April 3 21:28 scsi-1FUJITSU_300000690002-part7 -> ../../sdd7
```

Accordingly, it is possible to determine that "by-id" of "/dev/sdb" is "/dev/disk/by-id/scsi-1FUJITSU_300000690000".

Point

- "by-path" for the device that is connected to the Fibre Channel switch may change, therefore specify "by-id".
- Linux device nodes are displayed as compatible device name "sd?" in this software. The "by-id" and "by-path" are not displayed. Check the relationship using the command as shown above.

4.1.4 HP-UX server node

This software provides two methods for managing the HP-UX server node. In one method, Agent is installed on the node, in the other, it is not.

There is a difference in functionality depending on whether the agent was installed or whether it was not installed (with registration performed by manual embedding).



.....
Refer to "[3.2 Server node middleware for which management is possible](#)" for information on products that can be monitored by Agent.
.....

To manage the HBA mounted on an HP-UX server node, the HBA API library must be installed. When in doubt, contact your HBA sales representative.

4.1.5 AIX server node

This software provides two methods for managing the AIX server node. In one method, Agent is installed on the node, in the other, it is not.

There is a difference in functionality depending on whether the agent was installed or whether it was not installed (with registration performed by manual embedding).



.....
Refer to "[3.2 Server node middleware for which management is possible](#)" for information on products that can be monitored by Agent.
.....

To manage the HBAs that are installed in AIX server nodes, the HBA API contained OS standard FC driver must be installed. Refer to the AIX manuals for details.

Execute the following command to check that HBA API is installed.

```
# /usr/bin/lslpp -l | /usr/bin/egrep -c "devices.common.IBM.fc.hba-api"
```

When the execution result is "1" or more, HBA API is already installed.



.....
On an AIX agent installed server, the following problems may occur:

- It takes lots of time to register a server.
- It takes lots of time to reload configuration.
- The HBA port information for a target server may not be properly recognized.

If any of those mentioned above is seen, check all the HBA ports for proper connection. If there is any fibre channel device corresponding to an HBA port that is not connected, delete it if possible. To check HBA port-fibre channel device correspondence, refer to the AIX document. In addition, if the server is restarted, this operation may be needed again.

[Example of deleting unused fibre channel device fcs3]

```
# /usr/sbin/rmdev -Rdl fcs3
```

If a problem does not fall under those mentioned above, refer to "[B.1 Collecting the troubleshooting information](#)" to collect analysis material and contact Fujitsu Technical Support.
.....

4.1.6 Other server nodes (Supported OS or Solaris OS/Windows/Linux/HP-UX/AIX without Agent)

This software also provides a method for manually managing server nodes that are not supported by Agent or Solaris OS/Windows/Linux/HP-UX/AIX environments in which Agent is not installed.

Status inquiry or automatic reading of configuration data from a device cannot be performed, but the configuration can be changed by displaying the devices on the screen and manually editing the configuration.



See

.....
Refer to "[5.2.6 Registering a Manually Embedded Device](#)" for information on the procedure for registering the Managed Server without Agent.
.....

4.1.7 VMware server node

4.1.7.1 VMware vSphere 4 or later

This software supports VMware vSphere 4 or later.

If using VMware vSphere 4 or a later version, End to End display for the VM guests and storage devices can be supported by registering the VM host to the VMware vCenter Server.

It communicates directly with VMware ESX, VMware ESXi or VMware vCenter Server without using an Agent, and displays information about the VM host and VM guests.

Configuration management

This software communicates with the VM host (VMware ESX or VMware ESXi) to acquire information about the VM host itself and any VM guests (virtual machines and guest operating systems) on the VM host, and displays this information on the Web Console.

- Device registration

To register a VM host and its VM guests with this software, the IP address, login name and password of the VM host are required. By registering a VM host, all of the VM guests on the VM host are automatically registered.

It is not possible to register VM guests by specifying them individually.

For displaying the VM guests, the storage devices, and their End to End list:

- Registration of the VMware vCenter Server to which the VM host was registered is also necessary. An IP address, user name, and password are required for registering the VMware vCenter Server.
- When the VM host has been registered to the VMware vCenter Server using the IP address, specify the IP address registered to the VMware vCenter Server also when registering the VM host to this product.

If the IP address of a VM host is in IPv4 format, the IP addresses of its VM guests are displayed in the value that has set in IPv4 format.

If the IP address of a VM host is in IPv6 format, the IP addresses of its VM guests are displayed in the value that has set in IPv6 format.

- Device deletion

To delete a VM host from this product, it is required to first delete all the VM guests contained in the VM host. After deletion of the VM guests has completed, delete the VM host.

When a VM guest is specified, only the VM guest is deleted from this software.

- Access path management

This software supports setting up, deleting and inheriting the access paths associated with the HBA for the VM host.

This software does not support access path management for VM guests because it does not support HBA management.

When the access path environment modification (setting up, deleting and inheriting) is executed, reboot the VM host or execute the following procedures by using VMware Infrastructure Client.

1. Select the "Configuration" tab
2. Select "Storage Adapters" from Hardware lists.
3. From Hardware lists, select the device corresponding to HBA that the access path setting was changed.
At this time, select the device of the same name as logical HBA number displayed in the Web Console.
4. Execute "Rescan" from pop-up menu.

Fault management

- Receiving SNMP Trap

The fault management by using SNMP Trap function is not supported.

- Device polling

This software supports device polling for VM hosts. Device polling can be used to determine whether communications are possible between the Manager and VM hosts.

If a VM host cannot communicate, its VM guests will also be treated as though they cannot communicate.

This software cannot detect status changes for VM guests because it does not support device polling for VM guests.

Using the Web Console, perform [Reload Conf.] for the relevant device, and confirm the latest information.

Changing environment

- Changing the host name or IP address

When the hostname or IP address of a VM host is changed, it is necessary to delete its VM host from this software and register its VM host again after changing the hostname or IP address.

When the VM guest virtual machine name, the guest OS's IP address, or the guest OS's host name have been changed, perform [Reload Conf.] for the relevant device by using the Web Console.

- New creation of VM guest

When a new VM guest is created, perform [Reload Conf.] for the VM host containing the VM guest.

- User name and password

When the user name or password of the VM host has been changed, set the new username or password for this software using the Web Console.

- Moving VM guest between VM hosts

This software cannot automatically detect that a VM guest has been moved, whether it was moved with either VMware vMotion or VMware HA function. Communication with a moved VM guest is not possible. Therefore, when a VM guest is moved regardless whether the move was automatic or manual, perform the following procedures using the Web Console.

1. Delete the moved VM guest from its source VM host.
2. Perform [Reload Conf.] for the destination VM host to which the VM guest was moved.

If the source VM host from which the VM guest was moved is not registered on this product, execute only step 2 above.

If the destination VM host from which the VM guest was moved is not registered on this product, execute only step 1 above.



Note

- It is recommended that VMware Tools be installed on the guest operating system.
- VMware Tools must be running on the guest operating system in order to display information about the guest operating system (such as the IP address, host name, and the name and version of the operating system).
- If VMware Tools is not running, the virtual machine name will be displayed in the [name] for VM guests. When VMware Tools is started, the host name for the guest operating system will be displayed in the [name] for VM guests.
- If the same format (IPv4 or IPv6) IP address as the VM host is not set to VM guests, the IP addresses of the VM guests are not displayed.

- If VMware Tools is running, the name and the version of the guest operating system are displayed in the [OS]. (The OS version is not displayed in the [OS Level].) If VMware Tools is not running, the system name and the version number of VMware are displayed in the [OS] and [OS Level]
- If VMware Tools has been installed, the [Status] of VM guests will be "Normal" if VMware Tools is running. If VMware Tools is stopped, the device status will change to "Stop" (even if the guest operating system is running).
- If VMware Tools has not been installed, then the [Status] of VM guests will be "Normal" if the virtual machine is running and "Stop" if the virtual machine is stopped, regardless of the [Status] of the guest operating system.
- When it is not possible to communicate with the VM host because of inconsistency for user name and password, the [Status] of the VM host and its VM guest becomes "Warning".
- If more than one network adapter is defined in the VM guest, an IP address of the VM guest will be displayed only one. The IP address assigned to the network adapter with the highest number among the valid network adapters defined in the VM guest will be displayed.
- When operating an Exchange Server Database Availability Group (hereinafter referred to as "DAG") in the VM guest environment;
 - Set the IP address for management of the VM guest and the IP address for the DAG to another network adapter each. Assign the IP address for management of the VM guest to the network adapter with the highest number.
 - If the VM guest is a single network adaptor environment, newly allocate the network adaptor to the VM guest, and operate the network adaptor separately for IP address for DAG and IP address for the management of the VM guest.
 - IP address of the VM guest displayed with this product might be IP address for DAG in the DAG environment. In that case, add a new network adaptor to the VM guest, and set IP address for the management of the VM guest to it again. Perform [Reload Conf.] with the Web Console after setting.

4.2 Fibre Channel switch

4.2.1 SN200 (Brocade) Fibre Channel switch

This software supports ETERNUS SN200 series Fibre Channel switch, and PRIMERGY Fibre Channel switch blade.

The settings that must be directly defined on the device side before this software manages these Fibre Channel switches are explained below. Refer to the manual supplied with the respective device for details.

4.2.1.1 Setting

IP address, subnet mask, and gateway address (required)

Define the IP address, subnet mask, and gateway address for a LAN. If the Fibre Channel switch is equipped with an operation panel, these settings can be defined from the operation panel. If the Fibre Channel switch is equipped with a serial port, define them by issuing the ipAddrSet command via the serial port.

User name and password for Fibre Channel switch control

For Fibre Channel switch control, this software is used to log in using telnet to the device. Control requires a user name and password of the administrator security level. The factory default settings of user name and password are "admin" and "password", respectively.

If the password has been changed on the device side, when perform [Reload Conf.] for the relevant device with the Web Console, this software recognizes the change and the device status becomes a Warning display.

In order for the setting to match the changed device setting, perform a change to the account information for device management using the Web Console.

For some types of devices, the change of the password on the device side cannot be recognized automatically. Change the device management account information in the Web Console for these devices.

When connected to a cascade, some types of devices cannot automatically recognize the changed password. In this case, delete the device and register it again. Refer to ["5.2 Registering device"](#) for details on deleting and registering devices.

Domain name

A domain name is a unique name defined for a Fibre Channel switch in a SAN. Such names are necessary for a cascade connection of multiple Fibre Channel switches. Since domain names are automatically defined by firmware built into the individual Fibre Channel switches, the name need not be considered during definition and management of access paths using this software.

However, the domain names are important elements in manual port zoning. In such cases, make sure that no identical value is set for any two Fibre Channel switches in the cascade connection. If a Fibre Channel switch is equipped with an operation panel, a domain name can be set from the operation panel. If a Fibre Channel switch is equipped with a serial port or if network settings are defined for the Fibre Channel switch, log in to the switch, and set a domain name by executing the configure command.

SysName (recommended)

Register a switch name for Fibre Channel switch control. This software uses this switch name as SysName. SysName should be a name that is not identical to any other name registered with this software. If the Fibre Channel switch is equipped with an operation panel, a switch name can be set from the operation panel. If the Fibre Channel switch is equipped with a serial port or if the network settings are defined for the Fibre Channel switch, log in to the switch, and set a switch name by executing the switchName command.

Zoning setting

Zoning is recommended.

No zoning may be set for Fibre Channel switches. When Fibre Channel switches that are not set the zoning are connected to server nodes or storage devices, they are placed in a state where their security levels are undefined (which makes all of the Fibre Channel switches accessible from every server node). To prevent inadvertent access from destroying data on the storage side, recommend to set the temporary zone as follows. By this setting, it is able to stop all access paths of the Fibre Channel switches. After defining this setting, connect the server node and storage device to the Fibre Channel switch, and set up an access path using this software. When setting up a cascade connection between the Fibre Channel switch and another Fibre Channel switch for which zoning is already set, you need not define this setting because zoning information is copied. The setting is also not necessary if the default of zoning mode is set to "No Access" on the Default Zone function of the Fibre Channel switch.

```
zoneCreate"SNM_0001" , "00:0B:00:00:0E:00:00:00;00:0C:00:00:0E:00:00:00"  
cfgCreate"SNM_BCSI" , "SNM_0001"  
cfgEnable"SNM_BCSI"  
cfgSave
```

If the Fibre Channel switches are to be cascaded for operation, cascade the switches before executing the above command. Execute this command on a Fibre Channel switch where the latest firmware has been installed.

Note

- If the temporary zone has been created, all accesses will be blocked. For this reason, do not implement this measure while the target Fibre Channel switch environment is operating. Implement this measure either immediately after the Fibre Channel switch environment has been installed and before operations have started (or while operations are paused).
- The [storageadm zone command](#) cannot be used for the following Fibre Channel switches. In this cases, set the temporary zone.
 - Fibre Channel switches that the temporary zone is not set
 - Fibre Channel switches that default of zoning mode is not set to "No Access" on the Default Zone function

SNMP Community setting

This software handles fibre channel switches and SNMP transmissions.

The name of the SNMP Community used for SNMP transmission is specified when registering the switch. If the SNMP Community settings are at their defaults, this software communicates by using "public" or "private" for the SNMP Community name.

To change the SNMP Community name, change the device side, and then change the SNMP Community name in this software. It is possible to change the settings of this software from the Web Console.

SNMP-MIB setting

For the SNMP-MIB setting of the Fibre Channel switch (except for ETERNUS SN200 model 250M and Brocade AP7420), set the following by specifying the telnet command "snmpConfig --set mibCapability" or "snmpMibCapSet". Specify "yes" for the "FE-MIB", "SW-MIB", "FA-MIB", "HA-MIB" and "SW-TRAP" items. Leave the other items unspecified. Simply press ENTER for these unspecified items.

```
sn200:admin> snmpConfig --set mibCapability
  The SNMP Mib/Trap Capability has been set to support
(omitted)
FE-MIB (yes, y, no, n): [yes] yes
SW-MIB (yes, y, no, n): [yes] yes
FA-MIB (yes, y, no, n): [yes] yes
FICON-MIB (yes, y, no, n): [yes]
HA-MIB (yes, y, no, n): [yes] yes
FCIP-MIB (yes, y, no, n): [no]
ISCSI-MIB (yes, y, no, n): [no]
SW-TRAP (yes, y, no, n): [yes] yes
  swFCPortScn (yes, y, no, n): [yes]
  swEventTrap (yes, y, no, n): [yes]
  swFabricWatchTrap (yes, y, no, n): [yes]
  swTrackChangesTrap (yes, y, no, n): [yes]
(omitted)
sn200:admin>
```

The output of the above command may depend on the firmware version of the Fibre Channel switch. Change the settings of only the "FE-MIB", "SW-MIB", "FA-MIB", "HA-MIB" and "SW-TRAP" items.

Note that if HA-MIB items are not displayed, HA-MIB settings are not required.

If "FE-MIB" and "SW-MIB" are not set to "yes", searching and registering devices fail.

If "FA-MIB" is not "yes", physical connection information, port zoning information, and port speed (transfer rate) information on each port of the Fibre Channel switch is erroneously recognized.

The fault monitoring function will only run if "SW-TRAP" is set to "yes".

The director performance management function will only run if HA-MIB is set to "yes".

4.2.1.2 Zoning

This software uses the one-to-one WWPN zoning of the Fibre Channel switch as the basis for setting up and removing access paths (logical paths). However, it also supports other types of zoning settings at their respective levels. The functions that it supports for the different types of zoning are as follows:

No zoning setting (With this software, this is called the "no security state".)

This is a state that has no zoning setting. In this state, the Fibre Channel switch permits access between all ports. It is the factory default setting. However, if a Fibre Channel switch is connected in cascade to another Fibre Channel switch with a zoning setting, the zoning setting information is copied when cascade connection communication is established.

This software can perform management normally for the Fibre Channel switches without a zoning setting. Also, when registering a Fibre Channel switch with this software, you can specify whether to set zoning in response to a subsequent software attempt to set up an access path.

With no zoning setting, the Fibre Channel switch operates with security management delegated to the binding and affinity capabilities of server nodes and storage devices.

WWPN zoning setting

The WWPN zoning setting is a method by which zoning is defined based on the WWPN of a Fibre Channel port. A WWPN value that is unique throughout the world is defined for each port. As a result, no wrong access path is created even if the port connection place of the Fibre Channel switch is changed.

All access path control functions of this software are effective for access paths defined in the one-to-one WWPN zoning setting. For other defined access paths, this software can read access and display path information, but it cannot delete and inherit the access paths. However, it is possible to delete only zoning setup.

Port zoning setting

The port zoning setting is a method by which zoning is defined based on the specification of the port connection place of the Fibre Channel switch. A new port zoning setting must be defined if the port connection place of the Fibre Channel switch is changed.

As for the access path control functions, this software can read information about access paths for which port zoning is set, display the paths, and manage their status, but it cannot delete and inherit the access paths. However, it is possible to delete only zoning setup.

WWNN zoning setting

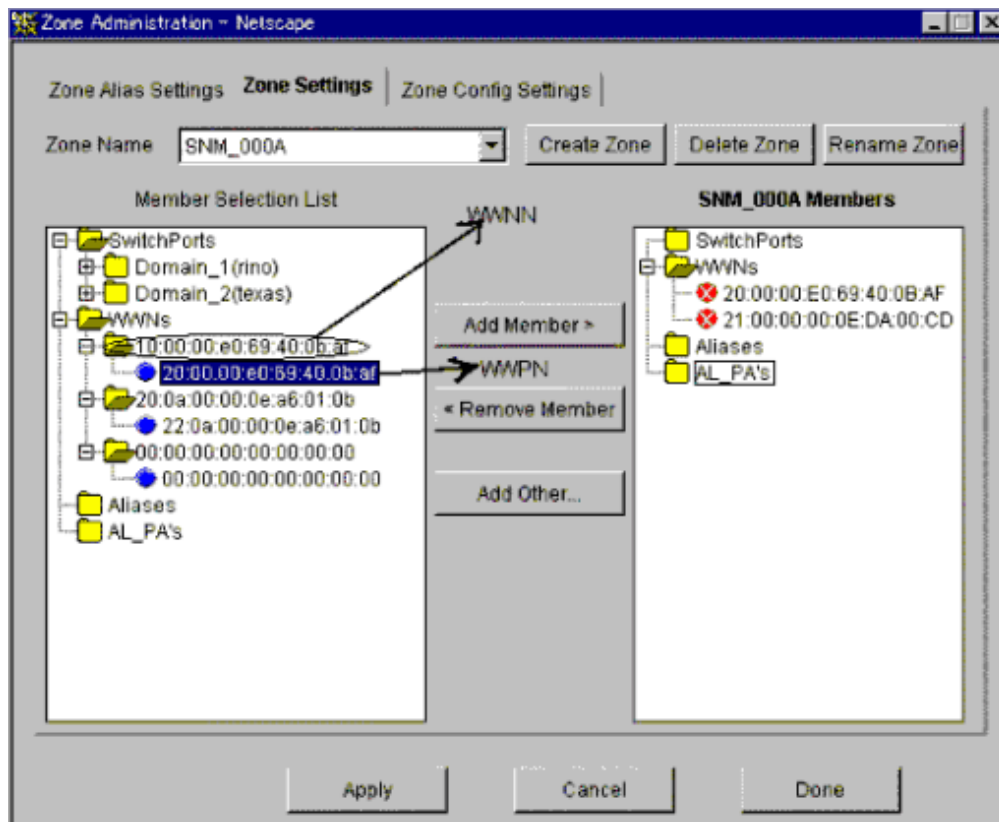
The WWNN zoning setting is a method by which zoning is defined based on the WWNN of a Fibre Channel port. Though a WWNN can be shared by several Fibre Channel ports, its definition differs from company to company.

As for the access path control functions, this software cannot display or delete access paths for which WWNN zoning is set. However, it can perform fault management of the Fibre Channel switch.

Different types of zoning settings can be defined for the Fibre Channel switch. To allow this software to provide complete zoning security, however, changing the existing zoning setting to the one-to-one WWPN zoning setting is recommended.

The zoning setting can be defined in the Zone Administration window of WEBTOOLS of the Fibre Channel switch. Note that settings in WEBTOOLS are dependent on the device and firmware.

For example, in the WEBTOOLS window of SN200M40 (v2.4) shown below, WWPNs are the values indicated by blue round disks on the Member Selection List and WWNNs are the values displayed next to the folder icons above the blue round disks.



4.2.1.3 Problem-handling (FAQ)

The device cannot be detected

- Check whether the SNMP Community settings on the device side agree with the settings of this software. Refer to "[SNMP Community setting](#)" for details.

- Check whether the SNMP MIB settings on the device side match the settings of this product. Refer to "[SNMP-MIB setting](#)" for details.
- For devices that do not support [Detect device in subnet] as described in "[1.2.7 Support levels](#)", use the IP address assignment.
- Check whether the Ethernet port communication speed has been set correctly.
- When setting the SNMP access control list, confirm the access from the manager is permitted.

A Warning for a device is displayed

- Check whether a hardware error (FC port, FAN, power supply, temperature, etc.) has occurred.
- Confirm whether or not the password is changed on the device side. If the password is changed on the device side, refer to "[User name and password for Fibre Channel switch control](#)" and change the registration information of this software.
- When the device is powered on or rebooted, initialization is performed in the device. perform [Reload Conf.] for the relevant device with the Web Console while the initialization is being performed, a Warning message for the device may appear. If no error occurs on the device, perform [Reload Conf.] for the relevant device using the Web Console after device initialization. The display then becomes Normal.

A Warning for an access path is displayed

- There is no zoning setting for configuring the access path.
- If a Warning is displayed on the screen, refer to "[A Warning for a device is displayed](#)".

An Error in an access path is displayed

- Check whether all the Fibre Channel switches connected in cascade are registered in this software. Register all the Fibre Channel switches that have not been registered.
- Make sure that the device in an access path is powered on and there is no problem with the LAN connection. Furthermore, check whether the SNMP Community settings on the device side agree with the settings of this software. Refer to "[SNMP Community setting](#)" for details.
If the network communication is disabled because of device replacement or maintenance, the physical connection line is not displayed.

A Warning for a server node is displayed (in yellow)

- Refer to "[An Error in an access path is displayed](#)".

When changing SNMP Community of a device

- Refer to "[SNMP Community setting](#)".

When changing the password of a device

- Refer to "[User name and password for Fibre Channel switch control](#)".

When PG-FCD101 or PG-FCD102 is not displayed

- Check whether there are zoning settings in the Fibre Channel switch that is connected to PG-FCD101 or PG-FCD102. If there are no zoning settings, refer to "[Zoning setting](#)" and then create a temporary zoning.

Note

- The ETERNUS SN200 series, Brocade Fibre Channel switch can define six monitoring device addresses (SNMP Trap transmission places) per device and a different SNMP Community name for each of these addresses. This software must be used by overwriting the entry where the name of SNMP Community is set in this public. If the device side is designed to change the name of SNMP Community of public and accordingly the settings of this software, the entry with the changed name of SNMP Community will be used.
- The ETERNUS SN200 series, Brocade Fibre Channel switch features the QuickLoop function that accomplishes FC-AL hub emulation. However, this software does not support Fibre Channel switches for which this function is enabled.
- This software communicates with the Fibre Channel switch using SNMP and telnet.

- It is recommended of Fibre Channel switch redundancy (cascading).

At present, the Fibre Channel switch zoning information cannot be restored from the database of this software. Therefore, multiple Fibre Channel switches must be connected in cascade to prevent the zoning information stored on the Fibre Channel switches from being erased. The zoning information is stored separately on each of the Fibre Channel switches connected in cascade. Even if one of the Fibre Channel switches fails, the zoning information is stored by the other switches.

The Fibre Channel switch zoning information is changed using the access path setting. When cascade connection is not used, be sure to save the device configuration information (configUpload file) after making changes in the settings. Refer to the manuals that come with the device for details on storing configuration information.

However, cascade connections should not be implemented between two or more ETERNUS VS900 model 300.

- To manage Fibre Channel switches with this software, all the Fibre Channel switches that are connected in cascade must be registered with this software. If any Fibre Channel switch is connected in cascade but not registered with this software, the SAN environment cannot be correctly managed.

- In consideration of incompatibility of Fibre Channel switch firmware, this software checks the firmware version number. If this software detects firmware that it does not support, all functions including the configuration management is restricted.

The following message is output to the event log. (XXXXXXX is the version number of the detected firmware.)

"Unsupported Firmware Version XXXXXX"

Contact your Fujitsu CE or SE because patches need to be applied to this software.

- The FC routing function is not supported.

If a cascade is connected using the FC routing function, the cascade connection line is not displayed in the Web Console.

For this reason, an error is displayed for the access path that goes through the cascade connection line, and a Warning is displayed for the server node that is used to configure the access path.

- To the GbE port, It may takes a time till SNMP Trap is notified.

Following SNMP Traps are displayed in the event log when execute disconnect/connect FC cable in a short time.

- When the cable is disconnected : [Link Down Trap]

- When the cable is connected : [Link Up Trap]

The port where the trouble occurs cannot be specified from the event log, also the event linkage function does not operate. Login to the Fibre Channel switch to specify the port where the trouble occurs, and confirm the state of the VE port and the GbE port.

* Also following event logs are displayed with above event log.

- When the cable is disconnected : [FC Port No.214 Offline]

- When the cable is connected : [FC Port No.214 Online]

- For GbE ports that are used in the FCIP tunneling function, virtual FC ports are displayed in the Web Console as follows.

Device	Number of virtual FC ports
SN200 model 450M Brocade 7500	16 (*1)
Brocade 7800	8
FCR/FCIP Blade (This is installed in SN200 model 540)	16 (*1)
Extension Blade (FC 8Gbps) (This is installed in Brocade DCX series)	20

*1: For firmware versions prior to v5.2.0, a Warning is displayed in the Web Console for the FC ports for which the FCIP tunneling function is disabled. Monitor the occurrence of errors using SNMP Trap.

- [1Gbit/s] is displayed as the VE port transfer speed.

- This software does not support the Administrative Domain (Admin Domain).

4.2.2 PRIMERGY Fibre Channel switch blade

Refer to "4.2.1 SN200 (Brocade) Fibre Channel switch" for information on how to set up the environment.

4.2.3 Brocade VDX series

This product supports the Brocade VDX series.

The following is a description of the items required to be preconfigured directly to the device side to manage the Brocade VDX series with this product. Refer to the manual provided with the device for details of those items.

4.2.3.1 Setting

Connecting to the Network (required)

Make the required settings for the Brocade VDX series which you use to connect to a network, and then connect to the network. Refer to the manuals provided with the respective devices for details on the setting method.

User name and password for Fibre Channel switch control

For Fibre Channel switch control, this software is used to log in using SSH to the device. Control requires a user name and password of the administrator security level. The factory default settings of user name and password are "admin" and "password", respectively.

If the password has been changed on the device side, when perform [Reload Conf.] for the relevant device with the Web Console, this software recognizes the change and the device status becomes a Warning display.

In order for the setting to match the changed device setting, perform a change to the account information for device management using the Web Console.

SysName (recommended)

Register a host name for Fibre Channel switch control. This software uses this host name as SysName. SysName should be a name that is not identical to any other name registered with this software.

Refer to the manuals provided with the respective devices for details on the setting method.

Zoning setting

Zoning is recommended.

No zoning may be set for Fibre Channel switches. When Fibre Channel switches that are not set the zoning are connected to server nodes or storage devices, they are placed in a state where their security levels are undefined (which makes all of the Fibre Channel switches accessible from every server node).

To prevent inadvertent access from destroying data on the storage side, recommend to set the temporary zone as follows.

By this setting, it is able to stop all access paths of the Fibre Channel switches. After defining this setting, connect the server node and storage device to the Fibre Channel switch, and set up an access path using this software.

When setting up a cascade connection between the Fibre Channel switch and another Fibre Channel switch for which zoning is already set, you need not define this setting because zoning information is copied.

The setting is also not necessary if the default of zoning mode is set to "No Access" on the Default Zone function of the Fibre Channel switch.

```
VDX-Sw# configure terminal
Entering configuration mode terminal
VDX-Sw(config)# zoning defined-configuration zone SNM_0001
VDX-Sw(config-zone- SNM_0001)# member-entry 00:0B:00:00:0E:00:00:00
VDX-Sw(config-zone-SNM_0001)# member-entry 00:0C:00:00:0E:00:00:00
VDX-Sw(config-zone-SNM_0001)# exit
VDX-Sw(config)# zoning defined-configuration cfg SNM_BCSI
VDX-Sw(config-cfg-SNM_BCSI)# member-zone SNM_0001
VDX-Sw(config-cfg-SNM_BCSI)# exit
VDX-Sw(config)# zoning enabled-configuration cfg-name SNM_BCSI
```

```
VDX-Sw Updating flash ...
VDX-Sw(config)# end
VDX-Sw#
```

If the Fibre Channel switches are to be cascaded for operation, cascade the switches before executing the above command.

Note

- If the temporary zone has been created, all accesses will be blocked. For this reason, do not implement this measure while the target Fibre Channel switch environment is operating. Implement this measure either immediately after the Fibre Channel switch environment has been installed and before operations have started (or while operations are paused).
- The `storageadm zone command` cannot be used for the following Fibre Channel switches. In this cases, set the temporary zone.
 - Fibre Channel switches that the temporary zone is not set
 - Fibre Channel switches that default of zoning mode is not set to "No Access" on the Default Zone function

SNMP Trap Settings

Although SNMP Trap is used in fault monitoring, the SNMP Trap send destination address automatic settings function is not supported for Brocade VDX series.

In order for SNMP Trap to be sent to the Management Server, log in to the device, execute the following commands in the given sequence, and then set the SNMP Trap send destination address.

If the Management Server is defined as a cluster, the logical IP address of the cluster needs to be set.

```
switch# configure terminal
switch(config)# snmp-server host [SNMP Trap send destination address] public version 1 udp-port 162
severity-level Warning
switch(config)# exit
```

Refer to the manuals provided with the respective devices for details on the setting method.

SNMP Community setting

If the SNMP Community settings are at their defaults, this software communicates by using "public" for the SNMP Community name.

To change the SNMP Community name, change the device side, and then change the SNMP Community name in this software. It is possible to change the settings of this software from the Web Console.

4.2.3.2 Zoning

This software uses the one-to-one WWPN zoning of the Fibre Channel switch as the basis for setting up and removing access paths (logicalpaths). However, it also supports other types of zoning settings at their respective levels. The functions that it supports for the different types of zoning are as follows:

No zoning setting

This is a state that has no zoning setting.

In this situation, if the default zoning mode is set to All Access, access is permitted across all the ports of the fibre channel switch. (This product refers to this situation as No Security status)

If the default zoning mode is set to No Access, access is blocked across all the ports of the Fibre Channel switch.

In the case of "No Access" or "All Access", if a Fibre Channel switch is connected in cascade to another Fibre Channel switch with a zoning setting, the zoning setting information is copied when cascade connection communication is established.

This software can perform management normally for the Fibre Channel switches without a zoning setting. Also, when registering a Fibre Channel switch with this software, you can specify whether to set zoning in response to a subsequent software attempt to set up an access path. With no zoning setting, the Fibre Channel switch operates with security management delegated to the binding and affinity capabilities of server nodes and storage devices.

WWPN zoning setting

The WWPN zoning setting is a method by which zoning is defined based on the WWPN of a Fibre Channel port.

A WWPN value that is unique throughout the world is defined for each port. As a result, no wrong access path is created even if the port connection place of the Fibre Channel switch is changed.

All access path control functions of this software are effective for access paths defined in the one-to-one WWPN zoning setting. For other defined access paths, this software can read access and display path information, but it cannot delete and inherit the access paths.

However, it is possible to delete only zoning setup.

WWNN zoning setting

The WWNN zoning setting is a method by which zoning is defined based on the WWNN of a Fibre Channel port. Though a WWNN can be shared by several Fibre Channel ports, its definition differs from company to company.

As for the access path control functions, this software cannot display or delete access paths for which WWNN zoning is set.



.....
In Brocade VDX series, the WWNN zoning can be set. To allow this software to provide complete zoning security, however, changing the existing zoning setting to the one-to-one WWPN zoning setting is recommended.
.....

4.2.3.3 Problem-handling (FAQ)

The device cannot be detected

- Check whether the SNMP Community settings on the device side agree with the settings of this software. Refer to "[SNMP Community setting](#)" for details.
- Check whether the Ethernet port communication speed has been set correctly.

A Warning for a device is displayed

- Check whether a hardware error (FC port, FAN, power supply, temperature, etc.) has occurred.
- Confirm whether or not the password is changed on the device side. If the password is changed on the device side, refer to "[User name and password for Fibre Channel switch control](#)" and change the registration information of this software.
- When the device is powered on or rebooted, initialization is performed in the device. perform [Reload Conf.] for the relevant device with the Web Console while the initialization is being performed, a Warning message for the device may appear. If no error occurs on the device, perform [Reload Conf.] for the relevant device using the Web Console after device initialization. The display then becomes Normal.

A Warning for an access path is displayed

- There is no zoning setting for configuring the access path.
- If a Warning is displayed on the screen, refer to "[A Warning for a device is displayed](#)".

An Error in an access path is displayed

- Check whether all the Fibre Channel switches connected in cascade are registered in this software. Register all the Fibre Channel switches that have not been registered.
- Make sure that the device in an access path is powered on and there is no problem with the LAN connection. Furthermore, check whether the SNMP Community settings on the device side agree with the settings of this software. Refer to "[SNMP Community setting](#)" for details.
At the registration process, check whether the device user name and password is changed or not. For more information, refer to "[User name and password for Fibre Channel switch control](#)".
If network communication is disabled due to the maintenance of device replacement, this error occurs.

When changing SNMP Community of a device

- Refer to "[SNMP Community setting](#)".

When changing the password of a device

- Refer to "[User name and password for Fibre Channel switch control](#)".

Note

- The connecting information is not displayed if connection type not supported by the device.
 - This product manages the device with the use of SNMP protocol version 1, SSH. For fault monitoring by SNMP Trap, SNMP protocol version 1 is also used.
 - This product supports only the operation mode in VCS modes. The standalone mode is not supported.
 - The switches managed by this product are all managed as a Fibre Channel switch.
 - This product manages RBridgeID as a domain ID.
 - It is recommended of Fibre Channel switch redundancy (cascading).
At present, the Fibre Channel switch zoning information cannot be restored from the database of this software. Therefore, multiple Fibre Channel switches must be connected in cascade to prevent the zoning information stored on the Fibre Channel switches from being erased. The zoning information is stored separately on each of the Fibre Channel switches connected in cascade. Even if one of the Fibre Channel switches fails, the zoning information is stored by the other switches.
The Fibre Channel switch zoning information is changed using the access path setting. When cascade connection is not used, be sure to save the device configuration information after making changes in the settings. Refer to the manuals that come with the device for details on storing configuration information.
 - To manage Fibre Channel switches with this software, all the Fibre Channel switches that are connected in cascade must be registered with this software. If any Fibre Channel switch is connected in cascade but not registered with this software, the connection cannot be correctly managed.
 - The beacon function is not supported.
 - If the user is logged on to the Fibre Channel switch using telnet or ssh, the Fibre Channel switch information cannot properly be obtained nor configured.
 - The FC routing function is not supported.
If a cascade is connected using the FC routing function, the cascade connection line is not displayed in the Web Console.
For this reason, an error is displayed for the access path that goes through the cascade connection line, and a Warning is displayed for the server node that is used to configure the access path.
 - If the transfer speed of FC port is configured by the Auto Negotiation function, this product displays the maximum transfer speed of FC port configured by the Auto Negotiation function.
 - FCoE port is not displayed.
 - As for the Ethernet port and FC port number, the following values are displayed in the Web Console based on the Index value output by "show fabric islports" command of Brocade VDX series.
 - When index value starts from 0 : Index value + 1
 - When index value starts from 1 : Index value
 - For Brocade VDX series firmware version 3.0.1 or later, if port disconnection or connection is done, the following SNMP Traps alone are displayed in the event log:
 - Cable disconnected : [Link Down Trap]
 - Cable connected : [Link Up Trap]
At this time, a failing port cannot be located from the event log. Also, the function in conjunction with event does not work. To locate the failing port, login to the Fibre Channel switch to check the port status.
 - 1GbE RJ45 port is not displayed.
-

4.2.4 PRIMERGY BX Ethernet Fabric Switch

Refer to "4.2.3 Brocade VDX series" for information on how to set up the environment.

4.3 Disk Array

4.3.1 Disk array ETERNUS DX series

4.3.1.1 Setting

To manage the ETERNUS DX series with this software, set up devices while keeping in mind the points listed below.



.....
Refer to the ETERNUS Web GUI manual supplied with the respective device for settings details.
.....

1. Community setting in SNMP (Agent) environment settings

This product communicates with an ETERNUS Disk storage system using SNMP. The SNMP Community name that this product uses for SNMP communication is specified when the ETERNUS Disk storage system is registered. If the SNMP Community name setting is default, this product communicates with the ETERNUS Disk storage system by "Community name: public". Therefore, the Community name on the ETERNUS Disk storage system side should be set to either of the following step a and b. Also, the Community name can be changed to other than "public". When using other than the default Community name, follow step c below for the device and set the Community name for this product from the Web Console.

In addition, for ETERNUS DX80 S2/DX90 S2/DX100 S3/DX200 S3, ETERNUS DX400 S2 series, ETERNUS DX500 S3/DX600 S3 and ETERNUS DX8000 S2 series, set "ViewALL" in the MIB view to the Community name.

- a. Community is not set. (default)
Many devices have "public" (Access: read Only, address: all hosts, and view: all Object) set as the default SNMP Community access.
However, the ETERNUS DX80 S2/DX90 S2/DX100 S3/DX200 S3, ETERNUS DX400 S2 series, ETERNUS DX500 S3/DX600 S3 and ETERNUS DX8000 S2 series have no default SNMP Community access. Access must be explicitly enabled. Enable access by following either step b or step c below.
- b. Specify "public" for the Community name explicitly.
In this case, specify either the IP address of the Management Server on which Manager is installed or 0.0.0.0 (to receive messages from all hosts) as the IP address.
- c. Specify other than "public" for the Community name explicitly.
Add the Community name and specify the Management Server's IP address. However, when the manager is running in a clustered system, the manager communicates with ETERNUS by using the physical IP address of the clustered system. Therefore the Community setup is described by the same number as the physical IP addresses.



.....
"ssc" is the specified Community name for SNMP communication with the Management Server (IP Address: 10.10.10.10):

```
community ssc 10.10.10.10
```

"sscom" is the specified Community name for SNMP communication with the Management Server operating as a clustered system operation (physical IP_A: 10.10.10.11, physical IP_B: 10.10.10.12):

```
community ssecom 10.10.10.11
community ssecom 10.10.10.12
```

2. Trap setting in SNMP Agent Configuration Setting

Since the manager's SNMP Trap receiving module has not judged this Community name, all SNMP Traps sent to the Management Server can be received. Even in an environment where the Community name is specified other than default, it is not necessary to change this Community name in trap setting. The Community name of the trap destination is recommended to be set as "public", not same as the Community name of SNMP Community under the consideration of security.

In the ETERNUS Disk Storage system, if the number of the SNMP Trap transmission destination is set to the maximum number of register, no new IP address can be added. Therefore, make sure that the number of SNMP Trap transmission destination is less than the maximum number.

3. Device name setting (SysName) in SNMP (Agent) environment settings

Register a nickname for storage management. This software uses this value as SysName.

When changing the device name while AdvancedCopy Manager CCM is in use, refer to "Changing the registered information for ETERNUS Disk storage system" in the *ETERNUS SF AdvancedCopy Manager Operation Guide for Copy Control Module* to change the registered information.

4. Network environment settings

If the Management Server resides outside the location indicated by the IP address, subnet mask, gateway, and subnet, the subnet of the Management Server must be registered as the destination network address.



When the Management Server is in a cluster:

If you specify the IP address of the Management Server as a destination network address, specify both physical IP address of each node on the Management Server in a cluster and IP address taken over.

5. Generation of SSH server key (ETERNUS DX80 S2/DX90 S2/DX100 S3/DX200 S3, ETERNUS DX400 S2 series, ETERNUS DX500 S3/DX600 S3 and ETERNUS DX8000 S2 series only)

Execute the generation of the SSH server key needed for the SSH communication between this software and the devices. The bit number of the SSH server keys is arbitrary.

6. Creation of Software role account (ETERNUS DX80 S2/DX90 S2/DX100 S3/DX200 S3, ETERNUS DX400 S2 series, ETERNUS DX500 S3/DX600 S3 and ETERNUS DX8000 S2 series only)

Create an account for this software to manage a device.

Note the following restrictions about the account.

- The root user cannot be used it to manage this software.
- The account should be a software role.
Select Software as the user level when creating the account
- Specify this account information when you register a device in this product.

If you have changed the user name or password on the device side after having registered the account to this software, performing "Reload Conf." for the relevant device causes this product to recognize the password change made on the device side and the device will have a Warning message displayed.

Change the device management account information in the Web Console to make it match with the change in settings made on the device side.

7. SSL Certificate generation or registration (ETERNUS DX80 S2/DX90 S2/DX100 S3/DX200 S3, ETERNUS DX400 S2 series, ETERNUS DX500 S3/DX600 S3 and ETERNUS DX8000 S2 series only)

This product uses an HTTPS connection to manage the storage devices (default).

In order to be able to use a HTTPS connection with the storage devices, choose one of the following settings:

- Create Self-signed SSL Certificate Setting

- Register SSL Certificate Setting

8. Logoff

Be sure to log off from the ETERNUS Web GUI after completing the setup in the ETERNUS Web GUI.

You must be logged off from the ETERNUS Web GUI in order to perform registration of the device to this product.

9. ETERNUS Web GUI network settings (ETERNUS DX60/DX60 S2/DX80/DX90, ETERNUS DX400 series and ETERNUS DX8000 series only)

- For the ETERNUS DX60/DX60 S2/DX80/DX90

Under the ETERNUS Web GUI Global Settings tab, click **Setup Network Environment** in the Network Settings and check the settings for the following items:

- Check that "Enable" is specified for Maintenance connections.
- Check that "Disable" is specified for Maintenance-Secure connections.

- For the ETERNUS DX400 series and ETERNUS DX8000 series

Click **Various Settings > Network Environment Configuration (USER Port)** in the main menu for ETERNUS Web GUI and check the settings for the following items:

- Check that "Enable" is specified for Maintenance Port.
- Check that "Disable" is specified for Maintenance-Secure Port.

Information

For this software, the host access control function of ETERNUS Disk storage system is called "host affinity function", and zone numbers are called "AffinityGroup numbers".

To use this software to set the server node and storage access path (the SAN environment containing the Fibre Channel switch), refer to "[6.2.3.1 Preparations](#)". The following settings must also be configured in the device.

The following settings can be set up from this product, so it is not necessary to perform setup from the device side.

- RAID Settings
- Storage's AffinityGroup/Zone Settings
- Connection Configuration Settings
- Host Interface Settings
- HostWWN Definition
- HostWWN-AffinityGroup/Zone Definition

Date-time settings

To set the date-time for the device, perform the procedure shown below. If the date-time is set during performance monitoring, briefly stop performance monitoring and then restart it.

1. Stop performance monitoring of the device for which date-time is set.
2. Set date-time for the device.
3. After the date-time settings are complete, restart performance monitoring of the device.

Device configuration changing

To change the configuration for the device, the device configuration information kept by performance management must be updated. Update the configuration information according to the procedure in "[7.2.9 Updating configuration information](#)".

4.3.1.2 Problem-handling (FAQ)

Unable to detect ETERNUS DX series

- This software uses SNMP communication to find devices. Therefore, a storage device whose SNMP function is inactive cannot be detected. The storage device's SNMP function must be started.
- This software may be unable to automatically detect the device if SNMP Trap transmissions are set to a specific server but a server which has Manager operating on it is not set as the SNMP Trap transmission destination. Check the settings for the SNMP Trap transmission destination.
- If the SNMP Community name is changed and Manager is in the cluster environment, settings on the storage device side may be incorrect. Refer to "[Changing SNMP Community name](#)" given below.
- Check that there are no problems with the settings for the storage device and its network environment. This includes network environment settings, access permission settings, transmission mode settings, and so on. Refer to the section "[4.3.1.1 Setting](#)" for network settings. For transmission mode settings, if transmission mode on one side of the connection is "Auto Negotiation" and "FULL (full duplex)" on the other, transmissions may be unable to be sent or slow down, so make sure that the transmission mode is set correctly.

Changing SNMP Community name

- The name of the SNMP Community used for SNMP transmission is specified when registering the ETERNUS Disk Storage system. If the SNMP Community settings are at their defaults, this software implements SNMP communication using the Community name public by default. If "Set SNMP Agent Environment"- "Set Community" is not set at all for ETERNUS Disk Storage system other than ETERNUS DX80 S2/DX90 S2/DX100 S3/DX200 S3, ETERNUS DX400 S2 series, ETERNUS DX500 S3/DX600 S3 and ETERNUS DX8000 S2 series, "public" (access: readOnly, address: all hosts, view: all objects) has been set as the initial value. If at least one community is set, this software communicates with only the specified community settings. When the SNMP Community name for the ETERNUS storage devices is to be changed, storage device settings are required. Refer to step 1 "Community setting in SNMP (Agent) environment setting" in "[4.3.1.1 Setting](#)".

Timeout occurs in communication

- Check that there are no problems with the settings for transmission mode in the storage device and its network environment. For transmission mode settings, if transmission mode on one side of the connection is "Auto Negotiation" and "FULL (full duplex)" on the other, transmissions may be unable to be sent or slow down, so make sure that the transmission mode is set correctly.

Status displayed by this software differs from the actual status of the device

- When the device is under the maintenance, the status displayed with this software might be different from an actual status of the device.
- If the redundant copy function was running on ETERNUS DX60/DX60 S2/DX80/DX90, the overall status on the ETERNUS Web GUI is "Error", but "Warning" is displayed by this software.

4.4 NetApp FAS Series and V-Series Network Disk Storage system

This software supports fault management and linkage to the Management Software for NetApp FAS Series and V-Series. Embed a device and register its IP address by referring to "[5.2.6 Registering a Manually Embedded Device](#)".

1. Connecting to the network

Make the required settings for the cache server NetApp FAS Series and V-Series to connect to a network, and then connect to the network.

Refer to the manual that comes with the NetApp FAS Series and V-Series unit for details on how to connect to a network.

2. Activating SNMP

The device polling function uses SNMP to acquire the device status of the NetApp FAS Series and V-Series. Enable the SNMP function so that device information can be acquired using SNMP. Refer to the manual that comes with the NetApp FAS Series and V-Series unit for detailed information on making settings.

If the SNMP Community name is default, this software uses the Community name "public." However, it is also possible to specify the Community name. It is possible to change the Community name this software uses for a device from the Web Console.

3. SNMP Trap setting

Make the required settings on the NetApp FAS Series and V-Series unit so that SNMP Traps of the NetApp FAS Series and V-Series unit will be sent to the Management Server.

If the Management Server is defined as a cluster, the logical IP address of the cluster needs to be set.

4. Management software cooperation

Use the attached management software for device management such as checking the detailed device status of the NetApp FAS Series and V-Series unit and the various settings. The management software can be called directly from the Web Console. As management software, setup the following IP address with the Web Console in advance:

- "http://device IP address/na_admin/"

4.5 ETERNUS VS850 Virtualization Storage

This product supports fault management for VS850. Refer to "[5.2.6 Registering a Manually Embedded Device](#)" and register the device.

1. Network settings

At the VS850, enter the network connection settings to connect to the network. Refer to the manual provided with the VS850 for details.

2. Cluster Name settings

The Management Server uses the Cluster Name set at the VS850 to specify the device. Therefore, the Cluster Name set at the VS850 must be unique amongst all sites, including remote sites. When registering the VS850 at the Management Server, enter the Cluster Name as the device name.

3. SNMP Trap setting

Enter settings at the VS850 side in order to send VS850 SNMP Traps to the Management Server. If the Management Server is in a cluster configuration, the logical IP address of the Management Server cluster must be set.

4. Management software linkage

Use the management software provided for the VS850 to check device status details and to enter settings, including volume virtualization settings. The management software is called directly from the Web Console. As management software, setup the following IP address with the Web Console in advance. svconsoleip is the IP address of the server where the management software is executed.

- "http://svconsoleip:9080/ica"



Note

- The VS850 is handled as a server node by the Management Server. To perform access path operations, treat the VS850 fibre channel port as a server node HBA port.
- The VS850 is registered at the Management Server as a cluster unit comprised of VS850 nodes. Set the logical IP address of the cluster containing the VS850 nodes as the IP address to be registered at the Management Server.
- If the IP address is not registered during device registration, the device cannot be polled for fault monitoring. Ensure that the IP address is registered.
- If the Cluster Name set at the VS850 and the device name registered at the Management Server are different, fault monitoring using SNMP Traps cannot be performed. Ensure that the device name and the Cluster Name are the same.

4.6 ETERNUS CS800 De-dupe Appliance

This software supports fault management (SNMP Trap monitoring only) for the CS800.

1. Connecting to the network

Perform the setup for connecting the CS800 to the network. Refer to the manual which came with the device for details on how to perform the setup.

2. SNMP Trap setting

Perform the setup of the SNMP Trap transmission destination for the device so that SNMP Traps of the CS800 can be transmitted to the Management Server. If the Management Server is operated in a cluster configuration, set the logical IP address of the cluster as the destination.

3. Registering the device

Refer to "[5.2.6 Registering a Manually Embedded Device](#)" for registering the device. Specify the IP address of the device during the registration operation.

4.7 Tape Library Device

4.7.1 Tape library device ETERNUS LT250/LT270

This software supports all functions except for performance monitoring for ETERNUS LT250 and ETERNUS LT270.

Note that this software does not support automatic device detection function. To detect ETERNUS LT250 or ETERNUS LT270, enter the IP address for the device in a device search.

1. Connecting to the network

Make the required settings for ETERNUS LT250 or ETERNUS LT270 to connect to a network, and then connect to the network. When connecting to the network, start up the SNMP Agent function.

Refer to the manual provided with the ETERNUS LT250 or ETERNUS LT270 for details on the setting method.

2. Community settings in SNMP environment settings

Specify "public" as the Community name (GET).

It is possible to change the Community name this software uses for a device from the Web Console.

3. Device name setting (SysName) in SNMP (Agent) environment settings

Register nicknames for managing ETERNUS LT250 or ETERNUS LT270.

This software uses this value as SysName.

4. SNMP Trap setting

Manager does not add the SNMP Trap send destination address to a device.

Set the SNMP Trap send destination address to the IP address for the Management Server on which this software is running, using management software for ETERNUS LT250 or ETERNUS LT270.

For the Management Server in a cluster configuration, the logical IP address of the cluster must be set.

5. Access path setting and display

This software does not set the Fibre Channel Interface for ETERNUS LT250 or ETERNUS LT270, but displays access paths by using SwitchZoning or StorageAffinity on the server node.

When setting the Fibre Channel Interface, use management software for ETERNUS LT250 or ETERNUS LT270.

4.7.2 Tape library device ETERNUS LT20/LT20 S2/LT40/LT40 S2/LT60/LT60 S2/LT200/LT210/LT220/LT230/LT270 S2

This software supports fault management and linkage to the management software, for ETERNUS LT20/LT20 S2/LT40/LT40 S2/LT60/LT60 S2/LT200/LT210/LT220/LT230/LT270 S2.

1. Connecting to the network

Make the required settings for a tape library device which you use to connect to a network, and then connect to the network.

Refer to the manuals provided with the respective devices for details on the setting method.

2. SNMP Trap setting

Set the SNMP Trap send destination address to the IP address for the Management Server on which this software is running, using management software for the tape library server you use.

For the Management Server in a cluster configuration, the logical IP address of the Management Server cluster must be set. Restart the device after the setting.

3. Management software linkage

Use the management software provided with a tape library device for device management such as checking the detailed status of the tape library device and the various settings.

The management software can be called directly from the Web Console. In advance, setup the following as the management software on the Web Console:

```
http://device IP address/
```

4. Access path setting and display

This software does not set the Fibre Channel Interface, but displays access paths by using SwitchZoning or StorageAffinity on the server node.

When setting the Fibre Channel Interface, use management software for the tape library device.

4.7.3 Virtual Tape Appliance ETERNUS CS2000

This software supports fault management (SNMP Trap monitoring only) for the ETERNUS CS2000.

1. Connecting to the network

Make the required settings for a virtual tape appliance which you use to connect to a network, and then connect to the network. Refer to the manuals provided with the respective devices for details on the setting method.

2. SNMP Trap setting

Make the required settings on the CS console so that SNMP Traps of the ETERNUS CS2000 will be sent to the Management Server. If the Management Server is defined as a cluster, the logical IP address of the cluster needs to be set.

3. Registering the device

Refer to "[5.2.6 Registering a Manually Embedded Device](#)" for registering the virtual tape appliance device. IP address of ETERNUS CS2000 must be set in "IP address" for the registration.

Chapter 5 Startup and Setting

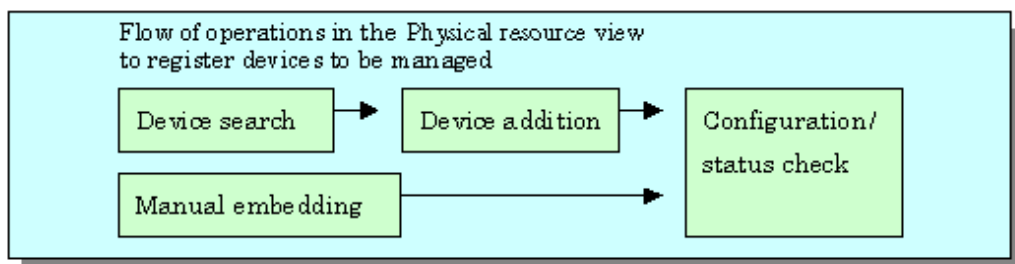
This chapter explains device definitions and operation flowcharts required for operating this software.

5.1 Opening and Closing

The Storage Cruiser function is operated from the Web Console.

Refer to the *ETERNUS SF Web Console Guide* for start up and shutdown.

5.2 Registering device



5.2.1 Device search

For device management using this software, it is necessary to first conduct a device search. There are two methods for conducting a device search.

- [Detecting for devices in a subnet automatically](#)
- [Detecting a device by specifying IP address](#)



Information

- The following devices are added automatically when devices are detected.
 - Storage Cruiser's agent
 - VM host and VM guest in VMware vSphere 4 or later
- Even when detected a server node, the host name may not be resolved. In this case, the host name is displayed in the format of "IP-IP address".
- Even if IPv6 address exists in the searched servers, the agents shown below support only search with IPv4 address.
 - Storage Cruiser's agent that does not support IPv6 address

Detecting for devices in a subnet automatically

To detect devices in a subnet automatically, specify the target subnet on the Web Console screen. Through detection of the devices within the subnet, the automatic detection-compatible devices supported by the Manager are displayed on the screen. SNMP-based broadcasting processes are performed internally, and the devices supported by this software are automatically displayed. Devices must have SNMP access enabled for the Manager.

Devices with IPv6 address are not searched. If any device registered with IPv6 address exists, this function is not available. When managing any device with IPv6 address, specify its IP address to search it.

Note

- Devices within subnets directly connected with the Management Server are subject to automatic detection regardless of the subnet being specified.
- An environment which has broadcast processing pass through the target subnet is required for SNMP-based broadcast processing to be performed internally.
- If the devices in the subnet cannot automatically be detected, check "[1.2.7 Support levels](#)". For devices that do not support [Detect device in subnet] as described in "[1.2.7 Support levels](#)", use the method described below "[Detecting a device by specifying IP address](#)".
- If the IP address of Slave CM in an ETERNUS Disk storage system is set, both IP addresses of Master CM and Slave CM are detected. Refer to "[5.2.2 Registering a Device](#)" to specify the device with the IP address of Master CM. If the IP address of Slave CM is specified, the access path cannot be set.

Detecting a device by specifying IP address

- To detect Storage Cruiser's agent
Specify the IP address for the target device.
- To detect the VM host and VM guest (VMware vSphere 4 or later)
Specify the IP address for the VM Host. Also, input the username and password used during login to the VM Host.

Information

- By registering a VM host, all of the VM guests on the VM host are automatically registered.
- From the Web Console, Execute [Reload Conf.] for the VM host to detect VM guests created after the VM host was registered.

Note

- To register a VM host (and its VM guests) with this software, the IP address, login name and password of the VM host are required.
- It is not possible to specify and register only VM guests.
- To detect any device other than above devices
Specify the IP address and SNMP Community name for the target device

Note

- If such a search for a product in the ETERNUS DX series fails, check the following items:
 - The SNMP environment has not been set up from ETERNUS Web GUI since installation of the device:
The SNMP agent of the device is not active. Set up the SNMP environment as instructed in "[4.3.1 Disk array ETERNUS DX series](#)".
 - In the case of ETERNUS DX60/DX60 S2, DX80/DX80 S2, DX90/DX90 S2/DX100 S3/DX200 S3, DX400 S2 series, DX500 S3/DX600 S3 and DX8000 S2 series
For the device detection, specify the IP address on the Master CM side. If the IP address on the CM slave side was specified for detection or registration, access path settings are not possible.
- If the search for Storage Cruiser's agent fails, check whether the Storage Cruiser's agent is activated and that its level is compatible. If not activate, Storage Cruiser's agent. If the level is not compatible, upgrade the Storage Cruiser's agent.

- If the search for ETERNUS SN200 Fibre Channel switch, Brocade Fibre Channel switch and PRIMERGY Fibre Channel switch blade fails, check the settings of SNMP MIB on the device side. Refer to "[SNMP-MIB setting](#)" in "[4.2.1 SN200 \(Brocade\) Fibre Channel switch](#)" for details.
- On an AIX agent installed server, the following problems may occur:
 - It takes lots of time to register a server.
 - It takes lots of time to reload configuration.
 - The HBA port information for a target server may not be properly recognized.

If any of those mentioned above is seen, check all the HBA ports for proper connection. If there is any fibre channel device corresponding to an HBA port that is not connected, delete it if possible. To check HBA port-fibre channel device correspondence, refer to the AIX document. In addition, if the server is restarted, this operation may be needed again.

[Example of deleting unused fibre channel device fcs3]

```
# /usr/sbin/rmdev -Rdl fcs3
```

If a problem does not fall under those mentioned above, refer to "[B.1 Collecting the troubleshooting information](#)" to collect analysis material and contact Fujitsu Technical Support.

5.2.2 Registering a Device

To make this product's managed device, it is necessary to register a device which has already been detected using the Web Console.

- User name and password

To manage the device, this software must recognize the user name and password associated with the device.

Since each device requires different information, the items displayed in the dialog change accordingly.

<Required information>

- For SN200 (Brocade) Fibre Channel switch, PRIMERGY Fibre Channel switch blade, Brocade VDX series and PRIMERGY BX Ethernet Fabric Switch a user name and password with administrator rights will be required.
- For the ETERNUS DX80 S2/DX90 S2/DX100 S3/DX200 S3, DX400 S2 series, DX500 S3/DX600 S3 and DX8000 S2 series, user name and password of Software roll will be required. For the ETERNUS Disk storage system other than stated above, a user name and password with administrator rights will be required.
- Check box of "Enable fault monitoring via SNMP Traps on this device"

When a device is added, this software automatically sets the SNMP Trap transmission place address for the device so that it can monitor for faults by using the SNMP Trap. Refer to "[1.2.7 Support levels](#)" for information about the device types for which the address automatic setting function can be used.

Information

- Refer to "[5.2.4 Function for setting event notification destinations](#)" for information about fault monitoring required for an added device after the function is disabled. Refer to "[5.2.5 SNMP Trap transmission place automatic setting function](#)" for a detailed explanation of the automatic setup.
- The check box of "Enable fault monitoring via SNMP Traps on this device" is invalid for the device which does not support the function of automatically setting SNMP Trap transmission place.
- Checkbox for enabling the zoning setting

When a fibre channel switch device is registered, this software sets up the device such that zoning setup can be done. Select this option if performing setup of the access path from this software. If you do not select this option, operations will start as is (i.e. with no security) for the fibre channel switch device which had no zoning setup performed (meaning this switch is in a No Security status).

Note

- If a device to be managed cannot be accessed, or if it is in any of the states described below, it cannot be registered.
 - Fibre Channel switch (Excluding Brocade VDX series and PRIMERGY BX Ethernet Fabric Switch)
 - Telnet was used to login to the target device.
Action: Log out, and then perform the registration process.
 - Brocade VDX series, PRIMERGY BX Ethernet Fabric Switch
 - SSH was used to login to the target device.
Action: Log out, and then perform the registration process.
 - ETERNUS DX series
 - User is logged into the target device's ETERNUS Web GUI.
Action: Log out, and then perform the registration process.
- During the device registration process, if telnet is used to login to the Fibre Channel switch connected to the device to be registered, the physical line between the Fibre Channel switch and the device cannot be displayed because information cannot be obtained from the Fibre Channel switch. In this event, log out and execute the device registration process.
- During the device registration process, if Brocade VDX series and PRIMERGY BX Ethernet Fabric Switch have already been manually registered, be sure to delete the manually registered devices first and then perform registration. If registration is performed when manually registered devices remain registered, no information can be obtained from the Fibre Channel switch. In this case, delete target manually registered devices.

5.2.3 Deletion

This function cancels the registration of a device being managed by this software, thereby deleting that device from the range of management. It is used in such cases as when a device has been removed.

Information

Individual VM guests for VMware vSphere 4 or later can be deleted from the management target for this product by first deleting the VM guest using VMware management software and then deleting the VM guest using this procedure. If the VM guest is still on the VM host it will be registered again automatically.

Note

- You cannot delete a server which has volume definition(s) of Backup management of AdvancedCopy Manager or Replication Group definition(s) of Replication management of AdvancedCopy Manager. You should delete the volume definition(s) of Backup management of AdvancedCopy Manager or Replication Group definition(s) of Replication management of AdvancedCopy Manager before the server deletion.
- To delete a VM host (VMware vSphere 4 or later) from this product, delete all VM guests on the VM host to be deleted in advance.
- In this product, even if a SNMP Trap send destination address is not automatically set, when deleting a target device, if the IP address of the Management Server is set to the SNMP Trap send destination address of the device, its setting is deleted.

Execute the deletion of the device from the Web Console. The disk storage system's copy sessions are not deleted.

If the deleted device has been detected again by this software's automatic device detection it will be re-displayed.

It is also possible to delete only the access path existing between the Managed Server and the device that is the target for deletion.

Note

When you delete a server, delete all the access paths connected the server in advance, and then execute the deletion of the server.

5.2.4 Function for setting event notification destinations

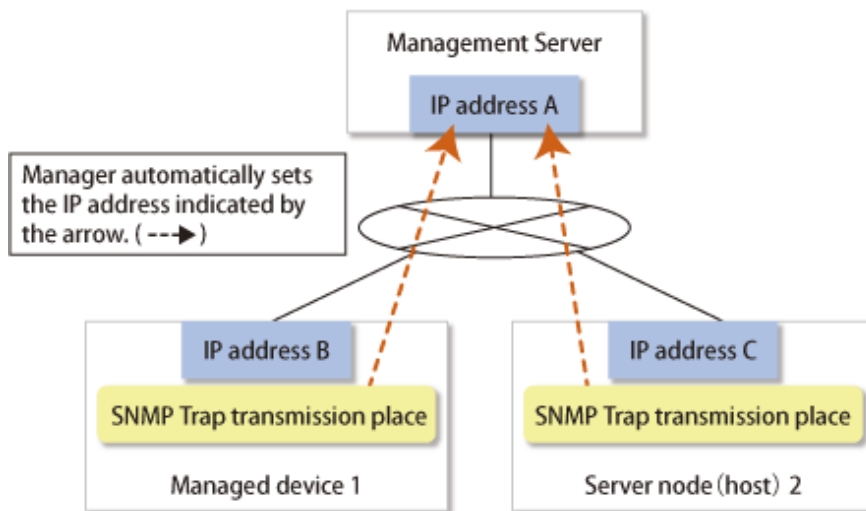
If fault monitoring is required for a device after the SNMP Trap transmission place address automatic setting function is disabled for the device during the device addition process, it is possible to perform setup from the Web Console.

5.2.5 SNMP Trap transmission place automatic setting function

The SNMP Trap transmission place automatic setting function, which is executed at the time of a device search or device addition, and its accuracy are explained with the figures below.

Management Server with only one IP address

This software automatically identifies IP address A of the Management Server and sets "IP address A" as the SNMP Trap transmission place for each managed device.

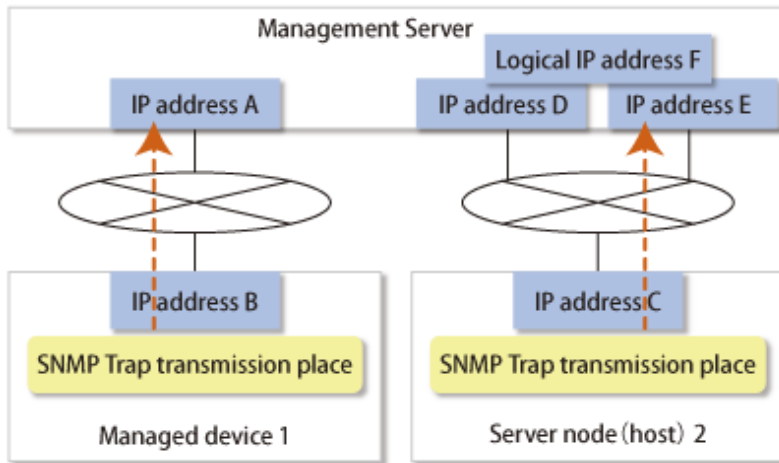


Management Server with two or more IP addresses

Such Management Server has a cluster or redundant LAN configuration or is connected to multiple subnets, and it has two or more IP addresses.

From the multiple IP addresses of the Management Server, this software selects the one that is most suitable as the transmission IP address for each device. However, this logic does not work in all cases. In the environment shown in the figure below, for example, this software may set "IP address D" as the SNMP Trap transmission place for Managed device 1. This is because addresses cannot be automatically detected in some cases due to the nature of current LAN technology. In such an environment, therefore, it is necessary to check the SNMP Trap transmission place setting of each device after the device addition process and, if required, set SNMP Trap transmission places directly on the device side.

In the figure below, specify "IP address A" as the SNMP Trap transmission place for Managed device 1, and "Logical IP address F" as the SNMP Trap transmission place for Server node 2. Refer to "2.1 Receiving SNMP Traps" for information about how to set SNMP Trap transmission place addresses of server nodes manually.



Point

In order for the server node to send the SNMP Trap, agent must be installed on the host.

5.2.6 Registering a Manually Embedded Device

Some devices (such as Managed Servers without an agent, tape units, and NAS devices) cannot be retrieved by device search. Register these devices with this software by using the manual embedding function.

5.3 Checking Management Status

Check whether the setup is correct. Use the following steps to check the setup:

[Test 1] Check whether every device (excluding the server node agent) can correctly receive SNMP Traps

This software receives generic traps 0 to 5, which are SNMP Traps not unique to a specific vendor, and it decodes their contents and displays information about each event (that does not use Systemwalker Centric Manager linkage or Shell/bat linkage.) As one of generic traps 0 to 5, a COLD START trap is issued by an ordinary device. When using this trap to test whether the software can correctly receive an SNMP Trap.

A device sends the COLD START trap and other traps by turning OFF and ON the device to be managed, performing a variety of setup tasks (setup of the SNMP environment for ETERNUS), doing other such work. Check whether the event is displayed with regard to the above operation and trap.

However, generic traps 0 to 5 are not normally required, so after the test is completed, you can disable display of generic traps 0 to 5 by using the following method:

Edit the following definition file:

Platform of Manager	File Location
Windows	\$ENV_DIR\Manager\etc\opt\FJSVssmgr\current\sanma.conf (\$ENV_DIR means "Environment Directory" specified at the Manager installation.)
Solaris OS, Linux	/etc/opt/FJSVssmgr/current/sanma.conf

Edit one description as follows (0=Hide, 1=Show): `DISPLAY_SNMP_STANDARD_EVENT = 0;`

Using the Web Console, execute re-read definition file and import the definition files into the program.

[Test 2] Check whether server node (agent) can correctly receive SNMP Traps

The server node (Agent) provides the following command that issue SNMP Trap for the test.

Platform of Agent	Command Location
Windows	\$INS_DIR\Agent\bin\traptest [<i>ip-address</i>] (<i>\$INS_DIR</i> means "Program Directory" specified at the Agent installation.)
Solaris OS, Linux, HP-UX, AIX	/opt/FJSVssage/bin/traptest [<i>ip-address</i>]

Only in the environment where the host holds two or more IP addresses, a server node's IP (Agent start IP address) address which the manager recognizes is specified to *ip-address*.

Make sure the IP address input is correct, if the event cannot be received correctly.

If the device was set up normally, an event will be issued to the Web Console when this command is executed.

SNMP Trap test command cannot linkage to Shell/bat. Modify the SNMP definition if necessary.

To modify SNMP Trap definition, modify ESC agent SNMP Trap definition file which is located 1_3_6_1_4_1_211_4_1_3_21_2_2.xml. SNMP Trap test is defined as the first number of "Specific Trap Type". You may change the action for this trap. Refer to "A.5 SNMP Trap XML Definition File" for SNMP Trap definition file.

 Information

- For VMware vSphere 4 or later, it is unnecessary to execute this test because the fault monitoring function by receiving SNMP Traps is not supported.
- The community name of a test SNMP Trap is fixed to "public".

[Test 3] Check Systemwalker Centric Manager linkage and Shell/bat linkage of events.

Events cannot be linked with Systemwalker Centric Manager or Shell/bat for the standard SNMP Trap. To test the Systemwalker Centric Manager linkage and Shell/bat linkage of an SNMP Trap from a device, execute a tentative SNMP Trap command for the test on the Management Server. This command changes internal information of an SNMP Trap so that the SNMP Trap seems to have been sent from a device being monitored, and it sends such an SNMP Trap to the system's own port for receiving the SNMP Trap. Since descriptions of events are linked to Systemwalker Centric Manager and Shell/bat, Systemwalker Centric Manager linkage and Shell/bat linkage can be tested. To test the Shell/bat linkage of an SNMP Trap of the server node agent, use the method described in [Test 2].

For the IP address of an argument, specify the IP address of a device (ETERNUS Disk storage systems or Fibre Channel switch) registered with this software. The contents of this simulated SNMP Trap are loaded into the event log.

The commands shown below are executed to generate a simulated SNMP Trap for the ETERNUS DX series device registered with this software. Using these commands, the manager creates the simulated trap, receives the same trap, and checks whether the displayed event and shell/bat linkage are correct. Here, the simulated trap is a fan fault with "public" as the Community name. This simulated trap has arbitrary test information that is distinct from actual trap information.

Also, the ETERNUS Disk storage systems can issue an SNMP Trap from the device by using the "SNMP Trap sending test" function of ETERNUS Web GUI. Though the test uses a simulated trap, its results are the same as those from a test that sends a real trap and checks the response, since the trap is sent from an actual ETERNUS Disk storage systems.

Platform of Manager	Command Location
Windows	\$INS_DIR\Manager\opt\FJSVssmgr\bin\grtraptest <i>ip-address</i> (<i>\$INS_DIR</i> means "Program Directory" specified at the Manager installation.)
Solaris OS, Linux	/opt/FJSVssmgr/bin/grtraptest <i>ip-address</i>

The commands shown below are executed to generate a simulated SNMP Trap for a Fibre Channel switch registered with this software. (A simulated error that is a port fault is issued.):

Platform of Manager	Command Location
Windows	\$INS_DIR\Manager\opt\FJSVssmgr\bin\swtraptest <i>ip-address</i> (<i>\$INS_DIR</i> means "Program Directory" specified at the Manager installation.)
Solaris OS, Linux	/opt/FJSVssmgr/bin/swtraptest <i>ip-address</i>

Chapter 6 Operation

Configuration management is made by using the Web Console. This chapter explains how to use window.

6.1 Resource Management

For the device registered to this product, it is possible to use various functions via the Web Console.

6.1.1 RAID Group Management

With this product, it is possible to manage the storage device's RAID Groups. It is possible to operate with the same operability without being aware of restrictions according to type of storage device and model.

The target device is selected with the Web Console, and processing is selected from the Action pane.

The executable operations are as follows:

- Display RAID Group Status
- Create/Delete RAID Group
- RAID Group Eco-Mode Settings

6.1.2 Volume Management

With this product, it is possible to manage the storage device's volume. It is possible to operate with the same operability without being aware of restrictions according to type of storage device and model.

The target device is selected with the Web Console, and processing is selected from the Action pane.

The executable operations are as follows.

- Create/Delete Volume
- Format Volume
- Expand Thin Provisioning Volume Capacity
- Delete Snap Data Pool Volume
- Encrypt Volume
- Equalize Thin Provisioning Volume
- Enabling/Disabling Extreme Cache(Read)

Note

- For the following models, management of encrypted volumes and configuration of the encryption mode cannot be performed with this product.
 - ETERNUS DX60/DX60 S2/DX80/DX90
 - ETERNUS DX400 series
 - ETERNUS DX8000 series
- The number of maximum volumes that can be made with this product at a time is 128. Make them by dividing into two or more times when you make volumes that exceed 128.

6.1.3 Thin Provisioning Management

With this product, it is possible to manage the storage device's Thin Provisioning. It is possible to operate with the same operability without being aware of restrictions according to type of storage device and model.

The target device is selected with the Web Console, and processing is selected from the Action pane.

The executable operations are as follows.

- Display the Thin Provisioning Pool
- Display the Thin Provisioning Pool status
- Change the Thin Provisioning Pool threshold value
- Create/Delete the Thin Provisioning Pool
- Display the Thin Provisioning Pool Capacity graph
- Expand the Thin Provisioning Pool Capacity
- Format the Thin Provisioning Pool

6.1.4 Advanced Copy Management

With this product, it is possible to manage the storage device's Advanced Copy. It is possible to operate with the same operability without being aware of restrictions according to type of storage device and model.

The target device is selected with the Web Console, and processing is selected from the Action pane.

The executable operations are as follows.

- Display Advanced Copy
- Set Up Copy Parameters
- Set Up REC path
- Acquire REC path information
- Collect REC Device Information
- Measure REC Response Delay Time
- Set Up REC Multiplicity
- Set Up REC Buffer

6.1.5 Connectivity Management

With this product, it is possible to manage the storage device's connectivity. It is possible to operate with the same operability without being aware of restrictions according to type of storage device and model.

The target device is selected with the Web Console, and processing is selected from the Action pane.

The executable operations are as follows:

- Display Connectivity Status (Set Up Host, Set Up Port, Reset Group)
- Create/Delete Host Affinity
- Set Up FC Host/iSCSI Host/SAS Host
- Set Up FC Port/iSCSI Port/SAS Port
- Set Up Affinity Group
- LUN Mapping (direct connection) display



-
- The iSCSI-RA port Transfer Rate cannot be changed in the Web Console.
If it needs to be changed, use the ETERNUS Web GUI.

- Setting the IP address, link local IP address, connection IP address, iSCSI name, or iSCSI alias name of an iSCSI port the same as another iSCSI port may not be allowed.

Refer to the following table for information on the duplicate registration:

Storage Model Name	Duplicate Registration				
	IP Address	Link Local IP Address	Connection IP Address	iSCSI Name (*1)	iSCSI Alias Name
ETERNUS DX80 S2/DX90 S2 ETERNUS DX100 S3/DX200 S3 ETERNUS DX400 S2 series ETERNUS DX500 S3/DX600 S3 ETERNUS DX8000 S2 series	N/A	N/A	N/A	N/A	N/A
ETERNUS DX60/DX60 S2/DX80/DX90 ETERNUS DX400 series ETERNUS DX8000 series	N/A	-	-	N/A	N/A

"A" indicates "Available", and "N/A" indicates "Not Available".

*1: If the default iSCSI name has been set, it is able to be registered by duplicating.

- Setting the IP address, iSCSI name, iSCSI alias name, and iSCSI host name of an iSCSI host the same as another iSCSI host may not be allowed.

Refer to the following table for information on the duplicate registration:

Storage Model Name	Duplicate Registration			
	IP Address	iSCSI Name	iSCSI Alias Name	iSCSI Host Name
ETERNUS DX80 S2/DX90 S2 ETERNUS DX100 S3/DX200 S3 ETERNUS DX400 S2 series ETERNUS DX500 S3/DX600 S3 ETERNUS DX8000 S2 series	A (*1)	A (*1)	N/A	N/A
ETERNUS DX60/DX60 S2/DX80/DX90 ETERNUS DX400 series ETERNUS DX8000 series	N/A	A	N/A	N/A

"A" indicates "Available", and "N/A" indicates "Not Available".

*1: If both the IP address and the iSCSI name are duplicated, it is not available. If one either is not duplicated, it is available.

6.1.6 How to control the Eco-mode

This software can use the Eco-mode that controls the ON/OFF status for the disk drive spindle rotation for storage devices. While the RAIDGroup that is being used from the server is being verified, the disk drive spindle rotation ON/OFF status for the RAIDGroup can be controlled.

There are two Eco-modes: the "storage device Eco-mode" and the "RAIDGroup Eco-mode". The ON/OFF status can be set for each.

When the storage device Eco-mode is set to ON, the RAIDGroup Eco-mode can be set to ON/OFF.

When the RAIDGroup Eco-mode is set to ON and its schedule is set to "External", the spindle rotation of the disk drive that is used to configure the RAIDGroup can control the ON/OFF status. However, the Eco-mode operation for the "[Uncontrollable RAID groups](#)" cannot be done.

For the Eco-mode operation, the target device is selected with the Web Console and the operation is executed.

The executable operations are as follows.

- Setting the device's Eco-mode to ON
- Setting the device's Eco-mode to OFF
- Setting the RAID Group's Eco-mode to ON
- Setting the RAID Group's Eco-mode to OFF
- Starting up the disk drive for which the RAID Group is configured
- Stopping the disk drive for which the RAID Group is configured

Note

When the RAID group corresponds to either following conditions, the disk drive cannot be stopped from the Web Console. Stop the disk drive by the [storageadm spindle stop command](#):

- The volume whose volume type is WSV exists in the target RAID group.
- The volumes in the target RAID group are concatenated with other RAID groups by the LUN Concatenation.

6.1.7 End to End list display

For the End to End list display, correlating information from the storage to the server is displayed. Using the Web Console, select [Correlation].

Note

- Only volumes that are connected by host affinity function are displayed at End to End list display.
- The [Mount Point] or the [Multipath Driver Device] is displayed only when you selected the [End to End View]. VMware and Hyper-V are not supported.
- When the Managed Server node OS is Windows or the installed Storage Cruiser's agent is version 15.0, a hyphen ("-") is displayed at the [Mount Point] and the [Multipath Driver Device].
- When the corresponding Multipath driver is not installed, a hyphen ("-") is displayed at the [Mount Point].

See

Refer to "[3.2 Server node middleware for which management is possible](#)" for the details on the corresponding Multipath drivers and file systems.

For VMware

To display the End to End list for VMware's VM guest and the storage device, register the VM host to the Management Server. It is also necessary to register to this software the VMware vCenter Server which manages the VM host registered to the Management Server.

Specify the following for registration of the VMware vCenter Server.

- IP address
- User name
- Password
- Communication port number of VMware vCenter Server (Default: 443)

Note

- The End to End list for VMware supports the display of information for storage devices connected to the VM host with FC, iSCSI and FCoE connections. Storage devices utilizing SAS connections, NPIV connections in an FC environment, and storage devices with the VM guests directly connected with iSCSI are not supported.
- When registering the VM host to the VMware vCenter Server using the host name, set it so that name lookup can be done on the Management Server for the VM host being registered to this product. Perform one of the following setups.
 - Register the IP address and host name for the VM host being set to the VMware vCenter Server to the DNS server which the Management Server references.
 - Define the IP address and host name for the VM host set to the VMware vCenter Server to the /etc/hosts file on the Management Server.

For Hyper-V (Windows, only for manager)

To display the End to End list for the VM guest on the Hyper-V host, install the agent to the Hyper-V host and then register it to the Management Server.

Next, register the target Hyper-V host in the End to End View (Hyper-V).

Specify the following for registration of the Hyper-V host.

- User name
 - When Hyper-V host is participating in the ActiveDirectory environment:
Specify users with administrator privileges in the format of "Domain name\User name".
 - When Hyper-V host is not participating in the ActiveDirectory environment:
Specify users with administrator privileges in the format of "NetBIOS computer name\User name".

If the user name is not specified in the formats listed above, incorrect information may be displayed.

- Password

Also, implement the following settings to the Hyper-V host and the Management Server.

To make settings, users must have administrator privileges to log in.

- Set up Hyper-V host

Perform the following procedure to give permission for Hyper-V host that is performing End to End display to remote management.

1. Click [start] - [Administrative Tools] - [Server Manager] to run Server Manager. Click [Configure Server Manager Remote Management] in [Computer Information] on Server Manager.
If [Enable remote management of this server from other computers] checkbox is unchecked, check it and click [OK].
2. Click [start] - [run]. Enter "cmd.exe", and click [OK].
Execute the following command at the command prompt.

```
C:\Users\administrator> winrm quickconfig [Enter]
```

If the remote management is not set, enter "y".

For the End to End list display for Hyper-V with iSCSI connection, set up the advanced settings for the connection when connecting to a target detected from iSCSI initiator property. Specify the IP address for the Hyper-V host adopter to the initiator IP in the advanced settings. If the settings are incorrect, the End to End list for Hyper-V is not displayed properly.

- Set up the Management Server

Click [start]-[run]. Enter "cmd.exe", and click [OK].

Execute the winrm command below on the console of cmd, and check the value for TrustedHosts.

Execution example)

```
C:\Users\administrator> winrm get winrm/config/client
```

Specify "*" for TrustedHosts or, only if the IP address for the Hyper-V host for which the End to End list is to be displayed has not been set, execute the winrm command below to specify the value for TrustedHosts.

Execution example)

```
C:\Users\administrator> winrm set winrm/config/client @{TrustedHosts="ipAddr"} [Enter]
```

For *ipAddr*, specify as the value for the previously confirmed TrustedHosts and the IP address for the Hyper-V host for which the End to End list of the VM guests is to be displayed. If you specify multiple IP addresses, specify them with the addresses separated by commas (as in "*ipAddr1, ipAddr2,...*"). For IPv6 format, surround the IP address with brackets "[]".

Example: When registering 192.168.1.10,fcde:555:444:333:222::1027,fcde:555:444:333:222::1154 in Trusted Hosts:

```
TrustedHosts="192.168.1.10, [fcde:555:444:333:222::1027], [fcde:555:444:333:222::1154]"
```

Note

- To use this function, the following need to be installed on the Management Server:
 - .NET Framework 2.0 or later
 - PowerShell 2.0 or later
 - WinRM2.0 or later

Note that the supported version of Hyper-V is 2.0 or later.

- The End to End list for Hyper-V supports the display of information for storage devices connected to the VM host with FC, iSCSI and FCoE connections. Storage devices utilizing SAS connections and storage devices with VM guests directly connected with iSCSI are not supported.
- For a multipath configuration, the End to End list for Hyper-V displays only one path.
A host name detected by the agent may not be consistent with a host name of the Hyper-V host displayed in the End to End list for Hyper-V. To be consistent with those host names, define the host name as a computer name in the /etc/hosts file of Hyper-V host.
- The information of virtual HBA on the Hyper-V guest is not displayed.
- If the same format (IPv4 or IPv6) IP address as the Hyper-V host is not set to its VM guests, the IP addresses of the VM guests are not displayed.

6.1.8 Extreme Cache Management

With this product, a storage device's Extreme Cache can be managed. Tasks can be performed with the same operability without having to be conscious of limitations due to the type or model of the storage device.

Operations regarding Extreme Cache can be executed to a storage device or volume. This section will explain the operations in relation to a storage device. Refer to "[6.1.2 Volume Management](#)" for information on operations in relation to a volume.

Select the target storage device with the Web Console, and select the operation from the Action pane.

The operations that can be executed are as follows:

- Extreme Cache Configuration
 - Enable/Disable
 - Size of Extreme Cache

Note

In order to utilize the Extreme Cache function, it is required that configuration for the storage device is enabled.

When the configuration for the storage device is disabled, the Extreme Cache function cannot be utilized, regardless of the enabled / disabled configurations of each volume.

6.2 Access Path Management

6.2.1 What is an access path?

In this software, a logical path between a server node and a storage device is defined as an access path.

Access paths are generated by the following access control functions of the server node, Fibre Channel switch, and storage.

Fibre Channel switch zoning

Switch vendors provide Fibre Channel switch zoning. Information such as the WWN/port number used by Fibre Channel for the host bus adapter (HBA) on the server node side and the WWN/port number of channel adapters (CAs) on the storage side is combined in a zone unit, and access from ports other than the port defined for the zone are restricted.

Storage host affinity

Storage vendors provide storage host affinity. The storage side recognizes the WWPN of the HBA on the server node side in order to restrict access. Associations of WWPNs of HBAs with storage areas (AffinityGroup/Zone) can also be set.

ETERNUS DX series refer to storage host affinity as "Set Affinity Group", "Set Host-Affinity Group".

Integrated access path control

This software integrates and manages these functions to facilitate definition of settings that make use of the characteristics of SAN security and each function.

It controls access paths according to the functions and settings of individual devices.

6.2.2 Access path display (display of the logical relationship between a server node and storage systems)

This software gathers information from each device and displays the status of access paths or the status of logical access paths from the server node. This function is effective for verifying the validity of system configuration setup and recognizing the effect of a resource error because it enables the logical relationship in the more complicated SAN environment to be easily determined.

If the server node operates under a Solaris OS environment and the storage system is a library or tape device, the tape-type drivers for which access paths can be displayed are as follows:

st, ftla, fsct, IBMtape, mt, lb, sg, sgen



The Solaris OS server node uses special file /dev/rdisk/cXtX, /dev/rmt to obtain WWPN binding information. For this reason, to recognize WWPN binding, this special file (device file) must be created in advance. If any unused special file is in /dev/rdisk/, /dev/rmt, it causes the access path display to be incorrect. If access path display by this software differs from that by system equipment, clarify the special files defined in the following operations:

- Solaris OS (For the environment which uses hard disk driver (HDDV), and does not use multipath control (ETERNUS Multipath Driver, MPLB, MPHD))

```
# touch /reconfigure
# /usr/sbin/shutdown -y -i6 -g0 (server node restart processing)
```

After the server node has been restarted

```
# format (Loading processing to HDDV driver's kernel)
# disks -C
```

- Solaris OS (For the environment which uses both hard disk driver (HDDV) and multipath control (ETERNUS Multipath Driver, MPLB, MPHD), uses only multipath control or uses neither.)

```
# touch /reconfigure
# /usr/sbin/shutdown -y -i6 -g0 (server node restart processing)
```

After the server node has been restarted

```
# disks -C
```





6.2.2.1 Access path status display

You can check the access path status connected by the Fibre Channel on the [status] column on the [Access Path] screen. The status of access paths are displayed as the following icons. When you click the each status, the corresponding error content message is displayed.

In addition, if you check the access path status, click the [Refresh] button in the access path status to make the status up-to-date.

Access Path Status	Description	Action
Normal	The access path is normal.	<p>None.</p> <p>However, for HBA shown below, you must take actions for making the operating system recognize LUN.</p> <ul style="list-style-type: none"> - If the HBA is XSEFC401AF, XSEFC402AF, SG-XPCIE2FC-EM4, or SG-XPCIE2FC-EM8: <ul style="list-style-type: none"> 1. In an environment connected to a Fibre Channel switch, configure the HBA N port settings. Refer to "4.1.1.2 N-port settings", and check the N-port settings. If the settings are incorrect, correct them. 2. Check the storage Ap_id by executing <code>cfgadm -al</code> command, and make the OS recognize the LUN by executing <code>cfgadm-c configure Ap_id</code> command. For details about the commands, check the man command. - If the HBA is SE0X7F21F, SE0X7F22F, SG-XPCI1FCQF2, SG-XPCI2FC-QF2, SGXPCI1FC-QL2, SG-XPCI2FCQF2-Z, SG-XPCI1FC-QF4, or SGXPCIE2FC-QF8: <p>Check the storage Ap_id by executing <code>cfgadm -al</code> command, and make the OS recognize the LUN by executing <code>cfgadm-c configure Ap_id</code> command. For details about the commands, check the man command.</p>
Warning	<p>The following possibilities are considered.</p> <ul style="list-style-type: none"> - The access path definition is inconsistent. 	<ul style="list-style-type: none"> - When the access path definition is inconsistent: <p>Click [status] to display the error content message. Refer to "Error Messages of Access Path" in the <i>ETERNUS SF Messages</i>, take actions according to the instructions for the error message.</p>

Access Path Status	Description	Action
	<ul style="list-style-type: none"> - The Fibre Channel switch is not registered. 	<ul style="list-style-type: none"> - When the Fibre Channel switch is not registered: Register the Fibre Channel switch.
 Error	<p>The following possibilities are considered.</p> <ul style="list-style-type: none"> - The access path is disconnected due to an error (if the multipath control mechanism is installed). - Another part failure caused an access path error. This state also occurs if a device in the access path is faulty. - The Fibre Channel cable on a route is disconnected. - The access path is set "Offline" by the user. - HBA was reduced or replaced. 	<p>Click [status] to display the error content message. Refer to "Error Messages of Access Path" in the <i>ETERNUS SF Messages</i>, take actions according to the instructions for the error message.</p> <p>In addition, if a part failure is suspected, click [Reload Conf.]:</p> <p>Reload the configuration to the device defined as an access path for identify whether a failure occurs or not.</p> <p>Replace the faulty part, and execute recovery processing.</p> <p>When the access path is set to "Offline", set it to "Online" as necessary.</p> <p>If HBA was reduced, delete the access path on the [Access Path] screen. Refer to "Delete Access Path" in the <i>ETERNUS SF Web Console Guide</i> for details on how to delete.</p> <p>If HBA was replaced, it is required to take corrective action that corresponds to the HBA status displayed on the [Server Detail] screen. Execute [Reload Conf.] as to the replaced HBA-installed device to perform the following steps:</p> <ul style="list-style-type: none"> - If the HBA status is "Changed": Perform access path modification operation. Refer to "9.3.1.2.1 Post-replaced HBA state is "Changed"" for details on the inheritance operation. - If the HBA status is "Unknown": Perform access path modification operation. Refer to "9.3.1.2.2 Post-replaced HBA state is "Unknown"" for details on the modification operation.
 Unknown	<p>The following possibilities are considered.</p> <ul style="list-style-type: none"> - The access path status needs to be updated. - Access path settings are incorrect. - HBA has been replaced. 	<p>Click the [Refresh] button in the access path status to make the status up-to-date. In the following configuration, display "Unknown" because the access path status cannot be obtained.</p> <ul style="list-style-type: none"> - The server is not registered on the Management Server. - The server is not installed Storage Cruiser's agent (a manually incorporated server). <p>For displaying the access path status, install Storage Cruiser's agent and register the server on the Management Server.</p> <p>If HBA was replaced, it is required to take corrective action that corresponds to the HBA status displayed on the [Server Detail] screen. Execute [Reload Conf.] as to the replaced HBA-installed device to perform the following steps:</p> <ul style="list-style-type: none"> - If the HBA status is "Changed": Perform access path modification operation. Refer to "9.3.1.2.1 Post-replaced HBA state is "Changed"" for details on the inheritance operation. - If the HBA status is "Unknown": Perform access path modification operation. Refer to "9.3.1.2.2 Post-replaced HBA state is "Unknown"" for details on the modification operation.
(-)hyphen	Access path cannot be displayed because the interface is iSCSI.	None.

Note

- The access path status is not updated automatically. When you check the access path status, click the [Refresh] button in the access path status to make the status up-to-date.
- In an environment not connected to a Fibre Channel switch, the access path status is not displayed correctly.
- It may take a few minutes to update the access path status. You can confirm the completion of the processing on the [Operation History] screen.

6.2.3 Access path setting

In a storage system where a Fibre Channel switch is between a server node and storage, this software automatically changes the security settings supported by each device and sets an access path, as shown in the figure below. If no security mechanism is provided on the device side, setting up security may not be possible. However, the security mechanisms of other devices create access paths. If none of the devices constituting these access paths is equipped with a security function, security cannot be set up but the access paths can be accessed from the server node.

Point

You can set the access path concurrently with assigning volumes to the server using the Web Console. Refer to "Assign ETERNUS Disk Storage System Volumes to Server" in the *ETERNUS SF Web Console Guide* for details on the operation.

Note

Each storage system has requirements, such as HBA types used, for guaranteeing operation according to the mutual connection verification status. Set each access path so that these requirements are satisfied. For more information about the requirements, contact the respective storage system distributor.

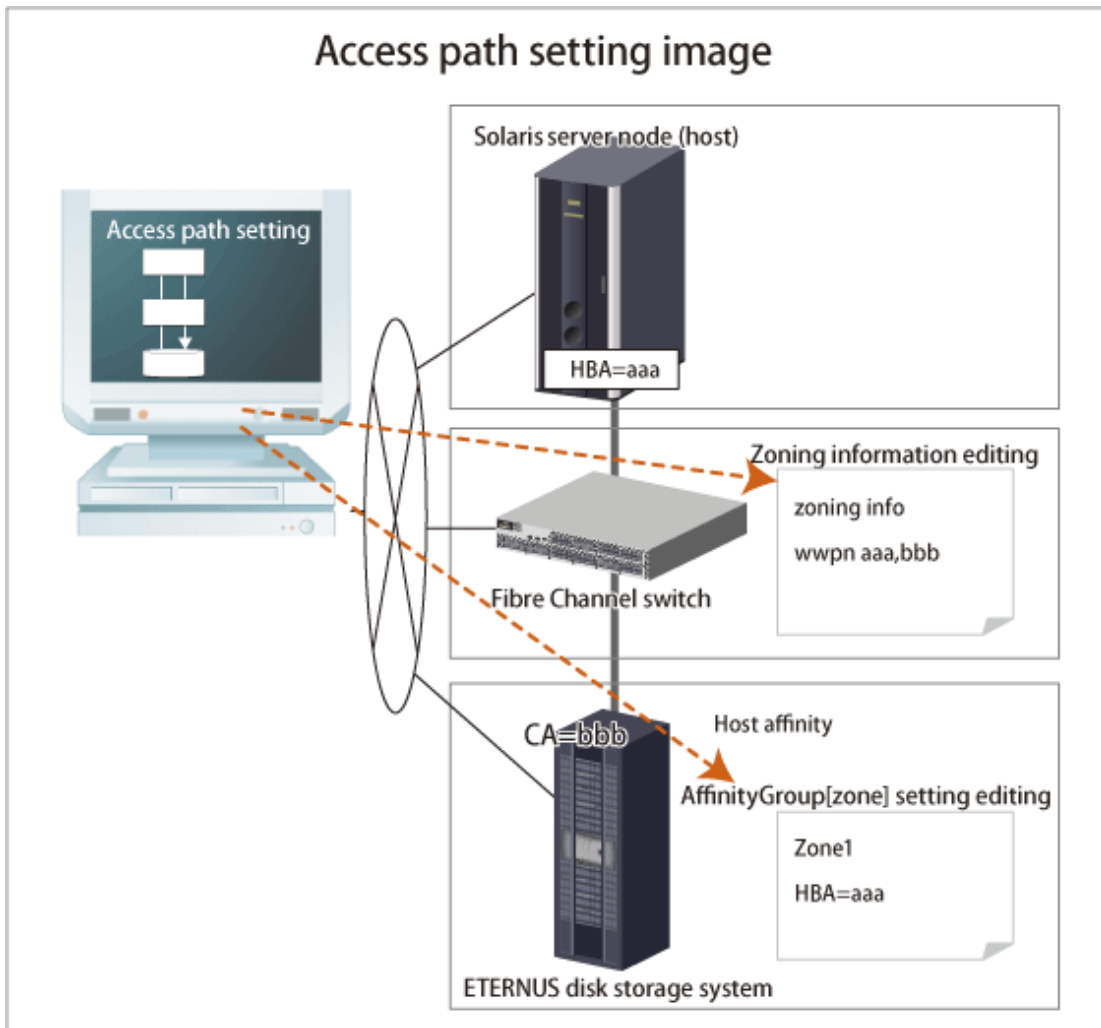


Table 6.1 Security information that this software sets in a device when setting an access path

Device Type		Contents Set by This Software
Solaris server node	Agent available/unavailable	No setting
Windows server node	Agent available/unavailable	No setting
Linux server node	Agent available/unavailable	No setting
HP-UX server node	Agent available/unavailable	No setting
AIX server node	Agent available/unavailable	No setting
Other server nodes	Agent unavailable	No setting
Fibre Channel switch	With zoning setting	WWPN one-to-one zoning is set. (However, this zoning is not set if the Fibre Channel switch side already has sufficient port zoning.)
	Without zoning setting	No setting
ETERNUS DX series	With security setting	Setting of HBA WWPN for security
	Host affinity (zone) setting	Setting of HBA WWPN to the affinity group (zone)
	Without security setting	No setting
Other storage/tapes		No setting

6.2.3.1 Preparations

Notes

- Only "System Administrator" account can set access paths.
- To change the specified AffinityGroup/zone name on the ETERNUS Disk storage system side of a set access path, delete the path and then set it again with a new zone.
- Verify that all Fibre Channel switches cascaded to the Fibre Channel switch associated with the access path setting are correctly recognized in the current status. Once an access path is changed because a Fibre Channel switch is temporarily disconnected from the cascade connection, the old cascade connection cannot easily be recovered. (In this event, execute the `cfgClear` command to delete zoning information for the Fibre Channel temporarily disconnected from the cascade connection. This enables cascade reconnection.)
- When setting an access path that is configured in the FC routing functionality LSAN zone in this software, manually set the LSAN zone in the device in advance.

Checking storage settings

Check the following settings on the storage side before setting an access path:

- ETERNUS DX series

By setting up the zone (host affinity) function, you can use storage areas efficiently on a storage area network. To use this zone (host affinity) function, you must set up a Affinity Group/zone on the storage side before setting an access path.

- ETERNUS DX60/DX60 S2/DX80/DX80 S2/DX90/DX90 S2/DX100 S3/DX200 S3, DX400 S2 series, DX500 S3/DX600 S3 and DX8000 S2 series

If linked affinity groups are used, then the WWN settings of the server nodes to be used must be set in advance.

Use ETERNUS Web GUI to set the WWN settings. When setting it, select a host response whose Host Specific Mode is in HP-UX Mode.

Connected state of the FC cable between devices

- When setting an access path, an HBA and CA must be physically connected via a Fibre Channel switch.

Device status

- Each HBA must be connected to a Fibre Channel switch and operate as the N port or NL public.
- All of a Fibre Channel switch on the way of the access path setting, HBAs, server nodes, CAs and storages should be operating normally.

6.2.3.2 Setting

Set access paths for the Fibre Channel.

Access path setting procedure

Configure the access path environment by installing additional storage and connecting a Fibre Channel cable, etc.

1. Preprocessing for the device driver definition file

- When ETERNUS Multipath Driver 2.0.1 or higher is used
No preprocessing needs to be performed.

- Solaris 9 OS

- This procedure changes the disk array control driver from sd to hddv when the grmpdautocon command is executed when the hot system expansion function (hddvadmM) is enabled for setting a hard disk driver (hereinafter abbreviated as hddv).

Check whether the hddv configuration information file (hddv.conf) has been created.

```
# ls /kernel/drv/hddv.conf
```

If the file is not found, execute the following command and create the hddv.conf file:

```
# hddvadm -M
```

When the file is found, check whether the file content is of class or parent type.

(Example)

Example of hddv.conf of the parent type

```
name="hddv" parent="scsi" target=16 lun=0;
```

Example of hddv.conf of the class type

```
name="hddv" class="scsi" target=16 lun=0;
```

The class type of file requires no preprocessing. (All hddv.conf files created by the hot system expansion command [hddvadm M] are of the class type.)

For the parent type of file, follow the instructions below to initialize the non-hot system expansion environment and move into the hot system expansion environment. To directly use the non-hot system expansion environment, follow the procedure for setting non-hot system expansion (hddvadm m).

1. Execute hddvadm -i.
2. Confirm that /kernel/drv/hddv.conf is not present.
3. Delete the entries made for recognizing the disk array device from the sd configuration information file (sd.conf).
4. Execute the following command and create an hddv configuration information file (hddv.conf):

```
# hddvadm -M
```

- In the MPLB2.0 or MPLB2.1 environment with non-hot system expansion specified (hddvadm -m) or in MPHD environment, the commands for adding and removing paths are not supported. Accordingly, the multipath configuration must be canceled once. Execute the destroy command of #iompadm to cancel the multipath configuration.
- In the multipath disk control (MPLB, MPHD, or HDDV) environment with non-hot system expansion is specified (hddvadm -m) or with normal setting (hddvadm-m), execute the following command on the target server node:

```
# hddvadm -i
```

By executing this hddvadm -i command, hddv.conf file moves to sd.conf and mphd.conf/mplb.conf file is saved. However, in the hot system expansion environment or in the hddvadm -M execution environment, hot system expansion can be performed without executing the hddvadm -i command. Therefore, this command need not be set.

2. Select the target server node and add an access path by using the Web Console.
3. [On a Solaris OS server node with multipath disk control (ETERNUS Multipath Driver 2.0.1 or later)] Execute the command below on the target server node to enable the server node to recognize the storage device.

- To automatically build a multipath device, execute the grmpdautoconf command. Refer to the driver manual for details on the command.

```
# /usr/sbin/grmpdautoconf
```

To automatically build a multipath device that uses the ETERNUS multipath driver and has a path passing through multiple Fibre Channel switches, execute the command after confirming path redundancy and specifying the "-X" option (because the grmpdautoconf command cannot check whether the redundancy of a path passing through multiple Fibre Channel switches is guaranteed).

```
# /usr/sbin/grmpdautoconf -X
```

4. [On a Solaris OS server node with multipath disk control (MPLB, MPHD, HDDV2.2 or later) and hot system expansion specified (hddvadm -M execution environment)] Execute the following command on the target server node so that the target server node recognizes the storage unit.

- In Solaris 9 OS, hddv.conf is edited if needed (refer to the multipath disk control (MPLB, MPHD, HDDV) various driver manuals). The following command is executed on the server node to fetch a storage device.

```
# update_drv -f hddv
```

With the above setting, the hddv driver can recognize the logical storage unit. If necessary, execute the command that builds an extension path to the multipath instance or the command that configures the multipath instance. Refer to the applicable driver manual for information about the commands (mplbconfig/iompadm add/iompadm new).

5. [On a Solaris OS server node, in the multipath disk control (MPLB, MPHD, HDDV) environment with non-hot system expansion is specified (hddvadm -m), or in the environment without multiple disk control] Execute the following command on the target server node to enable the server node to recognize the device:

- If the HBA is SE0X7F21F, SE0X7F22F, XSEFC401AF, XSEFC402AF, SG-XPCI1FC-QF2, SG-XPCI2FC-QF2, SG-XPCI1FC-QL2, SG-XPCI2FC-QF2-Z, SG-XPCI1FC-QF4, SG-XPCIE2FC-QF8, SG-XPCIE2FC-EM4 or SG-XPCIE2FC-EM8

Check the storage *Ap_id* using the `cfgadm -al` command, and make the OS recognize the LUN using the `cfgadm -c configure Ap_id` command. For details about the commands, check the man command.

- Non-MPLB, MPHD, or HDDV environment (including the tape environment)

```
# touch /reconfigure
# /usr/sbin/shutdown -y -i6 -g0
```

- Multipath disk driver control (MPLB, MPHD, HDDV) environment (hddvadm -m)

```
# touch /reconfigure
# /usr/sbin/shutdown -y -i6 -g0
# hddvadm -m (The required part of sd.conf is moved to hddv.conf, and the saved mphpd.conf/
mplb.conf file is restored.)
# touch /reconfigure
# /usr/sbin/shutdown -y -i6 -g0 (Existing instances for each driver (mplb/mphpd/hddv) are
configured when the definition file is restored. For new instances, hddv instances are
configured.)
```

According to the environment, execute the command that builds an extension path to the multipath instance or the command that configures the multipath instance. Refer to the applicable driver manual for information about the commands (mplbconfig/iompadm add/iompadm new).

6. [Solaris OS server node] Arrange the files in /dev/rdisk with # disks -C command.
7. [Windows] Restart the unit so that the device is recognized. Even if the device is automatically recognized by Windows 2003, it is recommended to restart the unit so that the device is recognized again.
8. [Linux server node] Restart the unit so that the device is recognized.
9. [HP-UX server node] Restart the unit to execute device recognition. After restart, check the connection of the device and search for the device file (for example, /dev/dsk/c5t1d0) with #ioscan -funC disk command. If the device file does not exist, create the device file by executing #insf-H <H/W pathname > -e command for H/W path in which the device file is not detected.
10. [AIX server node] Restart the unit to execute device recognition.
11. [Other server nodes] Perform operations for device recognition.

When the operating system is VMware vSphere 4 or later, reboot the VM host or, by using VMware Infrastructure Client, execute "Rescan" for the HBA that the access path has been set and perform [Reload Conf.] for applicable server node by using this software. Refer to "Access path management" in "Configuration management" in "4.1.7.1 VMware vSphere 4 or later" for the using method of VMware Infrastructure Client.

12. Check the access path from this software.

- [For Solaris OS server node]

/dev/rdisk/cXtXdX is created on the server node side and the access path is displayed.

- [Windows server node, Linux server node, HP-UX server node, or AIX server node]

A device is generated on the server node side, and the access path is displayed.



Note

Confirmation of the status of server node (HBA)-server node (HBA) and storage device (CA)-storage device (CA) access paths is performed by checking the zoning information for the fibre channel switch device using the Web Console. Deletion is performed by deleting the fibre channel switch device information in the Web Console.

Set the zoning shown below if the ETERNUS VS850 is operating. These are normally set during VS850 installation but can also be set on the Management Server.

- Host zone (zone between the host and the VS850)
- Storage zone (zone between the VS850 and storage)
- I/O group zone (zone for inter-node communication either within a VS850 I/O group or between I/O groups)
- Remote zone (zone for communication between different VS850 clusters)

These zonings are normally set during installation of the VS850, but for the storage zone, it is possible to set the switch device's zoning and the storage device's host affinity using this software's access path setting function.

For zones besides the storage zone, set the zoning for the switch device manually.

6.2.4 Deleting an access path

This software can delete access paths set by it and access paths for Fibre Channel switches.

Delete an access path for which one-to-one WWPN zoning is set for a Fibre Channel switch between server nodes (HBAs) or between storages (CAs) according to the zoning information in Fibre Channel switch properties.

The access path cannot be deleted to change the zone status of the switch to non-zoning (No Security). All the zoning settings of the switch are deleted when a user request to delete an access path is processed, this software creates a dummy zone. Although the loss of zone security as a result of deleting zoning can lead to inadvertent accessing of disk areas during operation, the dummy zone created prevents data destruction.

When changing the zone status of the switch to non-zoning (No Security), manually change the zone status of the switch to No Security. Note that this dummy zone will not be deleted even if access path addition processing is executed.

6.2.4.1 Preparations

Notes

- Only "System Administrator" account can delete access paths.
- You cannot delete access paths defined during setup other than for setting one-to-one WWPN zoning such as port zoning, WWNN zoning, or multi-port WWPN zoning in a Fibre Channel switch. (Only the one-to-one WWPN zoning setting is valid in this software.) In such cases, delete a zone from the zone information of Fibre Channel switch properties, or log in directly to the Fibre Channel, and change the setup.
- Verify that all Fibre Channel switches cascaded to the Fibre Channel switch associated with the access path setting can be correctly recognized in the current status. Once an access path is changed because a Fibre Channel switch is temporarily disconnected from the cascade connection, the old cascade connection cannot easily be recovered. (In this event, execute the `cfgClear` command to delete zoning information for the Fibre Channel temporarily disconnected from the cascade connection. This enables cascade reconnection.)

- When deleting an access path that is configured in the FC routing functionality LSAN zone in this software, manually delete the LSAN zone in the device in advance.

Server node setting

- If Fujitsu multipath disk control mechanism or msdsm on the Windows server node, be sure to shut down the server node before deleting an access path. If an access path is deleted while the server node is in operation, a very long time is required to shut down the server node later because of the operation of Windows path detection logic.
- To delete the access path of Fujitsu multipath disk control mechanism or msdsm on the same server node as the Management Server from this software, shut down the Management Server, disconnect the FC cable from the access path to be deleted, restart the admin server, and delete the access path.
- For Unix, execute umount for the access path to be deleted.

Physical removal (only for Solaris OS)

- When ETERNUS Multipath Driver 2.0.1 or higher is used and the access path to be deleted is physically connected to a Fibre Channel switch for which no zone is set, physically remove the access path in advance such as by disconnecting the cable for which access path deletion is to be executed.

6.2.4.2 Setting

Delete a set access path.

1. [Solaris OS (MPLB, MPHD environment)] Release the multipath setting.

Refer to the relevant driver's manual for information on the command and command parameters.

- If MPLB 2.2 and higher, execute the following command:

```
# mplbconfig (arguments are required, -d option)
```

- If MPLB 2.1 and former or MPHD, execute the following command:

```
# iompadm (arguments are required, destroy option)
```

MPLB2.1 or earlier and MPHD do not support the commands that add and remove paths. Delete the multipath instance by using the above command (iompadm destroy).

2. [Solaris OS (MPLB, MPHD, HDDV environment)] Release HDDV.

When the hot system expansion function of server node is disabled, execute the following commands:

```
# hddvadm -i
```

hddv.conf is moved to sd.conf, and the mphd.conf/mplb.conf file is saved.

3. [Windows] If Fujitsu multipath disk control mechanism or msdsm is set, shut down the Windows server node. If the Windows server node is active in this environment, this software suppresses access path deletion.
4. Using the Web Console, execute the deletion of the target access path.
5. [ETERNUS Multipath Driver 2.0.1 or higher] Execute the grmpdautoconf command to implement path removal. (Refer to the *ETERNUS Multipath Driver User's Guide* for details of the command specifications.)
6. [Solaris OS] Follow the procedure below so that the server node recognizes the storage unit.

In the hot system expansion (hddvadm -M) environment of ETERNUS Multipath Driver 2.0.1 or higher, MPLB, MPHD, or HDDV, execute the command shown below. After path removal, the server must be restarted to enable the Fibre Channel card definition of the server node.

```
# /usr/sbin/shutdown -y -i6 -g0 (restarts the server)
# disks -C
```

In an environment using MPLB2.2 or later, MPHD, and HDDV with non-hot system expansion or normal specified (hddvadm -m), execute the following operations:

- #touch /reconfigure
- # /usr/sbin/shutdown -y -i5 -g0
- Start it in single user mode.
- # hddvadm -m (The required part of sd.conf is moved to hddv.conf, and the saved mphd.conf/mplb.conf file is restored.)
- #touch /reconfigure
- # /usr/sbin/shutdown -y -i6 -g0 (Instances for each driver (mplb/mphd/hddv) are configured when the definition file is restored.)
- # disks -C

In an environment using MPLB2.1 or earlier

- #touch /reconfigure
- # /usr/sbin/shutdown -y -i5 -g0
- Start it in single user mode.
- # hddvadm -m (The required part of sd.conf is moved to hddv.conf, and the saved mphd.conf/mplb.conf file is restored.)
- #touch /reconfigure
- # /usr/sbin/shutdown -y -i6 -g0
- # disks -C
- Reconfigure the multipath by using the new #iompadm command.

In an environment where neither the hard disk driver (HDDV) nor multipath control (MPHD MPLB) is used

- #touch /reconfigure
- # /usr/sbin/shutdown -y -i6 -g0
- # disks -C

7. Check the access path from this software.
8. [Windows] Restart the device.
9. [Linux] Restart the device.
10. [HP-UX] Restart the device.
11. [AIX] Restart the device.
12. [Other server nodes] Perform operations for device deletion recognition.

When the operating system is VMware vSphere 4 or later, reboot the VM host or, by using VMware Infrastructure Client, execute "Rescan" for the HBA that the access path has been and perform [Reload Conf.] for applicable server node by using this software. Refer to "Access path management" in "Configuration management" in "4.1.7.1 VMware vSphere 4 or later" for the using method of VMware Infrastructure Client.

6.2.5 Access path inheritance

This software sets WWPN-based security settings on a device to form an access path. However, when the faulty part such as an adapter (controller) is replaced, the WWPN name may be changed because it is unique.

- Devices whose WWPNs are changed when the faulty part such as an adapter (controller) is replaced:
All HBAs and ETERNUS LT230, etc.
- Devices whose WWPNs are not changed when the faulty part such as an adapter (controller) is replaced:
ETERNUS Disk storage system, ETERNUS LT250/LT270, etc.

Operation can be performed as is if WWPNs are not changed. If WWPNs are changed because an adapter (controller) is replaced, security functions of the WWPNs constituting the access path must be changed to those of new WWPNs. This operation is defined as "access path inheritance" and it provides a function that changes the WWPN security settings managed by this software.

Refer to the following sections for the access path inheritance procedure after replacing the faulty parts.

- ["9.3.1.2 Access path inheritance after HBA replacement"](#)

6.2.6 To manage Fibre Channel switch that has already set in port zoning

One-to-one WWPN zoning setting is recommended in this software to realize the complete zoning security management as described in ["4.2.1 SN200 \(Brocade\) Fibre Channel switch"](#), though port zoning is possible to be performed. The procedure to change into one-to-one WWPN zoning setting is as follows.

1. Confirm that all the monitored devices are connected with all the switch ports.
2. Change the sanma.conf. Refer to ["A.2 sanma.conf Parameter"](#) and specify 1 in ["SET_SW_ZONING_ALWAYS"](#).
Either perform an update to the setting file using the Web Console or restart Manager to reflect the content of this file.
3. In the Web Console, add an access path corresponding to the port zoning.
4. After adding of the access path is complete, check that WWPN zoning which indicates information identical to that of the port zoning is displayed on the Web Console, and then delete the specified port zoning.

Note

For the multiple ports zoning setting, do not delete the multiple port zoning until WWPN zoning corresponding to each port zoning.

5. Repeat the procedure from steps 3 to 4.
6. If necessary, return the setting that is executed in step 2 to the former setting.
To change the zoning setting can be executed in zone administration window in WEBTOOLS in Fibre Channel switch and by Telnet function.

Point

The change to the zoning settings is performed on a Fibre Channel switch equipped with the latest firmware in the fabric (all of the Fibre Channel switches in the cascading connection) that contains the Fibre Channel switch selected when this properties window is opened.

6.3 Event Display and Linkage

This software receives and decodes an SNMP Trap that is sent from a device, and handles a device status change as an event for managing device errors.

The event is created based on the contents of SNMP Traps and user settings.

The processing described below is performed for generated events.

- [Displaying event logs](#)
- [Systemwalker Centric Manager linkage](#)

- [Shell/Bat linkage](#)
- [External script linkage](#)
- [E-mail notification](#)

As for the following event, this software only displays event logs, and other processing are not performed.

- Trap events common to devices (the trap common to devices in "Events in Notifications Sent from Monitored Devices" in the *ETERNUS SF Event Guide*)
- Start of performance data re-collection/Success of performance data re-collection event (Success of performance data re-collection, Success of performance data re-collection in "Performance Management Traps" in the *ETERNUS SF Event Guide*)
- Event that indicates when the state changes into error(red) in the device polling function ("When the state changes into error(red)" in the device polling function "Device Polling Event" in the *ETERNUS SF Event Guide*)



See

Refer to "[Appendix A Customization](#)" for detailed information on how to customize SNMP Trap processing.

Displaying event logs

Generated events are displayed in the event log of the Web Console. Events are displayed shown as below.

Displayed Items	Details
type	Displays the level of a displayed event.
date	Displays time and date event occurred in Month DD, YYYY HH:MM:SS AM (or PM).
device	Displays the name of a device on which the event occurred. This may not be displayed for events by user operations.
message	Indicates the event ID and its details. Displays this ID when the event has the corresponding ID. This ID is defined in the manager that is monitoring the event. Refer to the <i>ETERNUS SF Event Guide</i> for details about events.



Note

If multiple SNMP Traps comprised of the same information are received from a device at the same time and date, only the first received SNMP Trap will be displayed on the event log.

Systemwalker Centric Manager linkage

Also, generated events are reported to Systemwalker Centric Manager. Refer to "[11.1 Linkage with Systemwalker Centric Manager](#)" for information on settings required in advance. The importance levels of the events are also reported.



Note

Events of the server node agent is not reported to Systemwalker Centric Manager. (Shell/Bat linkage is operated.) Execute fault monitoring by message monitoring function of Systemwalker Centric Manager.

Shell/Bat linkage

A generated event is specified in the call argument of the Shell file, such shown as below.

Platform of Manager	File Name (Full Path)
Windows	\$ENV_DIR\ESC\Manager\etc\opt\FJSVssmgr\current\trapop.bat arg1 arg2 arg3 arg4 arg5 arg6 (\$ENV_DIR means "Environment Directory" specified at the Manager installation.)
Solaris OS, Linux	/etc/opt/FJSVssmgr/current/trapop.sh arg1 arg2 arg3 arg4 arg5 arg6

The "arg1" is the fault detail for the target device.

The "arg2" is the IP address for the target device.

The "arg3" is the server node name (FQDN) for the target device (if the full domain name cannot be confirmed, the IP address is set).

The "arg4" is the number of milliseconds that have elapsed from 00:00:00 GMT 01 Jan 1970 ("zero") to the current time.

The "arg5" is the fault level ("INFO", "WARNING", "ERROR").

The "arg6" is the name for the target device.

Rewriting the content of these shell/bat files enables the e-mail linkage of fault information or other Management Software linkage (such as issuing commands to Management Software and writing information to a log file managed by Management Software).

Sample Shell/Bat files are installed in the directories shown below. Copy this sample and create Shell/Bat files for linkage.

Platform of Manager	File Location
Windows	\$ENV_DIR\ESC\Manager\opt\FJSVssmgr\lib\sample\trapop.bat (\$ENV_DIR means "Environment Directory" specified at the Manager installation.)
Solaris OS, Linux	/opt/FJSVssmgr/lib/sample/trapop.sh

If the Shell/Bat linkage function is not used, there is no need to create these Shell/Bat files.

The following are examples of scripts output in the system log or event log if an event occurs:

For Windows:

```
@echo off
EVENTCREATE /L SYSTEM /ID 999 /SO StorageCruiser /T ERROR /D "%4 %5 %3 %2 %~1"
```

For Solaris OS or Linux:

```
#!/bin/sh
logger -- "$4 StorageCruiser $5 $3 $2 $1"
```

Note

- The IP address of a target device is included in the event message output in the system log or event log.
- Perform event output into in the system log or event log in a Manager environment that does not coexist with a server node agent. In the Manager and server node agent coexisting environment, a message may repeatedly be output.

External script linkage

Any external script other than trapop.sh/trapop.bat of Shell/Bat linkage can be executed. Up to two scripts can be defined in each SNMP Trap XML definition file. Arguments for calling such scripts are common to those for Shell/Bat linkage.

Refer to "[A.5 SNMP Trap XML Definition File](#)" for information about the methods for defining.

Note

- External script linkages must be defined in the SNMP Trap XML definition file. Therefore, they are not available on devices where XML definition files are not provided.

- For shell scripts or batch files in Shell/Bat linkages or external script linkages, do not output processing results and processing progress on the screen (for example, do not perform such a process as displaying a message with the echo command). Be sure to describe "@echo off" at the head under Windows.

E-mail notification

A created event is notified by e-mail in the following format:

```
Subject: ETERNUS SF Event Mail
From: $1
To: $2

Severity: $3
Date: $4
Device IP: $5
Device Name: $6
Message: $7
```

- \$1: Indicate e-mail address from where the notification is sent (You need to set it in advance.).
- \$2: Indicates e-mail address where the notification is sent (You need to set it in advance.).
- \$3: Indicates the fault level (Information, Warning, Error)
- \$4: Indicates time and date when the event occurred.
- \$5: Indicates IP address for the target device
- \$6: Indicates a name of the target device
- \$7: Indicates the fault detail

All Warning and Error events will be notified. For Information events, transition of the Thin Provisioning Pool using rate and reduction of Thin Provisioning Pool's capacity are notified. If you want to be notified other Information events, refer to "[A.5 SNMP Trap XML Definition File](#)".

Users can customize the displaying of events and descriptions of linkage for individual SNMP Traps. Refer to "[A.5 SNMP Trap XML Definition File](#)" for details.

Point

To perform Systemwalker Centric Manager linkage, Shell linkage, or external script linkage, either register the IP address and host name information for each device in the DNS server that is referenced by the Management Server, or define them in the /etc/hosts file on the Management Server so that the names of the devices registered in this software can be resolved.

6.4 Thin Provisioning Management

This product can manage storage capacity virtualization operations that use the Thin Provisioning function of the ETERNUS Disk storage system. The functions below are provided.

Threshold monitoring

This function monitors the threshold values for the Thin Provisioning Pool capacity used. It can also change the threshold values.

Capacity management

This function displays the changes in capacity used for the Thin Provisioning Pool graphically.

6.4.1 Threshold Monitoring

This function monitors the threshold values for the Thin Provisioning Pool capacity used.

Threshold values and Threshold monitoring status

The values of the "Caution threshold value" and the "Warning threshold value" set for each Thin Provisioning Pool and the Threshold monitoring status are displayed. The "Caution threshold value" and the "Warning threshold value" are prepared at the disk storage system, and are the threshold values for Thin Provisioning Pool capacity used.

Threshold value settings

The initial values for the "Caution threshold value" and the "Warning threshold value" are set by the disk storage system when a Thin Provisioning Pool is created. If required, change the settings for the capacity threshold values.

Procedure for setting threshold values

Set the threshold values by using the Web Console.

Action to take when threshold values are exceeded

If threshold values are exceeded, then follow the procedures below:

- Detection of status change

When a threshold value is exceeded, the product displays an SNMP Trap in the event log, which notifies the change in Thin Provisioning Pool status at the disk storage system.

- Refreshing

After checking the displayed event, perform [Reload Conf.] on the applicable storage system.

- Checking the status of the Thin Provisioning Pool

Start the Thin Provisioning Pool monitor window and check the Thin Provisioning Pool status. Extend disks or take other action in accordance with the exceeded threshold values.



See

.....
If the SNMP Trap that notifies of changes in the Thin Provisioning Pool status is not received due to packet loss or other reason, then the product detects the change by polling the Thin Provisioning Pool information of the disk storage system. Since the polling interval is one hour, the time from status change to detection is within one hour. The polling intervals can be customized. Refer to "[A.8 Polling Service Setting File](#)" for details.
.....



Information

.....
Even if capacity reaches "Caution threshold value" which is set for each LogicalVolume, SNMP Trap will not be sent. "Caution threshold value" for LogicalVolume is a threshold value for unallocated capacity of LogicalVolume which is at the disk storage system.
.....

6.4.2 Capacity Management

This function displays the Thin Provisioning Pool Capacity and its changes in the capacity used graphically to grasp the changes in the capacity used for the Thin Provisioning Pool.

This enables users to grasp the period to expand the size of the physical disk for the Thin Provisioning Pool, or to review the threshold setting according to the situation.



Information

.....
The information of the Thin Provisioning Capacity and its capacity used is displaying in graph. The information is obtained everyday at 1:00:00.

You can change the time to obtain the information by using a polling service setting file. Refer to "[A.8 Polling Service Setting File](#)" for details.
.....

6.4.2.1 Capacity Graph Window Types

It is possible to display the following graph.

One-month Graph window

The line graph displays data for the past 31 days from the present day.
The plot points are displayed on a daily basis.

One-year Graph window, One-decade Graph window

The line graph displays data for the past a year or a decade from the present day.
The plot points are displayed on a monthly basis.

6.5 Automated Storage Tiering Management

In this product, the Automated Storage Tiering function of the ETERNUS Disk storage system can be used by registering an optional license (ETERNUS SF Storage Cruiser Optimization Option). The Flexible Tier Volume (FTV) uses the Automated Storage Tiering function. However, FTV can be created and used without an optional license, by using the one layer Tier pool function explains in this section.

If you register the optional license to use the Automated Storage Tiering in the future, using FTV according to the instruction in this section reduces the work procedure.

Until the option license is registered, FTV is available as a volume that has the Thin Provisioning function.



See

Refer to the *ETERNUS SF Storage Cruiser Operation Guide for Optimization Function* for more information on the Automated Storage Tiering function.



Point

Operate one layer architecture explains in this section with the same Management Server. It does not occasionally operate correctly when operating it with two or more Management Servers.

Enable One Layer Operation

Enable the one layer operation (status of Automated Storage Tiering).

Refer to "Enable/Disable Automated Storage Tiering" in the *ETERNUS SF Web Console Guide* to enable it.



Note

To disable the one layer operation, it is required to delete all Tier pools.

Configure Tier Pool (One Layer)

Create a one layer Tier pool. For the created Tier pool, the following operations are available:

- Change Warning/Caution Threshold of Pool
- Change sub-pool name
- Expand sub-pool capacity
- Delete Tier pool



Point

When using a one layer Tier pool, the ETERNUS SF Storage Cruiser Optimization Option license is not required.

Configure FTV

Create an FTV in an existing one layer Tier pool. The created FTV can be deleted/changed/formatted.

6.5.1 Configure One Layer Tier Pool

A one layer Tier pool is registered as a FTRP in a storage device.

Creating a Tier pool from the Web Console creates both FTRP and FTSP in the storage device. Moreover, it is also made possible to create an FTV in the storage device from the Web Console.

Specify Master CM

A Master CM can be specified when performing the following operations.

- When creating a one layer Tier pool
- When expanding the capacity of the sub-pool

The Master CM is specified as a pair formed by a CM number and a CPU number. It is possible to specify more than one Master CM, and by specifying a Master CM in relation to the Tier pool, it is possible to specify a Master CM of the entire Tier pool.

When multiple Master CMs are specified to the Tier pool, the Master CM is decided from the specified Master CMs using the round-robin method.

When creating a sub-pool in the Tier pool, it is possible to specify a Master CM of the sub-pool from the multiple Master CMs specified to the Tier pool.

When expanding the capacity of the sub-pool, take into account the master CMs that have already been assigned to each sub-pool that has already been created, and assign a Master CM using the round-robin method. It is also possible to make a specification from the Master CM which is displayed in the Master CM list.

When a specification of a Master CM has been omitted, this will automatically be assigned according to the implementation of the storage device.

Table 6.2 CM Allocation Logic During New Creation in Storage Device Having 2 CMs

Specified Tier Pool	Sub-Pool Specification	Master CM to Be Set	Description
CM#0	-	CM#0	Configure CM#0 according to specification of pool
CM#0, CM#1	-	CM#0	Configure CM#0 in round-robin method based on specified Tier pool
CM#0, CM#1	CM#0	CM#0	Configure CM#0 according to specification of sub-pool
CM#0, CM#1	CM#1	CM#1	Configure CM#1 according to specification of sub-pool

Table 6.3 CM Allocation Logic During Capacity Expansion in Storage Device Having 2 CMs

Specified Tier Pool	Set Master CM	Master CM Which Are Newly Assigned	Description
CM#0	CM#0	CM#0	Configure CM#0 according to specification of pool
CM#0, CM#1	CM#0	CM#1	Configure CM#1 that is not assigned
CM#0, CM#1	CM#1	CM#0	Configure CM#0 that is not assigned

Disk Auto-Selection

The disk can be automatically selected when performing the following operations.

- When creating a one layer Tier pool
- When expanding the capacity of the sub-pool

Specify the necessary physical capacity when selecting automatically. The disk can also be selected manually.

6.5.1.1 Create One Layer Tier Pool

Create a one layer Tier pool. Refer to "Create One Layer Tier Pool" in *the ETERNUS SF Web Console Guide* for information on how to create it.

6.5.1.2 Change Single Layer Tier Pool

To change the operation of one layer Tier pool, change the definition of the Tier pool.

Changeable items are as shown in "Table 6.4 Change One Layer Tier Pool".

Table 6.4 Change One Layer Tier Pool

Item	Meaning
Warning Threshold of Pool	This is the threshold (%) of the usage rate of the Tier pool in order to monitor the available capacity of the Tier pool. It is necessary to specify a value that is greater than Caution Threshold of Pool . When this threshold is exceeded, a warning will be notified by the SNMP Trap.
Caution Threshold of Pool	This is the threshold (%) of the usage rate of the Tier pool in order to monitor the available capacity of the Tier pool. It is necessary to specify a value that is smaller than Warning Threshold of Pool . When this threshold is exceeded, a caution will be notified by the SNMP Trap. It is also possible to not configure this item.
FTSP name	This is a name of the sub-pool. It is necessary that this is a name that will be unique in the storage device.

Refer to "Display Tier Pool" in the *ETERNUS SF Web Console Guide* for information on how to display the current detailed information of a Tier pool.

Refer to "Change Tier Pool" in the *ETERNUS SF Web Console Guide* for information on how to change the Tier pool.



Point

- It is not possible to change the definition of multiple Tier pools at once. When changing the definition of multiple Tier pools, make changes to the each Tier pool at a time.
- The definition of a Tier pool in which Automated Storage Tiering has already been started cannot be changed.

6.5.1.3 Delete One Layer Tier Pool

Before operating the deletion, display the detailed information of the one layer Tier pool that you are about to delete and confirm that deleting this will not be a problem. Refer to "Display Tier Pool" in the *ETERNUS SF Web Console Guide* for information on how to display the detailed information of a Tier pool.

Refer to "Delete Tier Pool" in the *ETERNUS SF Web Console Guide* for information on how to delete a Tier pool.



Point

- Multiple Tier pools can be deleted at once.
- The following Tier pools cannot be deleted.
 - Tier pools on which FTVs are present
 - Tier pools in which Automated Storage Tiering has already been started

6.5.1.4 Expand Sub-Pool Capacity in One Layer Tier Pool

It is possible to expand the capacity of the sub-pools which configure a one layer Tier pool. Refer to "Expand Capacity of Sub Pool in Tier Pool" in the *ETERNUS SF Web Console Guide* for information on how to expand the capacity of a sub-pool.



Note

Expanding the capacity of the sub-pool leads to deviation of data in the sub-pool and brings about variations in access performance. Perform the Flexible Tier Pool Balancing using ETERNUS Web GUI or ETERNUS CLI in order to eliminate data deviation. Refer to the ETERNUS Web GUI Online Help for information on how to perform the Flexible Tier Pool Balancing.

Perform the Flexible Tier Pool Balancing after stopping Automated Storage Tiering in relation to the target Tier pool. When the Flexible Tier Pool Balancing is performed during the operation of Automated Storage Tiering, this may cause cases where Automated Storage

Tiering does not operate properly. Refer to "Start/Stop Automated Storage Tiering for Tier Pool" in the *ETERNUS SF Web Console Guide* for information on how to stop Automated Storage Tiering of a Tier pool.

6.5.2 Configure FTV

Only FTVs can be created in a one layer Tier pool.
Configuration of FTV is performed with the Web Console. This cannot be performed with the ETERNUS Web GUI.



Implement the changing / deletion / formatting of an FTV after updating the administration information of the FTV.

In order to update the administration information of an FTV, in relation to the ETERNUS Disk storage system of which the IP address thereof has been changed, perform the procedures listed under "Reload ETERNUS Disk Storage System Configuration Information" in the *ETERNUS SF Web Console Guide*.

6.5.2.1 Create FTV

Create an FTV.

Refer to "Create FTV" in the *ETERNUS SF Web Console Guide* for information on how to create an FTV.

6.5.2.2 Change FTV

The definition of an FTV is changeable.

Refer to "Change FTV" in the *ETERNUS SF Web Console Guide* for information on how to change it.



- The current details of the definition of an FTV can be confirmed by following the procedures listed under "Display FTV" in the *ETERNUS SF Web Console Guide*.
- It is not possible to change the definition of multiple FTVs at once.

6.5.2.3 Format FTV

Refer to "Format FTV" in the *ETERNUS SF Web Console Guide* for information on how to format an FTV.
Furthermore, as an FTV is automatically formatted when being created, it is unnecessary to format a newly created FTV.



It is not possible to format multiple FTVs at once.

6.5.2.4 Delete FTV

Before operating the deletion, display the detailed information of the FTV that you are about to delete and confirm that deleting this will not be a problem. Refer to "Display FTV" in the *ETERNUS SF Web Console Guide* for information on how to display the detailed information of an FTV.

Refer to "Delete FTV" in the *ETERNUS SF Web Console Guide* for information on how to perform the deletion.



- Multiple FTVs can be deleted at once.
- An FTV that is currently assigned to a server cannot be deleted.

6.5.3 Measures to be taken when Tier pool configuration has been changed with managed devices

When the configuration of the Tier pool to be managed is changed, there is a possibility that a difference will occur between the Tier pool information present on the ETERNUS SF Manager and the Tier pool information of the device. When status update of Automated Storage Tiering is performed while in a state where there is a difference, the esast3101 message will be output to the operation log.

When the esast3101 message has been output to the operation log, perform the following actions.

1. Execute the "esfast tierpool delete" command and delete only the information of the Tier pool subject to the esast3101 message.

```
> esfast tierpool delete -name name -mode file -s
```

For *name*, specify the name of the Tier pool subject to the esast3101 message.

2. In the Web Console, click **Automated Storage Tiering** > **Overview**, and click **Status Update** under **Automated Storage Tiering** on the Action pane.

Refer to "Command References" in the *ETERNUS SF Storage Cruiser Operation Guide for Optimization Function* for information on the "esfast tierpool delete" command.

6.5.4 Change to Multiple Layer Tier Pool

Registering the ETERNUS SF Storage Cruiser Optimization Option license allows changing a one layer Tier pool to a two layer or three layer Tier pool, and the Automated Storage Tiering can be operated.

The procedure for that is as follows:

1. Register the ETERNUS SF Storage Cruiser Optimization Option license.
Refer to "Register License" in the *ETERNUS SF Web Console Guide* for the registration procedure.
2. Change the layer number of the Tier pool, and operate the Automated Storage Tiering.
Refer to "Change Number of Layers of Tier Pool" in the *ETERNUS SF Storage Cruiser Operation Guide for Optimization Function* for information on how to change the layer number.

6.6 NAS Management

This product will manage ETERNUS Disk storage system models that are multi-protocol storage with a block access interface (SAN) and a file access interface (NAS). With the Web Console, various features for operation of the ETERNUS Disk storage system NAS file system can be utilized.

This section explains the following items necessary in order to perform NAS operation of the ETERNUS Disk storage system with this product.

- [Overview of Functions](#)
- [Required Setup Configuration](#)
- [Installation Steps](#)
- [Operation Method](#)



.....
This function cannot be used for ETERNUS DX200F.
.....

6.6.1 Overview of Functions

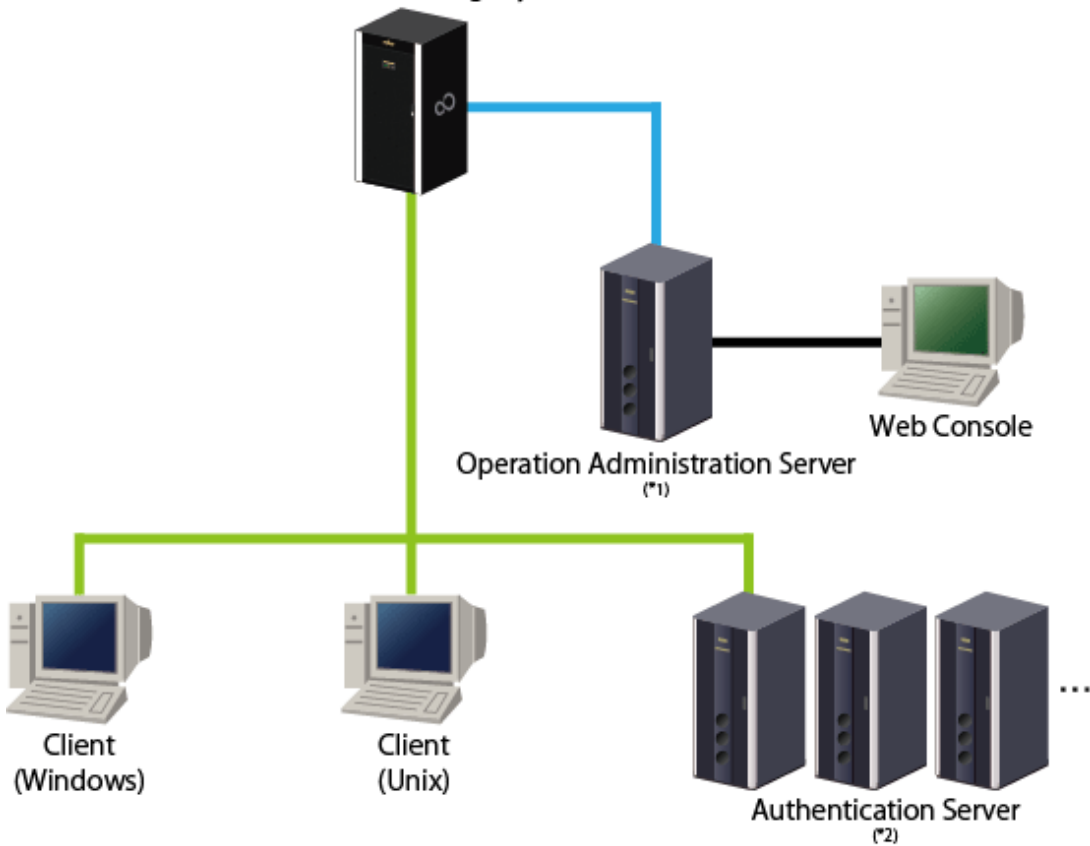
6.6.1.1 About NAS Management

NAS management of the ETERNUS Disk storage system will be explained.

6.6.1.1.1 Basic System Configuration

Basic system configurations required when operating NAS of the ETERNUS Disk storage system will be explained.

Figure 6.1 Basic System Configuration Diagram
ETERNUS Disk storage system



- As long a connection is established as a network, this may be either of an administration LAN or a task LAN
- Administration LAN
- Task LAN

*1: The server on which the ETERNUS SF Manager is installed

*2: It is possible for the system to be provided with multiple authentication servers

Configuration of NAS is performed from the Management Server.

Connect the Management Server and the ETERNUS Disk storage system with a management LAN. Access to the Management Server is performed from either the Management Server or the Web Console of a terminal within a network capable of HTTPS communication with the Management Server.

Utilization of NAS is performed from a client on the business LAN.

The client for accessing the shared folder of NAS and the ETERNUS Disk storage system is connected with a business LAN. In addition, in order to perform authentication administration for NAS access, authentication server(s) must be configured on the business LAN.

Point

When an authentication system is not used for the NAS file system, it is unnecessary to setup an authentication server on the system.

If an authentication system is not implemented then the NAS file system can be accessed from any clients connected to the business LAN. It is strongly recommended that an authentication server is properly configured and implemented.

6.6.1.1.2 Support Features

In order to perform NAS operation of the ETERNUS Disk storage system, this product is provided with the following features.

- [Easy Installation of a NAS File System using a Wizard](#)
- [Display of Configuration Information and Fault Monitoring](#)
- [Block Level Performance Management and Capacity Monitoring](#)
- [Backup/Restoration of NAS Volume](#)

Easy Installation of a NAS File System using a Wizard

The "creating of a shared folder" and the "creating of a NAS interface" which are necessary when installing a NAS file system can be configured easily by using a wizard.

Display of Configuration Information and Fault Monitoring

The configuration information resources being used for ETERNUS Disk Storage system NAS can be confirmed with the Web Console. In addition, when a failure occurs, the details of the failure will be displayed in the event log of the Web Console.

Block Level Performance Management and Capacity Monitoring

Performance monitoring of ETERNUS Disk storage system NAS volumes and capacity monitoring of NAS file system are implemented at a level similar to that for block volumes.



Information

The performance monitoring and threshold monitoring functions cannot be used for a NAS port.

Backup/Restoration of NAS Volume

Backup / restoration from a NAS volume to a NAS backup volume will be realized with QuickOPC. In addition, the NAS backup volume can be accessed as Read-Only which provides for file level recovery.

6.6.1.1.3 Configuration Items of the NAS File System

Configure the following with the Web Console in order to perform NAS operation of the ETERNUS Disk storage system.

- [Shared folder](#)
- [NAS Interface](#)
- [Authentication System](#)

An overview of each of the above mentioned items will be explained.

Shared folder

The shared folder refers to a folder made public on the network as a NAS file system. In this product, it is possible to configure access control or retrieve a backup by creating a shared folder.

When creating a shared folder from the Web Console, the following resources are also created simultaneously.

Resources	Explanation
NAS volume	A volume where the shared folder will be created. It is possible to create only one for a single ETERNUS Disk storage system. Multiple shared folders can be configured to a single NAS volume.
NAS backup volume	A volume for backup of the NAS volume. It is possible to create only one for a single ETERNUS Disk storage system. Creation of the NAS backup volume is optional.
NAS system volume	Multiple volumes to control NAS. It is created when a new NAS volume is created. It is created in the same Thin Provisioning Pool as NAS volume.
Copy group	Copy group used to back up NAS volume. It is created only when a NAS backup volume is created.

Resources	Explanation
Copy pair	A copy pair of a NAS volume and a NAS backup volume. This is created only when a NAS backup volume is created.

The shared folder that is created with this product can be accessed using the following protocols. As it is possible to use the following protocols simultaneously, it is possible to access a single shared folder from both UNIX and Windows clients.

- CIFS
This protocol is a developed version of SMB which is used in Windows file sharing.
- NFS
This protocol is a protocol used between UNIX based OSs.

NAS Interface

A NAS interface refers to the definition information of a network interface that manages, over a business LAN, a public IP address for access to the shared folder and information of the port to which this IP address is assigned. One IP address (NAS interface) can be configured in relation to one port from the Web Console.

Information

- By using the VLAN function of the ETERNUS Disk storage system, it is possible to assign multiple IP addresses to a single port. With the Web Console, by displaying the VLAN ID assigned to the NAS interface, it is possible to confirm whether VLAN configurations are present.
- There is no relation between the shared folder and the NAS interface. It is possible to reference the same shared folder from any NAS interface.

The NAS interface maybe assigned to a single port or 2 ports. The type of connections that can be configured are as follows.

- Active-Active connection
A method where 2 ports are used, and an IP address is configured to each. Both ports are enabled, and it is possible to access the shared folder from either port. In addition, 2 IP addresses can be publicized for clients, and it is possible to distribute the bandwidth load. In the event that one port is down, as the IP address configuration can be passed on to the other port automatically, operation with the same IP address can be continued even after recovering from the down time.

Information

During the time one port is down, operation is limited to a single port. It is not possible to distribute the bandwidth load across 2 ports.

- Active-Standby connection
A method where 2 ports are used, and a single IP address is configured. Of the 2, only one port will be enabled (Active port), and the other port will be disabled (Standby port). When the Active port is down, the IP address configuration can be passed on to the Standby port which is automatically enabled, making it possible to continue operation with the same IP address even after recovering from the down time.
- Single connection
A method where 1 port is used, and a single IP address is configured. When the port goes down, it will not be possible to access the shared folder.

Information

In order to continue business when a port is down, it is recommended to configure either Active-Active or Active-Standby connection for redundancy.

Authentication System

With this product, as access to the shared folder is controlled, an authentication system using a domain controller is provided. The domain controller centrally manages the account information of individual clients on the network, and conducts authentication in relation to each of these clients or permits access.

In case an authentication server goes down, it is possible to register a maximum of 3 authentication servers for each authentication method.

The authentication methods supported by this product are as follows.

- Kerberos Authentication Method with Active Directory

Kerberos is a network authentication protocol designed to provide strong authentication for client/server applications. A password received from a client is authenticated, and a ticket is issued. By utilizing the ticket, the client that has been authenticated is able to utilize the network service.

When accessing the shared folder with a CIFS protocol, and when managing access to directories and files, in order to perform authentication and access control using this authentication method, register an Active Directory domain controller.

- Authentication Method using LDAP

LDAP is a protocol for accessing the directory service. With the directory service, it is possible to easily use features such as the search function by centrally managing the account information of network equipment and clients.

When accessing the shared folder with the NFS protocol, and when performing access management to directories and files, in order to perform authentication and access control using this authentication method, register an LDAP server.

6.6.1.2 Backup of the NAS Environment

An overview of backup of the NAS environment in the ETERNUS Disk storage system will be explained.

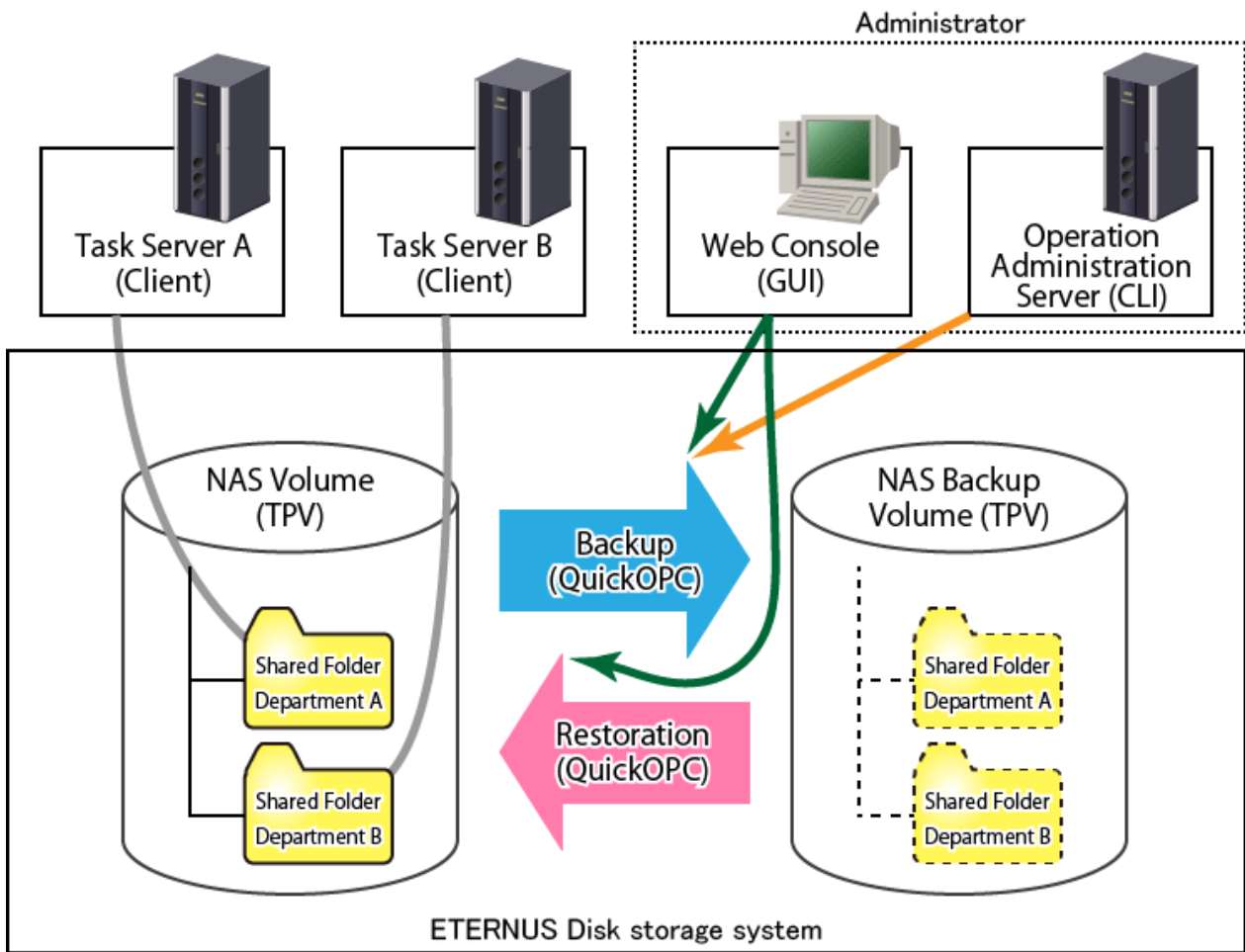


See

.....
Refer to "Backup of NAS environment" in the *ETERNUS SF AdvancedCopy Manager Operation Guide for Copy Control Module* for information on the backup operation for NAS environment.
.....

6.6.1.2.1 Backup/Restoration of NAS Volume

It is possible to back up the entire NAS volume configured with the Web Console to a NAS backup volume. In addition, it is possible to restore the entire NAS volume from the NAS backup volume.



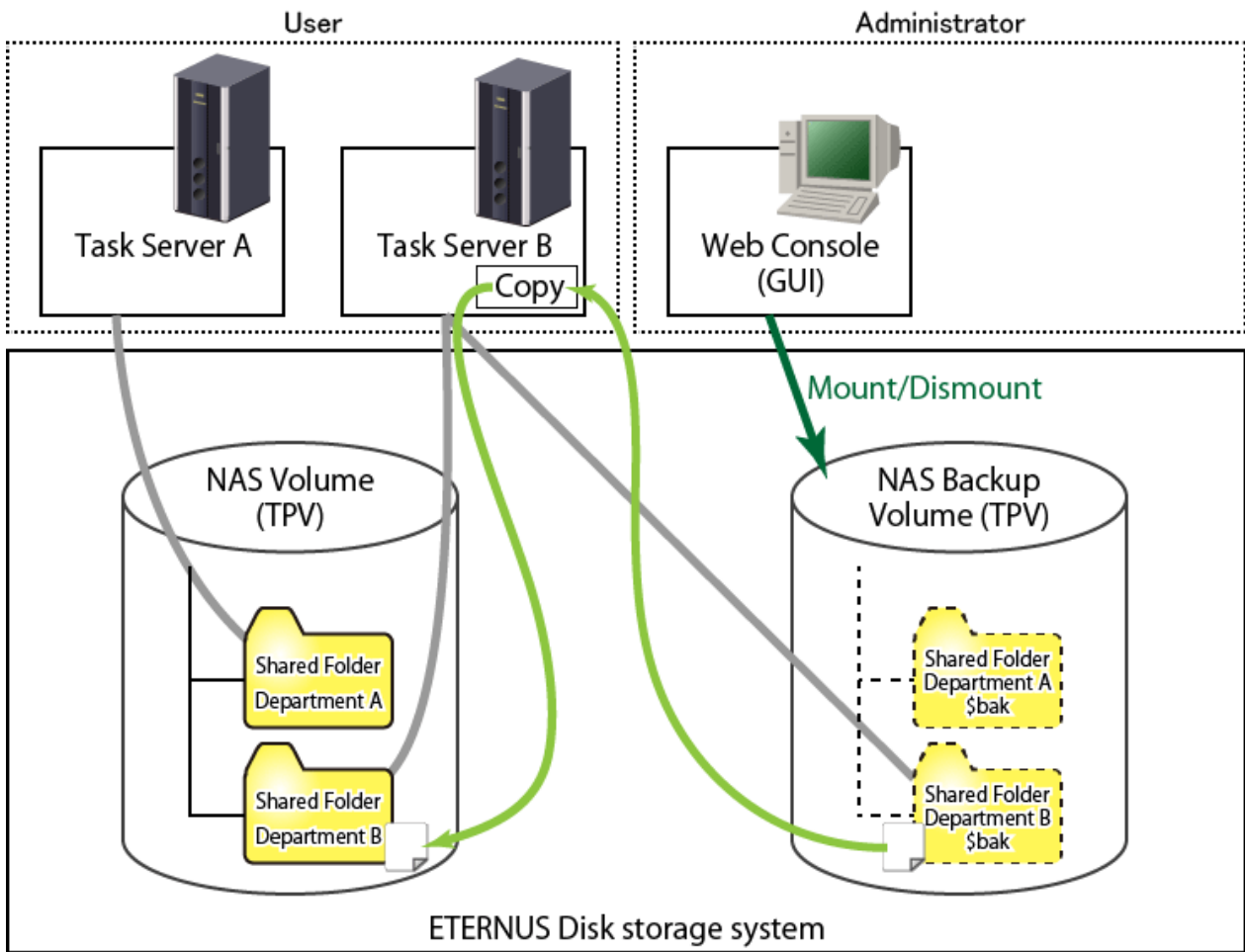
- Operations performed with the Web console
- Operations performed with the operation administration server (commands)

Information

- Backup of the NAS volume can either be executed with the Web Console, or be executed with commands from the Management Server. Restoration of the NAS volume can only be executed with the Web Console.
- When recovering individual files from the NAS backup volume, mount the NAS backup volume and manually copy the files.
- One each of a NAS volume and a NAS backup volume can be created for a single ETERNUS Disk storage system.

6.6.1.2.2 Mounting/Unmounting the NAS Backup Volume

The NAS backup volume that is the backup destination of the NAS volume can be mounted onto the NAS environment as Read-Only. By mounting the NAS backup volume, users can recover files themselves. In addition, a mounted NAS backup volume can be unmounted when recovery has been completed.



— Operations performed with the Web Console

Information

- Mounting and unmounting of the NAS backup volume can be done from the Web Console.
- While the NAS backup volume is mounted, it is not possible to backup or restore the NAS volume.
- The name of the shared folder on the NAS backup volume after being mounted is the name of the shared folder at the time of backup + "\$bak". Furthermore, the name of the shared folder of the NAS backup volume will not be displayed on the Web Console.

6.6.1.3 Operating Environment

The functions of the NAS option of the ETERNUS Disk storage system can be used with the following environments.

Object	Environment
Platform	Platforms on which the ETERNUS SF Manager can be operated.
Required licenses (software)	<ul style="list-style-type: none"> - ETERNUS SF Storage Cruiser Basic License (*1,*3) - ETERNUS SF Storage Cruiser Standard License (*1,*3) - ETERNUS SF AdvancedCopy Manager Local Copy License (*2)
ETERNUS Disk storage system	ETERNUS DX100 S3/DX200 S3/DX500 S3/DX600 S3 (ETERNUS DX200F excluded)
Required options (hardware)	NAS Option
Agent	Storage Cruiser's agent is not required.

Object	Environment
Authentication methods (*4)	[When accessing with the CIFS protocol] Active Directory [When accessing with the NFS protocol] LDAP

*1: Required to construct the NAS file system.

*2: Required to back up the NAS file system.

*3: Required to register either one.

*4: Required when performing access control using an authentication server for the NAS file system. When no authentication server is configured, all access will be permitted.

6.6.2 Required Setup Configuration

Requirements for installing ETERNUS Disk storage system NAS management will be explained.

Subject of Configuration	Configuration Details
ETERNUS Disk storage system	<ul style="list-style-type: none"> - Application of NAS Option - Preparing ETERNUS for Registration to This Product
Authentication server	<ul style="list-style-type: none"> - Registration of User/Group - Creating Redundant Authentication Servers
Management Server	<ul style="list-style-type: none"> - Device Registration - License Registration - Creating a Thin Provisioning Pool - Configuration of Connection Type of Advanced Copy

6.6.2.1 ETERNUS Disk Storage System Configuration

ETERNUS Disk storage system configuration will be explained.

The items to be configured are as follows:

- [Application of NAS Option](#)
- [Preparing ETERNUS for Registration to This Product](#)

Application of NAS Option

To apply the ETERNUS Disk storage system NAS option, refer to the ETERNUS Disk storage system manuals.

Skip this work if the NAS option has already been applied to the target ETERNUS Disk storage system.

Preparing ETERNUS for Registration to This Product

Prepare the ETERNUS Disk storage system to be registered to this product. Refer to "[4.3.1.1 Setting](#)" for details of the configuration.

Skip this work if the target ETERNUS Disk storage system has already been registered to this product.

6.6.2.2 Authentication Server Setup

Required configuration for the authentication server will be explained.

The items to be configured are as follows:

- [Registration of User/Group](#)
- [Creating Redundant Authentication Servers](#)

Registration of User/Group

On the domain controller or LDAP server, register the users and groups that have access to the shared folders. Refer to the LDAP or domain controller manuals for information on how to perform the registration.

Creating Redundant Authentication Servers

In this product, redundant authentication servers can be registered up to 3 units. Refer to the LDAP or domain controller manuals for information on how to create redundant configuration.

6.6.2.3 Prior Configurations for this Product

Prior configurations in relation to this product will be explained.

The details to be configured are as follows:

- [Device Registration](#)
- [License Registration](#)
- [Creating a Thin Provisioning Pool](#)
- [Configuration of Connection Type of Advanced Copy](#)

Device Registration

Register the ETERNUS Disk storage system to be managed with this product. Refer to "[5.2 Registering device](#)" for information on how to register the device.

When a target ETERNUS Disk storage system has already been registered to this product, and when application of the addition of the NAS option has been performed with "[6.6.2.1 ETERNUS Disk Storage System Configuration](#)", execute [Reload Conf.] for the ETERNUS Disk storage system.



See

.....
Refer to "Reload ETERNUS Disk Storage System Configuration Information" in the *ETERNUS SF Web Console Guide* for information on how to execute [Reload Conf.].
.....

License Registration

Register the ETERNUS Disk storage system NAS license, and any other required license that is not already registered.

Refer to required licenses (software) of the "[6.6.1.3 Operating Environment](#)" for required and optional licenses.

Skip this work if the license of the object has already been registered in this product.



See

.....
Refer to "Register License" in the *ETERNUS SF Web Console Guide* for information on how to register the license.
.....

Creating a Thin Provisioning Pool

A Thin Provisioning Pool in which the NAS volume is created will be created.

Skip this work if the Thin Provisioning Pool for the NAS volume has already been made.



See

.....
Refer to "Create Thin Provisioning Pool" in the *ETERNUS SF Web Console Guide* for information on how to create a Thin Provisioning Pool.
.....

Information

For increased reliability, it is recommended to create the primary NAS volume and the backup NAS volume in separate Thin Provisioning Pools. When performing NAS volume backup, create two Thin Provisioning Pools; one for the primary NAS volume and one for the backup NAS volume.

Configuration of Connection Type of Advanced Copy

Configure the access connection type for Advanced Copy in order to define the NAS volume backup.

Skip this work if the backup is not being used for NAS environment or if the connection has been configured already.

See

Refer to "Configure Connection Type for ETERNUS Disk Storage System" in the *ETERNUS SF Web Console Guide* for information on how to perform the configuration.

Information

For the configuration of the connection type, select "Access through volumes" or "Access through network".

6.6.3 Installation Steps

The installation steps for performing ETERNUS Disk storage system NAS operation is explained.

Installation is implemented in the following order.

Order	Installation Item	Title of Sections Listed in the Web Console Guide	Optional/Required (*1)
1	Creating Shared Folder	Create Shared Folder	Required
2	Creating NAS Interface	Create NAS Interface	Required
3	Configuration of Authentication Server	Configure Authentication Server	Optional

*1: Tasks that must be performed in order to operate the NAS file system are "Required", while tasks that may be omitted are "Optional".

Point

If an authentication system is not implemented then the NAS file system can be accessed from any clients connected to the business LAN. It is strongly recommended that an authentication server is properly configured and implemented.

6.6.3.1 Creating Shared Folder

Create a shared folder in order to configure the folder of the access destination of the NAS file system.

Configure the following for the shared folder:

- [Shared Folder Name](#)
- [Protocol](#)
- [Oplocks Setting](#)
- [Destination Volume to Create Shared Folder](#)
- [Volume Capacity](#)
- [NAS Backup Volume](#)

- [Access Configurations of the Shared Folder](#)
- [Host Access Configurations of Shared Folder](#)

Shared Folder Name

The name of the shared folder.

Protocol

The protocol to be used by the shared folder.

It is possible to select CIFS, NFS, or both of these protocols.

Oplocks Setting

This is the configuration of the Oplocks function that prevents concurrent file access.

It is possible to configure this only when using the CIFS protocol.

When the Oplocks function is enabled, although improvement of access performance from the client can be expected, it will become impossible to use the Alternate Data Stream. In addition, when selecting both protocols of CIFS and NFS, it is recommended that the Oplocks function is not enabled.

Destination Volume to Create Shared Folder

This is the volume where the shared folder is to be created.

It is possible to create a NAS volume only when a NAS volume does not exist. When a NAS volume does exist, the existing NAS volume will be specified.

Volume Capacity

This is the capacity of the NAS volume.

This is only to be specified when creating a new NAS volume.



Information

For NAS volume, a system area of 300GB is reserved. For this reason, the area available as a file system is the value after subtracting the system area from the area specified for the NAS volume.

e.g.: If a NAS volume of 3TB is created, the user area is 2.7TB and the system area is 0.3TB.

NAS Backup Volume

This is the volume for backing up the NAS volume. It is possible to create a new backup volume only when a NAS backup volume does not exist. When a NAS backup volume does exist, the existing NAS backup volume will be specified.

The NAS backup volume is created with the following details.

Volume Name	<i>nasVolumeName\$bakN(*1)</i>
Capacity	Same as the source NAS volume.
Volume type	Same as the source NAS volume.
Thin Provisioning Pool of the Creation Destination	User Selection

*1: "N" is a consecutive number from 0. The number of digits will vary.

When a NAS backup volume is created, the following copy group and copy pair will be automatically created.

- Copy group

The copy group is a group of copy pairs. A copy pair is comprised of a source NAS volume and a destination NAS backup volume.

Copy Group Name	NAS_QuickOPC_N(*1)
-----------------	--------------------

Copy Group Type	QuickOPC
-----------------	----------

*1: "N" is a consecutive number from 0. The number of digits will vary.

- Copy pair

The copy pair is a definition of a source NAS volume and a destination NAS backup volume. A copy pair is defined within a copy group.

In addition, it is also possible to make the NAS backup volume individually. Refer to "[6.6.4.6 Creating the NAS Backup Volume](#)" for this procedure.

Point

For increased reliability, it is recommended to create Thin Provisioning Pools of the creation destination for the NAS backup volume and the NAS volume in separate Thin Provisioning Pools.

Access Configurations of the Shared Folder

The owner and group that will issue access rights in relation to the shared folder will be configured. For the owner and group, configure a user or group on the authentication server configured with "[6.6.3.3 Configuration of Authentication Server](#)". When root is configured as the owner and group that has the access rights of the shared folder, it will be possible to access the shared folder from all clients on the business LAN.

Point

- Set root to the owner and the group when making first time of the shared folder or the authentication server is a unsetting. Refer to "[6.6.4.1 Changing the Shared Folder](#)" for the modification procedure when the access authority is given to a specific owner and the group after the authentication server is set.
- In order to perform detailed access control such as specifying Read-Only to individual users other than the owner, directly configure this in relation to the authentication server.

Host Access Configurations of Shared Folder

Configure host access, permitted and denials, to the shared folder. When a host to permit is not specified, access from all hosts will be permitted. Furthermore, it is possible to configure hosts to deny only when CIFS is specified for the protocol.

In addition, the following will be automatically configured when creating the shared folder.

- [Writing Authority of Shared Folder](#)
- [Shared Status of Shared Folder](#)

Writing Authority of Shared Folder

The state of whether writing to the shared folder is enabled or disabled will be displayed. The client can only write into a shared folder for which writing authority is enabled, or folders and files subordinate to such a shared folder.

When the shared folder is created, writing will be enabled by default.

Refer to "[6.6.4.1 Changing the Shared Folder](#)" for information on how to change write authority.

Shared Status of Shared Folder

The state of whether the sharing of the shared folder is active (Online) or inactive (Offline) will be displayed. For a folder where sharing has been made active, the client will be able to access files via the NAS interface.

When the shared folder is created, sharing will be in an active state by default.

Refer to "[6.6.4.4 Activating Sharing](#)" or "[6.6.4.5 Stopping Sharing](#)" for information on how to change the shared status.

Shared folders can be created up to 256 folders per device.



See

Refer to "Create Shared Folder" in the *ETERNUS SF Web Console Guide* for information on how to create using the Web Console.

6.6.3.2 Creating NAS Interface

Create a NAS interface in order to configure a public IP address and a port to access the shared folder.

The following can be configured with this function:

- [IP Address for Access](#)
- [Port for Access](#)
- [Connection Access Method](#)
- [Enable/Disable Routing Information Protocol \(RIP\)](#)

IP Address for Access

Configure IP address(es) for the NAS interface. It is possible to configure an IPv4 address, an IPv6 address, or both of these.

Port for Access

Configure the Allocation port and the Redundant port of the NAS interface. The shared folder will be accessed via the port configured as the Allocation port.

When the Allocation port is down, the shared folder can be accessed via the port configured as the Redundant port. It is also possible to use a single port operation format where a Redundant port is not configured.



Point

- For the Allocation port, it is only possible to specify a port that is not specified as an Allocation port of another NAS interface.
- Select the Redundant port from ports on a different CM than the CM with the Allocation port.
- When a Redundant port is not configured, it will not be possible to access the shared folder when the Allocation port goes down. For this reason, it is recommended that a Redundant port is configured.

Connection Access Method

Configure the Allocation port and Redundant port for the shared folder access connection method.

The method for configuration of the connection type is as follows.

Connection Settings	Configuration Method
Single connection	Specify only an Allocation port, and create a NAS interface.
Active-Standby connection	Specify an Allocation port and a Redundant port, and create a NAS interface.
Active-Active connection	There are the two following configuration methods. <ul style="list-style-type: none">- Method 1<ol style="list-style-type: none">1. Create a NAS interface of an Active-Standby connection.2. Again, create a NAS interface. During this, specify the "Redundant port of the NAS interface" created in step 1 as the port.- Method 2

Connection Settings	Configuration Method
	<ol style="list-style-type: none"> 1. Create a NAS interface of a Single connection. 2. Again, create a NAS interface. During this, specify the "port of the NAS interface" created in step 1 as the Redundant port.

Enable/Disable Routing Information Protocol (RIP)

Configure whether to enable / disable RIP configuration.

When RIP configuration is enabled, a routing table can be created dynamically based on the routing table broadcast from the router connected to the port, and the access route configured for the NAS interface can be automatically selected.

When RIP configuration is disabled, the dynamic creation of the routing table will not be performed.

Point

- When the RIP configuration is enabled, in order to dynamically create the NAS interface routing table, enable RIP configuration on the router connected to the NAS interface.
- When the RIP configuration is disabled, it is not possible for the NAS interface to select its own access route. Use the ETERNUS Web GUI or ETERNUS CLI to manually configure a routing table.

See

Refer to "Create NAS Interface" in the *ETERNUS SF Web Console Guide* for information on settings using the Web Console.

Information

With this product, it is not possible to configure a NAS interface using the VLAN Tagging function or the Link Aggregation function. When configuring access control to a shared folder using the VLAN Tagging function or the Link Aggregation function, configure it using the ETERNUS Web GUI or the ETERNUS CLI.

Note

To create a NAS interface, allocate a new NAS interface to NAS ports and then restart the service to access the shared folder by the CIFS protocol. Before the restart process is completed, the shared folder is not accessible from the existing NAS interface by the CIFS protocol. Wait a few moments to access it again.

6.6.3.3 Configuration of Authentication Server

Perform configuration of the authentication server to perform client access control to the NAS file system.

Depending on the type of protocol for access, specify the following for the authentication method:

- [Active Directory](#)
- [LDAP](#)

Active Directory

Specify this when accessing the NAS file system using the CIFS protocol.

LDAP

Specify this when accessing the NAS file system using the NFS protocol.

Note

- The authentication methods that can be operated differ with each protocol. For this reason, when the shared folder is accessed with an authentication method that is not supported, the authentication system will not operate.
- In the operation using Active Directory, it is required to synchronize the time between the ETERNUS Disk storage system and the Active Directory installed authentication server. It is recommended to automatically correct the time by Network Time Protocol (NTP).

It is possible to register a maximum of 3 authentication servers for each authentication method.

See

Refer to "Configure Authentication Server" in the *ETERNUS SF Web Console Guide* for information on settings using the Web Console.

Set the access authority to the owner and the group if necessary for the shared folder made by "6.6.3.1 Creating Shared Folder" after setting the authentication server.

6.6.4 Operation Method

The operation method for performing ETERNUS Disk storage system NAS operations with this product will be explained.

The access method to the shared folder is the following:

- [Access using the CIFS protocol](#)
- [Access using the NFS protocol](#)

Access using the CIFS protocol

The shared folder is accessible by the Windows file sharing or network drive mapping.

Enter the following to the address bar or to the network drive mapping window:

```
\\nasInterfaceIpAddress\sharedFolderName
```

When authenticating by Active Directory, the operation method varies depending on the presence of setup of an authentication server.

- If Active Directory is configured as an authentication server:
Enter the user name and password registered to Active Directory.
When connecting from the client participating in Active Directory, authentication is not needed.
- If an authentication server is not set up:
Enter the user name and password described in the ETERNUS Disk storage system manuals.

Information

Entering the IP address for NAS interface in the address bar can view sharable folders.

Access using the NFS protocol

The shared folder is accessible by performing the NFS mount from a UNIX server using the following procedure:

When authenticating through LDAP, there is no difference in operation method with the presence of setup of an authentication server. Make the UNIX server participate in the LDAP domain to perform the NFS mount.

1. Check the volume number of the NAS volume.

For the procedure to check the volume number, refer to "Display Shared Folder" in the *ETERNUS SF Web Console Guide*. "Volume No." displayed in the Basic tab for shared folder detail information is the volume number.

2. Log in to the UNIX server with administrator privileges.
3. Execute the mount command to mount the shared folder.

When executing the mount command, specify the following:

For Solaris

```
mount -F nfs nasInterfaceIpAddress:/mnt/nas/nvnasVolumeNumber/data/sharedFolderName  
mountDestinationDir
```

For Linux

```
mount -t nfs nasInterfaceIpAddress:/mnt/nas/nvnasVolumeNumber/data/sharedFolderName  
mountDestinationDir
```



Information

Executing the showmount command on the UNIX server can view NFS mountable shared folders.

```
showmount -e nasInterfaceIpAddress
```

After NFS mounted, logging in to the UNIX server as the user registered to LDAP can access the shared folder with the owner/group permissions set to the shared folder.

When not authenticating through LDAP, logging in to the UNIX server can access the shared folder.

The functions that can be executed during operation are as follows:

- [Changing the Shared Folder](#)
- [Changing the NAS Interface](#)
- [Changing the Authentication Server](#)
- [Activating Sharing](#)
- [Stopping Sharing](#)
- [Creating the NAS Backup Volume](#)
- [Performance Management of NAS Volume](#)
- [Capacity Management of Thin Provisioning Pool](#)
- [Expansion of NAS File System](#)
- [Disassembly of the NAS Environment](#)

6.6.4.1 Changing the Shared Folder

The values of the shared folder will be changed. The values that can be changed are as follows:

- Oplocks Configuration (when the protocol is CIFS or both CIFS and NFS)
- Owner/Group of Shared Folder
- Writing Authority
- Hosts Permitted Access
- Hosts Denied Access (when the protocol is CIFS or both CIFS and NFS)

Note

When the configuration of a shared folder is changed, sharing will temporarily be suspended and it will not possible to access the shared folder. When the changes to the shared folder are complete, sharing will be automatically resumed.

See

Refer to "Change Shared Folder" in the *ETERNUS SF Web Console Guide* for information on how to make changes to the shared folder using the Web Console.

6.6.4.2 Changing the NAS Interface

The values of the NAS interface will be changed.

The values that can be changed are as follows:

- IP Address
- RIP Setting
- Port
- Redundant port

Information

- Port configuration can only be changed when a new port is configured for a NAS interface for which a port has not yet been configured.
- Redundant port configuration can only be changed when a new Redundant port is configured for a NAS interface with Single configuration. If you want to modify Redundant ports, delete the set-up NAS interface and re-create a NAS interface.
- Only a port that has not been specified as an Allocation port of another NAS interface can be specified as the port.

See

Refer to "Change NAS Interface" in the *ETERNUS SF Web Console Guide* for information on how to change NAS interface using the Web Console.

6.6.4.3 Changing the Authentication Server

The values of the authentication server will be changed.

The steps for making changes and the values that can be changed are the same as those when configuring the authentication server. Refer to "[6.6.3.3 Configuration of Authentication Server](#)".

Point

When changing the domain administrator name of the authentication server, it is necessary to re-enter the password of the domain administrator. When changing items other than the domain administrator name, the password of the domain administrator is not required.

6.6.4.4 Activating Sharing

The sharing status of the shared folder will be activated.

When sharing is activated, it will be possible to access the shared folder via the NAS interface.



See

Refer to "Change NAS Interface" in the *ETERNUS SF Web Console Guide* for information on how to change NAS interface using the Web Console.

6.6.4.5 Stopping Sharing

The sharing status of the shared folder will be stopped.

When sharing is stopped, it will not be possible to access the shared folder.



See

Refer to "Start/Stop Sharing" in the *ETERNUS SF Web Console Guide* for information on the procedure using the Web Console.

6.6.4.6 Creating the NAS Backup Volume

NAS backup configuration will be setup to enable backing up of the NAS volume.

For the NAS backup configuration, apart from creating a NAS backup volume, a copy group and copy pair will be configured.

If NAS backup is not set up, this function is enabled to create a NAS volume backup system.

Configure the following for the NAS backup volume:

- [NAS Backup Volume](#)
- [Copy Group](#)
- [Copy Pair](#)

NAS Backup Volume

This is the volume for backup of the data of the NAS volume.

It is possible to create a new volume only when a NAS backup volume does not exist. When a NAS backup volume does exist, the existing backup volume will be specified.

The NAS backup volume is created with the following details.

Volume Name	<i>nas VolumeName\$bakN(*1)</i>
Capacity	Same as the source NAS volume
Volume Type	Same as the source NAS volume
Thin Provisioning Pool of the Creation Destination	User Selection

*1: "N" is a consecutive number from 0. The number of digits will vary.



Point

For increased reliability, it is recommended to create Thin Provisioning Pools of the creation destination for the NAS backup volume and the NAS volume in separate Thin Provisioning Pools.

Copy Group

This is a group for defining copy pairs of a NAS volume and a NAS backup volume.

If no copy group definition for backup exists, a copy group is automatically created with the following settings:

Copy Group Name	NAS_QuickOPC_N(*1)
-----------------	--------------------

Copy Group Type	QuickOPC
-----------------	----------

*1: "N" is a consecutive number from 0. The number of digits will vary.

Copy Pair

This is a copy pair of a source NAS volume and backup NAS volume.

It is created when creating a copy group.



See

Refer to "Create NAS Backup Volume" in the *ETERNUS SF Web Console Guide* for information on how to create NAS backup volume using the Web Console.



Point

When it is possible to execute this function from the Web Console, the NAS backup configuration is not setup or is incomplete. When constructing a backup system of the NAS volume, implement this task.

6.6.4.7 Performance Management of NAS Volume

Performance monitoring of ETERNUS Disk storage system NAS volumes is implemented at a level similar to that for block volumes.

Refer to "[Chapter 7 Performance Management](#)" for details.



See

Refer to "Operations for Performance Management of Storage Device" in the *ETERNUS SF Web Console Guide* for information on the procedure using the Web Console.



Information

The performance monitoring and threshold monitoring functions cannot be used for a NAS port.

6.6.4.8 Capacity Management of Thin Provisioning Pool

Capacity management for the Thin Provisioning Pool in which the NAS volume is created is implemented.

Refer to "[6.4 Thin Provisioning Management](#)" for details.



See

Refer to "Operations for Thin Provisioning" in the *ETERNUS SF Web Console Guide* for information on the procedure using the Web Console.

6.6.4.9 Expansion of NAS File System

Expansion of the NAS file system will be implemented.

- [Expansion of Thin Provisioning Pool](#)

This is implemented when there is a possibility that the used capacity of the Thin Provisioning Pool in which the NAS volume is created will exceed the total capacity.

Expansion of Thin Provisioning Pool

Expansion of the Thin Provisioning Pool in which the NAS volume is created is implemented with the following steps.

1. Confirm the capacity of the Thin Provisioning Pool.
Confirm the capacity of the Thin Provisioning Pool in which the NAS volume is created.
Refer to "[6.6.4.8 Capacity Management of Thin Provisioning Pool](#)".
Depending on the size of the available capacity of the Thin Provisioning Pool, perform the expansion of the capacity of the Thin Provisioning Pool with the following steps.
2. Expand the capacity of the Thin Provisioning Pool.
Perform the expansion of the capacity of the Thin Provisioning Pool from the Web Console.



Refer to the "Expand Capacity of/Format/Change Threshold Value of/Delete Thin Provisioning Pool" in the *ETERNUS SF Web Console Guide* to expand capacity.

6.6.4.10 Deleting of the NAS Environment

The steps for deleting the NAS environment will be explained.

The deletion is performed with the following steps.

Order	Item	Title of Sections Listed in the Web Console Guide
1	Deleting the Shared Folder	Delete Shared Folder
2	Removing the Authentication Server	Configure Authentication Server
3	Deleting the NAS Interface	Delete NAS Interface
4	Deleting the Copy Pair	Add/Display/Delete Copy Pair
5	Deleting the Copy Group	Create/Display/Delete Copy Group
6	Deleting the Volume for NAS	Delete Volume



When these steps are implemented, the NAS environment is deleted. All the data that had been stored on the NAS volume and the NAS backup volume will be deleted. Do not implement this step except when deleting the NAS environment.

Deleting the Shared Folder

The shared folder will be deleted.

When deleting the NAS environment, be sure to delete all shared folders. In order to delete a specific shared folder, specify a shared folder of choice and execute the deletion.



Refer to "Delete Shared Folder" in the *ETERNUS SF Web Console Guide* for information on how to delete.



When a shared folder is deleted, all of the folders and files created under the shared folder will be deleted.

Removing the Authentication Server

The authentication server is removed from the configuration.

Delete domain information and all authentication server information when you dismantle the NAS environment.



See

Refer to "Configure Authentication Server" in the *ETERNUS SF Web Console* for the procedure with the Web Console.

Deleting the NAS Interface

The NAS interface will be deleted.

When deleting the NAS environment, be sure to delete all NAS interfaces. In order to delete a specific NAS interface, specify the chosen NAS interface and execute the deletion.



See

Refer to "Delete NAS Interface" in the *ETERNUS SF Web Console Guide* for information on how to delete.



Point

When the following two conditions are met, the redundancy of ports is removed:

- All NAS interfaces are deleted from Allocation ports.
- A Redundant port is set to an Allocation port.

Deleting the Copy Pair

The copy pair for NAS defined with the NAS volume and the NAS backup volume will be deleted.



See

Refer to "Add/Display/Delete Copy Pair" in the *ETERNUS SF Web Console Guide* for information on how to delete.



Information

Even when all shared folders have been deleted, the copy pair automatically created for the NAS will not be deleted. When deleting the NAS backup configuration, delete the copy pair from the Web Console.

Deleting the Copy Group

The copy group for NAS will be deleted.



See

Refer to "Create/Display/Delete Copy Group" in the *ETERNUS SF Web Console Guide* for information on how to delete.



Information

Even when all shared folders have been deleted, the copy group automatically created for the NAS will not be deleted. When deleting the NAS backup configuration, delete the copy group from the Web Console.

Deleting the Volume for NAS

The volume for NAS will be deleted.



Refer to "Delete Volume" in the *ETERNUS SF Web Console Guide* for information on how to delete.



Even when all shared folders have been deleted, the volume for NAS will not be deleted. In order to delete the NAS volume, delete the NAS volume from the Web Console.



In the following cases, the volume for NAS cannot be deleted from the Web Console.

- When a shared folder is present on the NAS volume
- When the NAS backup volume is mounted
- When the volume is a NAS system volume

Delete the NAS system volume from the ETERNUS Disk storage system. Refer to the ETERNUS Disk storage system manuals for the deletion procedure.

Chapter 7 Performance Management

7.1 Overview

This software supports performance management functionality for fibre channel switch and ETERNUS Disk storage systems. This functionality enables users to get details about the operation and load statuses of devices.

Additionally, by knowing the number of active disks, it is possible to verify the Eco-mode status of the ETERNUS Disk storage system.



See

Refer to "[1.2.7 Support levels](#)" for details about supported devices.



Note

- Do not execute performance monitoring for a single device from more than one Management Server (administrative server) at the same time. The Softek Storage Cruiser administrative servers, the ETERNUS SF Storage Cruiser Management Server or the Systemwalker Resource Coordinator administrative servers
- The performance management functionality always starts up when the Management Server starts up. For devices in which performance management settings have been configured, performance information collection starts in the background. Accordingly, performance information is collected regardless of whether the Web Console is started or not. To stop performance information collection, execute performance management stop processing.

7.1.1 Performance Information Types

The following information can be managed: Performance monitoring can be set at different intervals, refer to "[7.2.3 Setting monitoring intervals](#)" for the settings available for each device.

On the following tables, "A" indicates "Available", "N/A" indicates "Not Available".

- Fibre Channel switch

	Performance Information (Unit)	Fibre Channel Switch
Port	Transfer rates of send/receive data (MB/S)	A
	Number of CRC errors	A

- ETERNUS Disk storage system

	Performance information (Unit)	ETERNUS DX400/DX400 S2 series, ETERNUS DX500 S3/DX600 S3, ETERNUS DX8000/DX8000 S2 series	ETERNUS DX60/DX60 S2, ETERNUS DX80/DX80 S2, ETERNUS DX90/DX90 S2, ETERNUS DX100 S3/DX200 S3
Logical Volume RAID Group	Read/Write count (IOPS)	A	A
	Read/Write data transfer rate (MB/S)	A	A
	Read/Write response time (msec)	A	A

	Performance information (Unit)	ETERNUS DX400/DX400 S2 series, ETERNUS DX500 S3/DX600 S3, ETERNUS DX8000/DX8000 S2 series	ETERNUS DX60/DX60 S2, ETERNUS DX80/DX80 S2, ETERNUS DX90/DX90 S2, ETERNUS DX100 S3/DX200 S3
	Read/Pre-fetch/Write cache hit rate (%)	A	A
	Read(Extreme Cache) cache hit rate (%)	A (ETERNUS DX500 S3/DX600 S3 only)	N/A
	Read(DRAM, Extreme Cache) cache hit rate (%)	A (ETERNUS DX500 S3/DX600 S3 only)	N/A
	Read QoS delay time (msec)	A (ETERNUS DX500 S3/DX600 S3 only)	A (ETERNUS DX100 S3/DX200 S3 only)
	Write QoS delay time (msec)	A (ETERNUS DX500 S3/DX600 S3 only)	A (ETERNUS DX100 S3/DX200 S3 only)
Disk drive	Disk busy rate (%)	A	A
CM	Load(CPU usage) rate (%)	A	A
	Copy remaining amount (GB)	A	A
CA	Read/Write count (IOPS)	A	N/A
	Read/Write data transfer rate (MB/S)	A	N/A
CM Port	Read/Write count (IOPS)	N/A	A
	Read/Write data transfer rate (MB/S)	N/A	A
Device	Number of active disks (Disk)	A	A (ETERNUS DX200F excluded)
	Power consumption (W)	A (ETERNUS DX400 S2 series, DX500 S3/DX600 S3 and DX8000 S2 series only)	A (ETERNUS DX200F excluded)
	Temperature (C)	A (ETERNUS DX400 S2 series, DX500 S3/DX600 S3 and DX8000 S2 series only)	A (ETERNUS DX200F excluded)

Note

- Do not simultaneously perform performance monitoring to a single device from multiple Management Server (administrative servers). The administrative server for Softek Storage Cruiser, the Management Server for ETERNUS SF Storage Cruiser, and the administrative server for Systemwalker Resource Coordinator are to be used for the performance monitoring.

- In order to prevent a discrepancy with the times shown on the performance graph due to a discrepancy in the internal clocks for the Management Server and the monitored device, it is recommended that you enable the NTP setting to the Management Server and the monitored device to synchronize the internal clocks.
- It is possible to reference performance information for the ETERNUS SF Storage Cruiser. However, there is some performance information which is not supported. Refer to the manual of Systemwalker Service Quality Coordinator for details.
- If the monitored device has been restarted while performance monitoring was in progress, you may be unable to acquire accurate performance data immediately after the restarting of the device. It is recommended that you first halt performance monitoring before performing any tasks which entail restarting the monitored device.
- Performance information about the ETERNUS Disk storage system main frame volume, MVV/SDV, and ODX Buffer Volume are not supported. The value for the performance information about the RAID Group containing SDV cannot be guaranteed. Performance information values for RAIDGroup, excluding Thin Provisioning and Flexible Tier, do not contain ODX Buffer Volume.
- Performance monitoring cannot be done for the ETERNUS Disk storage system which do not have LogicalVolume (LUN).
- The CA/CM Port performance information for the ETERNUS Disk storage system device displays the following information.

Device	Host Interface								
	FC			iSCSI			FCoE	SAS	NAS
	CA	RA	CA/RA	CA	RA	CA/RA			
ETERNUS DX400 series ETERNUS DX8000 series	A	A (*1)	N/A	A	A (*1)	N/A	N/A	N/A	N/A
ETERNUS DX90	A	A (*1)	N/A	N/A	N/A	N/A	N/A	N/A	N/A
ETERNUS DX60/DX60 S2 ETERNUS DX80	A	N/A	N/A	A	N/A	N/A	N/A	N/A	N/A
ETERNUS DX80 S2 ETERNUS DX100 S3	A	A (*1)	A (*2)	A	N/A	A (*2)	A	N/A	N/A
ETERNUS DX90 S2 ETERNUS DX200 S3 ETERNUS DX400 S2 series ETERNUS DX500 S3/DX600 S3 ETERNUS DX8000 S2 series	A	A (*1)	A (*2)	A	A (*1)	A (*2)	A	N/A	N/A

*1: Performance information during the execution of REC or ROPC is displayed as follows:

- It is displayed as Read performance information, if the port is set on the Initiator.
- It is displayed as Write performance information, if the port is set on the Target.

*2: Performance information during the execution of REC includes the following information.

- Read performance information includes the performance information during the execution of REC, if the port is set on the Initiator.
- Write performance information includes the performance information during the execution of REC, if the port is set on the Target.
- Performance information for VE ports used by 10 GbE(XGE) ports is not supported, and the values in the displayed performance information are not guaranteed. It is recommended that 0 be set for the transfer rate for VE ports used by 10 GbE(XGE) ports, and that performance and threshold values should not be monitored. Refer to "[A.9 Explanation of the Configuration Settings File](#)" for details on how to set this value.
- The CPU and ROE usage rates are displayed for the CM load (CPU usage) for ETERNUS DX400/DX400 S2 series and ETERNUS DX8000/DX8000 S2 series. For other ETERNUS Disk storage systems, the ROE usage rate is not displayed. Also, for ETERNUS Disk storage systems that do not have a ROE, the parity generation processing for RAID5 and RAID6 and encryption processing that would otherwise be performed by the ROE are performed by the CM and the CM-CPU.
- RDB performance information cannot be displayed in environments that use the REC Disk Buffered Consistency function.

7.1.2 Performance Graph Window Types

It is possible to display the following graphs.

One-hour Graph window

Based on the time selected as monitoring interval, a line graph for a one-hour period is displayed. For example, if the monitoring interval is 30 seconds, a line graph for a one-hour period with values obtained at an interval of 30 seconds is displayed.

One-day Graph window

Based on the mean values for 10-minute periods, a line graph for a one-day period is displayed.

One-week Graph window

Based on the mean values per hour, a line graph for a one-week period is displayed.



Information

- Following performance values are displayed as they are obtained from the device (not their mean values).
 - CM Copy remaining amount
 - Number of active disks
 - Power consumption
 - Temperature
 - If the summer time functionality of the operating system is enabled, a part of the graph that is supposed to show the data around the switch to summer time may not be displayed correctly.
 - Each performance graph may not be able to be displayed at every monitoring interval, per 10-minutes and per 60-minutes, depending on the LAN traffic condition or network environment (e.g. the Management Server and target device of the performance monitoring exist in the different subnets).
-

7.1.3 Threshold Monitoring Types

Threshold monitoring is supported for Fibre Channel switch and ETERNUS Disk storage systems.

The threshold monitoring functionality sends an alarm or report when Fibre Channel switch or ETERNUS Disk storage systems performance value reaches a certain level (threshold value) under certain conditions in daily transaction operations.

The advantage of using the threshold monitoring is that the symptom of Fibre Channel switch or ETERNUS Disk storage systems performance drop caused by changes in data processing rates and transaction processing rates can be automatically and reliably detected in daily transaction operations.

The effect that can be expected from the threshold monitoring functionality is that operations in the most suitable environment are enabled. This is accomplished by preventing the adverse effect of performance drops through early detection of bottleneck locations, identification of their causes, and improvement of device configuration.

The threshold monitoring functionality can manage the following information: You can set multiple threshold values.

- Fibre Channel switch
 - Port throughput (%)

A port throughput value (MB/s) is monitored as the percentage (%) of an allowable tolerance to a maximum transfer capability (MB/s).
- ETERNUS Disk storage system
 - Response time (msec) of LogicalVolume (OLU)
 - Average use (busy) rate (%) of RAIDGroup (RLU, LUN_R)
 - CM load (CPU usage) rate (%)

Note

- The threshold monitoring function is always started when the Management Server is started, and the functionality starts threshold monitoring and obtaining performance information at the same time for a device for which performance management is specified. Accordingly, performance information is obtained and thresholds are monitored regardless of whether the Web Console is started or not. To end threshold monitoring, stop threshold monitoring from this software.
- For the CM load (CPU usage) rate, the ROE usage rate is not monitored.

7.2 Flow of Performance Management

When a user gives an instruction for performance management of a target device using the Web Console, the performance management unit for this product saves the device performance data for each device, and stores them as performance data to the Management Server. This performance data is displayed on a graph.

7.2.1 Checking disk space on the Management Server

To conduct performance monitoring, sufficient disk space is required on the Management Server for performance data storage. Make sure that sufficient disk space is ensured referring to *ETERNUS SF Installation and Setup Guide*. This software is capable of deleting performance data overdue the specified holding period. The default is seven days and data exceeded this period are automatically deleted. This period can be modified. To change the number of days to store performance data refer to "[7.5 Definition File](#)".

7.2.2 Instruction for performance management

When performing performance management, configure and start the performance management by using the Web Console.

In ETERNUS Disk storage systems, enter the minimum and maximum values for the performance information securement target Logical Volume (LUN_V). Setting LogicalVolume can reduce the effect of obtaining performance information on disk areas where performance data is saved and reduce the load. Setting LogicalVolume prevents allocation of more space than necessary for Logical Volume. Consequently, the recommended entry for Logical Volume is the minimum value for obtaining performance data.

Information

Since performance information is obtained internally in units of 64 for Logical Volume, performance information in the neighboring area of the Logical Volume setting is also obtained.

For example, if a range of 70 to 80 is set for Logical Volume (LUN_V) on the screen, the information of Logical Volume between 64 and 127 is obtained internally.

After instructing it to start the performance management, the monitoring range which is displayed on the Web Console is not the value specified at the start time but the value converted to units of 64 for Logical Volume.

Point

The maximum transfer rate for the Fibre Channel switch VE port is set as 1Gbps by default.

If the FCIP trunking function or FCIP data compression function is enabled and a transfer rate of 1Gbps or more will occur for the VE port, then change the VE port transfer rate.

Refer to "[A.9 Explanation of the Configuration Settings File](#)" for details on how to set this value.

7.2.3 Setting monitoring intervals

Enter the interval at which performance information is secured in the ETERNUS Disk storage systems and Fibre Channel switch common settings. You can specify 5, 10, 30, 60, 300, or 600 seconds as the interval. However, intervals that can be specified vary depending on device models and the number of Logical Volumes indicating performance level being maintained.

Monitoring Condition		Specifiable Interval (seconds)					
Device Model Name	Number of Logical Volumes whose performance is maintained	5	10	30	60	300	600
ETERNUS DX60/DX60 S2/DX80/DX90	128 or less	A	A	A	A	A	N/A
	129 to 2,048	N/A	N/A	A	A	A	N/A
	2,049 or more	N/A	N/A	N/A	A	A	N/A
ETERNUS DX80 S2/DX90 S2	No limitation	N/A	N/A	A	A	A	N/A
ETERNUS DX100 S3/DX200 S3	1,472 or less	N/A	N/A	A	A	A	A
	1,473 to 3,200	N/A	N/A	N/A	A	A	A
	3,201 or more	N/A	N/A	N/A	N/A	A	A
ETERNUS DX400 series ETERNUS DX8000 series	256 or less	N/A	N/A	A	A	A	A
	257 to 1,024	N/A	N/A	N/A	A	A	A
	1,025 to 8,192	N/A	N/A	N/A	N/A	A	A
	8,193 or more	N/A	N/A	N/A	N/A	N/A	A
ETERNUS DX400 S2 series ETERNUS DX8100 S2	1,024 or less	N/A	N/A	A	A	A	A
	1,025 or more	N/A	N/A	N/A	A	A	A
ETERNUS DX500 S3/DX600 S3	1,024 or less	N/A	N/A	A	A	A	A
	1,025 to 2,752	N/A	N/A	N/A	A	A	A
	2,753 to 11,072	N/A	N/A	N/A	N/A	A	A
	11,073 or more	N/A	N/A	N/A	N/A	N/A	A
ETERNUS DX8700 S2	1,024 or less	N/A	N/A	N/A	A	A	A
	1,025 to 8,192	N/A	N/A	N/A	N/A	A	A
	8,193 to 16,384	N/A	N/A	N/A	N/A	N/A	A
ETERNUS SN200 series Brocade series	-	A	A	A	A	N/A	N/A

"A" indicates "Available", and "N/A" indicates "Not Available".

Point

In LAN traffic or cross-subnet (where there is a gateway between the performance monitoring target device and the Management Server) situations, it may not be possible to obtain the performance information inside the monitoring interval that was set. Please change the monitoring interval when you cannot acquire performance information on each monitoring interval.

Note

- The Fibre Channel switch and Fibre Channel switch blade as shown in the table below, set a monitoring interval according to the FC transfer rate. If this setting is incorrect, it might not be possible to obtain the correct performance value from the device.

Device Model Name	Monitoring Interval	Transfer Rate
ETERNUS SN200 series Fibre Channel switch	5 seconds	1-25Gbps
Brocade Fibre Channel switch (except for Brocade 6510, Brocade DCX8510-8/8510-4, and Brocade 6505)	10 seconds	1-12Gbps
	30 seconds	1-4Gbps
PRIMERGY Fibre Channel switch blade	60 seconds	1-2Gbps

- On the performance information for the number of active disks, power consumption and temperature, the performance monitoring interval sets 60 seconds if its interval is set to shorter than 60 seconds.

Since the performance management unit is started as a daemon of the Management Server, the unit continues obtaining performance information while the Management Server is active, without starting the Web Console.

The logical configuration of the storage device is recognized, and the obtaining of performance information starts. At the start of obtaining performance information of the selected storage system, an amount of time (tens of seconds to several minutes) is spent to obtain the logical configuration before any performance information is actually obtained.

Performance monitoring status, description and action are described as follows:

Performance Monitoring Status	Description	Action
Monitoring	Shows that performance monitoring works normally.	No action is required.
Recovering	Shows that performance monitoring is in recovery state.	Management Server cannot communicate to devices. Check the network and device conditions. If logged on to the ETERNUS Web GUI, log off from it.
Error	Shows that performance monitoring is in error state.	It is possible that writing to performance information file failed. Check the write access to file and the file system capacity and then perform the following steps. Refer to " 7.2.10 Performance data " for the location to store performance information file in: <ol style="list-style-type: none"> Record the performance monitoring settings contents <Recorded settings contents> <ul style="list-style-type: none"> - Interval before obtaining performance information (in seconds) - Performance monitoring targets (only for ETERNUS Disk storage system. Minimum LUN_V, Maximum LUN_V) Stop performance monitoring Refer to "7.2.8 Instruction for stopping performance management". Start performance monitoring based on the settings contents recorded in step 1 Refer to "7.2.2 Instruction for performance management" and "7.2.3 Setting monitoring intervals". <p>If despite of the above steps having been taken, any performance monitoring error is not resolved, internal error may be occurring. Contact Fujitsu Technical Support.</p>

7.2.4 Displaying performance information of the selected device

Confirm by displaying the graph using the Web Console.

In addition, the performance information can be output to the CSV format file by using the performance information operation command (storageadm perfdata).

7.2.5 Displaying Fibre Channel switch performance information

Select a port whose performance information you want to display in graph.

7.2.6 Displaying storage performance information

7.2.6.1 Displaying LogicalVolume and RAIDGroup performance information

Select the number of LogicalVolume or RAID Group whose performance information you want to display in graph.



Performance information about the ETERNUS Disk storage system main frame volume, MVV/SDV, and ODX Buffer Volume are not supported. The value for the performance information about the RAID Group containing SDV cannot be guaranteed. Performance information values for RAIDGroup, excluding Thin Provisioning and Flexible Tier, do not contain ODX Buffer Volume.

7.2.6.2 Displaying disk (physical drive) performance information

Select the number of the disk whose performance information you want to display in graph.

7.2.6.3 Displaying CM performance information

Select the CM or CM CPU whose performance information you want to display in graph.

7.2.6.4 Displaying CA and CMPort performance information

Select the CA or CM Port from a list of ports whose performance information you want to display in graph.

7.2.6.5 Displaying the number of active disks, power consumption, and temperature performance information

Select the performance information you want to display in graph.



When the specified ETERNUS Disk storage system has no Eco-mode function, the number of active disks, power consumption and temperature graph is not displayed. Refer to "[1.2.5 Energy-saving operation for storage device](#)" for the ETERNUS Disk storage systems that have the Eco-mode function.

Before the displaying the performance information for the number of active disks, power consumption and temperature, it is necessary to upgrade to the firmware that supports the Eco-mode operation and change the composition of the device.

7.2.7 Examples of use of performance management

If an I/O delay from the server node to a storage system occurs, the user can check for the cause in the storage system by using the methods described below. These are only examples, so all causes of I/O delays cannot be determined by use of these methods.

1. Identify the time when the I/O processing delay occurred and the access path where the delay occurred.
2. Use this software to check the AffinityGroup number and LogicalVolume number of the ETERNUS Disk storage system defined in the target access path.
3. Using performance management, display and check the target LogicalVolume performance values.
4. If a response of the LogicalVolume unit takes a long time, check RAID Group performance. If a response of RAID Group also takes a long time, find another Logical Volume belonging to RAID Group, and find the LUNs to which the Logical Volume is allocated. Check the I/O statuses of these LogicalVolumes, and check for a heavy load on RAID Group. If there is a heavy load, move the appropriate LogicalVolume to another RAID Group, or take other appropriate action.

7.2.8 Instruction for stopping performance management

Stop the performance management processing on the Web Console.

Refer to the following in the *ETERNUS SF Web Console Guide* for information on how to stop the processing:

- For storage devices
"Start/Change Settings of/Stop Performance Monitoring" in "Operations for Performance Management of Storage Device"
- For FC switches
"Start/Change Settings of/Stop Performance Monitoring" in "Operations for Performance Management of Network Device"

7.2.9 Updating configuration information

Device configuration information is independently maintained in the performance management functionality.

To change the device configuration, update the device configuration information that is maintained by the performance management functionality according to the procedure shown below. Also perform the update if the configuration for a device used to execute performance monitoring and threshold monitoring has been changed.

If the configuration for a device used to execute performance monitoring and threshold monitoring has been changed, the configuration information before the update is used for performance monitoring and threshold monitoring. Performance information and threshold monitoring, shown in the procedure below, cannot be guaranteed prior to the configuration information update.

<Configuration information update procedure>

1. Record the performance monitoring settings contents (if performance monitoring is used)

<Recorded settings contents>

- Range of Monitoring Volume No
- Monitoring Interval Time
- Minimum Monitoring Volume No (only for ETERNUS Disk storage system)
- Maximum Monitoring Volume No (only for ETERNUS Disk storage system)

2. Stop performance monitoring (if performance monitoring is used)

Refer to "[7.2.8 Instruction for stopping performance management](#)".

3. Change the configuration of the supported device.

4. Start performance monitoring based on the settings contents recorded in step 1. (if performance monitoring is used).

<Setting contents>

- Range of Monitoring Volume No (when specifying Performance monitoring targets, select "Partial")
- Minimum Monitoring Volume No (only for ETERNUS Disk storage system)
- Maximum Monitoring Volume No (only for ETERNUS Disk storage system)
- Monitoring Interval Time
- Create Device Configuration File (Select "Yes")

Refer to "[7.2.2 Instruction for performance management](#)" and "[7.2.3 Setting monitoring intervals](#)".

Note

If the scope of monitoring volumes has been changed, set the scope of monitoring volumes according to the change.

7.2.10 Performance data

Performance data is saved in CSV files in the following directory of the Management Server:

Platform for Manager	Location
Windows	\$TMP_DIR\Manager\var\opt\FJSVssmgr\current\perf (\$TMP_DIR means "Work Directory" specified at the Manager installation.)
Solaris OS, Linux	/var/opt/FJSVssmgr/current/perf

You can save these files by saving the entire directory as necessary, and you can display old information as necessary by recovering it in the same format.

However, the automatic deletion functionality operates in the performance data. When restoring, execute it after confirming days of the data retention duration. Refer to "[A.4 perf.conf Parameter](#)" for the data retention duration.

Example

Case of Solaris OS:

- Backup

```
# cd /var/opt/FJSVssmgr/current/perf/
# tar -hcf - csv |compress -c > csv.backup.tar.Z
```

- Restore

```
# cd /var/opt/FJSVssmgr/current/perf/
# uncompress -c /var/opt/FJSVssmgr/current/perf /csv.backup.tar.Z | tar -xvf -
```

7.3 Flow of Threshold Monitoring

When a user uses the Web Console to issue an instruction for threshold monitoring of the devices subject to performance management, this software then sequentially analyzes the performance data.

If a problem is detected from the performance information, it is displayed as an alarm in the Threshold Monitoring Alarms.

Information

When a problem is displayed as an alarm in the Threshold Monitoring Alarms, the event level is shown as [Warning].

7.3.1 Checking disk space on the Management Server

To monitor thresholds, disk capacity is required for the Management Server. About 4 MB is required. Make sure that the server has sufficient disk space.

7.3.2 Instruction for threshold management

Enable the threshold monitoring on the target device. Then you can set the threshold monitoring condition. To do so, however, performance information of the device must have already been obtained by performance management.

7.3.3 Setting the threshold monitoring hours

Setting the threshold monitoring hours enables to set a time period for threshold monitoring. If no time period is set, thresholds are monitored and alarms are reported for all time periods.

7.3.4 Setting the threshold monitoring information

Define threshold setting information of the target device, and issue an instruction to start monitoring. You can set multiple thresholds setting information on each device. Incidentally, since the threshold monitoring unit is started as a daemon of the Management Server along with the performance management unit, the threshold monitoring unit continues threshold monitoring while the Management Server is active, regardless of the access from the Web Console.

Note

For the CM load (CPU usage) rate, the ROE usage rate is not monitored.

7.3.5 Instruction for stopping threshold monitoring

Stop threshold monitoring for the target device. The Management Server continues to secure performance data from the device, but monitoring of the threshold is halted.

7.4 Evaluation Criteria for Thresholds in Threshold Monitoring

Storage thresholds

Standard storage thresholds are listed below.

	Online Response-Oriented System	Batch Throughput-Oriented System
LogicalVolume Response	30 ms or less	-
RAIDGroup Busy Rate	60% or less	80% or less

	Online Response-Oriented System	Batch Throughput-Oriented System
CM Busy Rate	80% or less	90% or less

For a response-oriented system such as for online applications, implementing LogicalVolume responses within 30 ms is a standard for stress-free storage operation. To implement responses within 30 ms, suppress the RAIDGroup busy rate to 60% or less and the CM busy rate to 80% or less.

In a throughput-oriented system such as for batch applications, LogicalVolume responses are extended to a few milliseconds because sequential access increases the cache hit ratios. However, the cache hit ratios are greatly affected by application access and the values change a great deal. As a result, responses may vary from a few milliseconds to 50 ms or more. Thus, for batch applications, there is no standard threshold for LogicalVolume responses.

To improve throughputs for batch applications, users must optimize the use of storage resources. Note, however, that performance may deteriorate rapidly if the above threshold is exceeded. For this reason, make it a standard to suppress the RAIDGroup busy rate to 80% or less and the CM busy rate to 90% or less.

During hours in which advanced copy is processing, advanced copy processing itself increases the CM busy rate. For this case, set thresholds in consideration of execution of advanced copy.

Thresholds of switch ports

The threshold and lower limit value vary depending on the type of applicable switch (1 Gbps, 2 Gbps etc). When the switch type is 1 Gbps, the maximum value (100% use rate) is 100 MBps. When the switch type is 2 Gbps, the maximum value is 200 MBps. For the threshold, specify the allowable utilization (%) corresponding to the maximum value.

For instance, when 90% is specified for the threshold of a 2 Gbps type switch, the threshold of the throughput is:
 $200 \text{ MBps} \times 90\% = 180 \text{ MBps}$ (total of reception and transmission)

An alarm is given when the throughput reaches 180 MBps.

Switch port threshold monitoring is effective when there is a difference in the numbers of paths between the server and storage.

Figure A Application + backup system

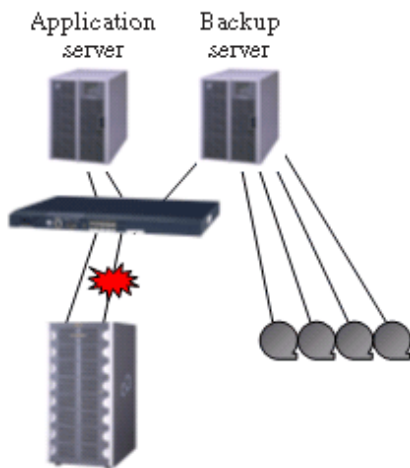
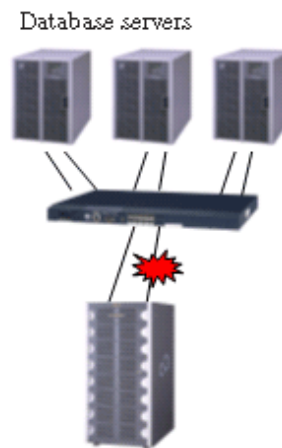


Figure B Cluster system (example: Oracle RAC)



7.5 Definition File

The following items for performance management can be set up in perf.conf file.

- The number of days to retain performance data
- The number of generations of log files (perflog.*)
- Whether to use the performance management for the number of active disks, power consumption and temperature
- Whether to use the performance management for iSCSI port



See

Refer to "A.4 perf.conf Parameter" for the settings.

7.6 Examples of Threshold Monitoring

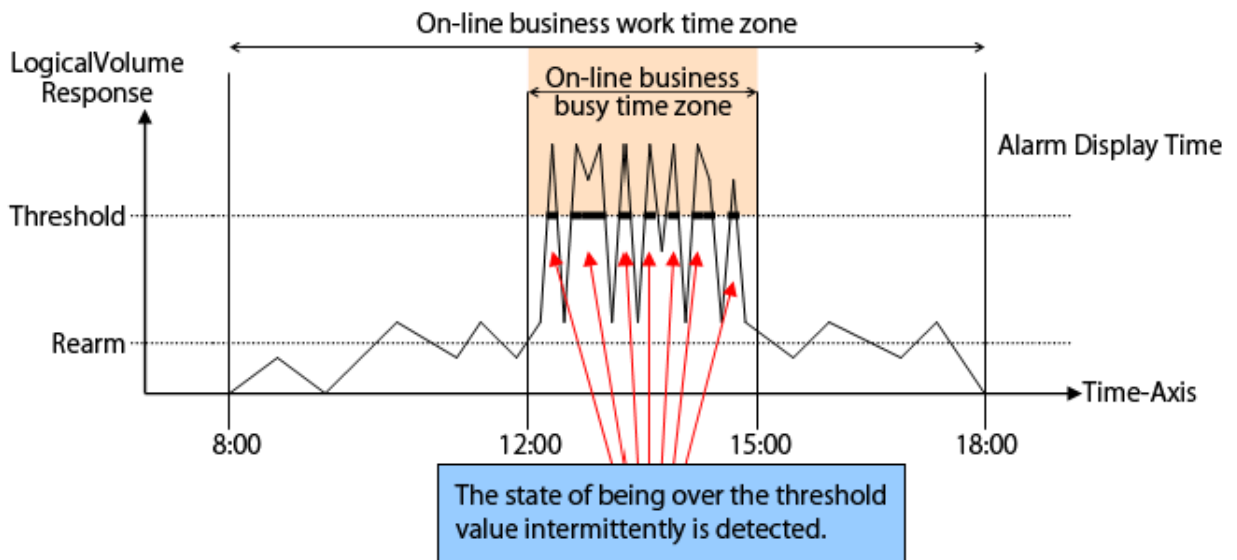
This section provides an overview of threshold monitoring in the form of key examples to enable users to determine what situations require thresholds and the types of thresholds that should be set for them.

Case 1: Online application system of company A

Material - System operation standard and performance requirements (excerpt)

1. Online application service hours: 8:00 to 18:00 everyday.
2. Online application busy hours: 12:00 to 15:00 everyday.
3. This system requires that operator terminal operation be stress-free even with workload during the busy hours. Therefore, the target performance of I/O response shall be "30 msec or less," which is a general standard. The target I/O response performance in hours other than the busy hours shall be "10 msec or less," one third of 30 msec, according to the workload proportion (the workload in the busy hours is about three times higher than that in other hours).
4. During the busy hours, processing for data reference, updating, and addition may occur concurrently and continue for up to 60 minutes. If a state in which an I/O response taking 30 msec or more occurs for a period equivalent to 10% (6 minutes) of the said continuous execution, operation at the operator terminal may undergo stress. Therefore, make the settings so that an alarm log will be displayed when such state occurs.
5. If I/O responses during the busy hours come down to 10 msec or less, the same as the performance target in other hours, the I/O response delays that occurred previously shall be deemed as instantaneous symptoms. Therefore, an alarm log need not be displayed when this state occurs.
6. The alarm log need not be displayed every time but can be displayed only once a day.

Figure 7.1 Illustration of operational status of company A's online application system (transition of LogicalVolume responses)



An example of threshold monitoring setting for company A's online application system

Table 7.1 "Time Setting" threshold monitoring time

Number Corresponding to Material	Setting Item	Setting
1	Starting time	8:00
1	Shutdown time	18:00

Table 7.2 "Time Setting" alarm display time

Number Corresponding to Material	Setting Item	Setting
1	Starting time	12:00
1	Shutdown time	15:00
5	Frequency	Day by Day

Table 7.3 "Volume Configuration" threshold monitoring information

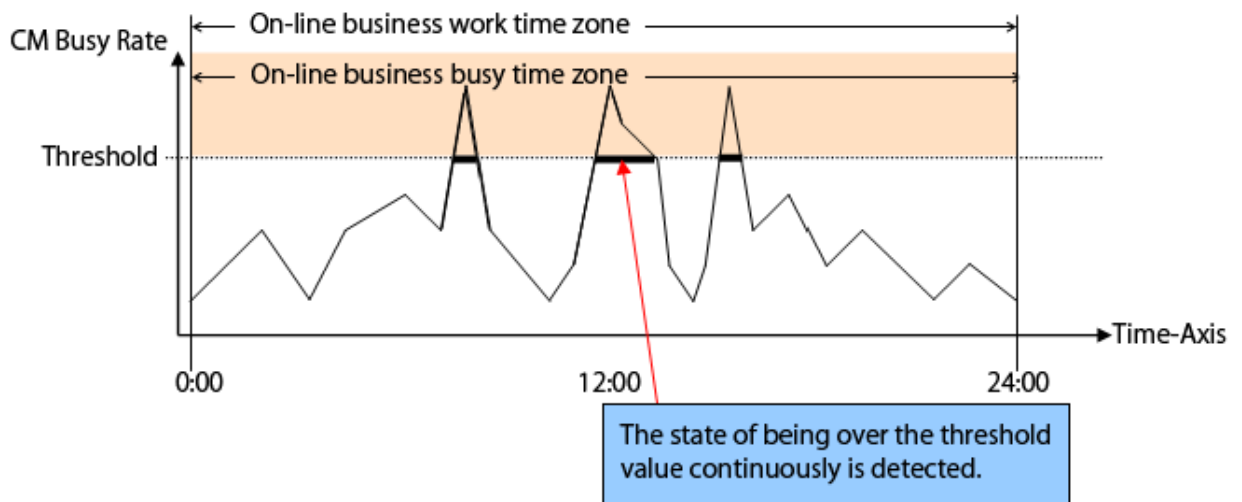
Number Corresponding to Material	Setting Item	Setting
2	Threshold	30msec
4	Lower limit	10msec
5	Alarm Tolerance Level	Total Time
5	Alarm Tolerance Time	360sec
5	Threshold monitoring Interval	60min

Case 2: Online shopping system of company B

Material - System operation standard and performance requirements (excerpt)

<ol style="list-style-type: none"> 1. Online application service hours: 24 hours a day for 365 days a year. 2. Online application busy hours: Cannot be specified. 3. This system features that the number of accesses gradually increases as the number of member customers increases after start of the production run. It is assumed that the load on storage will also increase gradually. Measures need to be taken when the busy rate of storage resources (CM and disk) comes over 60% to 80%. 4. This system executes credit card transactions every 5 minutes. Therefore, for five minutes immediately before each transaction, product retrieval and order processing must be executed without stress. If the storage resource is kept in busy state (a state in which the busy rate exceeds 60% to 80%) for five minutes, transactions may be affected. Therefore, make settings so that an alarm log will be displayed when such state occurs. 5. Alarm log shall be displayed every time.

Figure 7.2 Illustration of operational status of company B's online shopping system (transition of CM busy rate)



An example of threshold monitoring setting for the company B's online shopping system

Table 7.4 "Time Setting" threshold monitoring time

Number Corresponding to Material	Setting Item	Setting
1	Starting time	0:00
1	Shutdown time	24:00

Table 7.5 "Time Setting" alarm display time

Number Corresponding to Material	Setting Item	Setting
1	Starting time	0:00
1	Shutdown time	24:00
4	Frequency	All

Table 7.6 "CM Configuration" threshold monitoring information

Number Corresponding to Material	Setting Item	Setting
2	Threshold	60%
3	Alarm Tolerance Level	Continuous Time
3	Alarm Tolerance Time	300sec

Table 7.7 "RAID Group Configuration" threshold monitoring information

Number Corresponding to Material	Setting Item	Setting
2	Threshold	80%
3	Alarm Tolerance Level	Continuous Time
3	Alarm Tolerance Time	300sec

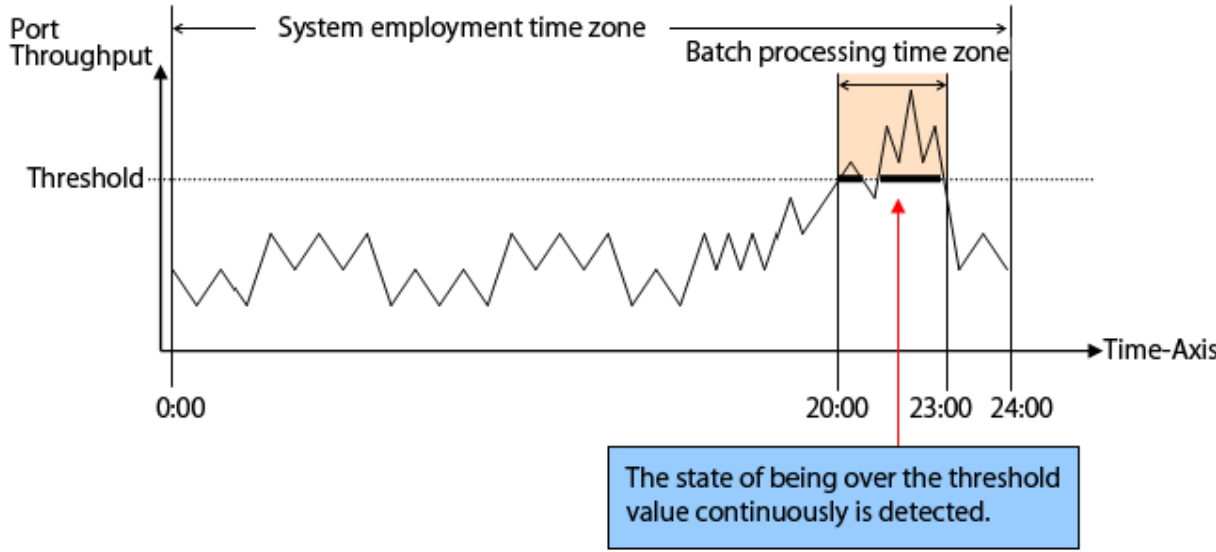
Case 3: Batch processing with multiple database servers (clustered system) of company C

Material - System operation standard and performance requirements

1. System service hours: 24 hours a day, 365 days a year.
2. Batch processing hours: 20:00 to 23:00 every night.

3. This clustered system is an Oracle RAC system consisting of three nodes. There is no problem with the batch processing performance because the amount of processed data is currently small. As the amount of data increases in the future, however, we have concerns over bottlenecks in the performance of FC path transfer between the FC switch and storage. If an FC path bottleneck occurs, it must be eliminated quickly.
4. Assume the state in which the port throughput reaches about 80% of the maximum transfer capability as an FC path bottleneck, and make settings so that an alarm log is displayed when such state continues for 30 minutes or more.
5. Alarm log need not be displayed every time but can be displayed only once even in the batch processing hours.

Figure 7.3 Illustration of batch processing with multiple database servers (clustered system) at company C (transition of port throughputs)



An example of threshold monitoring setting for business system backup operation at company C

Table 7.8 "Time Setting" threshold monitoring time

Number Corresponding to Material	Setting Item	Setting
1	Starting time	0:00
1	Shutdown time	24:00

Table 7.9 "Time Setting" alarm display time

Number Corresponding to Material	Setting Item	Setting
1	Starting time	20:00
1	Shutdown time	23:00
4	Frequency	All

Table 7.10 "Port Configuration" threshold monitoring information

Number Corresponding to Material	Setting Item	Setting
2	Threshold	80%
3	Alarm Tolerance Level	Continuous Time
3	Alarm Tolerance Time	1800sec

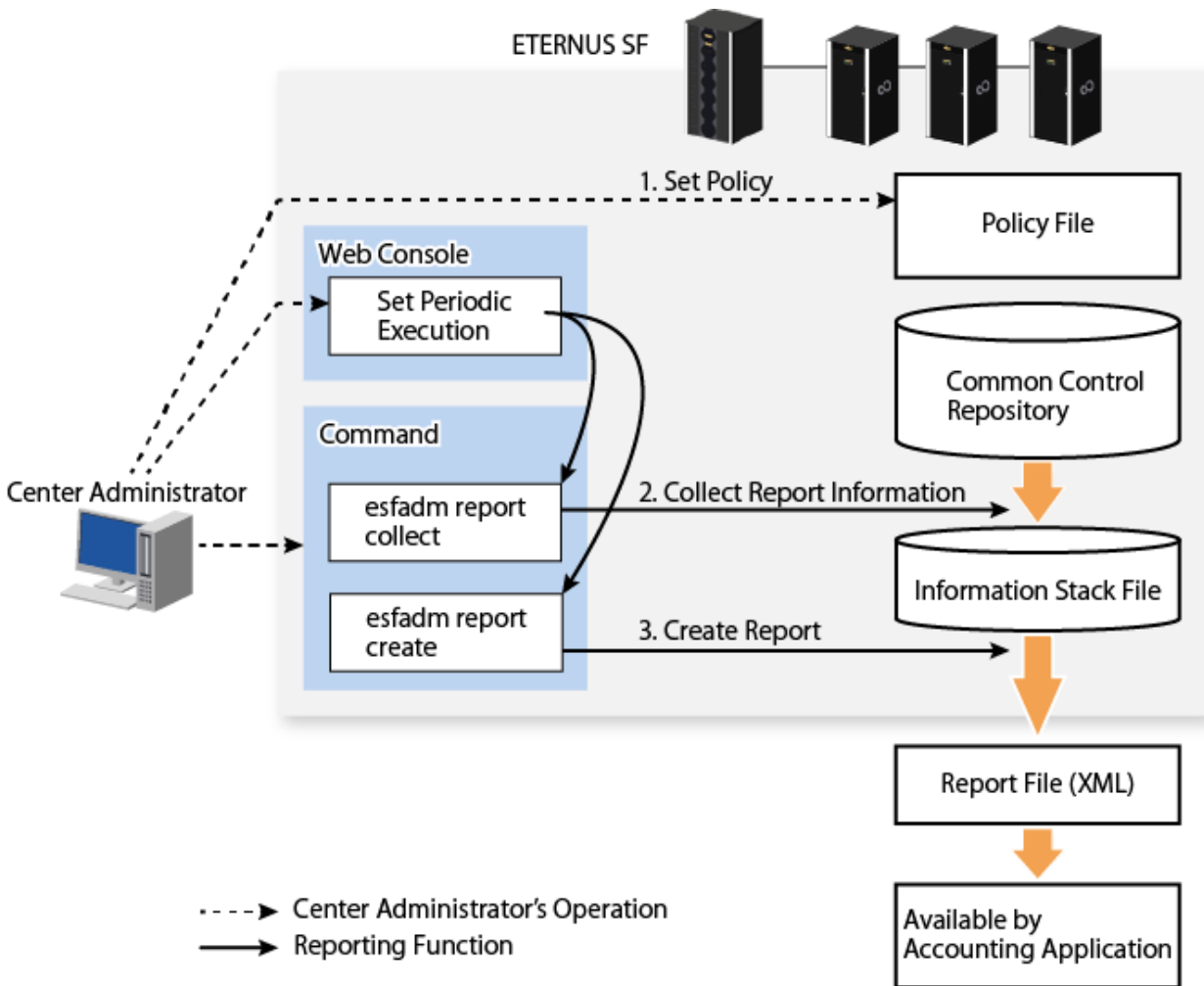
Chapter 8 Reporting Function

This chapter describes the Reporting function.

8.1 Overview

The Reporting function creates a report containing information required for charging.

The overview of the Reporting function is as follows:



Item	Description
Common Control Repository	Database that stores device configuration information managed by ETERNUS SF system
Report Information	Required information for charging (configuration information related to volumes)
Information Stack File	File that accumulates report information
Policy File	Configuration file for activities of the Reporting function
Report File	File that has output report information
Accounting Application	Application to make an invoice from a report file (made by the center administrator)

1. Set Policy

Set up a policy file for activities of the Reporting function.

2. [Collect Report Information](#)

Use the report information collection command to store report information in the information stack file from the common control repository.

3. [Create Report](#)

Use the report creation command to tally up report information in the information stack file based on the policy file and create a report file.

8.1.1 Set Policy

Overview

Set up requirements for the Reporting function in the file. They are handled as one policy in the system.

Policy file

This is loaded when the report creation command is run. The setting item is as follows:

- Data retention period of report information



See

Refer to "[8.3.2.2 Setup Policy](#)" for policy setup.

Refer to "[A.11 policy.conf Parameter](#)" for parameters about policy setup.

8.1.2 Collect Report Information

Overview

Running the [esfadm report collect command](#) to collect report information accumulates in the information stack file the report information stored in the common control repository.



See

Refer to "[Setup from Web Console](#)" in "[8.3.2.3 Setup Periodic Command Execution](#)" for information on how to activate the Reporting function.

Information to be collected

Collect configuration information for volumes connected to servers.

Target for which to collect information

The target for which to collect information is a volume that meets all of the following conditions:

- Volume is on a supported storage device registered to ETERNUS SF system.
(Refer to "[8.2 Supported Device](#)" for details.)
- Volume connected to a server registered to ETERNUS SF system.
("Connected to a server" indicates that access path is set up and server HBA is registered to ETERNUS SF system. Hereafter, this status is described as "connected to server".)
- Volume is on a storage system for which the Reporting function is set to "Activate" from the Web Console.



Note

For a volume connected to sever, note the following points:

- Whether the volume is targeted for reporting is determined by access path definition. For this reason, server usage and connection/disconnection between server and storage are not considered.
- Virtual server guest is not supported.

8.1.3 Create Report

Overview

Running the [esfadm report create command](#) to create a report obtains the report information within the period specified by the command, from the information stack file and creates a report file.

The report file can be viewed in the Web browser. If it is viewed in the Web browser, diverse information in the report can be viewed in colored tabular form.



See

.....
Refer to "[Setup from Web Console](#)" in "[8.3.2.3 Setup Periodic Command Execution](#)" for information on how to activate the Reporting function.
.....

If the [esfadm report create command](#) is periodically run, the created report files are stored at the location shown below. The storage location cannot be changed:

- Storage directory

Windows environment: `$INS_DIR\Common\var\report\auto`

(\$INS_DIR is an install directory.)

Solaris/Linux environment: `/var/opt/FJSVesfcm/report/auto`

- File name

`esfreport_auto_month_YYYYMMDDhhmmss.xml`

(*YYYYMMDDhhmmss* is command executed date and time and local time of ETERNUS SF system.)

Up to 12 report files created by running the [esfadm report create command](#) are save. When 12 files already exist, the oldest file is automatically deleted when the [esfadm report create command](#) is run.



Note

.....
If you want to save a report file, back it up before the old files are automatically deleted.
.....

Report file information

Created report files can be viewed by users with administrator privileges on the server operating system.

The output information and the HTML example of an XML file in the Web browser are as follows:

Server: name=194_30 os=Windows2008 IP-Address=

DiskArray :			
name	SerialNo	BusID	ec
IB4601309022	4691908022		1.3.6.1.4.1.201.1.21.1.150

Volume :									
name	number	Allocation(start)	Allocation(end)	type	capacity	encryption	multiPath	connectServerNumber	concatenationNumber
SDV_Volume	2896	2013-09-13T10:53:00+0900	2013-09-13T12:03:00+0900	SDV	1024	No	1	1	-

RAIDGroup :								
name	number	type	Disk					
			number	enclosureNumber	slotNumber	diskType	speed	
RAID_GP_0	7	Striping (RAID0)	12	0x00	12	SAS	10000	
			13	0x00	13	SAS	10000	

Volume :									
name	number	Allocation(start)	Allocation(end)	type	capacity	encryption	multiPath	connectServerNumber	concatenationNumber
TPP_Volume	1	2013-09-13T12:02:35+0900	2013-09-13T12:03:00+0900	TPV	5120	No	1	1	-

ThinProvisioningPool :	
name	number
TPP_1	3

RAIDGroup :								
name	number	type	Disk					
			number	enclosureNumber	slotNumber	diskType	speed	
RAID_GP_1	0	Mirroring (RAID1)	1	0x00	1	SAS	10000	
			257	0x01	1	SAS	10000	

Volume :									
name	number	Allocation(start)	Allocation(end)	type	capacity	encryption	multiPath	connectServerNumber	concatenationNumber
FTV_Volume	150	2013-09-13T10:53:00+0900	2013-09-13T11:42:00+0900	FTV	204800	No	1	1	-

TierPool :	
name	number
TIER_1	0

SubPool :		
name	number	level
FTSP_NAME#0	0	Low

RAIDGroup :								
name	number	type	Disk					
			number	enclosureNumber	slotNumber	diskType	speed	
FTSP_NAME#0_0	2	Mirroring (RAID1)	23	0x00	23	SAS	7200	
			279	0x01	23	SAS	7200	

SubPool :		
name	number	level
FTSP_NAME#1	1	Middle

RAIDGroup :								
name	number	type	Disk					
			number	enclosureNumber	slotNumber	diskType	speed	
FTSP_NAME#1_0	3	Mirroring (RAID1)	0	0x00	0	SAS	10000	
			256	0x01	0	SAS	10000	

SubPool :		
name	number	level
FTSP_NAME#2	2	High

RAIDGroup :								
name	number	type	Disk					
			number	enclosureNumber	slotNumber	diskType	speed	
FTSP_NAME#2_0	4	Mirroring (RAID1)	12	0x00	12	SSD	-	
			268	0x01	12	SSD	-	

The character encoding of XML files is output in UTF-8 format.
(On Windows, the destination directory privileges are inherited.)

Target

The report creation command creates a report file from the report information in the information stack file. For volumes that meet all of the following conditions, a report is created:

- Data accumulated in the information stack file
- Volume exited within the period specified by the report creation command

The number of volumes connected to the servers registered to ETERNUS SF system is output into the report information. The unit price charged per target is determined by the center administrator.

8.2 Supported Device

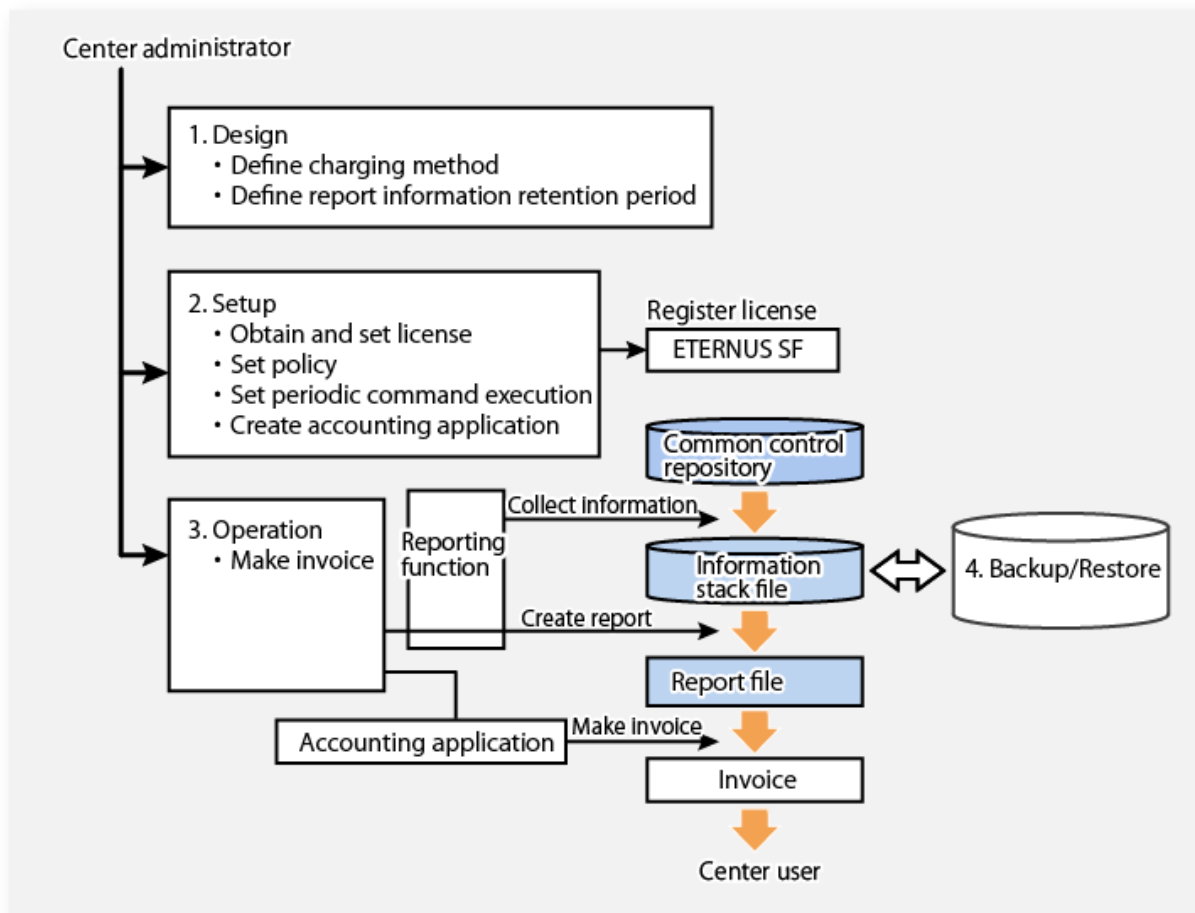
The devices for which the Reporting function is supported are as follows:

Device	Firmware Version
ETERNUS DX80 S2/DX90 S2 ETERNUS DX400 S2 series ETERNUS DX8000 S2 series	V10L40 or later
ETERNUS DX100 S3/DX200 S3 ETERNUS DX500 S3/DX600 S3	V10L10 or later

8.3 Operation

Using the Reporting function center users can be charged according to his (her) usage. To use the Reporting function, preparation is required in accordance with the operational environment. This section describes specific uses of the Reporting function including design, setup, operation and maintenance to charge fees.

The flow for creating an invoice is as follows:



1. Design

Define charging method and report information retention period.

2. Setup

The content of setup is as follows:

- Register the ETERNUS SF Storage Cruiser Standard Edition license.
- Set up a policy file based on the report information retention period.
- Activate periodic command execution in the Web Console so that report information can be collected and a report can be created, periodically.
Refer to "Setup from Web Console" in "8.3.2.3 Setup Periodic Command Execution" for information on how to activate the Reporting function.
- Create an accounting application.

3. Operation

Make an invoice using an accounting application based on a monthly created report.

4. Backup/Restore

Back up the information stack file periodically as required.

8.3.1 Design

8.3.1.1 Define Charging Method

For assistance in defining a charging method, the following example cases are provided. Based on the following requirements, do various settings of the Reporting function and create an accounting application:

- Range of charged servers
 - Charge a fee per server and send an invoice.
 - Charge a fee per group of multiple servers and send an invoice.
- Unit of charged time
 - Charge a fee per hour.
 - Charge a fee on a daily basis.
- How to calculate fees
 - Set a unit price per volume capacity to calculate fees based on allocation and usage period.
 - Set extra/reduced fees based on volume additional information.
- When and for which period to make an invoice
 - Charge usage fee for the previous week at 3:00 AM every Monday.
 - Charge usage fee for the previous month on the 10th of each month.
- How to deliver the invoice to the center user
 - Send usage fee to the user by e-mail.
 - Print out the invoice to send to the user by post.
- What to do if collecting charging information or making an invoice fails
 - Sound an alarm using the buzzer.
 - Send a notification E-mail to the center administrator.

8.3.1.2 Concept of Volume Allocation Period

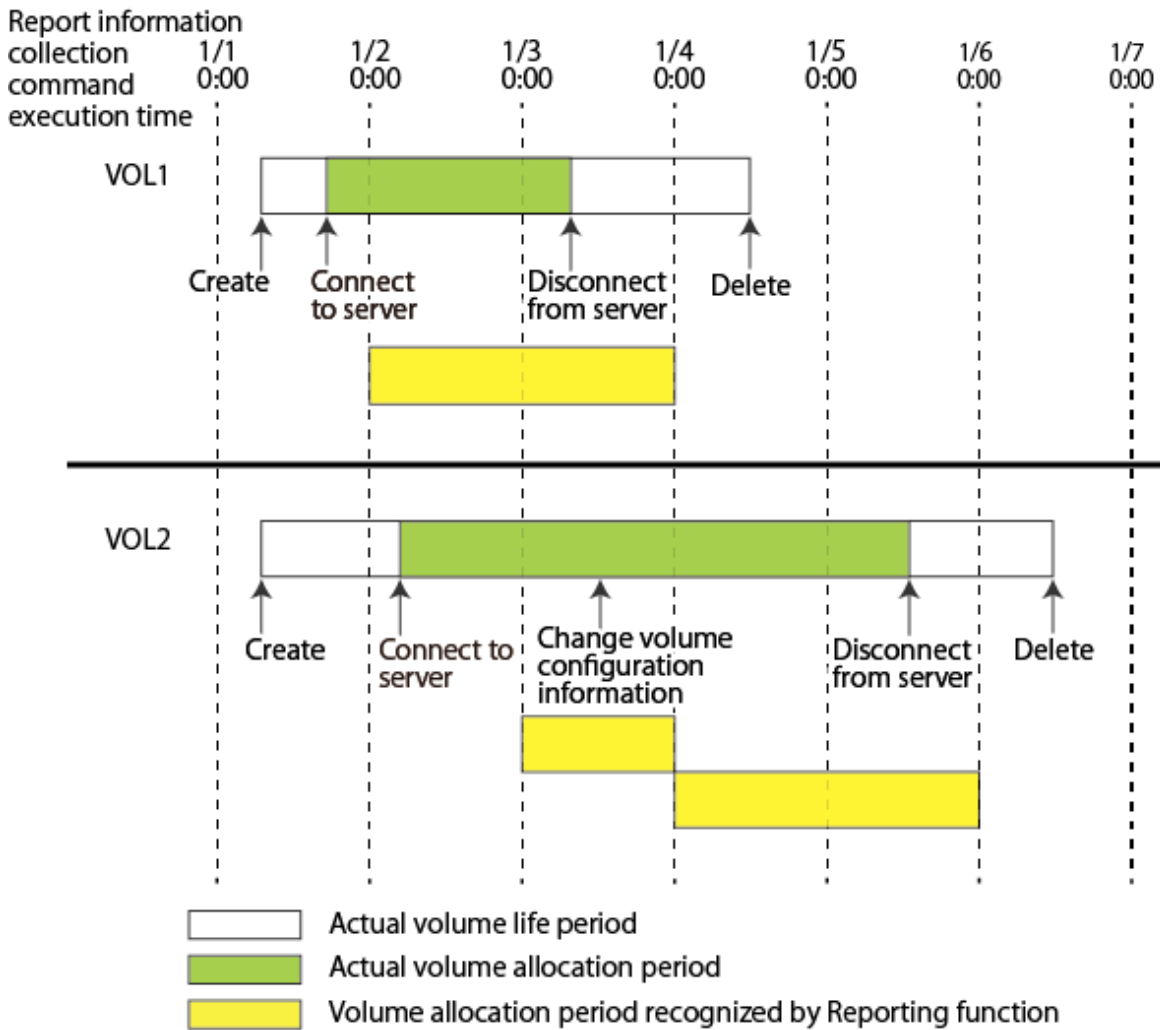
Concept of volume allocation period

Since the Reporting function calculates a volume allocation period from periodically collected information, the actual volume allocation period allocated by the center user is different from that recognized by the Reporting function. Basically, an allocation period for one volume is a period from when volume is connected to server to when volume is disconnected from server. However, if the configuration information for a volume connected to server has been changed, the volume is handled as a new volume. In this case, two volumes are output ("Volume configuration information is changed" indicates that any element other than the Header information written in "[Table 8.2 Attributes Maintained by Elements](#)" has been changed). The output on a per volume configuration basis makes it possible to charge fees in accordance with the volume configuration.

The start/end date and time of using a volume allocation period recognized by the Reporting function is defined as follows:

- Start date and time of use
Date and time when the report information collection command was run after server connection or configuration information for volume connected to server has been changed.
- End date and time of use
Date and time when the report information collection command was run after server disconnection or volume configuration information has been changed.

The following is an example of running the report information collection command per day:



The volume allocation period recognized by the Reporting function is as follows:

- VOL1
0:00 of 1/2 to 0:00 of 1/4 (2 days in all)
- VOL2
0:00 of 1/3 to 0:00 of 1/4, and 0:00 of 1/4 to 0:00 of 1/6 (3 days in all)

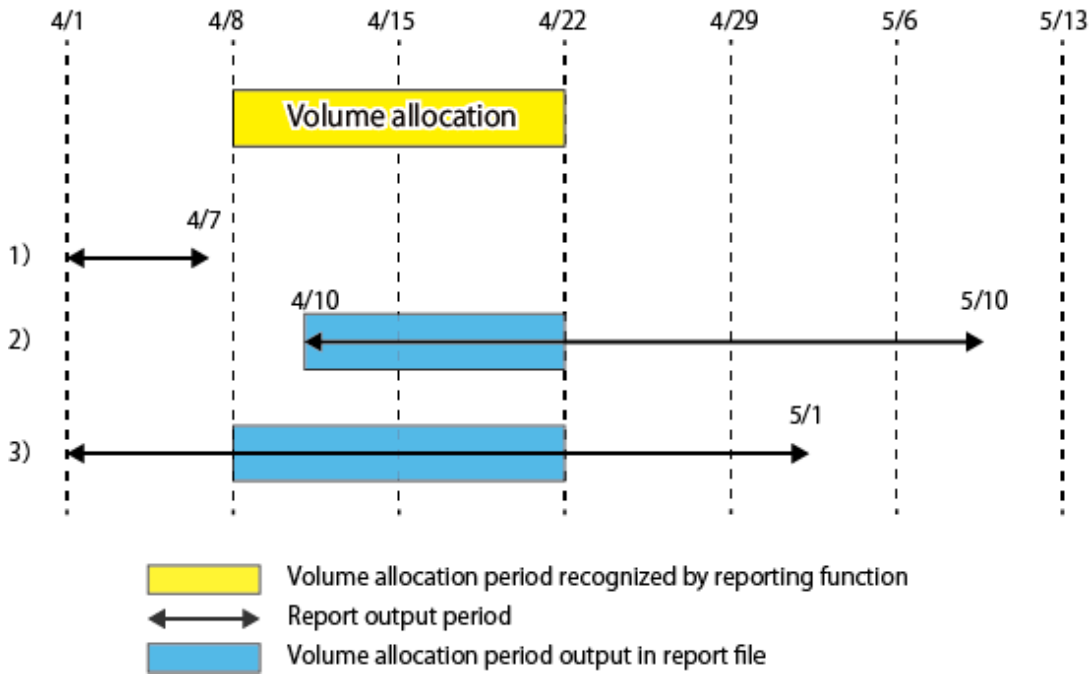
Since in this example a collection interval is set to one day, a maximum of 23 hours and 59 minutes of error is caused. The relation between information collection interval and error is as shown in "[Table 8.1 Influence Rate by Information Collection Interval and Collected Information Amount](#)".

Table 8.1 Influence Rate by Information Collection Interval and Collected Information Amount

Information Collection Interval	Accumulated Information Amount	Time Lag Reflected in Report Information
Long	Little	Large
Short	Large	Small

Concept of volume allocation within report output period

Report information is output in the report file based on the volume allocation period recognized by the Reporting function within a report output period. The point where the report output period specified by the user when creating a report overlaps the volume allocation period recognized by the Reporting function is a volume allocation period output into the report file.



The volume allocation period recognized by the Reporting function is 4/8 to 4/22. In the following report output period, a volume allocation period output in the report file is as follows:

No.	Report Output Period	Volume Allocation Period Output in Report File	Remark
1)	4/1-4/7	None	Report output period is out of volume allocation period.
2)	4/10-5/10	4/10-4/22	-
3)	4/1-5/1	4/8-4/22	-

8.3.1.3 Define Report Information Retention Period

The report creation command removes the old information exceeding the period preset by the policy from the information stack file.

First, define how long to retain report information. A report information retention period is defined based on the following factors:

- Possible restrictions from the purpose of use
 - Retention period by internal control
 - Backup interval of information stack file
 - Interval of creating a report
 - Interval of collecting information, etc.
- Quotation of the information stack file capacity based on the configuration of an assumed storage system

Refer to the *ETERNUS SF Installation Guide* for information on estimating the information stack file capacity.

The defined retention period is enabled by being set in the policy file.



Refer to "8.3.2.2 Setup Policy" for information on how to set a retention period.



Note

The report information is deleted based on the retention period set in the policy file when the report creation command is run. For this reason, if the report creation command is not run even though the report information in the information stack file exceeds the retention period, the report information is not deleted.

8.3.2 Setup

8.3.2.1 Obtain and Setup License

To use the Reporting function, the ETERNUS SF Storage Cruiser Standard Edition license is required.

For the ETERNUS Disk storage system to which the above license is not registered, reporting is not available. If the license is not registered for the ETERNUS Disk storage system and reporting is desired, register the license.



Information

The required license for ETERNUS Disk storage system is checked when the report information collection command is run. For this reason, even if the license is deleted while in use, already collected information is output in the report.

8.3.2.2 Setup Policy

Specify the report information retention period in the information stack file by setting up a policy.



See

Refer to "[A.11 policy.conf Parameter](#)" for information on how to set up a policy.

8.3.2.3 Setup Periodic Command Execution

Setup from Web Console

Select Storage from the Web Console to activate the Reporting function.

Periodic command execution of the Reporting function can be started and stopped on a per storage basis. Enabling the Reporting function runs the report information collection command at the 5th minute of every hour and the report creation command at 6:30 AM on the 1st of every month periodically. The period of the report made by periodic command execution is one month from 0:00 of the 1st of the previous month to 0:00 of the 1st of the month.

Set up periodic command execution by creating a unique application

If you want to run the report creation command with more detailed settings than the command execution interval set up from the Web Console, perform the following operations:

- Use the operating system periodic execution function
- Create an application to periodically invoke the report creation command



Note

For report period information specified for option of the report creation command, specify a proper value every time.

8.3.2.4 Create Accounting Application

A general charging method devised by the Reporting function is to charge usage fees for volumes used by servers within a report output period, which is calculated on a per server basis.

Server administrator privileges are required to view the report file.

The calculation formula for fees charged for volumes is as follows:

```
Fees charged for volume = Unit price (a) * Volume allocation (b) * Volume allocation time (c)
```

The following is an example of unit price per RAID level:

RAID Level	Unit Price per MB and per Hour
RAID0	1 dollar
RAID1	2 dollars
RAID1+0	3 dollars
RAID5	4 dollars
RAID6	5 dollars
RAID5+0	6 dollars

```
Fees charged for server = Sum of fees charged per volume
```

- The report file configuration output by the Reporting function is as follows:

```
Server information
  ETERNUS Disk storage system information
    Allocated volume information
      Information for volume (disk type, RAID level, etc.)
    Allocated volume information
    ...
  ETERNUS Disk storage system information
  ...
Server information
...
```

To calculate fees charged for volumes allocated per server, for example, create an accounting application to perform the following processing (element name in the brackets):

```
foreach <server information (Servers)> {
  Fee charged for server = 0
  foreach <ETERNUS Disk storage system information (DiskArrays)> {
    foreach <allocated volume information (Volumes)> {
      Obtain type of RAID group from RAID information (RAIDGroup).
      Get unit price from fee sheet according to obtained RAID group type. ... a
      Obtain volume allocation (capacity) from volume information (Volume). ... b
      Obtain volume allocation time (difference between end and start) from volume allocation
      information (Allocation). ... c
      Fee charged for allocated volume = a * b * c
      Fee charged for server += Fee charged for allocated volume }
    }
  Output the fee charged for server
}
```

Example

Calculate fees charged for server (charged for volume 1 and volume 2).

The conditions per volume are as follows:

- Volume1
 - RAID level: RAID0 (unit price: 1 dollar)

- Volume allocation: 100MB
- Volume allocation period: 12/1 5:00-12/2 1:30 (20.5 hours in all)
- Volume2
 - RAID level: RAID6 (unit price: 5 dollars)
 - Volume allocation: 500MB
 - Volume allocation period: 12/10 11:00-12/10 14:00 (3.0 hours in all)

Fee charged per volume is as follows:

- Fee charged for Volume1
 $1(\text{dollar}) * 100(\text{MB}) * 21(\text{hour}) = 2,100(\text{dollars})$
- Fee charged for Volume2
 $5(\text{dollars}) * 500(\text{MB}) * 3(\text{hour}) = 7,500(\text{dollars})$

Fee charged for server is as follows:

- Fee charged for server
 $2,100(\text{dollars}) + 7,500(\text{dollars}) = 9,600(\text{dollars})$

8.3.3 Operation

8.3.3.1 Create Invoice

The Reporting function outputs report information as a report. For the operation to charge fees mentioned in the later examples, the center administrator is responsible to do it.

- Input a report file in the accounting application to make an invoice.
 (On completion of output of the report file, the accounting application loads the report file.)
- Send an invoice to the center user.
- Charge usage fee based on the invoice.

Information

The Reporting function calculates charging information based on volume capacity and usage period. Also, ETERNUS system obtains performance information for storage systems and switches as well as configuration information for storage systems.

If you want to calculate charging information using performance information for each system, use the [storageadm perfddata command](#) to obtain the performance information.

8.3.4 Maintain

8.3.4.1 Backup/Restore of Report Related Files

For report related files (report information stack file, policy file, etc.) used in the Reporting function, it is recommended to back them up periodically, and restore them in an emergency so as to continue business.

See

Refer to "[10.1.1.2 Backup of Manager](#)" and "[10.1.1.3 Restoring Manager](#)" for the backup/restore procedure of report-related files.

8.3.4.2 Error When Running Report Information Collection Command

If an error occurs when running the report information collection command, the report information at that point in time is not stored in the information stack file. For example, if any error occurs on completion of information collection for Disk storage system A, the report information collection command terminates abnormally after the collected information for Disk storage system A has been deleted. If a force-quit is performed by [Ctrl] + [C] on the command side, the processing may be continued. In that case, check the Operation History of ETERNUS SF system.

If any error is found in the report information collection command, correct the cause and then re-execute the command.
If any error is found, the report information collection command notifies it in the following ways:

- Command resetting value (The value of 1 or more is returned for abnormal end)
- Command output message
- ETERNUS SF system Operation History

To set the report information collection command so that it is periodically run, it is necessary to read those values and make sure that no error is occurring.

If any error should occur, a return code and message identifying the cause are returned, so that proper corrective action can be taken.

8.3.4.3 Error When Running Report Creation Command

If an error occurs when running the report creation command, no report is created.

If any error is found in the report creation command, correct the cause and then re-execute the command.

If any error is found, the report creation command notifies it in the following ways:

- Command return code (The value of 1 or more is returned for abnormal end)
- Command output message
- ETERNUS SF system Operation History

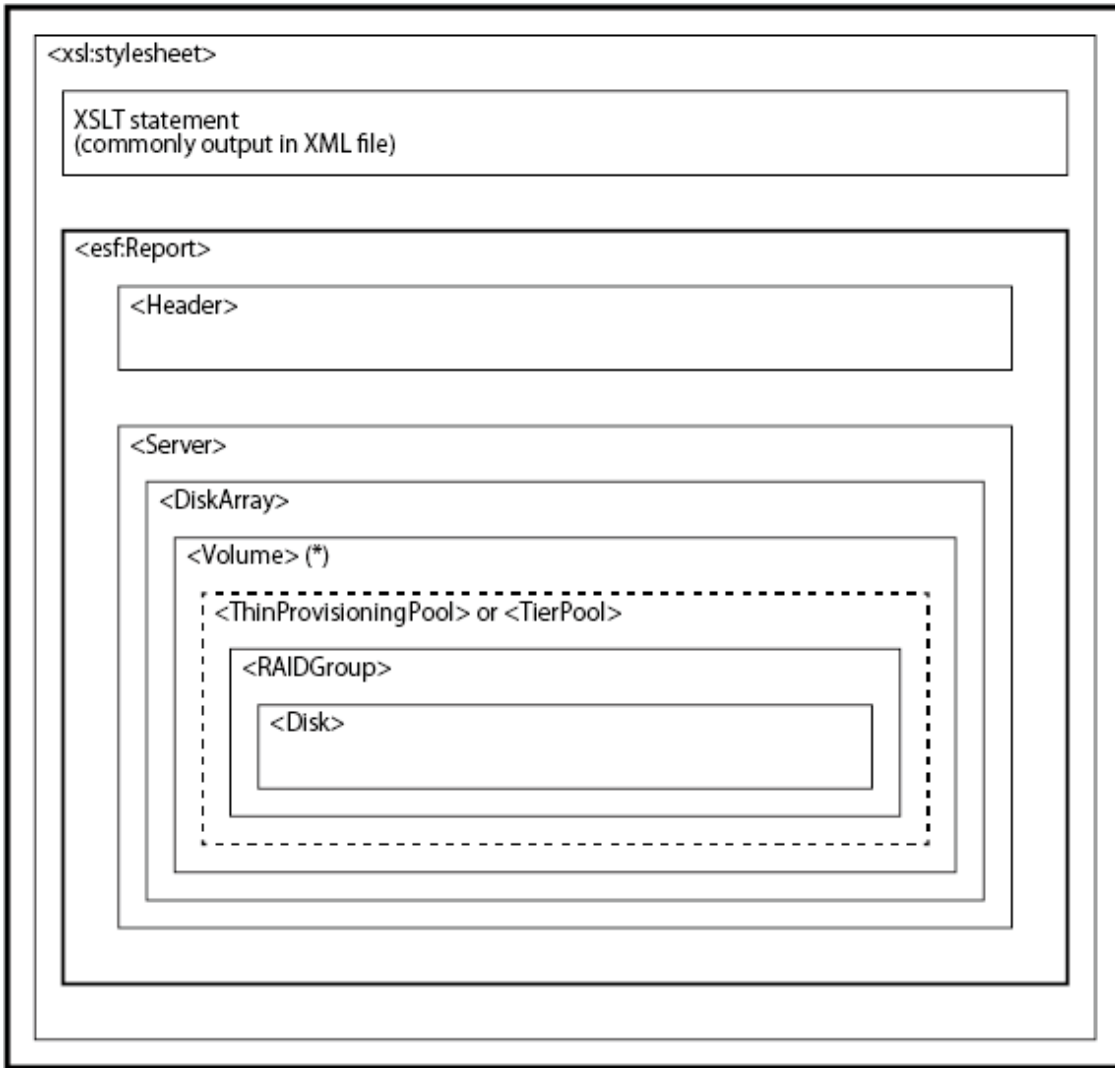
To set the report creation command so that it is periodically run, it is necessary monitor the results and make sure that no errors are occurring.

If any error should occur, a return code and message identifying the cause are returned, so that proper corrective action can be taken.

8.4 Configuration of Report File

Output overview

The output configuration of a XML report is as follows:



*: The content varies with volume type.

Output Detail

```
<?xml version="1.0" encoding="UTF-8" ?>
<?xml-stylesheet type="text/xsl" href="#esfreportxsl"?>
<!DOCTYPE Report [ <!ATTLIST xsl:stylesheet id ID #REQUIRED > ]>
<xsl:stylesheet id="esfreportxsl" xmlns:esf="localhost" ~ >

  XSLT statement
  (commonly output in XML file)

<esf:Report>
  <Header created="2013-09-13T12:03:25+0900" reportBegin="2013-09-13T10:53:00+0900"
reportEnd="2013-09-13T12:03:00+0900" version="1.00" />
  <Servers>
    <Server name="Server1" os="Windows2008" ipAddress="192.168.1.10">
      <DiskArrays>
        <DiskArray name="Storage1" serialNo="0000000001"
boxid=" " ec="1.3.6.1.4.1.211.1.21.1.150">
          <Volumes>
            Information per volume

          </Volumes>
        </DiskArray>
      </DiskArrays>
    </Server>
  </Servers>
</esf:Report>
</xsl:stylesheet>
```

The following is the information on a per volume type basis:

- For Standard Volume, SDV, WSV

```
<Volume name="SDV_Volume" number="2896" type="SDV" capacity="1024" encryption="No" multiPath="1"
connectServerNumber="1" concatenationNumber="-">
  <Allocation start="2013-09-13T10:53:00+0900" end="2013-09-13T12:03:00+0900" />
  <RAIDGroups>
    <RAIDGroup name="RAID_GP_0" number="7" type="Striping (RAID0)">
      <Disks>
        <Disk number="12" enclosureNumber="0x00" slotNumber="12" diskType="SAS" speed="10000" />
        <Disk number="13" enclosureNumber="0x00" slotNumber="13" diskType="SAS" speed="10000" />
      </Disks>
    </RAIDGroup>
  </RAIDGroups>
</Volume>
```

- For TPV

```
<Volume name="TPP_Volume" number="1" type="TPV" capacity="5120" encryption="No" multiPath="1"
connectServerNumber="1" concatenationNumber="-">
  <Allocation start="2013-09-13T12:02:35+0900" end="2013-09-13T12:03:00+0900" />
  <ThinProvisioningPool name="TPP_1" number="3">
    <RAIDGroups>
      <RAIDGroup name="RAID_GP_1" number="0" type="Mirroring (RAID1)">
        <Disks>
          <Disk number="1" enclosureNumber="0x00" slotNumber="1" diskType="SAS" speed="10000" />
          <Disk number="257" enclosureNumber="0x01" slotNumber="1" diskType="SAS" speed="10000" />
        </Disks>
      </RAIDGroup>
    </RAIDGroups>
  </ThinProvisioningPool>
</Volume>
```

- For FTV

```

<Volume name="FTV_Volume" number="158" type="FTV" capacity="204800" encryption="No"
multiPath="1" connectServerNumber="1" concatenationNumber="-">
  <Allocation start="2013-09-13T10:53:00+0900" end="2013-09-13T11:42:02+0900" />
  <TierPool name="TIER_1" number="0">
    <SubPools>
      <SubPool name="FTSP_NAME#0" number="0" level="Low">
        <RAIDGroups>
          <RAIDGroup name="FTSP_NAME#0_0" number="2" type="Mirroring (RAID1)">
            <Disks>
              <Disk number="23" enclosureNumber="0x00" slotNumber="23" diskType="SAS" speed="7200" /
            >
              <Disk number="279" enclosureNumber="0x01" slotNumber="23" diskType="SAS"
speed="7200" />
            </Disks>
          </RAIDGroup>
        </RAIDGroups>
      </SubPool>
      <SubPool name="FTSP_NAME#1" number="1" level="Middle">
        <RAIDGroups>
          <RAIDGroup name="FTSP_NAME#1_0" number="3" type="Mirroring (RAID1)">
            <Disks>
              <Disk number="0" enclosureNumber="0x00" slotNumber="0" diskType="SAS" speed="10000" />
              <Disk number="256" enclosureNumber="0x01" slotNumber="0" diskType="SAS"
speed="10000" />
            </Disks>
          </RAIDGroup>
        </RAIDGroups>
      </SubPool>
      <SubPool name="FTSP_NAME#2" number="2" level="High">
        <RAIDGroups>
          <RAIDGroup name="FTSP_NAME#2_0" number="4" type="Mirroring (RAID1)">
            <Disks>
              <Disk number="12" enclosureNumber="0x00" slotNumber="12" diskType="SSD" speed="-" />
              <Disk number="268" enclosureNumber="0x01" slotNumber="12" diskType="SSD" speed="-" />
            </Disks>
          </RAIDGroup>
        </RAIDGroups>
      </SubPool>
    </SubPools>
  </TierPool>
</Volume>

```

The attributes maintained by elements are as shown in "Table 8.2 Attributes Maintained by Elements".

Table 8.2 Attributes Maintained by Elements

Element Name	Description (Data Size)	Output Difference per Volume Type			Freque ncy
		FTV	TPV	Other	
Header	Information to differentiate report	A	A	A	1
created	Date and time when report was created (string, 24 bytes) (*1)	A	A	A	1
reportBegin	Start date and time of reporting period specified by esfadm report create command (string, 24 bytes) (*1)	A	A	A	1
reportEnd	End date and time of reporting period specified by esfadm report create command (string, 24 bytes) (*1)	A	A	A	1
version	Report format version information (string, max 8 bytes)	A	A	A	1

Element Name		Description (Data Size)	Output Difference per Volume Type			Frequency
Attribute Name			FTV	TPV	Other	
Servers		Maintain all Server elements. (All Server elements are sub-elements of this element)	A	A	A	1
Server		Number of servers connected to volumes	A	A	A	1 or more
	name	Server name (string, max. 255 bytes)	A	A	A	1
	os	Operating system type (string, max. 255 bytes)	A	A	A	1
	ipAddress	IP address (string, max. 64 bytes)	A	A	A	1
DiskArrays		Maintain all DiskArray elements related to servers (All DiskArray elements are sub-elements of this element)	A	A	A	1
DiskArray		Disk array information including volumes connected to servers	A	A	A	1 or more
	name	Disk array name (string, max. 255 bytes)	A	A	A	1
	serialNo	Serial number (string, max. 16 bytes)	A	A	A	1
	boxid	Box ID (string, 40 bytes)	A	A	A	1
	ec	Enterprise code (string, max. 255 bytes)	A	A	A	1
Volumes		Maintain Volume elements related to some DiskArray, connected to server (All Volume elements are sub-elements of this element)	A	A	A	1
Volume		Information for volume connected to server	A	A	A	1 or more
	name	Volume name (string, max. 16 bytes)	A	A	A	1
	number	Volume number (value: decimal, max. 10 bytes)	A	A	A	1
	type	Volume type (string, max. 16 bytes) Standard, WSV, SDV, TPV or FTV	A	A	A	1
	capacity	Volume capacity (MB) (value: decimal, max. 10 bytes) The meaning varies with volume type. Standard/WSV: Physical capacity SDV/TPV/FTV: Logical capacity	A	A	A	1
	encryption	Encryption status (string, max. 255 bytes) Yes: Enable No: Disable	A	A	A	1
	multiPath	Number of paths between server and volume (value: decimal, max. 10 bytes)	A	A	A	1
	connectServerNumber	Number of connected servers (value: decimal, max. 10 bytes)	A	A	A	1
	concatenationNumber	Number of concatenated LUNs in volume (string, max. 255 bytes) If LUN is not concatenated, a hyphen ("-") is displayed.	A	A	A	1
Allocation		Information for volume allocation	A	A	A	1
	start	Start date and time of volume allocation (string, 24 bytes) (*1)	A	A	A	1
	end	End date and time of volume allocation (string, 24 bytes) (*1)	A	A	A	1
TierPool		Tier pool information	A	N/A	N/A	1 or more
	name	Tier pool name (string, max. 64 bytes)	A	N/A	N/A	1

Element Name		Description (Data Size)	Output Difference per Volume Type			Frequency
Attribute Name			FTV	TPV	Other	
	number	Tier pool number (value: decimal, max. 10 bytes)	A	N/A	N/A	1
SubPools		Maintain sub-pool elements (All sub-pool elements are sub-elements of this element)	A	N/A	N/A	1
SubPool		Sub-pool information	A	N/A	N/A	1 or more
	name	Sub-pool name (string, max. 64 bytes)	A	N/A	N/A	1
	number	Sub-pool number (value: decimal, max. 10 bytes)	A	N/A	N/A	1
	level	Tier level (string, max. 32 bytes) Low: Low sub-pool Middle: Middle sub-pool High: High sub-pool For one layer Tier pool, a hyphen ("-") is displayed.	A	N/A	N/A	1
ThinProvisioningPool		Thin Provisioning Pool information	N/A	A	N/A	1 or more
	name	Thin Provisioning Pool name (string, max. 16 bytes)	N/A	A	N/A	1
	number	Thin Provisioning Pool number (value: decimal, max. 10 bytes)	N/A	A	N/A	1
RAIDGroups		Maintain RAID Group elements (All RAID Group elements are sub-elements of this element)	A	A	A	1 or more
RAIDGroup		RAID information	A	A	A	1 or more
	name	RAID Group name (string, max. 16 bytes)	A	A	A	1
	number	RAID Group number (value: decimal, max. 10 bytes)	A	A	A	1
	type	RAID Group type (string, max. 64 bytes) - Striping (RAID0) - Mirroring (RAID1) - High Performance (RAID1+0) - High Capacity (RAID5) - High Reliability (RAID6) - Reliability (RAID5+0) - Unknown	A	A	A	1
Disks		Maintain Disk elements (All Disk elements are sub-elements of this element)	A	A	A	1
Disk		Disk information	A	A	A	1 or more
	number	Disk number (value: decimal, max 10 bytes)	A	A	A	1
	enclosureNumber	Enclosure number (value: hexadecimal, 4 bytes) For disks contained in Controller Enclosure, "0x00" is displayed.	A	A	A	1
	slotNumber	Slot number (value: decimal, max. 10 bytes)	A	A	A	1
	diskType	Disk type (string, max. 255 bytes) SAS, SSD or SED-SAS	A	A	A	1

Element Name		Description (Data Size)	Output Difference per Volume Type			Frequency
Attribute Name			FTV	TPV	Other	
	speed	Disk rotation count (rpm) (value: decimal, max. 10 bytes) If there is no rotation count, a hyphen ("-") is displayed.	A	A	A	1

"A" indicates "Applicable", and "N/A" indicates "Not Applicable".

*1: For date and time, the local time of ETERNUS SF system is output in ISO8601 format.

Chapter 9 Maintenance of Devices to be Managed

9.1 Windows displayed in the event of a fault and troubleshooting

If a fault occurs on a device, an error description of the fault is output to the event log in the Web Console, the device status is also changed to [Error] or [Warning] if the support level of the device is A or B. The criteria of [Error] and [Warning] depends on the device definition. If this product can identify an access path affected by the fault, the access path status is changed to [Error].

For a device whose support level is I, an error description of a fault on the device is not output to the event log by default. The color of the device status also remains unchanged. However, if all of the following conditions are satisfied, it is possible to output an error description of the fault to the event log to change the color of the device status:

- The device supports SNMP Traps.
- The device IP address is specified during manual embedding.
- The SNMP Trap XML definition file has been created.



Refer to "[A.5 SNMP Trap XML Definition File](#)" for information on how to create the SNMP Trap XML definition file.

On the Web Console, check for faults in the order shown below and take corrective actions as required.

For middleware errors not including server node HBA and multipath faults, only events are reported. To troubleshoot middleware errors, refer to the appropriate middleware manuals.

If the ETERNUS Disk storage system is in an [Error] or [Warning] state

1. On the global navigation tab, click **Storage**.
2. On the Main pane in the disk storage system overview screen, click the target name.
3. On the Main pane in the disk storage system details screen, click the target name.
4. The Maintenance screen for the ETERNUS Disk storage system is started. Find the failed component in the ETERNUS Disk storage system.
For replacement of failed components, contact a Fujitsu customer engineer.

To view the status of CE, DE, ports and disks in the ETERNUS Disk storage system, click **Component** in the Category pane of the Web Console. Before checking the latest status of CE, DE, ports and disks, execute [Reload Conf.] for the ETERNUS Disk storage system.

If the tape library is in an [Error] or [Warning] state

1. On the global navigation tab, click **Storage**.
2. On the **Storage** pane, click **Tape Library**.
3. On the Main pane in the manually embedded tape library overview screen, click the target name.
4. On the Main pane in the tape library details screen, click the target name.
5. The Maintenance screen for the tape library is started. Find the failed component in the tape library.
For replacement of failed components, contact a Fujitsu customer engineer.

If the manually embedded disk storage system is in an [Error] or [Warning] state

1. On the global navigation tab, click **Storage**.
2. On the **Storage** pane, click **Disk Array(Manual)**.
3. On the Main pane in the manually embedded disk storage system overview screen, click the target name.

4. On the Main pane in the manually embedded disk storage system details screen, click the target name.
5. The Maintenance screen for the disk storage system is started. Find the failed component in the disk storage system.
For replacement of failed components, contact a Fujitsu customer engineer.

When replacing adapters (CA), refer to "If the adapter (CA) of manually embedded disk storage system and manually embedded tape library is replaced" in "[9.3.3 Replacing faulty components of a manually embedded device](#)". Moreover, the replacement of failed components, contact a Fujitsu customer engineer as required.

If the manually embedded tape library is in an [Error] or [Warning] state

1. On the global navigation tab, click **Storage**.
2. On the **Storage** pane, click **Tape Library(Manual)**.
3. On the Main pane in the manually embedded tape library overview screen, click the target name.
4. On the Main pane in the manually embedded tape library details screen, click the target name.
5. The Maintenance screen for the tape library is started. Find the failed component in the tape library.
For replacement of failed components, contact a Fujitsu customer engineer.

When replacing adapters (CA), refer to "If the adapter (CA) of manually embedded disk storage system and manually embedded tape library is replaced" in "[9.3.3 Replacing faulty components of a manually embedded device](#)". Moreover, the replacement of failed components, contact a Fujitsu customer engineer.

If the Fibre Channel switch is in an [Error] or [Warning] state

1. On the global navigation tab, click **Network**.
2. On the Main pane in the switch overview screen, click the target name.
3. On the Main pane in the switch details screen, click the target name.
4. The Maintenance screen for the Fibre Channel switch is started. Find the failed component in the Fibre Channel switch.
For replacement of failed components, contact a Fujitsu customer engineer.

If any port is in Error state due to SFP failure, the status of the affected access path is displayed as [Error].

If an access path is defined in the access path settings of this product, the zoning setting of the Fibre Channel switch is defined as WWPN zoning. Therefore, if a Fibre Channel switch port fails, the Fibre Channel cable connected to it can be reconnected to another Fibre Channel switch port, and operation can be restarted.

Also, refer to "A warning for a device is displayed" in "[4.2.1.3 Problem-handling \(FAQ\)](#)".

If the server node is in an [Error] or [Warning] state

1. On the global navigation tab, click **Server**.
2. On the **Server** pane, click **Access Path**.
3. Check the physical pathway of the access path with an [Error] state.
If no Error state device is on the route, check if a Fibre Channel cable along the route is disconnected. If you cannot identify the cause, contact a Fujitsu customer engineer.

On the server node where msdsm (the default Windows multipath driver, from Windows Server 2008 onward) is set, the server node enters the [Warning] state even if the single path (an access path that does not have a redundancy configuration) exists. This depends on the msdsm specification. Because the information for the access path that corresponds to the [Error] state disappears from the OS, this product cannot be distinguished from a single path. If access path is configured with the single path, disable msdsm.

Also, refer to "An Error in an access path is displayed" in "[4.2.1.3 Problem-handling \(FAQ\)](#)".

If an access path is in an [Error] state

If an access path of multipath disk control, follow the procedure below:

1. Obtaining path statuses
Check the current path configuration and status.

2. I/O stop related to a failed access path
3. Replacement of failed components (if necessary) or action for the Error
 - To replace a failed component, contact a Fujitsu customer engineer.
4. I/O restart of a stopped access path

For an access path not configured using Multipath Disk Control, a job performed with the target used volume is affected. Stop the job and take the appropriate action to resolve the fault. To replace a failed component, contact a Fujitsu customer engineer.

When replacing an HBA, refer to "[9.3.1.1 Host bus adapter \(HBA\) replacement of server node](#)".

Point

.....

In the case of an access path configured with multipath disk control, placing the access path offline causes the access path status to be [Error] and may display "Host Agent reports Access Path Status is degraded." as a message of access path failure.

In that case, put the access path back to online, and it returns to its former status.

.....

Actions to perform after component replacement

Execute [Reload Conf.] for the device whose component has been replaced to refresh the current device state.

When the device state is recovered by performing a replacement, the device state returns to and is displayed as the "Normal" state.

The state of NetApp FAS Series, V-Series and devices registered manually is not automatically recovered. On completion of device recovery, use the following procedure to return the device to the "Normal" state:

1. On the Action pane for the manually embedded device, click **Modify** to open the modify screen of the device.
2. Select "Normal" from the **Status** list on the modify screen and click **Modify**.

9.2 Replacing supported device

If any device registered on this product has been replaced, even executing [Reload Conf.] to the replaced device does not update to the new device information. Delete the replaced device once on the Web Console to add it again.

For procedures required by each device, see the description below.

9.2.1 Replacing a server node

When replacing a server node for each system, do it according to the operating system.

For Solaris OS

Before discovering a new server node on this product, delete all the access paths to the replaced server node to configure new access paths to the new server node.

For operating systems other than the Solaris OS

Use the following procedure to setting the access path:

1. Installing the Agent on the new server

For the new server assign a different IP address from that of the replaced server, then install the Agent.

If a new server cannot be configured with a different IP address from that of the replaced server, delete all the access paths to the replaced server before the new server is detected by this product and then specify new access paths for the new server.

2. Registering the new server to this product

1. On the global navigation tab, click **Server**.

2. On the Action pane, click **Register** under **Server**.
 3. Register the new server.
Check that the new server is displayed on the server overview screen.
3. Deleting the access path
1. On the global navigation tab, click **Server**.
 2. On the **Server** pane, click **Access Path**.
 3. On the Main pane, select the checkbox of the access path set for the HBA on the replaced server.
 4. On the Action pane, click **Delete** under **Access Path**.
 5. Delete the access path.
On the access path overview screen, check that the access path set for the HBA on the replaced server has been deleted.
4. Adding an access path
1. On the global navigation tab, click **Server**.
 2. On the **Server** pane, click **Access Path**.
 3. On the Action pane, click **Add (ETERNUS)** under **Access Path**.
 4. Register the access path. For access path definition, select the following:
 - Port: Port assigned to the new server
 - HBA: HBA loaded in the new server
 - Affinity Group: Affinity Group assigned to the replaced server
 On the access path overview screen, check that the access path using the HBA installed on the new server has been created.
5. Deleting the replaced server from this product
1. On the global navigation tab, click **Server**.
 2. On the Main pane, select the checkbox of the replaced servers.
 3. On the Action pane, click **Delete** under **Server**.
 4. Delete the replaced server.
On the server overview screen, check that the replaced server has been deleted.

9.2.2 Replacing ETERNUS Disk storage system

When replacing ETERNUS Disk storage system for each device, use the following procedure to setting the access path.

1. Integrating the configuration information
 1. Ensure that the configuration definition of the new device matches that of the replaced device.
 2. For the new device assign a different IP address from that of the replaced device.
If the new device cannot be configured with a different IP address from that of the replaced device, delete all the access paths to the replaced device before the new device is detected by this product and then specify new access paths for the new device.
2. Registering the new device to this product
 1. On the global navigation tab, click **Storage**.
 2. On the Action pane, click **Register** under **Storage**.
 3. Register the new device.
On the disk storage system overview screen, check that the new device is displayed.

3. Registering the license to the new device

1. On the global navigation tab, click **Storage**.
2. On the Main pane, click the new device name.
3. On the Category pane, click **System**.
4. On the Main pane, select the target license checkbox.
5. On the Action pane, click **Register** under **License**.
6. Register the license.
On the license overview screen, check the license registration status.

4. Deleting the access path

1. On the global navigation tab, click **Server**.
2. On the **Server** pane, click **Access Path**.
3. On the Main pane, select the checkbox of the access path set for the replaced device.
4. On the Action pane, click **Delete** under **Access Path**.
5. Delete the access path.
On the access path overview screen, check that the access path set for the replaced device has been deleted.

5. Adding an access path

1. On the global navigation tab, click **Server**.
2. On the **Server** pane, click **Access Path**.
3. On the Action pane, click **Add (ETERNUS)** under **Access Path**.
4. Register the access path. For access path definition, select the following:
 - Port: Port assigned to the new device
 - HBA: HBA logical connection to the replaced device
 - Affinity Group: Affinity Group that matches the replaced device and to be assigned to the new deviceOn the access path overview screen, check that the access path using the port assigned to the new device has been created.

6. Deleting the license of the replaced device

1. On the global navigation tab, click **Storage**.
2. On the Main pane, check the replaced device name.
3. On the Category pane, click **System**.
4. On the Main pane, select the target license checkbox.
5. On the Action pane, click **Delete** under **License**.
6. Delete the license.
On the license overview screen, check the license registration status.

7. Deleting the replaced device from this product

1. On the global navigation tab, click **Storage**.
2. On the Main pane, select the replaced device checkbox.
3. On the Action pane, click **Delete** under **Storage**.
4. Delete the replaced device.
On the disk storage system overview screen, check that the replaced device has been deleted.

8. Subsequent operation

The server node must be restarted for server nodes that do not support hot swapping configuration changes after creation of the access path is complete.

On the server nodes that support hot swapping configuration changes, it is necessary to execute commands to perform the hot swapping configuration changes for OS and HBA drivers. For example, when the HBA driver is FUJITSU PCI Fibre Channel, `chgcctl` or `clchgfc` must be executed.

9.2.3 Replacing ETERNUS LT250/LT270

When replacing an entire ETERNUS LT250/LT270, use the following the procedure provided below to resetting the access path.

1. Integrating the configuration information
 1. Ensure that the configuration definition of the new tape library matches that of the replaced tape library.
 2. For the new tape library assign a different IP address from that of the replaced tape library.
2. Registering the new tape library to this product
 1. On the global navigation tab, click **Storage**.
 2. On the **Storage** pane, click **Tape Library**.
 3. On the Action pane, click **Discover** under **Tape Library**.
 4. Register the new tape library.
On the tape library overview screen, check that the new tape library is displayed.
3. Deleting zoning
 1. On the global navigation tab, click **Network**.
 2. On the Main pane, check the switch name.
 3. On the Category pane, click **Zoning**.
 4. On the Main pane, select the checkbox of the WWPN zoning of the replaced tape library.
 5. On the Action pane, click **Delete** under **Zoning**.
 6. Delete zoning.
On the zoning overview screen, check that the WWPN zoning of the replaced tape library has been deleted.

Note

.....
If you are not using "one to one" zoning, ensure that other security settings are not affected.
.....

4. Adding an access path
 1. On the global navigation tab, click **Server**.
 2. On the **Server** pane, click **Access Path**.
 3. On the Action pane, click **Add (Other)** under **Access Path**.
 4. Register the access path. For access path definition, select the following:
 - Port: Port assigned to the new tape library
 - HBA: HBA logical connection to the replaced tape libraryOn the zoning overview screen, check that the WWPN zoning of the new tape library has been created.
5. Deleting the replaced tape library from this product
 1. On the global navigation tab, click **Storage**.

2. On the **Storage** pane, click **Tape Library**.
 3. On the Main pane, select the replaced tape library checkbox.
 4. On the Action pane, click **Delete** under **Tape Library**.
 5. Delete the replaced tape library.
On the tape library overview screen, check that the replaced tape library has been deleted.
6. Subsequent operation

The server node must be restarted for server nodes that do not support hot swapping configuration changes after creation of the access path is complete.

On the server nodes that support hot swapping configuration changes, it is necessary to execute commands to perform the hot swapping configuration changes for OS and HBA drivers. For example, when the HBA driver is FUJITSU PCI Fibre Channel, chgfcctl or clchgfc must be executed.

9.2.4 Replacing Fibre Channel switch

This section explains the replacement procedure for Fibre Channel switch (hereafter, refer to as switch) registered in this product.

Also, the procedure differs according to pre-replaced and post-replaced switch models and any change in IP address.

- If the pre-replaced and post-replaced switch models and the IP address are the same:
 1. Record the settings of threshold monitoring. (if thresholds are monitored)
 2. On completion of device replacement, perform [Reload Conf.] on the Web Console.
 3. Based on the settings at step 1, start to monitor thresholds. (if thresholds are monitored)
- If the pre-replaced switch model and the post-replaced switch model are different:
 1. Stopping the performance monitoring of the switch to be replaced (when it is not a monitored device, this operation is unnecessary).

If threshold monitoring is also set, stop the threshold monitoring first and then stop the performance monitoring.

1. On the global navigation tab, click **Network**.
 2. On the Main pane, click the switch to be replaced.
 3. On the Category pane, click **Performance**.
 4. On the **Performance** pane, click **Configuration**.
 5. On the Action pane, click **Stop** under **Performance**.
Check that the monitored status of the switch to be replaced is "Stop".
2. Deleting the replaced switch from this product
1. On the global navigation tab, click **Network**.
 2. On the Main pane, select the checkbox of the replaced switches.
 3. On the Action pane, click **Delete** under **Switch**.
 4. Delete the replaced switch.
On the switch overview screen, check that the replaced switch is not displayed.
3. Physical replacement of old and new switches

For device replacement, contact a Fujitsu customer engineer and perform the replacement according to the maintenance procedure manual for the device.

When replacing a switch that is not connected in cascade, you may have to manually perform zoning settings again if the switch configuration information (configUpload file) has not been stored. After registering the new switch in this product, perform step 6, "Setting of switch zoning" below. Refer to the manual that comes with this device for the switch configuration information (configUpload file).

4. Registering a new switch to this product

1. On the global navigation tab, click **Network**.
2. On the Action pane, click **Discover** under **Switch**.
3. Register the new switch.
On the switch overview screen, check that the new switch is displayed.

5. Refreshing the access path status

1. On the global navigation tab, click **Server**.
2. On the **Server** pane, click **Access Path**.
3. On the Action pane, click **Refresh** under **Access Path Status**.
On the access path overview screen, check that the access path status has been refreshed.

6. Setting the switch zoning

Since the zoning information specified for newly replaced switches that are managed by this product does not exist, access paths are displayed as definition inconsistency (Changed). Therefore, manually reset the zoning.

If no zoning is set for replaced switches or switches that are connected in a cascade, zoning resetting is not required.

If there is configuration information (the configUpload file), refer to the maintenance manual for the device.

Note

If the switch zoning information is as follows, the zoning access paths are not displayed regardless of pre- or post-switch replacement.

- Zoning other than HBA to CA access pathway managed by this product (HBA to HBA, CA to CA, HBA to UnknownFC, CA to UnknownFC, UnknownFC to UnknownFC)

Therefore, even after switch replacement, no Warning is displayed against the access path definition inconsistency such as between HBA and CA.

If zoning other than HBA to CA access pathway is configured with replaced switches, use Web Tools to configure the zoning for FC switch or Telnet command to FC switch.

7. Starting the performance monitoring of the new switch (when it is not a monitored device, this operation is unnecessary).

1. On the global navigation tab, click **Network**.
2. On the Main pane, click the target switch name.
3. On the Category pane, click **Performance**.
4. On the **Performance** pane, click **Configuration**.
5. On the Action pane, click **Start** under **Performance**.
Check that the monitored status of the new switch is "Monitoring".

Perform the threshold monitoring setting again once the threshold monitoring setting has been performed.

Note

If the configuration information has been customized, then check the content of the configuration settings file before starting performance monitoring.

Refer to "[A.9 Explanation of the Configuration Settings File](#)" for details.

9.2.5 Replacing manually embedded device

When replacing manually embedded device for each device, use the following the procedure provided below to resetting the access path.

1. Registering the new manually embedded device to this product.
 - In the case of manually embedded disk storage system:
 1. On the global navigation tab, click **Storage**.
 2. On the **Storage** pane, click **Disk Array(Manual)**.
 3. On the Action pane, click **Register** under **Storage**.
 4. Register the new manually embedded disk storage system.
Check that the new manually embedded disk storage system is displayed on the manually embedded disk storage system overview screen.
 - In the case of manually embedded tape library:
 1. On the global navigation tab, click **Storage**.
 2. On the **Storage** pane, click **Tape Library(Manual)**.
 3. On the Action pane, click **Register** under **Tape Library**.
 4. Register the new manually embedded tape library.
Check that the new manually embedded tape library is displayed on the manually embedded tape library overview screen.
2. Registering a post-replaced adapter (CA) of a manually embedded device.
 - For a manually embedded disk storage system:
 1. On the Main pane in the manually embedded disk storage system overview screen, click the target name.
 2. On the **Storage** pane, click **Port**.
 3. On the Action pane, click **Add** under **Port**.
 4. Registration of new port.
Check that the new port is displayed on the port overview screen of the manually embedded disk storage system.
 - For a manually embedded tape library:
 1. On the Main pane in the manually embedded tape library overview screen, click the target name.
 2. On the **Storage** pane, click **Port**.
 3. On the Action pane, click **Add** under **Port**.
 4. Register the new port.
Check that the new port is displayed on the port overview screen of the manually embedded tape library.
3. Deleting zoning
 1. On the global navigation tab, click **Network**.
 2. On the Main pane, click the target switch name.
 3. On the Category pane, click **Zoning**.
 4. On the Main pane, select the checkbox of the WWPN zoning of the replaced device.
 5. On the Action pane, click **Delete** under **Zoning**.
 6. Delete zoning.
On the zoning overview screen, check that the WWPN zoning of the replaced device has been deleted.



Note

.....
If you are not using "one to one" zoning, ensure that other security settings are not affected.
.....

4. Adding an access path

1. On the global navigation tab, click **Server**.
2. On the **Server** pane, click **Access Path**.
3. On the Action pane, click **Add (Other)** under **Access Path**.
4. Register the access path. For access path definition, select the following:
 - Port: Port assigned to the new manually embedded device
 - HBA: HBA logical connection to the new manually embedded device

On the zoning overview screen, check that the WWPN zoning of the new manually embedded device has been created.

5. Deleting the replaced device from this product

- For a manually embedded disk storage system:
 1. On the global navigation tab, click **Storage**.
 2. On the **Storage** pane, click **Disk Array(Manual)**.
 3. On the Main pane, select the checkbox of the manually embedded disk storage system that has been replaced.
 4. On the Action pane, click **Delete** under **Storage**.
 5. Delete the manually embedded disk storage system that has been replaced.
On the manually embedded disk storage system overview screen, check that the manually embedded disk storage system that has been replaced has been deleted.
- For a manually embedded tape library:
 1. On the global navigation tab, click **Storage**.
 2. On the **Storage** pane, click **Tape Library(Manual)**.
 3. On the Main pane, select the checkbox of the replaced manually embedded tape library.
 4. On the Action pane, click **Delete** under **Tape Library**.
 5. Delete the manually embedded tape library that has been replaced.
On the manually embedded tape library overview screen, check that the manually embedded tape library that has been replaced has been deleted.

6. Subsequent operation

After configuration, restart the server node if it does not support active configuration.

9.3 Replacing supported device components

The following explains how to replace the components of a supported device managed by this product.

For procedures required by each device, see the description below.

Type of Device	Replacing Faulty Components
Server node	<ul style="list-style-type: none">- For HBA replacement: Perform "9.3.1 Replacing server node components".- For other component replacement: Execute [Reload Conf.] after component replacement.
ETERNUS Disk storage system	Execute [Reload Conf.] after component replacement. Also, refer to "9.3.2 Replacing faulty components of ETERNUS Disk storage systems, ETERNUS LT250/LT270" .
ETERNUS LT250/LT270	
Fibre Channel switch	Execute [Reload Conf.] after component replacement.
Manually embedded server node	<ul style="list-style-type: none">- For HBA replacement:

Type of Device	Replacing Faulty Components
	Perform "9.3.3 Replacing faulty components of a manually embedded device". - For other component replacement: Execute [Reload Conf.] after component replacement.
Manually embedded disk storage system Manually embedded tape library	- For Adapter (CA) replacement: Perform "9.3.3 Replacing faulty components of a manually embedded device". - For other component replacement: Execute [Reload Conf.] after component replacement.

9.3.1 Replacing server node components

This section describes the procedure required for HBA replacement on the server nodes registered on this product.

Note

- Before executing access path inheritance, select **Network** from the global navigation tab on the Web Console, and verify that all Fibre Channel switches cascaded to the Fibre Channel switch related to access path setting are correctly recognized in the current status. Once an access path is changed in a state where a Fibre Channel switch is temporarily disconnected from the cascade connection, the old cascade connection cannot easily be recovered. In this event, execute `cfgClear` to delete the zoning information for the Fibre Channel temporarily disconnected from the cascade connection. This enables cascade reconnection.
- The basic conditions under which this product can recognize HBA replacement on a server node are as follows:
 - The agent has been installed in the server nodes.
 - HBA is exchanged on a server node same slot (physical port number).
 - The server node is registered in this product.
 - Access path is set to the pre-replaced HBA.
- When inheriting access path to HBA on this product, notice the following points:
 - Zoning configuration should be one-to-one WWPN zoning.

In the environment using the following zoning configuration, access path inheritance is not allowed:

- Port zoning
- World Wide Port Name (WWPN) zone setting not being one-to-one.
- The zoning configuration of the following devices is not allowed to be inherited:
 - Tape library unit
 - Other than ETERNUS Disk storage system
- The host number of host registration information is not allowed to be inherited. Host name is allowed to be inherited.
- If inheritance is done toward the access paths for which no zoning is configured, skip zoning creation and perform only host registration and host affinity configuration.
- For access path inheritance in environments that use the FC routing functionality, the settings for the LSAN zone that is required in the FC routing functionality cannot be modified using this product.

Before using access path inheritance, manually modify the required LSAN zone settings on the server nodes, Fibre Channel switches, and storage devices.

- For VMware vSphere 4 or later, perform either of the following steps after access path inheritance:
 - Reboot the VM host
 - For the access path inheritance-done HBA, execute `Rescan` from the VMware Infrastructure Client.

Refer to "4.1.7.1 VMware vSphere 4 or later" - "Configuration management" - "Access path management" for details on the operation of the VMware Infrastructure Client.

9.3.1.1 Host bus adapter (HBA) replacement of server node

When replacing HBA on a server node, do it according to the operating system.

9.3.1.1.1 [For Solaris OS server node] Host bus adapter (HBA) replacement

When replacing HBA on a Solaris server node, take the following procedure.

HBA replacement with server node shut down

For a server node that does not support the hot system replacement function, turn off the server node in order to replace the HBA. Do not restart or shut down the server node in reconfigure mode during replacement. (This is because the special file name is changed if the reboot -r command, boot -r command, or other such command is executed.)

1. Shutting down the server node.

Confirm that the /reconfigure file does not exist, and shut down the device.

```
# ls /reconfigure
/reconfigure: No such file or directory
```

If the /reconfigure file exists, take the following procedure:

a. To delete the "reconfigure" file, enter the following command.

```
# rm /reconfigure
```

b. Execute the ls command to re-check the presence of the /reconfigure file.

c. Do not reconfigure but shut down.

```
# /usr/sbin/shutdown -y -i0 -g0
```

Re-create the/reconfigure file after replacement operation. Afterward, restart the server node.

2. Replacing the HBA

To replace a failed component, contact a Fujitsu customer engineer.

3. Activating the server node

Activate the server node.

No access path, however, is recovered here. This is because the zoning is based on old HBA information is defined on the storage system and Fibre Channel switch.

4. Execute [Reload Conf.] for the server node from this product.

5. Inheriting access paths (resetting security)

Follow the process of "9.3.1.2 Access path inheritance after HBA replacement" from this product, and define the zoning setting so that the method of access based on the new HBA information can be the same as that for the previous access path of the storage system and Fibre Channel switch.

6. Reactivating the server node

Reboot the server node without reconfiguration (reboot -r, boot -r, etc. are prohibited.)

```
# /usr/sbin/shutdown -i6
```

The access paths and the paths of Multipath Disk Control are recovered.

HBA replacement without shutting down server node

On the server node that supports the hot system replacement function, HBA replacement is allowed without shutting down the server node. Refer to the appropriate device manuals for information on the hot system replacement.

1. HBA replacement without shutting the server node

Refer to the device manual to replace HBA without shutting the server node.

To replace a failed component, contact a Fujitsu customer engineer.

2. Execute [Reload Conf.] for the server node from this product.
3. Inheriting access paths (resetting security)

Follow the process of "[9.3.1.2 Access path inheritance after HBA replacement](#)" from this product, and define the zoning setting so that the method of access based on the new HBA information can be the same as that for the previous access path of the storage system and Fibre Channel switch.

9.3.1.1.2 [For operating systems other than the Solaris OS] Host bus adapter (HBA) replacement

When replacing HBA on a other than Solaris server node, take the following procedure.

HBA replacement with server node shut down

For a server node that does not support the hot system replacement function, turn off the server node in order to replace the HBA.

1. Shutting down the server node
2. Replacing the HBA
3. Starting the server node

No access path is recovered here. This is because zoning based on old HBA information is defined on the storage and Fibre Channel switch.

4. Execute [Reload Conf.] for the server node from this product.
5. Inheriting access paths (resetting security)

Follow the process of "[9.3.1.2 Access path inheritance after HBA replacement](#)" from this product, and define the zoning setting so that the method of access based on the new HBA information can be the same as that for the previous access path of the storage system and Fibre Channel switch.

6. Reactivating the server node

HBA replacement without shutting down server node

On the server node that supports the hot system replacement function, HBA replacement is allowed without shutting down the server node. Refer to the appropriate device manuals for information on the hot system replacement.

1. Replacing the HBA without shutting down the server node

Refer to the device manual to replace HBA without shutting the server node.

To replace a failed component, contact a Fujitsu customer engineer.

2. Execute [Reload Conf.] for the server node from this product.
3. Inheriting access paths (resetting security)

Follow the process of "[9.3.1.2 Access path inheritance after HBA replacement](#)" from this product, and define the zoning setting so that the method of access based on the new HBA information can be the same as that for the previous access path of the storage system and Fibre Channel switch.

9.3.1.2 Access path inheritance after HBA replacement

Inheriting the HBA access path requires that all steps for the target operating system in "[9.3.1.1 Host bus adapter \(HBA\) replacement of server node](#)" through "Execute [Reload Conf.] for the server node from this product" be completed. Make sure that preparatory work has been done, and perform proper operation in accordance with the HBA status.

- When the HBA status becomes "Changed":
Perform the operation mentioned in "[9.3.1.2.1 Post-replaced HBA state is "Changed"](#)".
- When the HBA status does not become "Changed":
Perform the operation mentioned in "[9.3.1.2.2 Post-replaced HBA state is "Unknown"](#)".



Note

- Whether the HBA status becomes "Changed" or not cannot be determined before [Reload Conf.] is performed from the Web Console after HBA replacement.

9.3.1.2.1 Post-replaced HBA state is "Changed"

In this product, after HBA replacement on an agent installed server node, if [Reload Conf.] is executed to the server node, it recognizes the HBA replacement and changes the HBA state displayed on the server detail screen of the Main pane to "Changed". This is detected when an HBA that has a different WWPN is installed in the same slot (physical port number) of the host.

The procedure for access path inheritance at this time is provided below.



Point

Before performing the procedures below, refer to the Notes in "[9.3.1 Replacing server node components](#)".

1. Checking the inherited HBA state
 1. On the global navigation tab, click **Server**.
 2. On the Main pane, check the server.
 3. On the Main pane, confirm that the HBA state is "Changed".
2. Inheriting access path
 1. On the global navigation tab, click **Server**.
 2. On the Main pane, click the target server name.
 3. On the Main pane, select the checkbox of the HBA whose state is "Changed".
 4. On the Action pane, click **Inherit** under **Access Path**.
3. Checking the access path inheritance
 1. On the global navigation tab, click **Server**.
 2. On the **Server** pane, click **Access Path**.
 3. Using the HBA of replacement destination, check if the access path has been set.

9.3.1.2.2 Post-replaced HBA state is "Unknown"

This product may not be able to set the "Changed" state for an HBA. According to the following status, execute this procedure.

HBA replacement on manually embedded server node

Refer to "[9.3.3 Replacing faulty components of a manually embedded device](#)".

In cases other than the above

Change access path by following procedure provided below.

If the device requires server node-side settings, the settings must be defined manually.

Point

.....
Before performing the procedures below, refer to the Notes in "9.3.1 Replacing server node components".
.....

1. Detecting the replaced destination HBA

Reload the configuration of the target server to detect the replaced destination HBA.

1. On the global navigation tab, click **Server**.
2. On the Main pane, select the target server checkbox.
3. On the Action pane, click **Reload Conf.** under **Server**.

2. Checking the replaced destination HBA

1. On the global navigation tab, click **Server**.
2. On the Main pane, click the server name.
3. On the Main pane, check that the HBAs of replacement source and replacement destination are displayed.

3. Changing the access path

1. On the global navigation tab, click **Server**.
2. On the **Server** pane, click **Access Path**.
3. On the Main pane, select the changed target access path checkbox.
4. On the Action pane, click **Modify** under **Access Path**.
5. Change the setting of access path.

4. Checking the access path changing

1. On the global navigation tab, click **Server**.
2. On the **Server** pane, click **Access Path**.
3. Using the replaced destination HBA, check whether access path has been set.

5. Subsequent operation

After configuration, restart the server node if it does not support active configuration.

9.3.2 Replacing faulty components of ETERNUS Disk storage systems, ETERNUS LT250/LT270

ETERNUS Disk storage systems, ETERNUS LT250/LT270 do not require the access path inheritance because the WWPN is not changed for the replacement of an adapter (CA) etc.

9.3.3 Replacing faulty components of a manually embedded device

If WWPN is changed because of a faulty component of a manually embedded device such as an HBA or adapter (CA) is replaced, the replacement device will not be automatically detected by this product. Perform the following procedures to set the access path after components of the device are exchanged.

If the HBA of manually embedded server node is replaced

1. Detecting the replaced destination HBA

Adding the HBA to the target server.

1. On the global navigation tab, click **Server**.
2. On the Main pane, click the target server name.
3. On the Action pane, click **Add** under **HBA**.
4. Register the HBA of replacement destination.

2. Checking the HBA of replacement destination

1. On the global navigation tab, click **Server**.
2. On the Main pane, click the target server name.
3. On the Main pane, check that the HBAs of pre-replacement and replacement destination are displayed.

3. Changing the access path

1. On the global navigation tab, click **Server**.
2. On the **Server** pane, click **Access Path**.
3. On the Main pane, select the target access path checkbox.
4. On the Action pane, click **Modify** under **Access Path**.
5. Change the access path settings.

4. Checking the access path changes

1. On the global navigation tab, click **Server**.
2. On the **Server** pane, click **Access Path**.
3. For the replaced destination HBA, check if the access path has been set.

5. Deleting the pre-replacement HBA

1. On the global navigation tab, click **Server**.
2. On the Main pane, click the target server name.
3. On the Main pane, select the checkbox of the pre-replacement HBA.
4. On the Action pane, click **Delete** under **HBA**.
5. Delete the pre-replacement HBA.

6. Subsequent operation

After configuration change, restart any server node if it does not support the hot system replacement function.

If the adapter (CA) of manually embedded disk storage system and manually embedded tape library is replaced

1. Registering the post-replaced adapter (CA) of manually embedded device

- For a manually embedded disk storage system:

1. On the manually embedded disk storage system overview screen, click the manually embedded disk storage system name.
2. On the **Storage** pane, click **Port**.
3. On the Action pane, click **Add** under **Port**.

4. Register the new port.
Check that the new port is displayed on the port overview screen of the manually embedded disk storage system.

- For a manually embedded tape library system:

1. On the manually embedded tape library system overview screen, click the manually embedded tape library system name.
2. On the **Storage** pane, click **Port**.
3. On the Action pane, click **Add** under **Port**.
4. Register the new port.
Check that the new port is displayed on the port overview screen of the manually embedded tape library.

2. Deleting zoning

1. On the global navigation tab, click **Network**.
2. On the Main pane, click the switch name.
3. On the Category pane, click **Zoning**.
4. On the Main pane, select the checkbox of the WWPN zoning of the manually embedded device.
5. On the Action pane, click **Delete** under **Zoning**.
6. Delete zoning.
On the zoning overview screen, check that the WWPN zoning of the manually embedded device has been deleted.



Note

.....
If you are not using "one to one" zoning, ensure that other security settings are not affected.
.....

3. Adding an access path

1. On the global navigation tab, click **Server**.
2. On the **Server** pane, click **Access Path**.
3. On the Action pane, click **Add (Other)** under **Access Path**.
4. Register the access path. For access path definition, select the following:
 - Port: Port assigned to the new manually embedded device
 - HBA: HBA logical connection to the manually embedded device

On the zoning overview screen, check that the WWPN zoning of the new manually embedded device has been created.

4. Deleting the pre-replacement adapter (CA) of manually embedded device

- For a manually embedded disk storage system:

1. On the manually embedded disk storage system overview screen, click the manually embedded disk storage system name.
2. On the **Storage** pane, click **Port**.
3. On the Main pane, select the checkbox of the pre-replacement port.
4. On the Action pane, click **Delete** under **Port**.
5. Delete the replaced port.
Check that the new manually embedded tape library is not displayed on the manually embedded tape library overview screen.

- For a manually embedded tape library:

1. On the manually embedded tape library system overview screen, click the manually embedded tape library system name.
2. On the **Storage** pane, click **Port**.

3. On the Main pane, select the checkbox of the pre-replacement port.
 4. On the Action pane, click **Delete** under **Port**.
 5. Delete the replaced port.
Check that the replaced port is not displayed on the port overview screen.
5. Subsequent operation
- After configuration, restart the server node if it does not support active configuration.

9.4 Adding supported device components

9.4.1 Adding ETERNUS LT270 S2 extended cabinet

When adding an extended cabinet for ETERNUS LT270 S2, if a cabinet-through rail is installed, remove the drive in the base cabinet and install it in the extended cabinet. Use the following procedure to change the port of the drive and reconfigure the access path:

1. Deleting zoning
 1. On the global navigation tab, click **Network**.
 2. On the Main pane, click the switch name.
 3. On the Category pane, click **Zoning**.
 4. On the Main pane, select the checkbox of the WWPN zoning of the removed drive.
 5. On the Action pane, click **Delete** under **Zoning**.
 6. Delete zoning.
On the zoning overview screen, check that the WWPN zoning of the removed drive has been deleted.



Note

If you are not using "one to one" zoning, ensure that other security settings are not affected.

2. Deleting the port of the drive
 1. On the global navigation tab, click **Storage**.
 2. On the **Storage** pane, click **Tape Library(Manual)**.
The registered tape libraries are displayed on the Main pane.
 3. On the Main pane, click the target tape library name.
 4. On the Category pane, click **Device**.
The devices registered on the tape library are displayed on the Main pane.
 5. On the Main pane, click the target device name.
The details of the device are displayed on the Main pane.
 6. On the Main pane, select the checkbox of the port of the target device.
 7. On the Action pane, click **Delete** under **Port**.
The information confirmation screen is displayed.
 8. Confirm the information, and then click **Delete**.
3. Adding an extended cabinet
Add an extended cabinet for ETERNUS LT270 S2.
4. Adding a port of the drive
 1. On the global navigation tab, click **Storage**.

2. On the **Storage** pane, click **Tape Library(Manual)**.
The registered tape libraries are displayed on the Main pane.
3. On the Main pane, click the target tape library name.
4. On the Category pane, click **Device**.
The devices registered on the tape library are displayed on the Main pane.
5. On the Main pane, click the target device name.
The details of the device are displayed on the Main pane.
6. On the Action pane, click **Add** under **Port**.
7. Enter the necessary information, and then click **Next**.
The information confirmation screen is displayed.
8. Confirm the information, and then click **Add**.

Point

.....
The interface type that allows ports to be added is only FC.
.....

5. Adding an access path

1. On the global navigation tab, click **Server**.
2. On the **Server** pane, click **Access Path**.
3. On the Action pane, click **Add (Other)** under **Access Path**.
4. Register the access path. For access path definition, select the following:
 - HBA: Logically connected to a replaced device.
 - Port: to the drive whose installed position was changed.
5. Confirm the information on the information confirmation screen, and then click **Add**.

6. Subsequent operation

After configuration, restart the server node if it does not support active configuration.

Chapter 10 Maintenance of the Administrative Environment

This chapter explains how to maintain databases, and it describes the appropriate action to take for troubleshooting.

10.1 Maintenance of Manager

10.1.1 Maintenance of manager

10.1.1.1 Collecting data for troubleshooting

If any problem occurs in a system that uses this software, collect troubleshooting information according to "[B.1 Collecting the troubleshooting information](#)".

10.1.1.2 Backup of Manager

Back up (save) the environment for the Storage Cruiser's manager if an error has occurred in the Management Server.

All of the tasks for backup of Manager are performed in the Management Server.

10.1.1.2.1 Backup of Solaris OS Manager

Follow the procedure below to save the environment for the Storage Cruiser's manager.



Information

About description in the procedure

- "\$BAK_DIR" signifies the backup destination directory.

1. Stop the ETERNUS SF Manager Tomcat Service.

Execute the following shell script to stop the service.

```
/opt/FJSVesfcm/bin/stop-webservice.sh
```

2. Create the backup data.

Create the directory for the backup data.

```
mkdir -p $BAK_DIR/Common
```

Execute the following command to create the backup data. Specify the default value 15432 to *<port-number>*, however, if you have changed the port number, specify the changed port number to *<port-number>*. The backup data is then created using the file name designated in *<filename>*.

```
/opt/FJSVesfcm/postgres/bin/pg_dump -U esfpostgres -C --attribute-inserts  
-p <port-number> -f $BAK_DIR/Common/<filename> esfdb
```

A prompt is displayed with the server awaiting input. Input the following keyword.

```
master01!
```

- Execute the following shell script to stop ETERNUS SF Manager services.

```
/opt/FJSVesfcm/bin/stopesf.sh
```

Note

Upon executing the shell script, multiple messages stating that the ETERNUS SF Manager Tomcat has already been stopped will be displayed. These messages do not pose a problem and can be ignored.

- Back up the files related to the performance management function.

This step can be skipped if you are not using the performance management function. Backup is not required if there are no subdirectories or files.

Note

If a pile of files related to the performance management function exists, calculate the backup time according to the amount of files.

Create the directories for the backup data.

```
mkdir -p $BAK_DIR/etc/opt/FJSVssmgr/current
mkdir -p $BAK_DIR/var/opt/FJSVssmgr/current/perf
```

Copy the subdirectories and files to the backup locations.

```
cp -p /etc/opt/FJSVssmgr/current/perf.conf $BAK_DIR/etc/opt/FJSVssmgr/current/
cp -Rp /var/opt/FJSVssmgr/current/perf/* $BAK_DIR/var/opt/FJSVssmgr/current/perf/
```

- Back up the other files which can be customized.

It is unnecessary to back up the files or the directories which are not existed.

Create the directories for the backup data.

```
mkdir -p $BAK_DIR/etc/opt/FJSVssmgr/current
mkdir -p $BAK_DIR/etc/opt/FJSVssmgr/current/eventmail
```

Copy the subdirectories and files to the backup locations.

```
# cp -p /etc/opt/FJSVssmgr/current/sanma.conf $BAK_DIR/etc/opt/FJSVssmgr/current/
# cp -p /etc/opt/FJSVssmgr/current/ssmgr.conf $BAK_DIR/etc/opt/FJSVssmgr/current/
# cp -p /etc/opt/FJSVssmgr/current/trapop.sh $BAK_DIR/etc/opt/FJSVssmgr/current/
# cp -p /etc/opt/FJSVssmgr/current/traprm.sh $BAK_DIR/etc/opt/FJSVssmgr/current/
# cp -Rp /etc/opt/FJSVssmgr/current/eventmail/* $BAK_DIR/etc/opt/FJSVssmgr/current/eventmail/
```

- Back up the SNMP Trap XML definition files.

This step can be skipped if you are not customizing the SNMP Trap XML definition files.

Below is an example for if the SNMP Trap XML definition file 1_3_6_1_1588_2_1_1_1.xml has been customized. As shown in this example, back up each customized file one at a time.

Create the directory for the backup data.

```
mkdir -p $BAK_DIR/etc/opt/FJSVssmgr/current/snmpth
```

Copy the file to the backup location.

```
# cp -p /etc/opt/FJSVssmgr/current/snmpth/1_3_6_1_1588_2_1_1_1.xml $BAK_DIR/etc/opt/FJSVssmgr/current/snmpth/
```

7. Back up the device polling setting files.

This step can be skipped if you are not customizing the device polling setting files.

Below is an example for if the device polling setting file, DP_config.xml, has been customized. As shown in this example, back up each customized file one at a time.

Create the directory for the backup data.

```
# mkdir -p $BAK_DIR/etc/opt/FJSVssmgr/current/devicepolling
```

Copy the file to the backup location.

```
# cp -p /etc/opt/FJSVssmgr/current/devicepolling/DP_config.xml $BAK_DIR/etc/opt/FJSVssmgr/current/devicepolling/
```

8. Back up the polling service setting file.

This step can be skipped if you are not customizing the polling service setting file.

If you have customized the polling service setting file pollingService.xml, back up this file using the step shown below.

Create the directory for the backup data.

```
# mkdir -p $BAK_DIR/etc/opt/FJSVssmgr/current/polling
```

Copy the file to the backup location.

```
# cp -p /etc/opt/FJSVssmgr/current/polling/pollingService.xml $BAK_DIR/etc/opt/FJSVssmgr/current/polling/
```

9. Save the files related to copy group and copy pair definitions.

Perform this step only if you are using the AdvancedCopy function.

Create the directories for the backup data.

```
mkdir -p $BAK_DIR/CCM/etc
mkdir -p $BAK_DIR/CCM/etc/db
mkdir -p $BAK_DIR/CCM/etc/db/cg
mkdir -p $BAK_DIR/CCM/etc/prop
mkdir -p $BAK_DIR/CCM/var/micc/database
```

Copy the subdirectories and files to the backup locations.

```
cp -p /etc/opt/FJSVccm/db/eternus.xml $BAK_DIR/CCM/etc/db
cp -p /var/opt/FJSVccm/micc/database/DeviceRegList.xml $BAK_DIR/CCM/var/micc/database
cp -p /etc/opt/FJSVccm/prop/user.properties $BAK_DIR/CCM/etc/prop
cp -p /etc/opt/FJSVccm/acc/etc/stxc.alias $BAK_DIR/CCM/etc
cp -p /etc/opt/FJSVccm/acc/etc/stxc_ext.alias $BAK_DIR/CCM/etc
cp -p /etc/opt/FJSVccm/acc/etc/stxcvolinf $BAK_DIR/CCM/etc
cp -Rp /etc/opt/FJSVccm/db/cg/* $BAK_DIR/CCM/etc/db/cg
```

10. Back up the license management database.

Create the directory for the backup data.

```
mkdir -p $BAK_DIR/LM
```

Execute the following command. The backup data is created using the file name specified in <filename>.

```
/opt/FJSVesflm/bin/esflm backup $BAK_DIR/LM/<filename>
```

11. Back up the files associated with the Reporting function. (For Reporting Function only)

Create the directories for the backup data.

```
mkdir -p $BAK_DIR/etc/opt/FJSVesfcm/conf/report
mkdir -p $BAK_DIR/etc/opt/FJSVesfcm/conf/scheduler
mkdir -p $BAK_DIR/var/opt/FJSVesfcm/report
```

Copy the subdirectories and files to the backup locations.

```
cp -p /etc/opt/FJSVesfcm/conf/report/* $BAK_DIR/etc/opt/FJSVesfcm/conf/report/
cp -p /etc/opt/FJSVesfcm/conf/scheduler/* $BAK_DIR/etc/opt/FJSVesfcm/conf/scheduler/
cp -Rp /var/opt/FJSVesfcm/report/* $BAK_DIR/var/opt/FJSVesfcm/report/
```

12. Back up the Optimization Option environment. (For Optimization Option only)

Create the directories for the backup data.

```
mkdir -p $BAK_DIR/etc/opt/FJSVssast/data/policy
mkdir -p $BAK_DIR/etc/opt/FJSVssast/data/pool
mkdir -p $BAK_DIR/var/opt/FJSVssast/data/perf
```

Copy the subdirectories and files to the backup locations.

```
cp -p /etc/opt/FJSVssast/data/policy/TierPolicy.xml $BAK_DIR/etc/opt/FJSVssast/data/policy/
cp -p /etc/opt/FJSVssast/data/pool/* $BAK_DIR/etc/opt/FJSVssast/data/pool/
cp -Rp /var/opt/FJSVssast/data/perf/* $BAK_DIR/var/opt/FJSVssast/data/perf/
```

13. Back up the Quality of Service Management Option environment. (For Quality of Service Management Option only)

Create the directories for the backup data.

```
mkdir -p $BAK_DIR/etc/opt/FJSVesfcm/conf/qos
```

Copy the subdirectories and files to the backup locations.

```
cp -p /etc/opt/FJSVesfcm/conf/qos/* $BAK_DIR/etc/opt/FJSVesfcm/conf/qos/
```

14. Execute the following shell script to start the ETERNUS SF Manager services.

```
/opt/FJSVesfcm/bin/startesf.sh
```

10.1.1.2.2 Backup of Solaris OS Manager (cluster environment)

For cluster environment, follow the procedure below to save the environment for the Storage Cruiser's manager.

1. Stop all cluster services which the Manager belongs to.

Refer to "Cluster transaction and local transaction" in the *ETERNUS SF Cluster Environment Setup Guide* for details of cluster transaction.

2. Mount the shared disk on the primary node.

3. Start the ETERNUS SF Manager Postgres service.

Execute the following command to start the ETERNUS SF Manager Postgres service:

```
/etc/init.d/startSFmanager start-postgres
```

4. Perform steps 2 and step 4 to 13 of "10.1.1.2.1 Backup of Solaris OS Manager" on the primary node.

5. Stop the ETERNUS SF Manager Postgres service.

Execute the following command to stop the ETERNUS SF Manager Postgres service:

```
/etc/init.d/startSFmanager stop-postgres
```

6. Unmount the shared disk mounted in step 2.

7. Start all cluster transactions which the Manager belongs to.

10.1.1.2.3 Backup of Linux Manager

Since the procedure for backup of the Linux version of Manager is identical to that for backup of the Solaris OS version, refer to "[10.1.1.2.1 Backup of Solaris OS Manager](#)" for performing this operation.

10.1.1.2.4 Back up of Linux Manager (cluster environment)

Since the procedure for backup of the Linux version of Manager is identical to that for backup of the Solaris OS versions in cluster environment, refer to "[10.1.1.2.2 Backup of Solaris OS Manager \(cluster environment\)](#)" for performing this operation.

10.1.1.2.5 Backup of Windows Manager

Follow the procedure below to save the environment for the Storage Cruiser's manager.



Information

About description in the procedure

- \$BAK_DIR means the backup destination directory.
- \$INS_DIR means "Program Directory" specified at the ETERNUS SF Manager installation.
- \$ENV_DIR means "Environment Directory" specified at the ETERNUS SF Manager installation.
- \$TMP_DIR means "Work Directory" specified at the ETERNUS SF Manager installation.

1. Stop the ETERNUS SF Manager Tomcat Service.

Open Service Control Manager and stop the following service.

- ETERNUS SF Manager Tomcat Service

2. Create the backup data.

Create the following directory for the backup data in Explorer or a similar program.

- \$BAK_DIR\Common

Execute the following command to create the backup data. Specify the default value 15432 to *<port-number>*, however, if you have changed the port number, specify the changed port number to *<port-number>*. The backup data will be created with the name specified in *<filename>*.

```
$INS_DIR\Common\sys\postgres\bin\pg_dump -U esfpostgres -C --attribute-inserts  
-p <port-number> -f $BAK_DIR\Common\<filename> esfdb
```

A prompt is displayed, with the server awaiting input. Input the following keyword.

```
master01!
```

3. Execute the following batch to stop the ETERNUS SF Manager services.

```
$INS_DIR\Common\bin\Stop_ESFservice.bat
```


Note

Upon executing the batch, multiple messages stating that the ETERNUS SF Manager Tomcat Service has already been stopped will be displayed. These messages do not pose a problem and can be ignored.

4. Back up the files related to the performance management function.

This step can be skipped if you are not using the performance management function.

This backup is also not required if there are no subdirectories or files.

Note

If a pile of files related to the performance management function exists, calculate the backup time according to the amount of files.

Create the following directories for the backup data in Explorer or a similar program.

- \$BAK_DIR\ESC\Manager\etc\opt\FJSVssmgr\current
- \$BAK_DIR\ESC\Manager\var\opt\FJSVssmgr\current\perf

Using Explorer or a similar program, copy the following file to the backup location.

Copy Source File	Copy Destination Directory
\$ENV_DIR\ESC\Manager\etc\opt\FJSVssmgr\current\perf.conf	\$BAK_DIR\ESC\Manager\etc\opt\FJSVssmgr\current

Using Explorer or a similar program, copy the subdirectories and files belonging to the following directories to their backup locations.

Copy Source Directory	Copy Destination Directory
\$TMP_DIR\ESC\Manager\var\opt\FJSVssmgr\current\perf	\$BAK_DIR\ESC\Manager\var\opt\FJSVssmgr\current\perf

5. Back up the other files which can be customized.

It is unnecessary to back up the files or the directories which are not existed.

Create the following backup directories in Explorer or a similar program.

- \$BAK_DIR\ESC\Manager\opt\FJSVssmgr\bin
- \$BAK_DIR\ESC\Manager\etc\opt\FJSVssmgr\current
- \$BAK_DIR\ESC\Manager\etc\opt\FJSVssmgr\current\eventmail

Using Explorer or a similar program, copy the following files to their backup locations.

Copy Source File	Copy Destination Directory
\$ENV_DIR\ESC\Manager\etc\opt\FJSVssmgr\current\sanma.conf	\$BAK_DIR\ESC\Manager\etc\opt\FJSVssmgr\current
\$ENV_DIR\ESC\Manager\etc\opt\FJSVssmgr\current\ssmgr.conf	
\$ENV_DIR\ESC\Manager\etc\opt\FJSVssmgr\current\trapop.bat	
\$ENV_DIR\ESC\Manager\etc\opt\FJSVssmgr\current\traprm.bat	

Using Explorer or a similar program, copy the subdirectories and files belonging to the following directory to their backup location.

Copy Source Directory	Copy Destination Directory
\$ENV_DIR\ESC\Manager\etc\opt\FJSVssmgr\current\eventmail	\$BAK_DIR\ESC\Manager\etc\opt\FJSVssmgr\current\eventmail

6. Back up the SNMP Trap XML definition files.

This step can be skipped if you are not customizing the SNMP Trap XML definition files.

Below is an example for if the SNMP Trap XML definition file 1_3_6_1_1588_2_1_1_1.xml is being customized. As in this example, back up each file one at a time.

Create the following backup directory in Explorer or a similar program.

- \$BAK_DIR\ESC\Manager\etc\opt\FJSVssmgr\current\snmpth

Using Explorer or a similar program, copy the following file to its backup location.

Copy Source File	Copy Destination Directory
\$ENV_DIR\ESC\Manager\etc\opt\FJSVssmgr\current\snmpth\1_3_6_1_1588_2_1_1_1.xml	\$BAK_DIR\ESC\Manager\etc\opt\FJSVssmgr\current\snmpth

7. Back up the device polling setting files.

This step can be skipped if you are not customizing the device polling setting files.

Below is an example for if the device polling setting file DP_config.xml is being customized. As in this example, back up each file one at a time.

Create the following backup directory in Explorer or a similar program.

- \$BAK_DIR\ESC\Manager\etc\opt\FJSVssmgr\current\devicepolling

Using Explorer or a similar program, copy the following file to its backup location.

Copy Source File	Copy Destination Directory
\$ENV_DIR\ESC\Manager\etc\opt\FJSVssmgr\current\devicepolling\DP_config.xml	\$BAK_DIR\ESC\Manager\etc\opt\FJSVssmgr\current\devicepolling

8. Back up the polling service setting file.

This step can be skipped if you are not customizing the polling service setting file.

If customizing the polling service setting file pollingService.xml, follow the step below to back it up.

Create the following backup directory in Explorer or a similar program.

- \$BAK_DIR\ESC\Manager\etc\opt\FJSVssmgr\current\polling

Using Explorer or a similar program, copy the following file to its backup location.

Copy Source File	Copy Destination Directory
\$ENV_DIR\ESC\Manager\etc\opt\FJSVssmgr\current\polling\pollingService.xml	\$BAK_DIR\ESC\Manager\etc\opt\FJSVssmgr\current\polling

9. Back up the registry.

Create the following backup directory in Explorer or a similar program.

- \$BAK_DIR\ACM\etc

Using Explorer or a similar program, copy the following files to the backup location.

Copy Source File	Copy Destination Directory
\$ENV_DIR\ACM\etc\swnode.ini	\$BAK_DIR\ACM\etc
\$ENV_DIR\ACM\etc\device.ini	

10. Save the files related to copy group and copy pair definitions.

Perform this step only if you are using the AdvancedCopy function.

Create the following directories for the backup data in Explorer or a similar program.

- \$BAK_DIR\CCM\etc
- \$BAK_DIR\CCM\etc\db
- \$BAK_DIR\CCM\etc\db\cg
- \$BAK_DIR\CCM\etc\prop
- \$BAK_DIR\CCM\var\micc\database

Using Explorer or a similar program, copy the following files to their backup locations.

Copy Source File	Copy Destination Directory
\$ENV_DIR\CCM\etc\db\eternus.xml	\$BAK_DIR\CCM\etc\db
\$TMP_DIR\CCM\var\micc\database\DeviceRegList.xml	\$BAK_DIR\CCM\var\micc\database

If copy source files exist, copy the following files to their backup locations using Explorer or a similar program.

Copy Source File	Copy Destination Directory
\$ENV_DIR\CCM\etc\prop\user.properties	\$BAK_DIR\CCM\etc\prop
\$ENV_DIR\CCM\etc\stxc.alias	\$BAK_DIR\CCM\etc
\$ENV_DIR\CCM\etc\stxc_ext.alias	
\$ENV_DIR\CCM\etc\stxcvolinf	

Using Explorer or a similar program, copy the files belonging to the following directory to their backup location.

Copy Source Directory	Copy Destination Directory
\$ENV_DIR\CCM\etc\db\cg	\$BAK_DIR\CCM\etc\db\cg

11. Back up the license management database.

Create the following backup directory in Explorer or a similar program.

- \$BAK_DIR\LM

Execute the following command. The backup data will be created with the file name specified in <filename>.

```
$INS_DIR\LM\bin\esflm backup $BAK_DIR\LM\<filename>
```

12. Back up the files associated with the Reporting function. (For Reporting Function only)

Create the following backup directories using Explorer or the like:

- \$BAK_DIR\Common\etc\report
- \$BAK_DIR\Common\etc\scheduler
- \$BAK_DIR\Common\var\report

Copy the files under the following directories to the backup location using Explorer or the like:

Copy Source Directory	Copy Destination Directory
\$ENV_DIR\Common\etc\report	\$BAK_DIR\Common\etc\report
\$ENV_DIR\Common\etc\scheduler	\$BAK_DIR\Common\etc\scheduler

Copy the files under the following directories to the backup location using Explorer or the like:

Copy Source Directory	Copy Destination Directory
\$TMP_DIR\Common\var\report	\$BAK_DIR\Common\var\report

13. Back up the Optimization Option environment. (For Optimization Option only)

Create the following directories for the backup data in Explorer or a similar program.

- \$BAK_DIR\AST\Manager\etc\opt\FJSVssast\data\policy
- \$BAK_DIR\AST\Manager\etc\opt\FJSVssast\data\pool
- \$BAK_DIR\AST\Manager\var\opt\FJSVssast\data\perf

Using Explorer or a similar program, copy the following files to their backup locations.

Copy Source File	Copy Destination Directory
\$ENV_DIR\AST\Manager\etc\opt\FJSVssast\data\policy\TierPolicy.xml	\$BAK_DIR\AST\Manager\etc\opt\FJSVssast\data\policy

Using Explorer or a similar program, copy the subdirectories and files belonging to the following directory to their backup location.

Copy Source Directory	Copy Destination Directory
\$ENV_DIR\AST\Manager\etc\opt\FJSVssast\data\pool	\$BAK_DIR\AST\Manager\etc\opt\FJSVssast\data\pool
\$TMP_DIR\AST\Manager\var\opt\FJSVssast\data\perf	\$BAK_DIR\AST\Manager\var\opt\FJSVssast\data\perf

14. Back up the Quality of Service Management Option environment. (For Quality of Service Management Option only)

Create the following backup directory using Explorer or the like:

- \$BAK_DIR\Common\etc\qos

Copy the files under the following directory to the backup location using Explorer or the like:

Copy Source Directory	Copy Destination Directory
\$ENV_DIR\Common\etc\qos	\$BAK_DIR\Common\etc\qos

15. Execute the following batch to start ETERNUS SF Manager services.

\$INS_DIR\Common\bin\Start_ESFservice.bat

10.1.1.2.6 Backup of Windows Manager (cluster environment)

For cluster environment, follow the procedure below to save the environment for the Storage Cruiser's manager.

1. Stop all cluster services which the Manager belongs to.

Refer to "Cluster transaction and local transaction" in the *ETERNUS SF Cluster Environment Setup Guide* for details of cluster transaction.

2. Mount the shared disk on the primary node.

3. Start the ETERNUS SF Manager Postgres service.

Open Service Control Manager to start the following service:

- ETERNUS SF Manager Postgres Service

4. Perform steps 2 and step 4 to 14 of "[10.1.1.2.5 Backup of Windows Manager](#)" on the primary node.

Directory description in "[10.1.1.2.5 Backup of Windows Manager](#)" are replaced to the following directories.

- \$BAK_DIR means the backup destination directory.

- \$INS_DIR means "Program Directory" specified at the ETERNUS SF Manager installation.
 - \$ENV_DIR means "Environment Directory" specified at the ETERNUS SF Manager installation.
 - \$TMP_DIR means "Work Directory" as specified during installation.
5. Stop the ETERNUS SF Manager Postgres service.
Open Service Control Manager to stop the following service:
 - ETERNUS SF Manager Postgres Service
 6. Unmount the shared disk mounted in step 2.
 7. Start all cluster transactions which the Manager belongs to.

10.1.1.3 Restoring Manager

Restore the environment for the Storage Cruiser's manager if an error has occurred in the Management Server.
All of the tasks for restoring Manager are performed in the Management Server.

10.1.1.3.1 Restoring Solaris OS Manager

Follow the procedure below to restore the environment for the Storage Cruiser's manager.

For restoration after reinstalling Manager, be sure to complete installation and setup before restoration. Refer to "Installing ETERNUS SF Manager" and "Setting Up ETERNUS SF Manager" in the *ETERNUS SF Installation and Setup Guide* for installation and setup.



Information

About description in the procedure

- "\$BAK_DIR" signifies the backup destination directory.

1. Re-setup Storage Cruiser's manager.

Install ETERNUS SF Manager and set it up as Storage Cruiser's manager.

Refer to "Installing ETERNUS SF Manager" and "Setting Up ETERNUS SF Manager" in the *ETERNUS SF Installation and Setup Guide* for installation and setup.

2. Stop the ETERNUS SF Manager Tomcat Service.

Execute the following shell script to stop the service.

```
/opt/FJSVesfcm/bin/stop-webservice.sh
```

3. Restore the backup data.

Execute the following command. Specify the default value 15432 to *<port-number>*, however, if you have changed the port number, specify the changed port number to *<port-number>*.

```
/opt/FJSVesfcm/postgres/bin/psql -U esfpostgres -p <port-number> postgres
```

A prompt is displayed, with the server awaiting input. Input the following keywords in the sequence shown below.

```
master01!  
drop database esfdb;  
\q
```

Execute the following command to restore the backup data. Specify the default value 15432 to *<port-number>*, however, if you have changed the port number, specify the changed port number to *<port-number>*. For *<filename>*, input the file name specified when the backup data was created.

```
/opt/FJSVesfcm/postgres/bin/psql -U esfpostgres -p <port-number>
-f $BAK_DIR/Common/<filename> postgres
```

A prompt is displayed, with the server awaiting input. Input the following keyword.

```
master01!
```

4. Execute the following shell script to stop the ETERNUS SF Manager services.

```
/opt/FJSVesfcm/bin/stopesf.sh
```

Note

Upon executing the shell script, multiple messages stating that the ETERNUS SF Manager Tomcat Service has already been stopped will be displayed. These messages do not pose a problem and can be ignored.

5. Restore the files related to the performance management function.

This step can be skipped if you are not using the performance management function or the files related to the performance management function are not backed up.

Delete the subdirectories and files belonging to the restore destination directory.

However, be sure not to delete the restore destination directory itself. If the restore destination directory itself does not exist, create one.

```
rm -f /etc/opt/FJSVssmgr/current/perf.conf
rm -rf /var/opt/FJSVssmgr/current/perf/*
```

Copy the subdirectories and files from the backup location.

```
cp -p $BAK_DIR/etc/opt/FJSVssmgr/current/perf.conf /etc/opt/FJSVssmgr/current/
cp -Rp $BAK_DIR/var/opt/FJSVssmgr/current/perf/* /var/opt/FJSVssmgr/current/perf/
```

6. Restore the other files which can be customized.

This restoration is unnecessary for the files or the directories which have not been backed up.

Copy the subdirectories and files from the backup location.

```
# cp -p $BAK_DIR/etc/opt/FJSVssmgr/current/sanma.conf /etc/opt/FJSVssmgr/current/
# cp -p $BAK_DIR/etc/opt/FJSVssmgr/current/ssmgr.conf /etc/opt/FJSVssmgr/current/
# cp -p $BAK_DIR/etc/opt/FJSVssmgr/current/trapop.sh /etc/opt/FJSVssmgr/current/
# cp -p $BAK_DIR/etc/opt/FJSVssmgr/current/traprm.sh /etc/opt/FJSVssmgr/current/
# cp -Rp $BAK_DIR/etc/opt/FJSVssmgr/current/eventmail/* /etc/opt/FJSVssmgr/current/eventmail/
```

7. Restore the SNMP Trap XML definition files.

This restoration is unnecessary for the files which have not been backed up.

Copy the SNMP Trap XML definition files from the backup location.

```
# cp -p $BAK_DIR/etc/opt/FJSVssmgr/current/snmpth/*.xml /etc/opt/FJSVssmgr/current/snmpth/
```

8. Restore the device polling setting files.

This restoration is unnecessary for the files which have not been backed up.

Copy the files from the backup location.

```
# cp -p $BAK_DIR/etc/opt/FJSVssmgr/current/devicepolling/*.xml /etc/opt/FJSVssmgr/current/
devicepolling/
```

9. Restore the polling service setting file.

This restoration is unnecessary for the files which have not been backed up.

Copy the file from the backup location.

```
# cp -p $BAK_DIR/etc/opt/FJSVssmgr/current/polling/*.xml /etc/opt/FJSVssmgr/current/polling/
```

10. Restore the files related to copy group and copy pair definitions.

Perform this step only if you are using the AdvancedCopy function.

Delete the subdirectories and files belonging to the restore destination directory.

```
rm -rf /etc/opt/FJSVccm/db/cg/*
rm -f /etc/opt/FJSVccm/prop/user.properties
rm -f /etc/opt/FJSVccm/acc/etc/stxc.alias
rm -f /etc/opt/FJSVccm/acc/etc/stxc_ext.alias
rm -f /etc/opt/FJSVccm/acc/etc/stxcvolinf
```

Copy the subdirectories and files from the backup location.

```
cp -p $BAK_DIR/CCM/etc/db/eternus.xml /etc/opt/FJSVccm/db
cp -p $BAK_DIR/CCM/var/micc/database/DeviceRegList.xml /var/opt/FJSVccm/micc/database
cp -p $BAK_DIR/CCM/etc/prop/user.properties /etc/opt/FJSVccm/prop
cp -p $BAK_DIR/CCM/etc/stxc.alias /etc/opt/FJSVccm/acc/etc
cp -p $BAK_DIR/CCM/etc/stxc_ext.alias /etc/opt/FJSVccm/acc/etc
cp -p $BAK_DIR/CCM/etc/stxcvolinf /etc/opt/FJSVccm/acc/etc
cp -Rp $BAK_DIR/CCM/etc/db/cg/* /etc/opt/FJSVccm/db/cg
```

11. Restore the license management database.

Execute the following command. For <filename>, input the file name which was specified when the backup data was created.

```
/opt/FJSVesflm/bin/esflm restore $BAK_DIR/LM/<filename>
```

12. Restore the files associated with the Reporting function. (For Reporting Function only)

If the files associated with the Reporting function are not backed up, this procedure is not needed.

Delete the subdirectories and files belonging to the restore destination directory.

However, be sure not to delete the restore destination directory itself. If the restore destination directory itself does not exist, create one.

```
rm -f /etc/opt/FJSVesfcm/conf/report/*
rm -f /etc/opt/FJSVesfcm/conf/scheduler/*
rm -rf /var/opt/FJSVesfcm/report/*
```

Copy the subdirectories and files from the backup location.

```
cp -p $BAK_DIR/etc/opt/FJSVesfcm/conf/report/* /etc/opt/FJSVesfcm/conf/report/
cp -p $BAK_DIR/etc/opt/FJSVesfcm/conf/scheduler/* /etc/opt/FJSVesfcm/conf/scheduler/
cp -Rp $BAK_DIR/var/opt/FJSVesfcm/report/* /var/opt/FJSVesfcm/report/
```

13. Restore the Optimization Option environment. (For Optimization Option only)

Delete the subdirectories and files belonging to the restore destination directory.

However, be sure not to delete the restore destination directory itself. If the restore destination directory itself does not exist, create one.

```
rm -f /etc/opt/FJSVssast/data/policy/TierPolicy.xml
rm -f /etc/opt/FJSVssast/data/pool/*
rm -rf /var/opt/FJSVssast/data/perf/*
```

Copy the subdirectories and files from the backup location.

```
cp -p $BAK_DIR/etc/opt/FJSVssast/data/policy/TierPolicy.xml /etc/opt/FJSVssast/data/policy/
cp -p $BAK_DIR/etc/opt/FJSVssast/data/pool/* /etc/opt/FJSVssast/data/pool/
cp -Rp $BAK_DIR/var/opt/FJSVssast/data/perf/* /var/opt/FJSVssast/data/perf/
```

14. Restore the Quality of Service Management Option environment. (For Quality of Service Management Option only)

Delete the subdirectories and files belonging to the restore destination directory.

However, be sure not to delete the restore destination directory itself. If the restore destination directory itself does not exist, create one.

```
rm -f /etc/opt/FJSVesfcm/conf/qos/*
```

Copy the subdirectories and files from the backup location.

```
cp -p $BAK_DIR/etc/opt/FJSVesfcm/conf/qos/* /etc/opt/FJSVesfcm/conf/qos/
```

15. Execute the following shell script to start ETERNUS SF Manager services.

```
/opt/FJSVesfcm/bin/startesf.sh
```

10.1.1.3.2 Restoring Solaris OS Manager (cluster environment)

For cluster environment, follow the procedure below to restore the environment for the Storage Cruiser's manager.

For restoration after reinstalling Manager, be sure to complete installation and setup before restoration. Refer to "Customization for Management Server Transaction" in the *ETERNUS SF Cluster Environment Setup Guide* for installation and setup.

1. Stop all cluster transaction which the Manager belongs to.

Refer to "Cluster transaction and local transaction" in the *ETERNUS SF Cluster Environment Setup Guide* for details of cluster transaction.

2. Mount the shared disk on the primary node.

3. Start the ETERNUS SF Manager Postgres service.

Execute the following command to start the ETERNUS SF Manager Postgres service:

```
/etc/init.d/startSFmanager start-postgres
```

4. Perform steps 3 and step 5 to 14 of "[10.1.1.3.1 Restoring Solaris OS Manager](#)" on the primary node.

5. Stop the ETERNUS SF Manager Postgres service.

Execute the following command to stop the ETERNUS SF Manager Postgres service:

```
/etc/init.d/startSFmanager stop-postgres
```

6. Unmount the shared disk mounted in step 2.

7. Start all cluster transactions which the Manager belongs to.

10.1.1.3.3 Restoring Linux Manager

Since the procedure for restoring the Linux version of Manager is identical to that for restoring the Solaris OS versions, refer to "[10.1.1.3.1 Restoring Solaris OS Manager](#)" for performing this operation.

10.1.1.3.4 Restoring Linux Manager (cluster environment)

Since the procedure for restoring the Linux version of Manager is identical to that for restoring the Solaris OS versions in cluster environment, refer to "[10.1.1.3.2 Restoring Solaris OS Manager \(cluster environment\)](#)" for performing this operation.

10.1.1.3.5 Restoring Windows Manager

Follow the procedure below to restore the environment for Storage Cruiser's manager.

For restoration after reinstalling Manager, be sure to complete installation and setup before restoration. Refer to "Installing ETERNUS SF Manager" and "Setting Up ETERNUS SF Manager" in the *ETERNUS SF Installation and Setup Guide* for the installation and setup procedures.

Information

About description in the procedure

- \$BAK_DIR means the backup destination directory.
- \$INS_DIR means "Program Directory" specified at the ETERNUS SF Manager installation.
- \$ENV_DIR means "Environment Directory" specified at the ETERNUS SF Manager installation.
- \$TMP_DIR means "Work Directory" specified at the ETERNUS SF Manager installation.

1. Re-setup Storage Cruiser's manager.

Install ETERNUS SF Manager and set it up as Storage Cruiser's manager.

Refer to "Installing ETERNUS SF Manager" and "Setting Up ETERNUS SF Manager" in the *ETERNUS SF Installation and Setup Guide* for installation and setup procedures.

2. Stop the ETERNUS SF Manager Tomcat Service.

Open the Service Control Manager and stop the following service.

- ETERNUS SF Manager Tomcat Service

3. Restore the backup data.

Execute the following command. Specify the default value 15432 to *<port-number>*, however, if you have changed the port number, specify the changed port number to *<port-number>*.

```
$INS_DIR\Common\sys\postgres\bin\psql -U esfpostgres -p <port-number> postgres
```

A prompt is displayed, with the server awaiting input. Input the following keywords in the sequence shown below.

```
master01!  
drop database esfdb;  
\q
```

Execute the following command to restore the backup data. Specify the default value 15432 to *<port-number>*, however, if you have changed the port number, specify the changed port number to *<port-number>*. For *<filename>*, input the file name which was specified when the backup data was created.

```
$INS_DIR\Common\sys\postgres\bin\psql -U esfpostgres -p <port-number>  
-f $BAK_DIR\Common\<filename> postgres
```

A prompt is displayed, with the server awaiting input. Input the following keyword.

```
master01!
```

4. Execute the following batch to stop the ETERNUS SF Manager services.

```
$INS_DIR\Common\bin\Stop_ESFservice.bat
```

 **Note**

Upon executing the batch, multiple messages stating that the ETERNUS SF Manager Tomcat Service has already been stopped will be displayed. These messages do not pose a problem and can be ignored.

5. Restore the files related to the performance management function.

This step can be skipped if you are not using the performance management function or the files related to the performance management function are not backed up.

Using Explorer or a similar program, delete the subdirectories and files belonging to the following restore destination directory.

However, be sure not to delete the restore destination directory itself. If the restore destination directory itself does not exist, create it.

- \$TMP_DIR\ESC\Manager\var\opt\FJSVssmgr\current\perf

Using Explorer or a similar program, copy the following file from its backup location.

Copy Source File	Copy Destination Directory
\$BAK_DIR\ESC\Manager\etc\opt\FJSVssmgr\current\perf.conf	\$ENV_DIR\ESC\Manager\etc\opt\FJSVssmgr\current

Using Explorer or a similar program, copy the subdirectories and files belonging to the following directory from their backup location.

Copy Source Directory	Copy Destination Directory
\$BAK_DIR\ESC\Manager\var\opt\FJSVssmgr\current\perf	\$TMP_DIR\ESC\Manager\var\opt\FJSVssmgr\current\perf

6. Restore the other files which can be customized.

This restoration is unnecessary for the files or the directories which have not been backed up.

Using Explorer or a similar program, copy the following files from the backup locations.

Copy Source File	Copy Destination Directory
\$BAK_DIR\ESC\Manager\etc\opt\FJSVssmgr\current\sanma.conf	\$ENV_DIR\ESC\Manager\etc\opt\FJSVssmgr\current
\$BAK_DIR\ESC\Manager\etc\opt\FJSVssmgr\current\ssmgr.conf	
\$BAK_DIR\ESC\Manager\etc\opt\FJSVssmgr\current\trapop.bat	
\$BAK_DIR\ESC\Manager\etc\opt\FJSVssmgr\current\traprm.bat	

Using Explorer or a similar program, copy the subdirectories and files belonging to the following directory from their backup location.

Copy Source Directory	Copy Destination Directory
\$BAK_DIR\ESC\Manager\etc\opt\FJSVssmgr\current\eventmail	\$ENV_DIR\ESC\Manager\etc\opt\FJSVssmgr\current\eventmail

7. Restore the SNMP Trap XML definition files.

This restoration is unnecessary for the files which have not been backed up.

Using Explorer or a similar program, copy the SNMP Trap XML definition files from their backup location.

Copy Source File	Copy Destination Directory
\$BAK_DIR\ESC\Manager\etc\opt\FJSVssmgr\current\snmph*.xml	\$ENV_DIR\ESC\Manager\etc\opt\FJSVssmgr\current\snmph

8. Restore the device polling setting files.

This restoration is unnecessary for the files which have not been backed up.

Using Explorer or a similar program, copy the device polling setting file from its backup location.

Copy Source File	Copy Destination Directory
\$BAK_DIR\ESC\Manager\etc\opt\FJSVssmgr\current\devicepolling\DP_config.xml	\$ENV_DIR\ESC\Manager\etc\opt\FJSVssmgr\current\devicepolling

9. Restore the polling service setting file.

This restoration is unnecessary for the files which have not been backed up.

Using Explorer or a similar program, copy the polling service setting file from its backup location.

Copy Source File	Copy Destination Directory
\$BAK_DIR\ESC\Manager\etc\opt\FJSVssmgr\current\polling\pollingService.xml	\$ENV_DIR\ESC\Manager\etc\opt\FJSVssmgr\current\polling

10. Restore the registry.

Using Explorer or a similar program, copy the following files from their backup location.

Copy Source File	Copy Destination Directory
\$BAK_DIR\ACM\etc\swnode.ini	\$ENV_DIR\ACM\etc
\$BAK_DIR\ACM\etc\device.ini	

11. Restore the files related to copy group and copy pair definitions.

Perform this step only if you are using the AdvancedCopy function.

Using Explorer or a similar program, delete the files belonging to the following restore destination directory.

- \$ENV_DIR\CCM\etc\db\cg

Delete the following files if they exist.

- \$ENV_DIR\CCM\etc\prop\user.properties
- \$ENV_DIR\CCM\etc\stxc.alias
- \$ENV_DIR\CCM\etc\stxc_ext.alias
- \$ENV_DIR\CCM\etc\stxcvolinf

Using Explorer or a similar program, copy the following files from their backup locations.

Copy Source File	Copy Destination Directory
\$BAK_DIR\CCM\etc\db\eternus.xml	\$ENV_DIR\CCM\etc\db
\$BAK_DIR\CCM\var\micc\database\DeviceRegList.xml	\$TMP_DIR\CCM\var\micc\database

If copy source files exist, copy the following files from the backup location using Explorer or a similar program.

Copy Source File	Copy Destination Directory
\$BAK_DIR\CCM\etc\prop\user.properties	\$ENV_DIR\CCM\etc\prop
\$BAK_DIR\CCM\etc\stxc.alias	\$ENV_DIR\CCM\etc

Copy Source File	Copy Destination Directory
\$BAK_DIR\CCM\etc\stxc_ext.alias	
\$BAK_DIR\CCM\etc\stxcvolinf	

Using Explorer or a similar program, copy the files belonging to the following directory from their backup location.

Copy Source Directory	Copy Destination Directory
\$BAK_DIR\CCM\etc\db\cg	\$ENV_DIR\CCM\etc\db\cg

12. Restore the license management database.

Execute the following command. For <filename>, input the file name which was specified when the backup data was created.

```
$INS_DIR\LM\bin\esflm restore $BAK_DIR\LM\<filename>
```

13. Restore the files associated with the Reporting function. (For Reporting Function only)

If the files associated with the Reporting function are not backed up, this procedure is not needed.

Delete the subdirectories and files belonging to the restore destination directory.

However, be sure not to delete the restore destination directory itself. If the restore destination directory itself does not exist, create one.

- \$TMP_DIR\Common\var\report

Copy the files under the following directories from the backup location using Explorer or the like:

Copy Source Directory	Copy Destination Directory
\$BAK_DIR\Common\etc\report	\$ENV_DIR\Common\etc\report
\$BAK_DIR\Common\etc\scheduler	\$ENV_DIR\Common\etc\scheduler

Copy the files under the following directory from the backup location using Explorer or the like:

Copy Source Directory	Copy Destination Directory
\$BAK_DIR\Common\var\report	\$TMP_DIR\Common\var\report

14. Restore the Optimization Option environment. (For Optimization Option only)

Delete the subdirectories and files belonging to the restore destination directory.

However, be sure not to delete the restore destination directory itself. If the restore destination directory itself does not exist, create one.

- \$TMP_DIR\AST\Manager\var\opt\FJSVssast\data\perf

Using Explorer or a similar program, copy the following files from their backup locations.

Copy Source File	Copy Destination Directory
\$BAK_DIR\AST\Manager\etc\opt\FJSVssast\data\policy\TierPolicy.xml	\$ENV_DIR\AST\Manager\etc\opt\FJSVssast\data\policy

Using Explorer or a similar program, copy the subdirectories and files belonging to the following directory from their backup location.

Copy Source Directory	Copy Destination Directory
\$BAK_DIR\AST\Manager\etc\opt\FJSVssast\data\pool	\$ENV_DIR\AST\Manager\etc\opt\FJSVssast\data\pool
\$BAK_DIR\AST\Manager\var\opt\FJSVssast\data\perf	\$TMP_DIR\AST\Manager\var\opt\FJSVssast\data\perf

15. Restore the Quality of Service Management Option environment. (For Quality of Service Management Option only)

Copy the files under the following directories from the backup location using Explorer or the like:

Copy Source Directory	Copy Destination Directory
\$BAK_DIR\Common\etc\qos	\$ENV_DIR\Common\etc\qos

16. Execute the following batch to start ETERNUS SF Manager services.

```
$INS_DIR\Common\bin\Start_ESFservice.bat
```

10.1.1.3.6 Restoring Windows Manager (cluster environment)

For cluster environment, follow the procedure below to restore the environment for the Storage Cruiser's manager.

For restoration after reinstalling Manager, be sure to complete installation and setup before restoration. Refer to "Installing ETERNUS SF Manager" and "Customization for Management Server Transaction" in the *ETERNUS SF Cluster Environment Setup Guide* for installation and setup.

1. Stop all cluster transactions which the Manager belongs to.

Refer to "Cluster transaction and local transaction" in the *ETERNUS SF Cluster Environment Setup Guide* for details of cluster transaction.

2. Mount the shared disk on the primary node.

3. Start the ETERNUS SF Manager Postgres service.

Open Service Control Manager to start the following service:

- ETERNUS SF Manager Postgres Service

4. Perform steps 3 and step 5 to 15 of "[10.1.1.3.5 Restoring Windows Manager](#)" on the primary node.

Directory description in "[10.1.1.3.5 Restoring Windows Manager](#)" are replaced to the following directories.

- \$BAK_DIR means the backup destination directory.
- \$INS_DIR means "Program Directory" specified at the ETERNUS SF Manager installation.
- \$ENV_DIR means "Environment Directory" specified at the ETERNUS SF Manager installation.
- \$TMP_DIR means "Work Directory" specified at the ETERNUS SF Manager installation.

5. Stop the ETERNUS SF Manager Postgres service.

Open Service Control Manager to stop the following service:

- ETERNUS SF Manager Postgres Service

6. Unmount the shared disk mounted in step 2.

7. Start all cluster transactions which the Manager belongs to.

10.1.2 Changing the operating environment

10.1.2.1 Changing the IP address of the Management Server

Refer to "Changing the IP Address of Management Server" in the *ETERNUS SF AdvancedCopy Manager Operation Guide*.

10.1.2.2 Changing the IP address of a server node (host)

Follow the procedure given below to change the IP address of a server node.

- Changing the IP address of a server node for which Agent is installed
 1. Change the system IP address on the server node.
 2. Stop the server node Agent on the server node.
 3. Execute the agent information change command on the server node to change the start IP of server node Agent.
Refer to "Agent information change command" in "[Chapter 12 Command References](#)" for detailed information of the agent information change command.
 4. Restart the server node Agent on the server node.
 5. Change the IP address of the server node from the Web Console.
- Changing the IP address of a VM host for which Agent is not installed
 1. Change the IP address of the VM host.
 2. Change the IP address information of the VM host from the Web Console.
- Changing the IP address of a guest operating system for which Agent is not installed
 1. Change the IP address of the guest operating system.
 2. Change the IP address information of the VM guest from the Web Console.



Point

.....

Refer to "Changing the IP address of Managed Server" in the *ETERNUS SF AdvancedCopy Manager Operation Guide* when you install the AdvancedCopy Manager's agent in a server node.

.....

10.1.2.3 Changing the server name of the Management Server

Refer to "Changing the server name of Management Server transaction or Managed Server transaction" in the *ETERNUS SF AdvancedCopy Manager Operation Guide*.

10.1.2.4 Changing the name of a server node (host)

Follow the procedure given below to change the name of a server node.

- Changing the name of a server node on which the Agent is installed
 1. Change the server node name on the server node.
 2. Stop the server node Agent on the server node.
 3. Execute the agent information change command on the server node to change the setting of server node Agent.
Refer to "Agent information change command" in "[Chapter 12 Command References](#)" for detailed information of the agent information change command.
 4. Restart the server node Agent on the server node.
 5. Using the Web Console, perform [Reload Conf.] on the server node.
- Changing the host name of a VM host on which an Agent is not installed
 1. Change the host name of the VM host.
 2. Using the Web Console, perform [Reload of setting] for the VM host.
- Changing the virtual machine name of a VM guest or the host name of a guest operating system, on which an Agent is not installed
 1. Change the virtual machine name of the VM guest or the host name of a guest operating system.
 2. Using the Web Console, perform [Reload Conf.] for the VM host that has the target VM guest.

Point

Refer to "Changing the server name of Management Server transaction or Managed Server transaction" in the *ETERNUS SF AdvancedCopy Manager Operation Guide* when you install the AdvancedCopy Manager's agent in a server node.

10.1.2.5 Changing the IP address or the SNMP Community name of a supported device

To change the IP address of a device with support level A or B registered with this software or to change the SNMP Community name (for reading), follow the procedure below:

1. Change the IP address or the SNMP Community name of each target device.
2. Record the settings of threshold monitoring. (if thresholds are monitored)
3. Change the IP address or the SNMP Community name of the target device using the Web Console.
4. Based on the settings at step 2, start to monitor thresholds. (if thresholds are monitored)

See

Refer to "[Chapter 4 Environment Configuration](#)" for the SNMP Community name of each target device.

Note

To change the SNMP Trap community name at a Linux Manager, refer to "[A.10 snmptrapd.conf Configuration File](#)" and also change the snmptrapd.conf settings.

10.1.2.6 Changing the operation management of the clustered system (node name takeover)

Refer to "Changing the IP address of Management Server" in the *ETERNUS SF AdvancedCopy Manager Operation Guide*.

10.1.2.7 Changing the configuration of supported devices

For changing the device configuration

If the following change, the update of the set up information is needed in the support device:

- Upgrade of firmware with support device
- Configuration change by increase/decrease of hardware (in case of storage device, its CM, port, etc.)
- Addition/deletion/change in composition (in the case of a disk storage system, its RAID Group, LogicalVolume, etc.) in device

Method of updating set up information is as follows:

- Execute [Reload Conf.] for the relevant device to update the information for the target device.
- Update the configuration information of the performance management function by referring to "[7.2.9 Updating configuration information](#)". (Only when you are using the performance management function)

For applying Model upgrade options for ETERNUS Disk storage system

The device configuration is changed when applying Model upgrade options for ETERNUS Disk storage system. Perform the following operation after applying Model upgrade options for ETERNUS Disk storage system.

Before Applying Model Upgrade Options	After Applying Model Upgrade Options	Operation
ETERNUS DX60	ETERNUS DX80	Perform the procedure of "Operation on Model upgrade for ETERNUS DX60 to ETERNUS DX80, for ETERNUS DX80 S2 to ETERNUS DX90 S2, for ETERNUS DX410 S2 to ETERNUS DX440 S2" in the <i>ETERNUS SF Web Console Guide</i> . When using the performance management function, update the configuration information of the performance management function in reference to " 7.2.9 Updating configuration information " after performing the procedure above.
ETERNUS DX80 S2	ETERNUS DX90 S2	
ETERNUS DX410 S2	ETERNUS DX440 S2	
ETERNUS DX80 S2/DX90 S2	ETERNUS DX410 S2/DX440 S2	Perform the procedure of "Operation on Model upgrade for ETERNUS DX80 S2 or ETERNUS DX90 S2 to ETERNUS DX410 S2 or ETERNUS DX440 S2" in the <i>ETERNUS SF Web Console Guide</i> .

10.1.2.8 Changing the password of supported devices

Change the passwords for the following devices registered to this product to take the following conduction:

Objected Device	Conduction
ETERNUS SN200 series (Brocade) Fibre Channel switch PRIMERGY fibre channel switch blade	Change the account information for management of the device in the Web Console.
Brocade VDX series PRIMERGY BX Ethernet Fabric Switch	
VMware vSphere 4 or later	
ETERNUS DX series	

Except for the devices described above, there is no necessary to do any deal with this software when change the device's password.

10.2 [Solaris OS Version] Maintenance of Agent

10.2.1 Action to take for troubleshooting

Provided are the main examples for problems and their troubleshooting methods.

- If a new HBA has been added and the agent detected an environment error (during a time besides replacement of the HBA)
It is possible the server node has not started up in re-configuration mode after the HBA was added. In this sort of situation, restart the node in re-configuration mode.
- If a new HBA driver has been installed and the agent has detected an environment error
It is possible the server node was not started up in re-configuration mode after the installation of the driver. In this sort of situation, restart the node in re-configuration mode.

10.2.2 Collecting data for troubleshooting

If any problem occurs in Agent, collect troubleshooting information according to "[B.1 Collecting the troubleshooting information](#)".

10.2.3 Changing the administrative environment

10.2.3.1 Changing the IP address of a server node (host)

Refer to "[10.1.2.2 Changing the IP address of a server node \(host\)](#)" for detail.

10.3 [Windows Version] Maintenance of Agent

10.3.1 Action to take for troubleshooting

Major errors related to Agent running on a Windows Server 2003 server node and the corrective action to be taken are explained below. In the Event viewer or the GUI window, confirm the occurrence of the errors described below.

Manager cannot detect Agent.

- If all access paths under multipath control have been deleted by mistake, follow the recovery procedure given below.
 - Restart the Windows server node.
After an access path is deleted, multipath control no longer controls the path, and the related device is not recognized.
 - For the respective devices deleted by mistake on the access path, execute [Reload Conf.].
 - Set the access path that was deleted by mistake.
- Too many devices are connected to the Windows server node.
If too many devices are recognized by the Windows server node, Agent cannot perform processing within the response time, leading to a communication failure. In this event, check the connection configuration, and reduce the number of devices recognized by the Windows server node.
Access paths can be set for approximately 100 devices per one Windows server node, but the number of devices varies depending on the server node environment.

The GUI window contents differ from the physical configuration.

- An access path from an Emulex HBA cannot be drawn.
The Topology value in a driver parameter in the registry may be incorrect.
This caused by values in the registry being reset to default values, which occurs at either of the times: when a driver is re-installed; and when a driver is automatically re-installed because of the installation a new HBA having a different model number from that of a HBA already installed in a Windows Server 2003 machine (e.g., LP9802 and LP1050).
Using the registry editor, check the driver parameters of the HBA, correct any incorrect value that you find, and then select [Reload Conf.].
Refer to "[4.1.2 Windows server node](#)" for information about driver parameters.

10.3.2 Collecting data for troubleshooting

If any problem occurs in Agent, collect troubleshooting information according to "[B.1 Collecting the troubleshooting information](#)".

10.3.3 Changing the administrative environment

10.3.3.1 Changing the IP address of a server node (host)

Refer to "[10.1.2.2 Changing the IP address of a server node \(host\)](#)" for detail.

10.4 [Linux Version] Maintenance of Agent

10.4.1 Collecting data for troubleshooting

If any problem occurs in Agent, collect troubleshooting information according to "[B.1 Collecting the troubleshooting information](#)".

10.4.2 Changing the administrative environment

10.4.2.1 Changing the IP address of a server node (host)

Refer to "[10.1.2.2 Changing the IP address of a server node \(host\)](#)" for detail.

10.5 [HP-UX Version] Maintenance of Agent

10.5.1 Collecting data for troubleshooting

If any problem occurs in Agent, collect troubleshooting information according to "[B.1 Collecting the troubleshooting information](#)".

10.5.2 Changing the administrative environment

10.5.2.1 Changing the IP address of a server node (host)

Refer to "[10.1.2.2 Changing the IP address of a server node \(host\)](#)" for detail.

10.6 [AIX Version] Maintenance of Agent

10.6.1 Collecting data for troubleshooting

If any problem occurs in Agent, collect troubleshooting information according to "[B.1 Collecting the troubleshooting information](#)".

10.6.2 Changing the administrative environment

10.6.2.1 Changing the IP address of a server node (host)

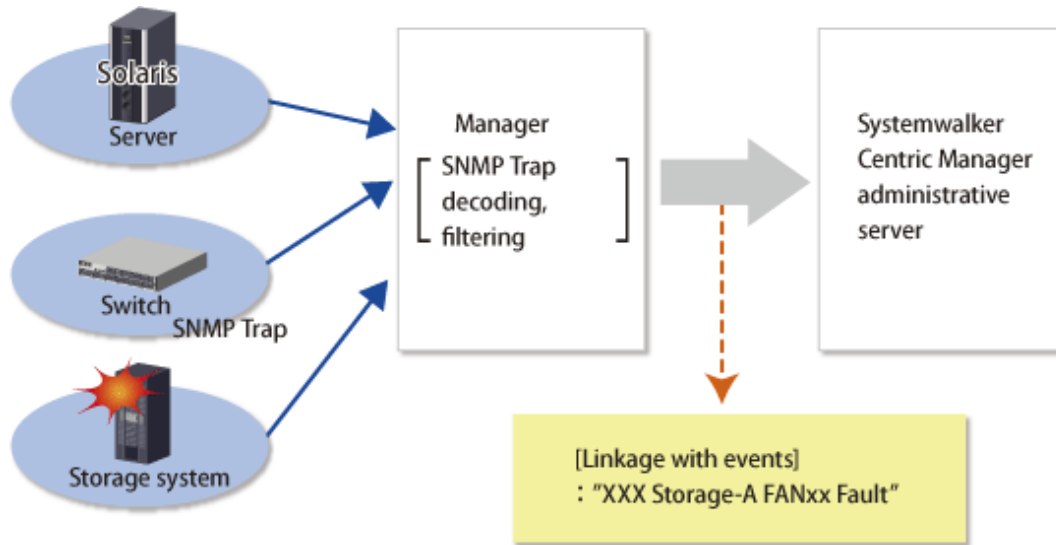
Refer to "[10.1.2.2 Changing the IP address of a server node \(host\)](#)" for detail.

Chapter 11 Linkage to Other Software

This chapter describes the operating methods conducting centralized administration in Systemwalker Centric Manager and other administrative software.

11.1 Linkage with Systemwalker Centric Manager

Linkage with Systemwalker Centric Manager enables it to be used for centralized monitoring of storage devices. In addition, linkage through window operations enables smooth troubleshooting of storage devices.



Note

Event Linkage is done not through the system log or event log on the operating system.

11.1.1 Linkage function with Systemwalker Centric Manager

Centralized event monitoring

Icons of the devices managed by this software are displayed in the monitoring window of the Systemwalker Centric Manager administrative client.

When an SNMP Trap is received from a monitored device, this software obtains only an event related to a fault and decodes it appropriately. This event is sent to Systemwalker Centric Manager to display the event. As a result, Systemwalker Centric Manager can be used to integrate existing server node management and storage device monitoring of this software. Moreover, functions such as Systemwalker Centric Manager e-Mail and pager can then be used for fault monitoring of the server node and storage devices.

By directly managing the storage equipment from Systemwalker Centric Manager, easier setup is achieved and more comprehensible troubleshooting reports are produced.

The icon for a device where a fault has occurred is indicated by "X" in Systemwalker Centric Manager, and information about the fault is displayed as event contents. When the event content is checked and action is taken for the fault, "Action" will be marked for the event. This operation clears the "X" state. The "X" state is not restored automatically by recovery from the fault.

"SSC" is indicated in the message for an event linked by this function to Systemwalker Centric Manager.

Linkage through window operations

On the Systemwalker Centric Manager monitoring window, select a menu item that was added to this software from the pop-up menu of a node of the faulty storage device, and then start it. This facilitates troubleshooting of the faulty storage device.

11.1.2 Required versions

Linkage of Systemwalker Centric Manager with this software requires one of the following versions of Systemwalker Centric Manager:

- Solaris OS , Linux
SystemWalker Centric Manager GEE V11 or later
SystemWalker Centric Manager-M EE/SE V11 or later
- Windows
SystemWalker Centric Manager-M EE/SE V11 or later

11.1.3 Preparations

Preparations for linkage of Systemwalker Centric Manager with this software are described below.

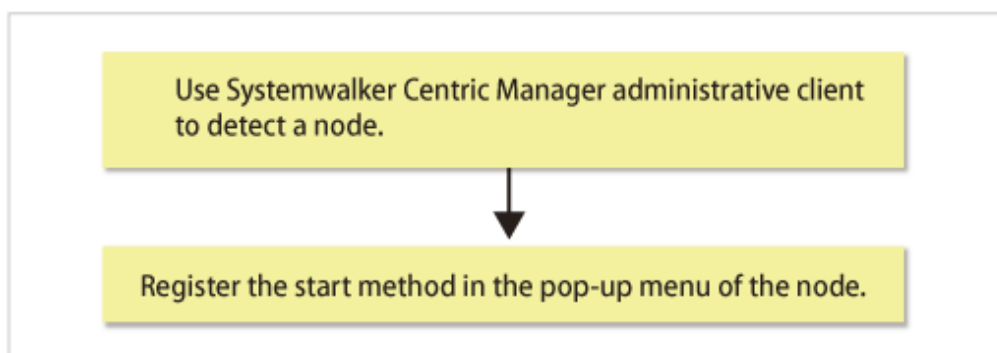
- Register the storage devices to be managed with this software before setting up a link with Systemwalker Centric Manager.
- So that the names of the devices registered in this software can be resolved, either register the IP address and host name information for each device in the DNS server that is referenced by the Management Server, or define them in the `/etc/hosts` file on the Management Server.
- To detect node names and achieve software linkage, the Systemwalker Centric Manager administrative server and the Management Server of this software should both be managed by the DNS server, and have the same `/etc/hosts` definition. Confirm the settings.
- The Systemwalker Centric Manager administrative server must be the same server, or Systemwalker Centric Manager Agent must be installed on the Management Server of this software.
Also, the Systemwalker Centric Manager administrative server or Systemwalker Centric Manager Agent on the same server must be operating during the linkage operation.

11.1.4 Setup procedure

Follow the procedure below on the Systemwalker Centric Manager operation management client.

Log in to the administrative client with a user name belonging to the Administrators group of the local group.

11.1.4.1 Setup on Systemwalker Centric Manager administrative client



1. On the Systemwalker Centric Manager administrative client, perform the procedure to detect a node in a subnet that contains storage devices.

2. Register the window start method in the pop-up menu of the node.

Register the start method of this software in the pop-up menu of the node of the storage device, using the Systemwalker Centric Manager mpapreg command.

The example below uses "ESC" as the menu name and "server1" as the server node name. Change these names according to the environment if necessary.

```
mpapreg -a -m ESC -p server1 -c "\"<Web browser execution path>\" \"https://<IP-address>:<port_number>/\""
```

- For <Web browser execution path>

- If using Internet Explorer:

- Specify the absolute path of iexplore.exe.

- If using Firefox:

- Specify the absolute path of firefox.exe.

- For <IP-address>

- Specify the IP address or Fully Qualified Domain Name (FQDN) of the Management Server.

- For <port_number>

- Specify the port number of "Web Console service (ETERNUS SF Manager Apache service)" specified when installing this software. Default is 9855.

Enclose the entire start command (-c option value) specified with the mpapreg command within double quotation marks ("), and enclose the start command (C:\Program Files\...\rcxclient.exe) with [\"] and [\\].

Note

- The operating environment must be set up in such a way that the Management Server recognizes the association between "Name" and "IP" in case that Systemwalker Centric Manager detects the server node by "Name", but not "IP". Please confirm that the name is registered in /etc/hosts or on the DNS server. Software linkage from this software to Systemwalker Centric Manager will fail if the Management Server does not recognize the association between an IP number and a node name.
- Perform this operation each time a new storage device is added.
- When the event that is displayed as Info in the status item of the event log window is reported to Systemwalker Centric Manager, it is regarded as "Display Mode: general" and is not displayed on the monitoring window. If you want to display it, execute [Display Mode in the Monitored Viewer] from **Action > Action Setting > Message** on the Systemwalker Centric Manager menu. Refer to the Systemwalker Centric Manager manual for details about [Display Mode in the Monitored Viewer].
- If the starting method of this software's Management Server is changed, execute the following command to delete the registered menu, and register it again. (In the example below, the menu name is "ESC.")

```
mpapreg -d -m ESC
```

- Confirm the content of registration by the following commands when the icon of this software is not displayed in the pop-up menu of the node though the menu addition by the mpapreg command has normally. (In the example below, the menu name is "ESC.")

```
mpapreg -v -m ESC
```

- After completing the procedure, restart the Systemwalker Centric Manager server of an administrative client, and execute "node detection" in the monitoring area. Updating of registered icons is enabled in the display.
- A parameter error (swsag5101) occurs if the mpapreg command contains an invalid parameter when starts from the batch file.

11.1.4.2 Action to be taken if Systemwalker Centric Manager administrative server and this software Management Server are the same server

If the Systemwalker Centric Manager administrative server and the Management Server of this software are the same server, both Systemwalker Centric Manager and this software receive and display SNMP Traps from devices. Perform the following task to prevent Systemwalker Centric Manager from directly receiving and displaying SNMP Traps from devices:

Suppressing Systemwalker Centric Manager reception of SNMP Traps from devices managed by this software

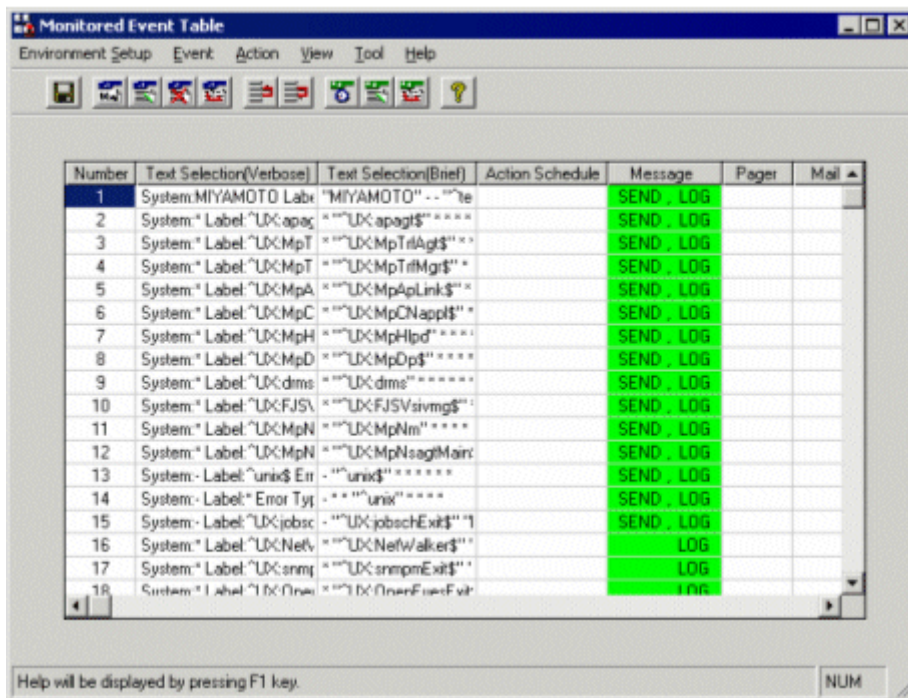
If one server node has the Systemwalker Centric Manager administrative server and Management Server of this software, the following steps prevent Systemwalker Centric Manager from direct reception of SNMP Traps of devices managed by this software. As a result, SNMP Traps would be received and decoded by this software and only SNMP Traps necessary for fault monitoring would be posted to Systemwalker Centric Manager. Consequently, when the SNMP Trap display function supported by Systemwalker Centric Manager is used, multiple traps appear for a single event or unnecessary SNMP Traps are displayed.

Information

These settings are not required if the Systemwalker Centric Manager-supported SNMP Trap display function is enabled.

1. From a Systemwalker Centric Manager administrative client, select [Event] - [Action Definition] in "System Monitoring."

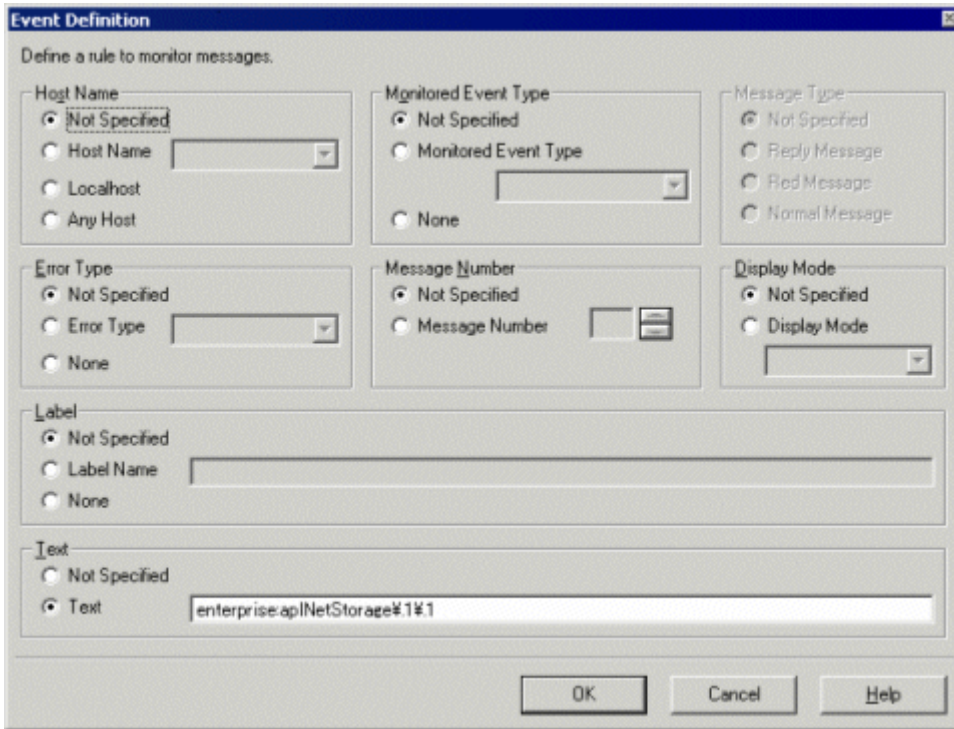
The Monitored Event Table dialog appears.



Number	Text Selection (Verbose)	Text Selection (Brief)	Action Schedule	Message	Pager	Mail
1	System:MIYAMOTO Label	"MIYAMOTO" - - "te		SEND LOG		
2	System: Label: ^UX: apoc	"^UX: apagt\$""		SEND LOG		
3	System: Label: ^UX: MpT	"^UX: MpTrAg\$""		SEND LOG		
4	System: Label: ^UX: MpT	"^UX: MpTrMgr\$""		SEND LOG		
5	System: Label: ^UX: MpA	"^UX: MpApLink\$""		SEND LOG		
6	System: Label: ^UX: MpC	"^UX: MpCNAppl\$""		SEND LOG		
7	System: Label: ^UX: MpH	"^UX: MpHpd\$""		SEND LOG		
8	System: Label: ^UX: MpD	"^UX: MpDp\$""		SEND LOG		
9	System: Label: ^UX: dims	"^UX: dims\$""		SEND LOG		
10	System: Label: ^UX: FJSV	"^UX: FJSVsvimg\$""		SEND LOG		
11	System: Label: ^UX: MpN	"^UX: MpNm\$""		SEND LOG		
12	System: Label: ^UX: MpN	"^UX: MpNsgtMainv		SEND LOG		
13	System: Label: ^unix\$ Err	"^unix\$""		SEND LOG		
14	System: Label: Error Typ	"^unix\$""		SEND LOG		
15	System: Label: ^UX: jobsc	"^UX: jobschExit\$""		SEND LOG		
16	System: Label: ^UX: NetV	"^UX: NetWalker\$""		LOG		
17	System: Label: ^UX: snmp	"^UX: snmpExit\$""		LOG		
18	System: Label: ^UX: Onse	"^UX: OnseFncExit\$"		LOG		

2. Select [Event] - [Event Addition] in the Monitored Event Table dialog.

The Event Definition dialog appears.



Define the following items:

Host Name

Check "Not specified".

Monitored Event Type

Check "Not specified".

Error Type

Check "Not specified".

Message Number

Check "Not specified".

Display Mode (only for Systemwalker Centric Manager 5.1 or later)

Check "Not specified".

Label

Check "Not specified".

Text

Specify one of the values shown below for an event definition.

Be sure to define this item only when individual devices are being managed. Otherwise, the item need not be defined.

Table 11.1 Lists of text

Device	Value
ETERNUS DX series	enterprise:aplNetStorage\.1 or enterprise:enterprises\.211\.4\.1\.1\.126\.1 (*1)
ETERNUS LT20 (SCSI)	enterprise:enterprises\.11\.2\.36\.1
ETERNUS LT20/LT20 S2/LT40/LT40 S2/LT60/LT60 S2 (SAS/FC)	enterprise:enterprises\.20884\.10893\.2\.101\.3

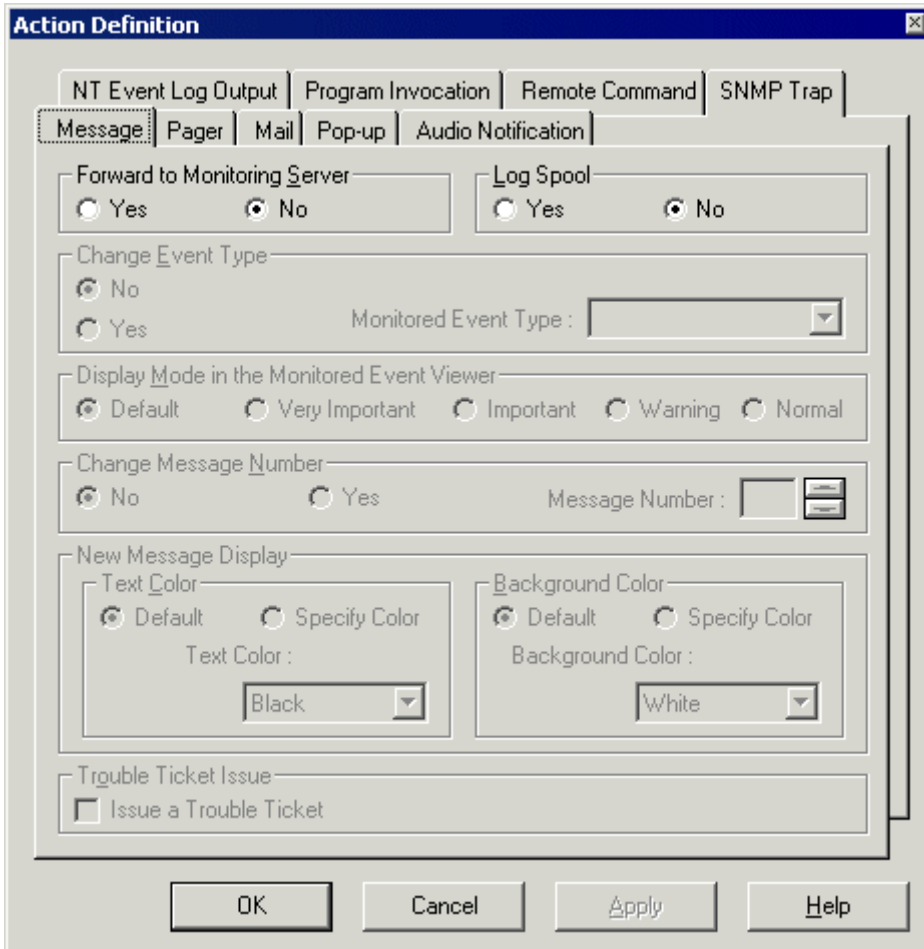
Device	Value
HP Surestore	enterprise:enterprises\.11\2\3\9\7\1 enterprise:enterprises\.11\2\3\9\7\2
ETERNUS LT200	enterprise:enterprises\.119\1\83\1\21
ETERNUS LT210/LT220/LT230	enterprise:enterprises\.119\1\83\1\1 enterprise:enterprises\.119\1\83\1\2
ETERNUS LT250	enterprise:aplNetStorage\3\5 or enterprise:enterprises\.211\4\1\1\126\3\5 (*1)
ETERNUS LT270	enterprise:aplNetStorage\3\2 or enterprise:enterprises\.211\4\1\1\126\3\2 (*1)
ETERNUS LT270 S2	enterprise:aplNetStorage\3\6 or enterprise:enterprises\.211\4\1\1\126\3\6 (*1)
NetApp FAS Series and V-Series	enterprise:enterprises\.789
Brocade Fibre Channel switch ETERNUS SN200 series Fibre Channel switch PRIMERGY Fibre Channel switch blade Brocade VDX series PRIMERGY BX Ethernet Fabric Switch	enterprise:enterprises\.1588\2\1\1
Performance Agent trap Device polling	enterprise:aplSANMgr or enterprise:enterprises\.211\4\1\3\21 (*1)
Brocade Fibre Channel switch, ETERNUS SN200 series Fibre Channel switch, PRIMERGY Fibre Channel switch blade common	enterprise:experimental\94 (*2)
ETERNUS VS850	enterprise:enterprises\2\6\190
ETERNUS CS2000	enterprise:enterprises\.231\2\48\2\0

*1: Specify it when Systemwalker Centric Manager cannot recognize "aplNetStorage" or "aplSANMgr".

*2: The device not supported with Storage Cruiser includes the device which reports on SNMP Trap of this experimental\94 and the event of those devices is controlled.

3. Select [Action] - [Action Setting] for the event set in step 2.

The Action Definition dialog appears.



Select the [Message] tab, and define the following items:

Forward to Monitoring Server

Check "No"

Log Spool

Check "No"

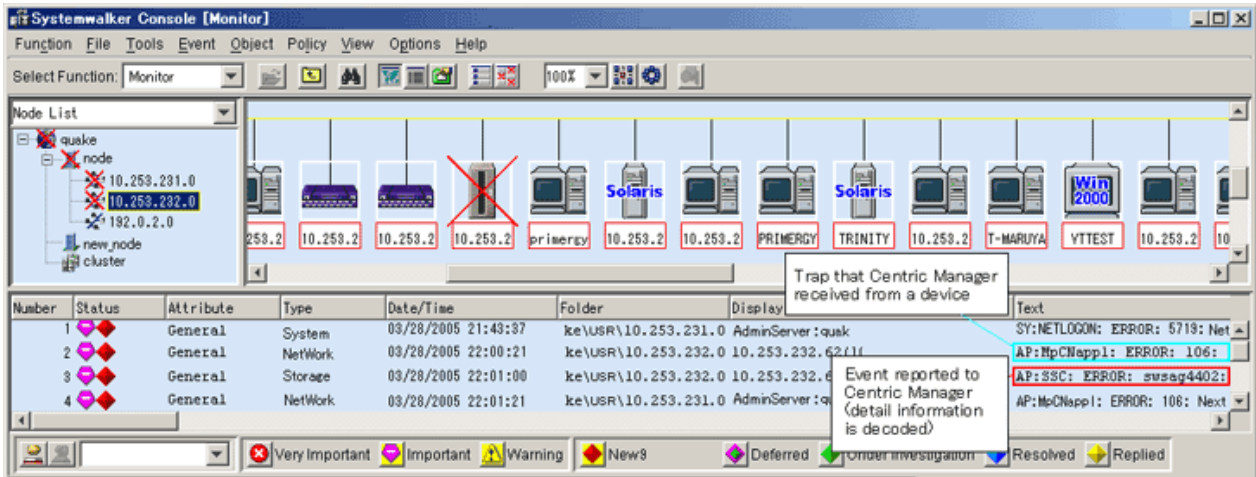
- Repeat steps 1 to 3 for each of the text messages in the "Table 11.1 Lists of text".

If the SNMP standard trap is reported as an event from a storage device, refer to the above description, and suppress transmission of the SNMP standard trap according to your operation mode.

11.1.4.3 Setting confirmation test

If the management device is an ETERNUS DX series or Fibre Channel switch device, a procedure and command are provided which allow you to check if the Systemwalker Centric Manager linkage is correctly set. Execute the "5.3 Checking Management Status" to check if it is properly running.

The figure below shows an example of the Systemwalker Centric Manager window displayed during event linkage with Systemwalker Centric Manager.



11.2 Linking with Systemwalker Service Quality Coordinator

Linkage with Systemwalker Service Quality Coordinator, Systemwalker Service Quality Coordinator can make use of performance information of storage devices and Fibre Channel switches.

Refer to the *Systemwalker Service Quality Coordinator User's Guide* or the *Systemwalker Service Quality Coordinator User's Guide* for the procedure for linkage.

Items that can be linked to Systemwalker Service Quality Coordinator

Fibre Channel switch

	Performance Information (Unit)
Port	Transfer rates of send/receive data (MB/S)
	Number of CRC errors

ETERNUS Disk storage systems

	Performance Information (Unit)
LUN LogicalVolume RAIDGroup	Read/Write count (IOPS)
	Read/Write data transfer rate (MB/S)
	Read/Write response time (msec)
	Read/Pre-fetch/Write cache hit rate (%)
Disk drive	Disk busy rate (%)
CM	Load (CPU usage) rate (%)

Note

- The performance information that can be managed depends on the version of Systemwalker Service Quality Coordinator.
- The CM load (CPU usage) rate for ETERNUS DX400/DX400 S2 series and ETERNUS DX8000/DX8000 S2 series includes the ROE load (CPU usage) rate.

11.3 Linkage with Other Administrative Software

Events can be sent to other administrative software.

The Shell/bat linkage function is used for such linkage. Refer to "[6.3 Event Display and Linkage](#)" for details.

Chapter 12 Command References

This chapter explains how to use commands.

12.1 Manager Commands

This section explains command operations on the Management Server for Solaris OS.

12.1.1 Commands for operating environment management

The following sub sections explain the commands for managing the operating environment.

12.1.1.1 sanadmsh chtraprcvip (SNMP Trap transmission place IP address change command)

NAME

sanadmsh chtraprcvip - changes SNMP Trap transmission place IP address

SYNOPSIS

```
sanadmsh chtraprcvip -h
```

```
sanadmsh chtraprcvip -all -oldip ol di paddr [-newip newi paddr]
```

```
sanadmsh chtraprcvip Devi ceID -oldip ol di paddr [-newip newi paddr]
```

COMMAND PATH

Windows environment

```
$INS_DIR\ESC\Manager\opt\FJSVssmgr\bin\sanadmsh chtraprcvip
```

(\$INS_DIR means "Program Directory" specified at the ETERNUS SF Manager installation.)

Solaris or Linux environment

```
/opt/FJSVssmgr/bin/sanadmsh chtraprcvip
```

DESCRIPTION

After the IP address of the Management Server is changed, delete the old IP address of the Management Server that is the SNMP Trap transmission place from the devices registered with this software, and add the new IP address.

In the Windows environment, only a user of the Administrators group can execute this command.

In the Solaris or Linux environment, only OS administrator (root) user can execute this command.

Although the SNMP Trap transmission place setting for a device may be changed with the Management Software on the device, this software provides this command to facilitate changing.

OPERANDS

DeviceID

Applies SNMP Trap transmission place setting to the limited devices. Specify the device type according to the following tables. Afterwards, specify how to recognize the device.

Device Type	Device Recognition Method
-host -storage -library -switch	One of which must be specified. - ip:IP address of a device - sysname:SysName name of a device SNMP setting

OPTIONS

-h

Displays help about the argument format of this command.

-all

Applies SNMP Trap transmission place setting to all devices managed by this software. Executing the command specified with this argument outputs device names and execution results in execution order to the standard output. If the Management Server has more than one IP address, for example, the Management Server is connected to multiple subnets, a device may not be set with the correct SNMP Trap transmission place. After this setting is performed, check whether the correct Management Server address is set as the SNMP Trap transmission place setting on the device side.

-oldip *oldipaddr*

Specify the old IP address of the Management Server for *oldipaddr*. Delete this IP address from the SNMP transmission place address of managed devices.

-newip *newipaddr*

Specify the new IP address of the Management Server for *newipaddr*. Add this IP address to the SNMP transmission place address. If this option is omitted, the new IP address of the new Management Server is automatically specified. It is recommended to specify this option considering the Management Server that has multiple IP addresses.

USAGE

Execute the command after changing the IP address of Manager. The command may be executed for all devices managed by this software by the one command or for a specific device.

Devices that can be targets of the command are devices for which SNMP Trap transmission place settings can be defined automatically from this software.

The status of every target device must be Normal.

EXAMPLES

- Execute the SNMP Trap transmission place change on all managed devices that can automatically execute SNMP Trap transmission place setting.

```
> sanadmsh chtraprcvip -all -oldip 10.10.10.10 -newip 20.20.20.20
```

- Execute the SNMP Trap transmission place change on server nodes that sysname is defined in "host1".

```
> sanadmsh chtraprcvip -host sysname:host1 -oldip 10.10.10.10 -newip 20.20.20.20
```

12.1.1.2 swtraptest (SNMP Trap test for Fibre Channel switch)

NAME

swtraptest - tests of SNMP Trap

SYNOPSIS

```
swtraptest ipaddr
```

COMMAND PATH

Windows environment

```
$INS_DIR\ESC\Manager\opt\FJSVssmgr\bin\swtraptest
```

(\$INS_DIR means "Program Directory" specified at the ETERNUS SF Manager installation.)

Solaris or Linux environment

```
/opt/FJSVssmgr/bin/swtraptest
```

DESCRIPTION

This command checks whether this software can receive a SNMP Trap correctly, display an event, and cooperate with Systemwalker Centric Manager and Shell/Bat.

A simulated Fibre Channel switch SNMP Trap (FC Port fault) is created and issued to the Management Server.

OPERANDS

ipaddr

Specify the IPv4 address of the Fibre Channel switch which is to check the SNMP Trap setting by this command. IPv6 address cannot be specified.

The Fibre Channel switch must be a device managed by this software.

OPTIONS

None.

EXAMPLES

- Executing this command for the Fibre Channel switch whose IP address is 11.11.11.11

```
> swtraptest 11.11.11.11
```

NOTES

- Even the input IP address is not for a Fibre Channel switch device, this command can be executed. In this case, it executes as the event of device which IP address is input.
- Following Fibre Channel switch can be tested by using this command:
SN200 (Brocade), PRIMERGY switch blade, Brocade VDX series, PRIMERGY BX Ethernet Fabric Switch
- The SNMP Trap community name that is issued using this command, is fixed to "public".

12.1.1.3 grtraptest (SNMP Trap test for ETERNUS Disk storage system)

NAME

grtraptest - tests of SNMP Trap

SYNOPSIS

```
grtraptest ipaddr
```

COMMAND PATH

Windows environment

```
$INS_DIR\ESC\Manager\opt\FJSVssmgr\bin\grtraptest
```

(\$INS_DIR means "Program Directory" specified at the ETERNUS SF Manager installation.)

Solaris or Linux environment

```
/opt/FJSVssmgr/bin/grtraptest
```

DESCRIPTION

This command checks whether this software can receive a SNMP Trap correctly, display an event, and cooperate with Systemwalker Centric Manager and Shell/Bat.

A simulated SNMP Trap (FAN fault) for the ETERNUS Disk storage system is created within the Management Server and is issued to the Management Server itself.

OPERANDS

ipaddr

Specify the IPv4 address of the ETERNUS Disk storage system which is to check the SNMP Trap settings. IPv6 address cannot be specified.

The ETERNUS Disk storage system must be a device managed by this software.

OPTIONS

None.

EXAMPLES

- Executing this command for the ETERNUS Disk storage system whose IP address is 12.12.12.12.

```
> grtraptest 12.12.12.12
```

NOTES

- This command can be executed even if you have input the IP address for a device other than an ETERNUS Disk storage system. In that case, the command is executed as an event of the device corresponding to the designated IP address.
- The SNMP Trap community name that is issued using this command, is fixed to "public".

12.1.1.4 storageadm zone (Host affinity and zoning operation command)

NAME

storageadm zone - operates the host affinity and zoning

SYNOPSIS

```
storageadm zone add -storage cawwpn,affinitygroup -hba hbawwpn [-ipaddr ipaddr[,ipaddr]] [-hostrsp hostresponse] [-update all] [-f [-s]]
```

```
storageadm zone delete -storage cawwpn,affinitygroup -hba hbawwpn [-ipaddr ipaddr[,ipaddr]] [-update all] [-s]
```

```
storageadm zone info [-ipaddr ipaddr[,ipaddr,...]] [-check]] [-fast] [-csv] [-hex] [-hostresp]
```

COMMAND PATH

Windows environment

```
$INS_DIR\ESC\Manager\opt\FJSVssmgr\sbin\storageadm zone
```

(\$INS_DIR means "Program Directory" specified at the ETERNUS SF Manager installation.)

Solaris or Linux environment

```
/opt/FJSVssmgr/sbin/storageadm zone
```

DESCRIPTION

This command is used to set/delete/display the storage device host affinity and Fibre Channel switch zoning.

In the Windows environment, only a user of the Administrators group can execute this command.

In the Solaris or Linux environment, only OS administrator (root) user can execute this command.

Specify the storage device CA WWPN, affinity group, and WWPN of the set HBA in the command parameter to set/delete the storage device host affinity and Fibre Channel switch zoning. The set host affinity and zoning is also displayed.

The target storage device and Fibre Channel switch must be devices managed by this software.

OPERANDS

add

This sets the host affinity and zoning.

delete

This deletes the host affinity and zoning.

info

This displays the host affinity and zoning.

OPTIONS

Options of the "add" operand

```
-storage cawwpn,affinitygroup
```

Designate the WWPN and affinity group number for the CA of the storage device for which host affinity is being set.

The CA WWPN is specified with a 16-character long hexadecimal number or a 23-character long hexadecimal number with each two digits separated by a colon (":"). For example, if separating the characters with colons, the WWPN is written in a manner such

as "11:11:11:11:11:11:11".

The affinity group number is specified by a decimal or hexadecimal number. For example, specify affinity group number 16 as either "-storage 1111111111111111,16" in decimal notation or "-storage 1111111111111111,0x10" in hexadecimal notation.

-hba *hbawwpn*

Specify the WWPN for the HBA to be set to the host affinity and zoning.

The WWPN for the HBA is written with a 16-character long hexadecimal number or a 23-character long hexadecimal number with each two digits separated by a colon (":"). For example, if separating the characters with colons, the WWPN is written in a manner such as "22:22:22:22:22:22:22:22".

-ipaddr *ipaddr[,ipaddr]*

Set the IP address of a storage device and/or Fibre Channel switch. To specify the IP addresses of both devices, separate the two IP addresses with a comma (","). The two IP addresses can be specified in either order.

Specified Device	Command Action
Storage device	The command checks that the status allows for setting the host affinity to the affinity group of the CA for the storage device designated with the -storage option. The command sets the host affinity to the storage device only if the status allows the setting. If the status does not allow for the setting to be made, the command will terminate with an error.
Fibre Channel switch	The command checks that the status allows for setting the WWPN and zoning for the HBA specified with the -hba option within the fabric which includes the Fibre Channel switches connected to the CA of the storage device specified with the -storage option (i.e. all Fibre Channel switches connected in a cascade connection). The command sets the zoning to the Fibre Channel switch only if the status allows the setting. If the status does not allow the setting, the command will terminate with an error.
Both storage device and Fibre Channel switch	The command checks that the status allows you to set the host affinity or zoning to the respective devices. The command sets the host affinity and zoning only if the status allows for the settings to be made for both devices. If the status is such that the setting cannot be made to either of the devices, the command will terminate with an error.

-hostresp *hostresponse*

Specify the host response being used by the HBA.

If this option is omitted, the storage device's default host response will be set.

-update all

Specify this option to update the information this software is managing to the latest information after the completion of the setup. If this option is omitted, the information managed by this software will not be updated. To update the information, be sure to execute the "info" operand without specifying the -fast option.

This option is effective for when there are few settings needing to be updated. The "info" operand is effective for updating information after performing multiple settings at one time.

-f

Specify this option if forcibly setting WWPN zoning to a Fibre Channel switch in a status of not having zoning set up.

Check the security settings for the Fibre Channel switch when specifying this option. Specify this option only if setting WWPN zoning.

Moreover, if you specify this option under the conditions described below, the operand will be executed the same as if this option was omitted.

- If only a storage device is specified for the -ipaddr option
- If zoning is already set for the Fibre Channel switch to which you intend to set the zoning

-s

Continues the processing without a confirmation message being output.
This option can be specified only when the -f option is specified.

Options of the "delete" operand

-storage *cawwpn,affinitygroup*

Designate the WWPN and affinity group number for the CA of the storage device for which host affinity is being deleted.

The CA WWPN is specified with a 16-character long hexadecimal number or a 23-character long hexadecimal number with each two digits separated by a colon (":"). For example, if separating the characters with colons, the WWPN is written in a manner such as "11:11:11:11:11:11:11".

The affinity group number is specified by a decimal or hexadecimal number. For example, specify affinity group number 16 as either "-storage 1111111111111111,16" in decimal notation or "-storage 1111111111111111,0x10" in hexadecimal notation.

-hba *hbawwpn*

Specify the WWPN for the HBA from which the host affinity and zoning to be deleted.

The WWPN for the HBA is written with a 16-character long hexadecimal number or a 23-character long hexadecimal number with each two digits separated by a colon (":"). For example, if separating the characters with colons, the WWPN is written in a manner such as "22:22:22:22:22:22:22".

-ipaddr *ipaddr[,ipaddr]*

Set the IP address of a storage device and/or Fibre Channel switch. To specify the IP addresses of both devices, separate the two IP addresses with a comma (","). The two IP addresses can be specified in either order.

Specified Device	Command Action
Storage device	The command checks that the status allows for deleting the host affinity from the affinity group of the CA for the storage device designated with the -storage option. The command deletes the host affinity from the storage device only if the status allows the deletion. If the status does not allow the deletion, the command will terminate with an error.
Fibre Channel switch	The command checks that the status allows for deleting the WWPN and zoning for the HBA specified with the -hba option within the fabric which includes the Fibre Channel switches connected to the CA of the storage device specified with the -storage option (i.e. all Fibre Channel switches connected in a cascade connection). The command deletes the zoning to the Fibre Channel switch only if the status allows the deletion. If the status does not allow the deletion, the command will terminate with an error.
Both storage device and Fibre Channel switch	The command checks that the status allows for deleting the host affinity or zoning from the respective devices. The command deletes the host affinity and zoning only if the status allows for the deletion for both devices. If the status is such that the deletion cannot be made to either of the devices, the command will terminate with an error.

-update all

Specify this option to update the information this software is managing to the latest information after the completion of the setup. If this option is omitted, the information managed by this software will not be updated. To update the information, be sure to execute the "info" operand without specifying the -fast option specified.

This option is effective for when there are few deletion. The "info" operand is effective for updating information after performing multiple deletions at one time.

-s

Processing continues without output of a confirmation message.

Options of the "info" operand

-ipaddr *ipaddr[,ipaddr, ...]*

Displays the zoning information for the Fibre Channel switches corresponding to the specified IP addresses or host affinity information for the host affinities set to the CA of the storage devices. To display information for multiple storage devices and Fibre Channel switches, specify the IP addresses separated by comma (",").

If this option is omitted, the operand will display the information for all storage devices and Fibre Channel switches registered with this software.

However, the operand will display information for the following storage devices which are not registered with this software (but detected).

- ETERNUS DX60/DX60 S2/DX80/DX90
- ETERNUS DX400 series
- ETERNUS DX8000 series

-check

Checks that the devices specified with the -ipaddr option are storage devices or Fibre Channel switches which are registered to this software.

However, the specified devices will be included for display even if they have not been registered with this software (but detected) if they are one of the following devices.

- ETERNUS DX60/DX60 S2/DX80/DX90
- ETERNUS DX400 series
- ETERNUS DX8000 series

Checks that the status allows for display of the information. The information for the designated devices is displayed only if the status allows for it. If the status does not allow for information to be displayed or if the devices are not devices applicable to this display, the command will terminate with an error.

This option can be specified when the -ipaddr option is specified.

-fast

Specify this to display storage device and Fibre Channel switch information from the existing information managed by this software. If this option is omitted, the storage device and Fibre Channel switch information will be displayed after the information managed by this software has been updated to the latest information.

This option is effective for displaying information after you have executed the "add" operand or the "delete" operand with the -update all option specified.

-csv

Displays the storage device and Fibre Channel switch information in CSV format.

If this option is omitted, the information is displayed in a table format.

-hex

Specify this to display the storage device and Fibre Channel switch information in hexadecimal format. If this option is specified, the affinity group numbers for storage devices will be displayed in hexadecimal format.

-hostresp

If this option is specified, the host response number used by the HBA and the host response's alias name will be displayed.

If this option is omitted, the host response number and host response alias name, including the table border and column names will not be displayed.

EXAMPLES

- Adding the host affinity and zoning

```
> storageadm zone add -storage 1111111111111111,3 -hba 2222222222222222
```

- Deleting the host affinity and zoning

```
> storageadm zone delete -storage 1111111111111111,3 -hba 2222222222222222
```

- Displaying the host affinity and zoning

```
> storageadm zone info
<<< FC Switch Zone Information >>>
DEVICE_NAME(IP_ADDRESS)      ZONE_NAME      ZONE_WWPN
-----
Switch1(10.10.10.10)         SNM_0001       1111111111111111;2222222222222222
                               SNM_0002       3333333333333333;4444444444444444
-----
```

```
<<< FC CA Zone Information >>>
DEVICE_NAME(IP_ADDRESS)      CA_WWPN        AFFINITY_GROUP  HBA_WWPN
-----
E4000M300(10.10.10.11)       1111111111111111 3                2222222222222222
-----
```

- Displaying the host affinity and zoning in CSV format and in hexadecimal format.

```
> storageadm zone info -csv -hex
DEVICE_NAME(IP_ADDRESS),ZONE_NAME,ZONE_WWPN
Switch1(10.10.10.10),SNM_0001,1111111111111111;2222222222222222
,SNM_0002,3333333333333333;4444444444444444

DEVICE_NAME(IP_ADDRESS),CA_WWPN,AFFINITY_GROUP,HBA_WWPN
E4000M300(10.10.10.11),1111111111111111,0x0003,2222222222222222
```

NOTES

- The storage device and Fibre Channel switch for which set/delete/display is performed must have been registered with this software. However, the information for the following storage devices which are not registered with the software (but detected) is displayed.
 - ETERNUS DX60/DX60 S2/DX80/DX90
 - ETERNUS DX400 series
 - ETERNUS DX8000 series

This command cannot be used to register Fibre Channel switches if zoning has not been set. Create a temporary zone and then register the Fibre Channel switch with this software. Refer to "Zoning setting" in "Setting" of the target device of "[4.2 Fibre Channel switch](#)" for details on creating a temporary zone.

By specifying the -f option, you can forcibly set zoning even to those Fibre Channel switches for which zoning has not been set.

However, if you have created a temporary zone or performed a forcible setting using the -f option, all access except to the zoning specified with the -f option will be blocked. Therefore, be sure not to perform this task while the environment for the target Fibre Channel switch is operating. Perform this task either before starting the operation of the environment after the installation of the Fibre Channel switch environment or while the operation of the environment is stopped.

- The zoning for the Fibre Channel switch is set within the fabric which includes the Fibre Channel switches connected to the CA of the specified storage device (i.e. all Fibre Channel switches connected in a cascade connection) to the fibre switches equipped with the latest firmware.
- The Fibre Channel switch and storage device must be connected using a Fibre Channel cable. If the Fibre Channel cable is not connected, Fibre Channel switch zoning is not set. Connect the Fibre Channel cable, and then re-execute the command.
- Zone settings (AffinityGroup creation) must be configured in the ETERNUS Disk storage system in advance, using ETERNUS Web GUI.
- Only the ETERNUS SN200 (except model 250M) and Brocade (except AP7420) Fibre Channel switch, PRIMERGY Fibre Channel switch blades, Brocade VDX series and PRIMERGY BX Ethernet Fabric Switch are supported.

- A confirmation message will be output in the situation below. Enter "y" to continue or "n" to cancel. The confirmation message can be surpass by specifying the -s option.
- If the -f option is specified with the "add" operand but -s option is not specified.
- If the -s option is not specified with the "delete" operand.

A confirmation message is as follows:

```
Are you sure? [y/n]:
```

12.1.1.5 storageadm iscsizone (Host affinity operation command)

NAME

storageadm iscsizone - operates iSCSI host affinity

SYNOPSIS

```
storageadm iscsizone add -ipaddr i paddr -storage {port_i paddr, port_i scsi_name, affinity group / portID, affinity group} -server {server_port_i paddr, server_port_i scsi_name | server_port_i scsi_name} [-svalias server_alias] [-svname server_name] [-svhostrsp server_hostresponse] [-check]
```

```
storageadm iscsizone delete -ipaddr i paddr -storage {port_i paddr, port_i scsi_name, affinity group / portID, affinity group} -server {server_port_i paddr, server_port_i scsi_name | server_port_i scsi_name} [-check] [-s]
```

```
storageadm iscsizone info [-ipaddr i paddr[, i paddr, ...] [-check]] [-csv] [-hex] [-expand]
```

COMMAND PATH

Windows environment

```
$INS_DIR\ESC\Manager\opt\FJSVssmgr\sbin\storageadm iscsizone
```

(\$INS_DIR means "Program Directory" specified at the ETERNUS SF Manager installation.)

Solaris or Linux environment

```
/opt/FJSVssmgr/sbin/storageadm iscsizone
```

DESCRIPTION

This command is used to set, delete, and display the host affinity of the storage device iSCSI.

In the Windows environment, only a user of the Administrators group can execute this command.

In the Solaris or Linux environment, only OS administrator (root) user can execute this command.

In the command operands, specify the IP address and iSCSI name of the storage device iSCSI port, the affinity group, and the IP address and iSCSI name of the server being set. Use these operands to set and delete the host affinity of the storage device and to display the host affinity that is set.

The targeted storage device must be a device managed by this software.

OPERANDS

add

This sets the host affinity.

delete

This deletes the host affinity.

info

This displays the host affinity.

OPTIONS

Options of the add operand

-ipaddr *ipaddr*

Specify the IP address of the storage device.

-storage {*port_ipaddr,port_iscsi_name,affinitygroup* | *portID,affinitygroup*}

Specify the iSCSI port IP address and iSCSI name of the storage device for which the host affinity is set and the affinity group number, or specify the port ID and the affinity group number.

Specify the affinity group number as a decimal or hexadecimal number. Specification example is as follows:

```
[Decimal specification]
-storage 172.16.4.38,iqn.2000-09.com.fujitsu:storage-system.e2000:0000000029,3

[Hexadecimal specification]
-storage 172.16.4.38,iqn.2000-09.com.fujitsu:storage-system.e2000:0000000029,0x3
```

For ETERNUS DX60/DX60 S2/DX80/DX90, the port ID is the CM number and the port number entered.
For ETERNUS DX80 S2/DX90 S2/DX100 S3/DX200 S3, DX400/DX400 S2 series, DX500 S3/DX600 S3 and DX8000/DX8000 S2 series, the port ID is the CM number, the CA number and the port number entered. Specification example is as follows:

```
[To specify CM number 1, CA number 2, port number 1, and affinity group number 6]
-storage 121,6
```

-server {*server_port_ipaddr,server_port_iscsi_name* | *server_port_iscsi_name*}

Specify the iSCSI port IP address and the iSCSI name of the server for which the host affinity is set.

If the device supports non-setting of the iSCSI host IP address, the server can be specified with the iSCSI host IP address omitted.

-salias *server_alias*

This specifies the iSCSI alias of the server being set for the host affinity.

If this option is omitted, an alias is not set.

-svname *server_name*

This specifies the host alias of the server being set for the host affinity.

If this option is omitted, the specification is as follows:

Storage Device	Specification when this option is omitted
ETERNUS DX60/DX60 S2 ETERNUS DX80/DX80 S2 ETERNUS DX90/DX90 S2 ETERNUS DX100 S3/DX200 S3 ETERNUS DX400 S2 series ETERNUS DX500 S3/DX600 S3 ETERNUS DX8000 S2 series	An alias is set automatically.
ETERNUS DX400 series ETERNUS DX8000 series	An alias is not set.

-svhostrsp *server_hostresponse*

This specifies the host response number of the server being set for the host affinity.

If this option is omitted, then host response number #0 is set.

-check

This checks whether the server specified in the -server option is already set as the host affinity setting for the device at the IP address specified in the -ipaddr option. If it is not already set as the host affinity, processing continues and the host affinity is set. If it is already set as the host affinity, an error occurs.

If this option is omitted, processing continues without checking.

Options of the delete operand

-ipaddr *ipaddr*

Specify the IP address of the storage device.

-storage {*port_ipaddr,port_iscsi_name,affinitygroup* | *portID,affinitygroup*}

Specify the iSCSI port IP address and iSCSI name of the storage device for which the host affinity is being deleted and the affinity group number, or specify the port ID and the affinity group number.

Specify the affinity group number as a decimal or hexadecimal number. Specification example is as follows:

```
[Decimal specification]
-storage 172.16.4.38,iqn.2000-09.com.fujitsu:storage-system.e2000:0000000029,3

[Hexadecimal specification]
-storage 172.16.4.38,iqn.2000-09.com.fujitsu:storage-system.e2000:0000000029,0x3
```

For ETERNUS DX60/DX60 S2/DX80/DX90, the port ID is the CM number and the port number entered.

For ETERNUS DX80 S2/DX90 S2/DX100 S3/DX200 S3, ETERNUS DX400/DX400 S2 series, ETERNUS DX500 S3/DX600 S3 and ETERNUS DX8000/DX8000 S2 series, the port ID is the CM number, the CA number and the port number entered. Specification example is as follows:

```
[To specify CM number 1, CA number 2, port number 1, and affinity group number 6]
-storage 121,6
```

-server {*server_port_ipaddr,server_port_iscsi_name* | *server_port_iscsi_name*}

Specify the iSCSI port IP address and the iSCSI name of the server for which the host affinity is being deleted.

If the device supports non-setting of the iSCSI host IP address, the server can be specified with the iSCSI host IP address omitted.

-check

This checks whether the server specified in the -server option is already set as the host affinity setting for the device at the IP address specified in the -ipaddr option. If it is not already set as the host affinity, an error occurs. If it is already set as the host affinity, processing continues and the setting is deleted.

If this option is omitted, processing continues without checking.

-s

Processing continues without output of a confirmation message.

Options of the info operand

-ipaddr *ipaddr*

This displays the host affinity information of the storage device at the specified IP address. To display information of multiple storage devices, specify the IP addresses successively, separated by commas (",").

If this option is omitted, information is displayed for all the storage devices registered with this software.

However, the information for the following storage devices which are not registered with the software (but detected) is displayed.

- ETERNUS DX60/DX60 S2/DX80/DX90
- ETERNUS DX400 series
- ETERNUS DX8000 series

-check

This checks whether the devices at the IP address specified in the -ipaddr option are storage devices registered with this software. If all devices at the specified IP address are registered with this software, processing continues and the setting information is displayed. If at least one device at the specified IP address is not registered with this software, an error occurs.

If this option is omitted, processing continues without checking.

When a device whose IP address has been specified is one of the following, the process continues and the setting information is displayed even if it has not been registered with this software (but detected).

- ETERNUS DX60/DX60 S2/DX80/DX90
- ETERNUS DX400 series
- ETERNUS DX8000 series

This option can be specified only when the `-ipaddr` option is specified.

`-csv`

Output is in CSV format.

`-hex`

The affinity group number is displayed as a hexadecimal number.

`-expand`

This adds the following to the host affinity information to display:

- IPv6 link local address
- IPv6 connection IP address

Added information depends on the version of the ETERNUS SF system. Upgrading the version of the ETERNUS SF system may increase displayed information.

When this option is omitted, a list of host affinities is displayed.

EXAMPLES

- Add a host affinity.

```
> storageadm iscsizone add -ipaddr 1.2.3.4 -storage 172.16.4.38,iqn.2000-09.com.fujitsu:storage-
system.e2000:0000000029,3 -server 172.16.4.198,eui.22222222222222222222 -svalias alias2222 -svname
name2222 -svhostrsp 2
INFO:swsag0001:Command terminated normally.
```

- Delete a host affinity.

```
> storageadm iscsizone delete -ipaddr 1.2.3.4 -storage 172.16.4.38,iqn.2000-09.com.fujitsu:storage-
system.e2000:0000000029,3 -server 172.16.4.198,eui.22222222222222222222
INFO:swsag0001:Command terminated normally.
```

- Display the host affinity in table format.

```
> storageadm iscsizone info -ipaddr 1.2.3.4
<<< iSCSI CA Zone Information >>>
DEVICE NAME(IP ADDRESS)      PORT  ISCSI CA      ISCSI CA      AFFINITY SERVER      SERVER
                               ID   IP ADDRESS    ISCSI NAME     GROUP   IP ADDRESS          ISCSI NAME
-----
DX60(1.2.3.4)                00   172.16.4.38   iqn.2000-09.com.fujitsu:storage-
system.e2000:0000000029 6 172.16.4.198 eui.22222222222222222222
                               01   172.16.4.39   iqn.2000-09.com.fujitsu:storage-
system.e2000:0000000029 6 172.16.4.198 eui.22222222222222222222
                               01   172.16.4.39   iqn.2000-09.com.fujitsu:storage-
system.e2000:0000000029 6 172.16.4.199 eui.33333333333333333333
                               10   172.16.4.40   iqn.2000-09.com.fujitsu:storage-
system.e2000:0000000029 - - -
                               11   172.16.4.41   iqn.2000-09.com.fujitsu:storage-
system.e2000:0000000029 - - -
E4000(1.2.3.5)                000 172.16.4.38   iqn.2000-09.com.fujitsu:storage-
system.e4000:0000000001 3 172.16.4.198 eui.22222222222222222222
```

```

120 172.16.4.40      iqn.2000-09.com.fujitsu:storage-
system.e4000:0000000001 3 172.16.4.158 eui.4444444444444444
-----

```

```

INFO:swsag0001:Command terminated normally.

```

- Display the host affinity in CSV format.

```

> storageadm iscsizone info -ipaddr 1.2.3.4 -csv
DEVICE NAME(IP ADDRESS),PORT ID,ISCSI CA IP ADDRESS,ISCSI CA ISCSI NAME,AFFINITY GROUP,SERVER IP
ADDRESS,SERVER ISCSI NAME
DX60(1.2.3.4),00,172.16.4.38,iqn.2000-09.com.fujitsu:storage-
system.e2000:0000000029,6,172.16.4.198,eui.2222222222222222
,01,172.16.4.39,iqn.2000-09.com.fujitsu:storage-system.e2000:0000000029,6,172.16.4.198,eui.
2222222222222222
,01,172.16.4.39,iqn.2000-09.com.fujitsu:storage-system.e2000:0000000029,6,172.16.4.199,eui.
3333333333333333
,10,172.16.4.40,iqn.2000-09.com.fujitsu:storage-system.e2000:0000000029,-,-,-
,11,172.16.4.41,iqn.2000-09.com.fujitsu:storage-system.e2000:0000000029,-,-,-
E4000(1.2.3.5),000,172.16.4.38,iqn.2000-09.com.fujitsu:storage-
system.e4000:0000000001,3,172.16.4.198,eui.2222222222222222
,120,172.16.4.38,iqn.2000-09.com.fujitsu:storage-system.e4000:0000000001,3,172.16.4.158,eui.
4444444444444444

```

- Display the host affinity in table format including additional information.

```

> storageadm iscsizone info -ipaddr 1.2.3.4 -expand
<<< iSCSI CA Zone Information >>>
DEVICE NAME(IP ADDRESS)      PORT ID ISCSI CA IP ADDRESS ISCSI CA ISCSI NAME AFFINITY GROUP SERVER IP ADDRESS ISCSI NAME
SERVER ISCSI CA LINK LOCAL IP ADDRESS ISCSI CA CONNECT IP ADDRESS
ID IP ADDRESS ISCSI NAME GROUP IP ADDRESS ISCSI NAME
-----
DX60(1.2.3.4) 00 172.16.4.38 iqn.2000-09.com.fujitsu:storage-
system.e2000:0000000029 6 172.16.4.198 eui.2222222222222222 fe80::128c:24d8:3016:250a:
56ff:fe67:a524 2001:100a:ab13:cd24:ef3f:db72:fe11:cd21
01 172.16.4.39 iqn.2000-09.com.fujitsu:storage-
system.e2000:0000000029 6 172.16.4.198 eui.2222222222222222 fe80::128c:24d8:3016:250a:
56ff:fe67:a525 2001:100a:ab13:cd24:ef3f:db72:fe11:cd22
01 172.16.4.39 iqn.2000-09.com.fujitsu:storage-
system.e2000:0000000029 6 172.16.4.199 eui.3333333333333333 fe80::128c:24d8:3016:250a:
56ff:fe67:a525 2001:100a:ab13:cd24:ef3f:db72:fe11:cd22
10 172.16.4.40 iqn.2000-09.com.fujitsu:storage-
system.e2000:0000000029 - - - -
11 172.16.4.41 iqn.2000-09.com.fujitsu:storage-
system.e2000:0000000029 - - - -
E4000(1.2.3.5) 000 172.16.4.38 iqn.2000-09.com.fujitsu:storage-
system.e4000:0000000001 3 172.16.4.198 eui.2222222222222222 fe80::254b:781a:4b35:c531:1a3d:198e:
30c6 2001:100a:451f:fd32:230b:12ac:dd2a:a2e5
120 172.16.4.40 iqn.2000-09.com.fujitsu:storage-
system.e4000:0000000001 3 172.16.4.158 eui.4444444444444444 fe80::254b:781a:4b35:c531:1a3d:198e:
30d5 2001:100a:451f:fd32:230b:12ac:dd2a:a289
-----

```

```

INFO:swsag0001:Command terminated normally.

```

- Display the host affinity in CSV format including additional information.

```

> storageadm iscsizone info -ipaddr 1.2.3.4 -expand -csv
DEVICE NAME(IP ADDRESS),PORT ID,ISCSI CA IP ADDRESS,ISCSI CA ISCSI NAME,AFFINITY GROUP,SERVER IP
ADDRESS,SERVER ISCSI NAME, ISCSI CA LINK LOCAL IP ADDRESS,ISCSI CA CONNECT IP ADDRESS
DX60(1.2.3.4),00,172.16.4.38,iqn.2000-09.com.fujitsu:storage-
system.e2000:0000000029,6,172.16.4.198,eui.2222222222222222,fe80::128c:24d8:3016:250a:
56ff:fe67:a524,2001:100a:ab13:cd24:ef3f:db72:fe11:cd21

```

```

DX60(1.2.3.4),01,172.16.4.39,iqn.2000-09.com.fujitsu:storage-
system.e2000:0000000029,6,172.16.4.198,eui.2222222222222222,fe80::128c:24d8:3016:250a:
56ff:fe67:a525,2001:100a:ab13:cd24:ef3f:db72:fe11:cd22
DX60(1.2.3.4),01,172.16.4.39,iqn.2000-09.com.fujitsu:storage-
system.e2000:0000000029,6,172.16.4.199,eui.3333333333333333,fe80::128c:24d8:3016:250a:
56ff:fe67:a525,2001:100a:ab13:cd24:ef3f:db72:fe11:cd22
DX60(1.2.3.4),10,172.16.4.40,iqn.2000-09.com.fujitsu:storage-system.e2000:0000000029,-,-,-,-
DX60(1.2.3.4),11,172.16.4.41,iqn.2000-09.com.fujitsu:storage-system.e2000:0000000029,-,-,-,-
E4000(1.2.3.5),000,172.16.4.38,iqn.2000-09.com.fujitsu:storage-
system.e4000:0000000001,3,172.16.4.198,eui.2222222222222222,fe80::254b:781a:4b35:c531:1a3d:198e:
30c6,2001:100a:451f:fd32:230b:12ac:dd2a:a2e5
E4000(1.2.3.5),120,172.16.4.38,iqn.2000-09.com.fujitsu:storage-
system.e4000:0000000001,3,172.16.4.158,eui.4444444444444444,fe80::254b:781a:4b35:c531:1a3d:198e:
30d5,2001:100a:451f:fd32:230b:12ac:dd2a:a289

```

NOTES

- Storage devices must be registered with this software in order to add, delete, and display settings. However, the information for the following storage devices which are not registered with the software (but detected) is displayed.
 - ETERNUS DX60/DX60 S2/DX80/DX90
 - ETERNUS DX400 series
 - ETERNUS DX8000 series
- Zone settings (Affinity group creation) must be configured in the ETERNUS Disk storage system in advance, using ETERNUS Web GUI.
- The message below is displayed when the "delete" operand is specified. Enter "y" to continue, or "n" to cancel. Note that this message is not displayed if the -s option is specified.

```
Are you sure? [y/n]:
```

12.1.1.6 storageadm perfdata (Performance information operation command)

NAME

storageadm perfdata - operates the performance information

SYNOPSIS

```
storageadm perfdata export outdir name -ipaddr ipaddr [-date start_time[-end_time]]
```

COMMAND PATH

Windows environment

```
$INS_DIR\ESC\Manager\opt\FJSVssmgr\sbin\storageadm perfdata
```

(*\$INS_DIR* means "Program Directory" specified at the ETERNUS SF Manager installation.)

Solaris or Linux environment

```
/opt/FJSVssmgr/sbin/storageadm perfdata
```

DESCRIPTION

This command outputs the performance information of the storage devices and Fibre Channel switches.

In the Windows environment, only a user of the Administrators group can execute this command.

In the Solaris or Linux environment, only OS administrator (root) user can execute this command.

By specifying the IP address of the device that outputs the performance information and the date in the command operand, the storage device and Fibre Channel switch performance information is output in CSV format.

The target storage device and Fibre Channel switch must be devices managed by this software when performance monitoring is either still running or already completed.

The supported devices are as follows:

- ETERNUS DX series
- The Fibre Channel switches and Fibre Channel switch blades which support the performance monitoring.

The details of CSV files are as follows.

The port information of Fibre Channel switch

Items	Explanation
File name	PORT.csv
Header line	Date,PortX - Tx Throughput, PortX - Rx Throughput, PortX - CRC Error, ...
Data line	<p><i>date,port0s,port0r,port0e, ... ,portNs,portNr,portNe</i></p> <p>The following information is output for each field. After <i>date</i>, the information is repeated for the actual number of ports.</p> <p><i>date</i> : Performance Information Acquisition Time (YYYY/MM/DD hh:mm:ss format)</p> <p><i>port0s</i> : Port0 Transfer rates of send data at <i>date</i> (Decimal notation. The unit is MB/S.)</p> <p><i>port0r</i> : Port0 Transfer rates of receive data at <i>date</i> (Decimal notation. The unit is MB/S.)</p> <p><i>port0e</i> : Port0 Number of CRC errors at <i>date</i> (Decimal notation. The unit is Count.)</p> <p><i>portNs</i> : PortN Transfer rates of send data at <i>date</i> (Decimal notation. The unit is MB/S.)</p> <p><i>portNr</i> : PortN Transfer rates of receive data at <i>date</i> (Decimal notation. The unit is MB/S.)</p> <p><i>portNe</i> : PortN Number of CRC errors at <i>date</i> (Decimal notation. The unit is Count.)</p>

The CM performance information of storage device

ETERNUS DX60/DX60 S2/DX80/DX80 S2/DX90/DX90 S2/DX100 S3/DX200 S3/DX500 S3/DX600 S3

Items	Explanation
File name	CM.csv
Header line	Date, CM0xXX - CPU Use Rate, CM0xXX - Copy Remain, ...
Data line	<p><i>date,CM00u,CM00r, ... ,CMNNu,CMNNr</i></p> <p>The following information is output for each field. After <i>date</i>, the information is repeated for the actual number of CMs.</p> <p><i>date</i> : Performance Information Acquisition Time (YYYY/MM/DD hh:mm:ss format)</p> <p><i>CM00u</i> : CM0x00 CPU Load at <i>date</i> (Decimal notation. The unit is %.)</p> <p><i>CM00r</i> : CM0x00 CM Copy remaining amount at <i>date</i> (Decimal notation. The unit is GB.)</p> <p><i>CMNNu</i> : CM0xNN CPU Load at <i>date</i> (Decimal notation. The unit is %.)</p> <p><i>CMNNr</i> : CM0xNN CM Copy remaining amount at <i>date</i> (Decimal notation. The unit is GB.)</p>

ETERNUS DX400/DX400 S2 series and ETERNUS DX8000/DX8000 S2 series

Items	Explanation
File name	<p><i>CM/nnnn.csv</i></p> <p>(<i>nnnn</i> indicates the CM number by hexadecimal notation. CM numbers are assigned in ascending order, starting with 0000 for the lowest CM CPU number in the device.</p> <p>CM0x0 CPU0 is 0000,</p>

Items	Explanation
	CM0x0 CPU1 is 0001, CM0x1 CPU0 is 0002, CM0x1 CPU1 is 0003, : CM0x7 CPU0 is 000E, CM0x7 CPU1 is 000F.)
Header line	Date, CM0xXX:CPUX - CPU Use Rate, CM0xXX:CPUX(ROE) - CPU Use Rate, CM0xXX:CPUX - Copy Remain
Data line	<i>date,cpu,roe,remain</i> The following information is output for each field. <i>date</i> : Performance Information Acquisition Time (YYYY/MM/DD hh:mm:ss format) <i>cpu</i> : CM0xXX:CPUX CPU Load at <i>date</i> (Decimal notation. The unit is %.) <i>roe</i> : CM0xXX:CPUX ROE Load at <i>date</i> (Decimal notation. The unit is %.) <i>remain</i> : CM0xXX:CPUX CM Copy remaining amount at <i>date</i> (Decimal notation. The unit is GB.)

The LogicalVolume performance information of storage device

Items	Explanation
File name	LogicalVolume/ <i>nnnn</i> .csv (<i>nnnn</i> indicates the LogicalVolume number by hexadecimal notation.)
Header line	Date, LogicalVolume0xXXXX - Read IOPS, LogicalVolume0xXXXX - Write IOPS, LogicalVolume0xXXXX - Read Throughput, LogicalVolume0xXXXX - Write Throughput, LogicalVolume0xXXXX - Read Response Time, LogicalVolume0xXXXX - Write Response Time, LogicalVolume0xXXXX - Read Cache Hit Rate, LogicalVolume0xXXXX - Write Cache Hit Rate, LogicalVolume0xXXXX - Prefetch Cache Hit Rate, LogicalVolume0xXXXX - Read Cache Hit Rate(Extreme Cache), LogicalVolume0xXXXX - Read Cache Hit Rate(DRAM + Extreme Cache), LogicalVolume0xXXXX - Read QoS Delay Time, LogicalVolume0xXXXX - Write QoS Delay Time
Data line	<i>date,read,write,through-r,through-w,resp-r,resp-w,hit-r,hit-w,fetch, hit-r-extreme-cache, hit-r-dram-extreme-cache, delay-r-qos, delay-w-qos</i> The following information is output for each field. <i>date</i> : Performance Information Acquisition Time. (YYYY/MM/DD hh:mm:ss format) <i>read</i> : Read Count at <i>date</i> . (Decimal notation. The unit is IOPS.) <i>write</i> : Write Count at <i>date</i> . (Decimal notation. The unit is IOPS.) <i>through-r</i> : Read data transfer rate at <i>date</i> . (Decimal notation. The unit is MB/S.) <i>through-w</i> : Write data transfer rate at <i>date</i> (Decimal notation. The unit is MB/S.) <i>resp-r</i> : Read Response Time at <i>date</i> . (Decimal notation. The unit is msec.) <i>resp-w</i> : Write Response Time at <i>date</i> . (Decimal notation. The unit is msec.) <i>hit-r</i> : Read Cache Hit Rate at <i>date</i> . (Decimal notation. The unit is %.) <i>hit-w</i> : Write Cache Hit Rate at <i>date</i> . (Decimal notation. The unit is %.) <i>fetch</i> : Read Pre-fetch Cache Hit Rate at <i>date</i> . (Decimal notation. The unit is %.) <i>hit-r-extreme-cache</i> : Read Cache Hit Rate at <i>date</i> . (Extreme Cache) (Decimal notation. The unit is %.) (*1, *2) <i>hit-r-dram-extreme-cache</i> : Read Cache Hit Rate at <i>date</i> . (DRAM + Extreme Cache) (Decimal notation. The unit is %.) (*1, *2) <i>delay-r-qos</i> : Read QoS Delay Time at <i>date</i> . (Decimal notation. The unit is msec.) (*3, *4) <i>delay-w-qos</i> : Write QoS Delay Time at <i>date</i> . (Decimal notation. The unit is msec.) (*3, *4)

*1: When this function is disabled for a device that supports Extreme Cache performance information, "0" will be output.

```
Example: For a device that supports Extreme Cache performance information (function disabled)
...,hit-r-extreme-cache,hit-r-dram-extreme-cache
...,0,0
```

*2: For a device that does not support Extreme Cache performance information, a value will not be output and instead a series of commas will be output.

```
Example: For a device that does not support Extreme Cache performance information
...,hit-r-extreme-cache,hit-r-dram-extreme-cache
,,,,,
```

*3: When this function is disabled for a device that supports Host-LU QoS performance information (QoS Delay Time), "0" will be output.

```
Example: For a device that supports Host-LU QoS performance information (function disabled)
...,delay-r-qos,delay-w-qos
...,0,0
```

*4: For a device that does not support Host-LU QoS performance information (QoS Delay Time), a value will not be output and instead a series of commas will be output.

```
Example: For a device that does not support Host-LU QoS performance information
...,delay-r-qos,delay-w-qos
,,,,,
```

The RAID group performance information of storage device

Items	Explanation
File name	RAIDGroup/ <i>nnnn</i> .csv (<i>nnnn</i> indicates the RAID group number by hexadecimal notation.)
Header line	Date, RAIDGroup0xXXXX - Read IOPS, RAIDGroup0xXXXX - Write IOPS, RAIDGroup0xXXXX - Read Throughput, RAIDGroup0xXXXX - Write Throughput, RAIDGroup0xXXXX - Read Response Time, RAIDGroup0xXXXX - Write Response Time, RAIDGroup0xXXXX - Read Cache Hit Rate, RAIDGroup0xXXXX - Write Cache Hit Rate, RAIDGroup0xXXXX - Prefetch Cache Hit Rate, RAIDGroup0xXXXX - Read Cache Hit Rate(Extreme Cache), RAIDGroup0xXXXX - Read Cache Hit Rate(DRAM + Extreme Cache), RAIDGroup0xXXXX - Read QoS Delay Time, RAIDGroup0xXXXX - Write QoS Delay Time
Data line	<i>date,read,write,through-r,through-w,resp-r,resp-w,hit-r,hit-w,fetch, hit-r-extreme-cache,hit-r-dram-extreme-cache,delay-r-qos,delay-w-qos</i> The following information is output for each field. <i>date</i> : Performance Information Acquisition Time. (YYYY/MM/DD hh:mm:ss format) <i>read</i> : Read Count at <i>date</i> . (Decimal notation. The unit is IOPS.) <i>write</i> : Write Count at <i>date</i> . (Decimal notation. The unit is IOPS.) <i>through-r</i> : Read data transfer rate at <i>date</i> . (Decimal notation. The unit is MB/S.) <i>through-w</i> : Write data transfer rate at <i>date</i> . (Decimal notation. The unit is MB/S.) <i>resp-r</i> : Read Response Time at <i>date</i> . (Decimal notation. The unit is msec.) <i>resp-w</i> : Write Response Time at <i>date</i> . (Decimal notation. The unit is msec.) <i>hit-r</i> : Read Cache Hit Rate at <i>date</i> . (Decimal notation. The unit is %.) <i>hit-w</i> : Write Cache Hit Rate at <i>date</i> . (Decimal notation. The unit is %.) <i>fetch</i> : Read Pre-fetch Cache Hit Rate at <i>date</i> . (Decimal notation. The unit is %.) <i>hit-r-extreme-cache</i> : Read Cache Hit Rate at <i>date</i> . (Extreme Cache) (Decimal notation. The unit is %.) (*1, *2) <i>hit-r-dram-extreme-cache</i> : Read Cache Hit Rate at <i>date</i> . (DRAM + Extreme Cache) (Decimal

Items	Explanation
	notation. The unit is %.) (*1, *2) <i>delay-r-qos</i> : Read QoS Delay Time at <i>date</i> . (Decimal notation. The unit is msec.) (*3, *4) <i>delay-w-qos</i> : Write QoS Delay Time at <i>date</i> . (Decimal notation. The unit is msec.) (*3, *4)

*1: When this function is disabled for a device that supports Extreme Cache performance information, "0" will be output.

Example: For a device that supports Extreme Cache performance information (function disabled)

```
...,hit-r-extreme-cache,hit-r-dram-extreme-cache
...,0,0
```

*2: For a device that does not support Extreme Cache performance information, a value will not be output and instead a series of commas will be output.

Example: For a device that does not support Extreme Cache performance information

```
...,hit-r-extreme-cache,hit-r-dram-extreme-cache
,,,,,
```

*3: When this function is disabled for a device that supports Host-LU QoS performance information (QoS Delay Time), "0" will be output.

Example: For a device that supports Host-LU QoS performance information (function disabled)

```
...,delay-r-qos,delay-w-qos
...,0,0
```

*4: For a device that does not support Host-LU QoS performance information (QoS Delay Time), a value will not be output and instead a series of commas will be output.

Example: For a device that does not support Host-LU QoS performance information

```
...,delay-r-qos,delay-w-qos
,,,,,
```

The Disk performance information of storage device

Items	Explanation
File name	Disk/ <i>nnnn</i> .csv (<i>nnnn</i> indicates the DE number by hexadecimal notation.)
Header line	- For disk mounted on CE: Date, CE(DE0x00):DiskX - busy time, ... - For disk mounted on DE: Date, DE0xXX:DiskX - busy time, ...
Data line	<i>date</i> , <i>Disk0</i> , ... , <i>DiskN</i> The following information is output for each field. (After <i>date</i> , the information is repeated for the actual number of Disks.) <i>date</i> : Performance Information Acquisition Time (YYYY/MM/DD hh:mm:ss format) <i>Disk0</i> : Disk0 Disk busy rate at <i>date</i> (Decimal notation. The unit is %.) <i>DiskN</i> : DiskN Disk busy rate at <i>date</i> (Decimal notation. The unit is %.)

The CA/CM Port performance information of storage device

Items	Explanation
File name	Port/ <i>nnnn</i> .csv (<i>nnnn</i> indicates the CA/CM Port number by hexadecimal notation. CA/CM port numbers are assigned in ascending order, starting with 0000 for the lowest CA/CM port number in the device. CM0x0 CA0x0 Port0 is 0000, CM0x0 CA0x0 Port1 is 0001, :

Items	Explanation
	CM0x7 CA0x3 Port2 is 007E, CM0x7 CA0x3 Port3 is 007F.)
Header line	- Case of CA Port Date, CM0xX:CA0xX:PortX - Read IOPS, CM0xX:CA0xX:PortX - Write IOPS, CM0xX:CA0xX:PortX - Read Throughput, CM0xX:CA0xX:PortX - Write Throughput - Case of CM Port Date, CM0xX:PortX - Read IOPS, CM0xX:PortX - Write IOPS, CM0xX:PortX - Read Throughput, CM0xX:PortX - Write Throughput
Data line	<i>date,read,write,through-r,through-w</i> The following information is output for each field. <i>date</i> : Performance Information Acquisition Time (YYYY/MM/DD hh:mm:ss format) <i>read</i> : Read Count at <i>date</i> (Decimal notation. The unit is IOPS.) <i>write</i> : Write Count at <i>date</i> (Decimal notation. The unit is IOPS.) <i>through-r</i> : Read data transfer rate at <i>date</i> (Decimal notation. The unit is MB/S.) <i>through-w</i> : Write data transfer rate at <i>date</i> (Decimal notation. The unit is MB/S.)

Note: According to the port mode of the target CA/CM Port, the following is added at the end of each port name in the header line.

Port Mode	FC	iSCSI
CA	-	(iSCSI-CA)
RA	(FC-RA)	(iSCSI-RA)
CA/RA	(FC-CA/RA)	(iSCSI-CA/RA)

The number of active disks performance information of storage device (ETERNUS DX200F excluded)

Items	Explanation
File name	ACTIVE_DISK.csv
Header line	Date, Total Disks, Active Disks
Data line	<i>date,total,active</i> The following information is output for each field. <i>date</i> : Performance Information Acquisition Time (YYYY/MM/DD hh:mm:ss format) <i>total</i> : Overall number of loaded disk devices at <i>date</i> (Decimal notation. The unit is Disk.) <i>active</i> : Overall number of active disk devices at <i>date</i> (Decimal notation. The unit is Disk.)

Power consumption performance information of storage device (ETERNUS DX60/DX60 S2/DX80/DX80 S2/DX90/DX90 S2/DX100 S3/DX200 S3, ETERNUS DX400 S2 series, ETERNUS DX500 S3/DX600 S3 and ETERNUS DX8000 S2 series only. However, ETERNUS DX200F excluded)

Items	Explanation
File name	SYSTEM_POWER_CONSUMPTION.csv
Header line	Date, System Power Consumption
Data line	<i>date, power</i> The following information is output for each field. <i>date</i> : Performance Information Acquisition Time (YYYY/MM/DD hh:mm:ss format) <i>power</i> : Power used by the device as a whole at <i>date</i> (Decimal notation. The unit is Watt.)

Temperature performance information of storage device (ETERNUS DX60/DX60 S2/DX80/DX80 S2/DX90/DX90 S2/DX100 S3/DX200 S3, ETERNUS DX400 S2 series, ETERNUS DX500 S3/DX600 S3 and ETERNUS DX8000 S2 series only. However, ETERNUS DX200F excluded)

Items	Explanation
File name	SYSTEM_TEMPERATURE.csv
Header line	Date, System Temperature
Data line	<p><i>date, temperature</i></p> <p>The following information is output for each field.</p> <p><i>date</i> : Performance Information Acquisition Time (YYYY/MM/DD hh:mm:ss format)</p> <p><i>temperature</i> : Air intake temperature at device at <i>date</i> (Decimal notation. The unit is degrees Centigrade.)</p>

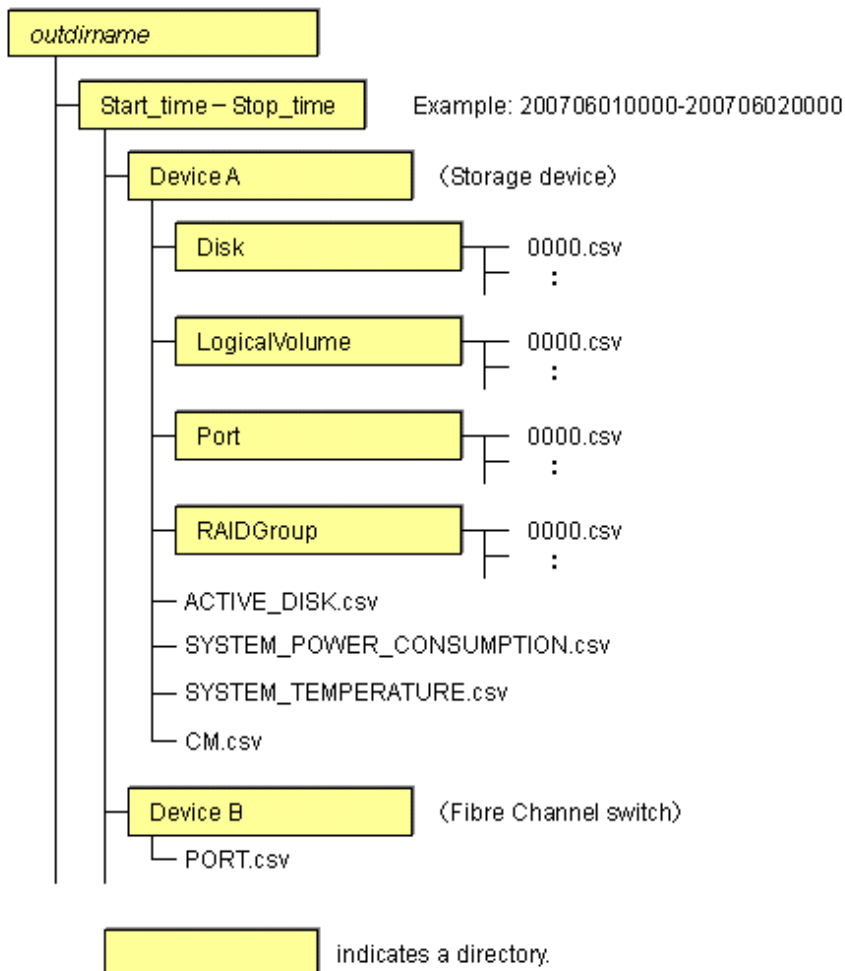
OPERANDS

export

Outputs performance information for the specified date in the CSV format.

outdirname

Specify the directory that outputs performance information. The full path of an existing directory must be specified in *outdirname*. Performance information is output to the *outdirname* directory based on the following configuration.



OPTIONS

-ipaddr *ipaddr*

Specify the IP address of the device that outputs performance information.

The output target device must satisfy the following conditions:

- The device is registered with this software, and it is one of the following performance monitoring targets:
 - ETERNUS DX series
 - The Fibre Channel switches and Fibre Channel switch blades which support the performance monitoring.

Refer to "[7.2.2 Instruction for performance management](#)" for the settings of performance monitoring.

-date *start_time*[-*end_time*]

Specify the start and end times for the output of performance information in YYYYMMDDhhmm format. The start and end times must be concatenated using a hyphen ("-"), as follows:

YYYYMMDDhhmm-YYYYMMDDhhmm

If the hyphen ("-") and end time are omitted, the command execution time will be the end time.

The time that is specified for the **-date** option start time must be earlier than the end time. Additionally, the time that is specified for the start and end times must be later than 00:00 on 01/08/2001, and earlier than the command execution time.

If this option is omitted, a time 30 minutes before the command execution time will be the start time, and the command execution time will be the end time.

EXAMPLES

Windows environment

- Output of performance information from 00:00 on 01/01/2012 to 23:59 on 01/01/2012 for a device with IP address 10.101.12.13 to the c:\work directory:

```
> storageadm perfdata export "C:\work" -ipaddr 10.101.12.13 -date 201201010000-201201012359
```

- Output of performance information from 00:00 on 01/01/2012 to now for a device with IP address 10.101.12.13 to the c:\work directory:

```
> storageadm perfdata export "C:\work" -ipaddr 10.101.12.13 -date 201201010000
```

Solaris or Linux environment

- Output of performance information from 00:00 on 01/01/2012 to 23:59 on 01/01/2012 for a device with IP address 10.101.12.13 to the /tmp/work directory:

```
> storageadm perfdata export /tmp/work -ipaddr 10.101.12.13 -date 201201010000-201201012359
```

- Output of performance information from 00:00 on 01/01/2012 to now for a device with IP address 10.101.12.13 to the /tmp/work directory:

```
> storageadm perfdata export /tmp/work -ipaddr 10.101.12.13 -date 201201010000
```

12.1.1.7 storageadm spindle (Disk control command)

NAME

storageadm spindle - controls disks

SYNOPSIS

```
storageadm spindle start -ipaddr i paddr {-raid RAIDgroup_number[,RAIDgroup_number,...] | -server} [-sync [-time timeout]]
```

```
storageadm spindle stop -ipaddr i paddr {-raid RAIDgroup_number[,RAIDgroup_number,...] | -server} [-sync [-time timeout]] [-s] [-f]
```

```
storageadm spindle info -ipaddr i paddr [{-raid RAIDgroup_number[,RAIDgroup_number,...] | -server}]
```

COMMAND PATH

Windows environment

```
$INS_DIR\ESC\Manager\opt\FJSVssmgr\sbin\storageadm spindle
```

(\$INS_DIR means "Program Directory" specified at the ETERNUS SF Manager installation.)

Solaris or Linux environment

```
/opt/FJSVssmgr/sbin/storageadm spindle
```

DESCRIPTION

Starts or stops the storage device RAID disk rotation.

In the Windows environment, only a user of the Administrators group can execute this command.

In the Solaris or Linux environment, only OS administrator (root) user can execute this command.

If a storage device was specified when the status was displayed, the rotation status of the disk that was used to configure RAID is displayed.

If a server was specified, the storage device RAID group number and volume number used by the server are displayed.

By specifying the storage device IP address and RAID group number in the command operand, the rotation of the disk that was used to configure the storage device RAID is started or stopped.

By specifying the server IP address, the rotation of the storage device disk used by the server is started or stopped.

The target storage device and server must be devices managed by this software.

OPERANDS

start

Starts the disk that is used to configure the storage device RAID group.

stop

Stops the disk that is used to configure the storage device RAID group.

info

Displays the storage device RAID group Eco-mode information, or the storage device information used by the server.

OPTIONS

Options of the start operand

-ipaddr *ipaddr*

Specify the storage device or server IP address.

-raid *RAIDgroup_number*[,*RAIDgroup_number*,...]

Specify the start target RAID group number using hexadecimal notation.

If more than one RAID group number is specified, separate each number using a comma (",").

Specify this option when the storage device IP address has been specified in the -ipaddr option.

-server

The rotation of the storage device disk used by the specified server is started.
Specify this option when the server IP address has been specified in the `-ipaddr` option.

-sync

There is no return until processing is complete, or the time specified in the `-time` option has elapsed.

-time *timeout*

Specify the timeout value (unit: seconds) if the `-sync` option has been specified. Specify a number from 1 to 86400.
If this option is omitted, the timeout value will be 600 seconds.

Options of the stop operand

-ipaddr *ipaddr*

Specify the storage device or server IP address.

-raid *RAIDgroup_number*[,*RAIDgroup_number*,...]

Specify the stop target RAID group number using hexadecimal notation.
If more than one RAID group number is specified, separate each number using a comma (",").
Specify this option when the storage device IP address has been specified in the `-ipaddr` option.

-server

The rotation of the storage device disk used by the specified server is stopped.
Specify this option when the server IP address has been specified in the `-ipaddr` option.

-sync

There is no return until processing is complete, or the time specified in the `-time` option has elapsed.

-time *timeout*

Specify the timeout value (unit: seconds) if the `-sync` option has been specified. Specify a number from 1 to 86400.
If this option is omitted, the timeout value will be 600 seconds.

-s

Processing continues without the output of a confirmation message.

-f

Related RAID group disks are forcibly stopped.

Options of the info operand

-ipaddr *ipaddr*

Specify the storage device or server IP address.

-raid *RAIDgroup_number*[,*RAIDgroup_number*,...]

Specify the status display target RAID group number using hexadecimal notation.
If more than one RAID group number is specified, separate each number using a comma (",").
Specify this option when the storage device IP address has been specified in the `-ipaddr` option.

If this option is omitted, the information for all RAID groups in the specified storage device is displayed.

-server

The storage device RAID group Eco-mode information and volume number used by the specified server are displayed.
Specify this option when the server IP address has been specified in the `-ipaddr` option.

EXAMPLES

- Starting the disk that is used to configure the RAID group by specifying the storage device IP address and RAID group number:

```
> storageadm spindle start -ipaddr 10.10.10.10 -raid 0x0000,0x0001
```

- Stopping the disk that is used to configure the RAID group by specifying the storage device IP address and RAID group number:

```
> storageadm spindle stop -ipaddr 10.10.10.10 -raid 0x0001
```

- Stopping the disk that is used by the server by specifying the server:

```
> storageadm spindle stop -ipaddr 10.10.10.20 -server
```

- Displaying the Eco-mode status of all RAID groups in a storage device:

```
> storageadm spindle info -ipaddr 10.10.10.10
<<< ECO Mode RAID Group Information >>>
RAIDGROUP_NUMBER(NAME)  MODE DISK_STATUS          CONTROL SCHEDULE
-----
0x0000(data1)           ON   Idle                    OFF    External
0x0001(data2)           ON   in the boot process    ON     01-NAME0001
0x0002                  OFF  Active                  -
0x0003                  -    Active                  -
-----
```

The explanation of the information displayed in each field is as follows.

Field Title	Explanation
RAIDGROUP_NUMBER(NAME)	Displays the RAID group number by the hexadecimal number of four digits. When the name is set on the RAID group, its name is displayed by enclosing in ().
MODE	Displays the Eco-mode status that is set on the RAID group. <ul style="list-style-type: none"> - "ON": Eco-mode is enabled. - "OFF": Eco-mode is disabled. - "-"(hyphen): Eco-mode cannot be set.
DISK_STATUS	Displays the status of disks that compose the RAID group. <ul style="list-style-type: none"> - "Active": Disks are active. - "Idle": Disks are inactive. - "In the boot process": Disks start in progress. - "In the stop process": Disks stop in progress.
CONTROL	Displays the disk control status set on the RAID group. <ul style="list-style-type: none"> - "ON": Disk starting is requested. - "OFF": Disk stopping is requested. - "-"(hyphen): Uncontrollable.
SCHEDULE	Displays the Eco-mode schedule set on RAID group by the following format. The schedule name of External is displayed as "External". number-name The "number" is displayed in decimal number, and "name" is displayed in eight characters or less.

- Displaying the storage device RAID group number and volume number that are used by the server:

```
> storageadm spindle info -ipaddr 10.10.10.20 -server
<<< ECO Mode RAID GROUP information for Server >>>
IP_ADDRESS  RAID  MODE DISK_STATUS          CONTROL STOP
-----
10.10.10.10  0x0000 ON   Idle                    OFF
              0x0001 ON   Active                  ON      *
```

<<< Disk use information on Server >>>

```
IP_ADDRESS      RAID    VOLUME
-----
10.10.10.10    0x0000 0x0000,0x0001,0x0002,0x0003,0x0004,0x0005,0x0006,0x0007,
                                0x0008,0x0009,0x000A,0x000B,0x000C,0x000D,0x000E,0x000F,
                                0x0001 0x0010,0x0011,0x0012,0x0013,0x0014,0x0015,0x0016,0x0017,
                                0x0018,0x0019,0x001A,0x001B,0x001C,0x001D,0x001E,0x001F
-----
```

The explanation of the information displayed in each field is as follows.

- <<< ECO Mode RAID GROUP information for Server >>> information

Field Title	Explanation
IP_ADDRESS	Displays the IP address of the storage device connected with the specified server.
RAID	Displays the RAID group number by the hexadecimal number of four digits. The RAID group including the volume used from the specified server is displayed.
MODE	Displays the Eco-mode status that is set on the RAID group. <ul style="list-style-type: none"> - "ON": Eco-mode is enabled. - "OFF": Eco-mode is disabled. - "-"(hyphen): Eco-mode cannot be set.
DISK_STATUS	Displays the status of disks that compose the RAID group. <ul style="list-style-type: none"> - "Active": Disks are active. - "Idle": Disks are inactive. - "In the boot process": Disks start in progress. - "In the stop process": Disks stop in progress.
CONTROL	Displays the disk control status set on the RAID group. <ul style="list-style-type: none"> - "ON": Disk starting is requested. - "OFF": Disk stopping is requested. - "-"(hyphen): Uncontrollable.
STOP	Although the stopping the disks used from the specified server is directed, when any disks in this RAID group are used from other server or this RAID group cannot be stopped because of any following states, displays "*". <ul style="list-style-type: none"> - The RAID group for which the system disk is included - The RAID group for which it is set in the NAS area - The RAID group for which the mainframe volumes, MVV volumes, or MVV Concatenation volumes are registered

- <<< Disk use information on Server >>> information

Field Title	Explanation
IP_ADDRESS	Displays the IP address of the storage device connected with the specified server.
RAID	Displays the RAID group number by the hexadecimal number of four digits. The RAID group including the volume used from the specified server is displayed.
VOLUME	Displays the volume number by the hexadecimal number of four digits. The volumes used from the specified server are displayed.

NOTES

- Storage devices must be registered with this software in order to start or stop disk rotation, or to display the rotation status of the disk. However, rotation statuses of disks for the following devices which are not registered with this software (but registered) are displayed.
 - ETERNUS DX60/DX60 S2/DX80/DX90
 - ETERNUS DX400 series
 - ETERNUS DX8000 series
- There are RAID groups that cannot do the Eco-mode operation. Refer to "Uncontrollable RAID groups" in "1.2.5 Energy-saving operation for storage device".
- The RAID group Eco-mode must be ON to operate the RAID group start/stop control. Refer to "6.1.6 How to control the Eco-mode" for details on the procedure for setting the RAID group Eco-mode to ON.
- If disk rotation is started and stopped by specifying the server IP address, do not change the storage device connection.
- For the following cases, the disk rotation cannot be stopped by specifying the server IP address:
 - If one or more share disks are contained on the stopped disks.

Check the status of all servers that use their share disks, and judge whether share disks can be stopped or not. If share disks can be stopped, specify the -f option.
 - If the disks used from other server are included in the RAID group that stop target disk exists.

To stop the disk rotation, either specify server IP address for all servers that use the disk of its RAID group, or specify the -f option. When you specify -f option, check the status of all related servers, and judge whether disks can be stopped or not. It is recommended that the server and the RAID group be the compositions of couple 1.
 - If the RAID group including unused disks.

Re-execute either specify the -f option or specify the RAID group.
 - If the RAID group including the stop target disk is any of "Uncontrollable RAID groups".
- If the volume that belongs to the specified stop target RAID group is concatenated with a different RAID group using the LUN concatenation functionality, the disk is not stopped even if the "stop" operand is specified. To stop all related RAID group disks, either specify all of the related RAID groups, or specify the -f option. However, if the related RAID group is any of "Uncontrollable RAID groups", the disk control cannot be executed.
- The message below is output when the "stop" operand is specified. To continue, enter "y". To cancel, enter "n". This message is not output when the -s option is specified.

```
Are you sure? [y/n]:
```

- The information of storage device that can control disks is displayed on the storage device information used by the server. The information of storage device that cannot control disks is not displayed. When both the disk controllable storage device and the disk uncontrollable storage device are connected with the server, the information of disk controllable storage device is only displayed.
- The disk does not stop when the RAID group status is as follows:
 - Part of the storage device controller module and the module for the disk drive access route contain a fault.
 - The disk drive that was used to configure the RAID group is faulty.
 - There is a copy data of Advanced Copy.
 - There is an EC/REC session (including when there is no copy data. However, the disk will stop when the EC/REC status is Suspend.
 - There is a QuickOPC/SnapOPC session (including when there is no copy data).

12.1.1.8 storageadm remcs (REMCS notification command)

NAME

storageadm remcs - REMCS notification (Windows environment only)

SYNOPSIS

```
storageadm remcs send -ipaddr ipaddr -type type
```

COMMAND PATH

Windows environment

```
$INS_DIR\ESC\Manager\opt\FJSVssmgr\sbin\storageadm remcs
```

(\$INS_DIR means "Program Directory" specified at the ETERNUS SF Manager installation.)

DESCRIPTION

This command is used to send REMCS notification of Fibre Channel switch which is registered with this software.

OPERANDS

send

As for REMCS notification of the Fibre Channel switch whose IP address is specified, sends a test mail.

OPTIONS

Options that can be specified when the send operand is specified

-ipaddr ipaddr

Specify the IP address of Fibre Channel switch.

-type type

Specify the type of the sending mail.

Make sure to specify "test".

EXAMPLES

- Send a test mail.

```
> storageadm remcs send -ipaddr 10.10.10.10 -type test
```

NOTES

- The Fibre Channel switch to be specified must be registered with this software.
- The settings for REMCS notification must be done in advance.

12.1.1.9 esfsnap (Troubleshooting information collection of Manager)

NAME

esfsnap - Collects the troubleshooting information of Manager

SYNOPSIS

```
esfsnap -dir dirname [-all]
```

COMMAND PATH

Windows environment

```
$INS_DIR\Common\bin\esfsnap
```

(\$INS_DIR means "Program Directory" specified at the ETERNUS SF Manager installation.)

Solaris or Linux environment

```
/opt/FJSVesfcm/bin/esfsnap
```

DESCRIPTION

Collect information of the Manager on the Management Server.

Only OS administrator user can execute this command.

The esfsnap is the command used to collect information on the Management Server when a problem occurs. Submit the information to Fujitsu technical staff.

OPTIONS

-dir *dirname*

Specify the directory that stores the troubleshooting information for *dirname*.

In the Windows environment, specify the full path name that starts from the drive letter for *dirname*. The maximum length that can be specified for *dirname* is 70 bytes.

In the Solaris or Linux environment, specify the full path name for *dirname*.

In the Windows environment, the collected information is stored in the directory that its name starts with "esfsnap_". In the Solaris or Linux environment, the collected information is gathered in the file that its name starts by "esfsnap_". Before executing this command, confirm that *dirname* directory has the following free space.

Collected Information	Required Free Space
Initial investigation information	more than 40MB
All troubleshooting information	more than "80 + (2 * Number_of_registered_devices)" MB

-all

Collects all troubleshooting information on servers. Data includes lots of information, which will increase the size of the data. This option is not necessary for initial investigation.

EXAMPLES

Windows environment

- Collecting the troubleshooting information for initial investigation on D:\temp directory.

```
> esfsnap -dir D:\temp
```

Solaris or Linux environment

- Collecting the troubleshooting information for initial investigation on /tmp directory.

```
> esfsnap -dir /tmp
```

12.1.2 Commands for storage management

The following sub sections explain the commands for managing the storage device.

In the Windows environment, only a user of the Administrators group can execute this command.

In the Solaris or Linux environment, only OS administrator (root) user can execute this command.

The following table shows the relationship between commands and the storage devices where they can be used. The storage device must be registered with this software.

Command Name	ETERNUS DX80 S2 ETERNUS DX90 S2 ETERNUS DX100 S3/DX200 S3 ETERNUS DX400 S2 series ETERNUS DX500 S3/DX600 S3 ETERNUS DX8000 S2 series	ETERNUS DX60/DX60 S2 ETERNUS DX80 ETERNUS DX90 ETERNUS DX400 series ETERNUS DX8000 series
storageadm disk	Available	Available (*1)
storageadm raid	Available (*3)	Available (*1)
storageadm volume	Available	Available (*1)
storageadm affinity	Available	Available (*1)
storageadm ecomode	Available (*4)	Available (*1)
storageadm port	Available	Available (*1)
storageadm iscsiport	Available	Available (*1 and *2)
storageadm progress	Available	Available (*1)

*1: Its information can be displayed even if the device is not registered with this software (but detected).

*2: For ETERNUS DX60/DX60 S2/DX80, only iSCSI model device is supported.

*3: ecomode operand does not support ETERNUS DX200F.

*4: This command does not support ETERNUS DX200F.

12.1.2.1 storageadm disk (Disk management command)

NAME

storageadm disk - Manages disks

SYNOPSIS

```
storageadm disk info -ipaddr ipaddr [-csv]
```

COMMAND PATH

Windows environment

```
$INS_DIR\ESC\Manager\opt\FJSVssmgr\sbin\storageadm disk
```

(\$INS_DIR means "Program Directory" specified at the ETERNUS SF Manager installation.)

Solaris or Linux environment

/opt/FJSVssmgr/sbin/storageadm disk

DESCRIPTION

This command displays information of disks in the ETERNUS Disk storage system that is registered with this software.

OPERANDS

info

Displays detail information of disks in the ETERNUS Disk storage system that is registered with this software.

OPTIONS

Options of the info operand

-ipaddr *ipaddr*

Specify the IP address of the storage device.

-csv

Displays the disk information in the CSV format.

If this option is omitted, it is displayed in the table format.

EXAMPLES

- Displaying the disk information in the table format.

```
> storageadm disk info -ipaddr 192.168.0.1
<<< Disk Information >>>
NUMBER DE   SLOT USAGE           STATUS   RGNO   SIZE  DISKTYPE MOTOR
-----
0      0x00 0    System Disk   Available 0x0002 300GB SAS   Active
1      0x00 1    System Disk   Available 0x0001 300GB SAS   Idle
2      0x00 2    System Disk   Available 0x0002 300GB SAS   In the boot process
3      0x00 3    System Disk   Available 0x0003 300GB SAS   In the stop process
4      0x00 4    Data Disk     Available 0x0003 300GB SAS   Active
-----
INFO:swsag0001:Command terminated normally.
```

- Displaying the disk information in the CSV format.

```
> storageadm disk info -ipaddr 192.168.0.1 -csv
NUMBER,DE,SLOT,USAGE,STATUS,RGNO,SIZE,DISKTYPE,MOTOR
0,0x00,0,System Disk,Available,0x0002,300GB,SAS,Active
1,0x00,1,System Disk,Available,0x0001,300GB,SAS,Idle
2,0x00,2,System Disk,Available,0x0002,300GB,SAS,In the boot process
3,0x00,3,System Disk,Available,0x0003,300GB,SAS,In the stop process
4,0x00,4,Data Disk,Available,0x0003,300GB,SAS,Active
```

12.1.2.2 storageadm raid (RAID management command)

NAME

storageadm raid - Manages RAID groups

SYNOPSIS

```
storageadm raid add -ipaddr ipaddr -disk
DE_number:slot_number,DE_number:slot_number[,DE_number:slot_number,...] -level RAIDlevel [-name
alias_name] [-cm assigned_CM] [-csv]

storageadm raid delete -ipaddr ipaddr -raidgroup RAIDgroup_number [-f] [-s]

storageadm raid info -ipaddr ipaddr [-raidgroup RAIDgroup_number] [-remote BOX-ID] [-csv]

storageadm raid ecomode -ipaddr ipaddr -raidgroup RAIDgroup_number[,RAIDgroup_number,...] -on|-off [-s]
```

COMMAND PATH

Windows environment

```
$INS_DIR\ESC\Manager\opt\FJSVssmgr\sbin\storageadm raid
```

(\$INS_DIR means "Program Directory" specified at the ETERNUS SF Manager installation.)

Solaris or Linux environment

```
/opt/FJSVssmgr/sbin/storageadm raid
```

DESCRIPTION

This command is used to create/delete/display and sets the Eco-mode for a RAID group in the ETERNUS Disk storage system that is registered with this software.

OPERANDS

add

Creates a RAID group

delete

Deletes a RAID group

info

Displays a RAID group information

ecomode

Sets the Eco-mode for the RAID group

OPTIONS

Options of the add operand

-ipaddr *ipaddr*

Specify the IP address of the storage device.

-disk *DE_number.slot_number,DE_number.slot_number[,DE_number.slot_number,...]*

Specify DE numbers and slot numbers for the storage device using either decimal or hexadecimal notation, placing a colon (":") in the middle of each DE number and slot number pair, and using commas (",") to separate pairs. For example, two pairs can be specified as "-disk 1:1,1:2" in decimal notation or "-disk 0x1:0x1,0x1:0x2" in hexadecimal notation.

Be sure to specify at least two DE number/slot number pairs.

-level *RAIDlevel*

Specify the RAID level by the minuscule as follows.

Characters that can be specified	Created RAID Level
raid0	RAID0
raid1	RAID1
raid1+0	RAID1+0
raid5	RAID5
raid5+0	RAID5+0
raid6	RAID6

-name *alias_name*

Specify an alias for the RAID group to be created.

Only alphanumeric characters (a to z, A to Z and 0 to 9) and the following symbols can be used for aliases: !@#\$\$%^&*()-= ` _ + | ~[]{};:~"/<>?. However, "?" is not supported for ETERNUS DX80 S2/DX90 S2/DX100 S3/DX200 S3, ETERNUS DX400 S2 series, ETERNUS DX500 S3/DX600 S3 and ETERNUS DX8000 S2 series. If the alias contains a space, enclose the entire alias in double quotes (e.g., -name "123 567").

If this option is omitted, the specification is as follows:

Storage Device	Specification when this option is omitted
ETERNUS DX60/DX60 S2 ETERNUS DX80/DX80 S2 ETERNUS DX90/DX90 S2 ETERNUS DX100 S3/DX200 S3 ETERNUS DX400 S2 series ETERNUS DX500 S3/DX600 S3 ETERNUS DX8000 S2 series	An alias name is set automatically.
ETERNUS DX400 series ETERNUS DX8000 series	An alias name is not set.

-cm *assigned_CM*

Specify the assigned CM number for the RAID group using two digits, as in the following table. If this option is omitted, the assigned CM number will be set up automatically ("auto" will be specified).

Storage Device	Assigned CM	Characters to be specified	Remarks
ETERNUS DX60/DX60 S2 ETERNUS DX80/DX80 S2 ETERNUS DX90/DX90 S2 ETERNUS DX100 S3/DX200 S3 ETERNUS DX500 S3/DX600 S3	CM#0	00	For the first digit, enter the assigned CM number. For the second character, always enter "0".
	CM#1	10	
ETERNUS DX400 series ETERNUS DX400 S2 series ETERNUS DX8000 series ETERNUS DX8000 S2 series	CM#0 CPU#0	00	For the first digit, enter the assigned CM number. For the second digit, enter the number of the CPU within the CM entered for the first digit.
	CM#0 CPU#1	01	
	CM#1 CPU#0	10	
	CM#1 CPU#1	11	
	:	:	
	CM#7 CPU#0	70	
	CM#7 CPU#1	71	

-csv

Displays the RAID group number in the CSV format.
If this option is omitted, it is displayed in the table format.

Options of the delete operand

-ipaddr *ipaddr*

Specify the IP address of the storage device.

-raidgroup *RAIDgroup_number*

Specify the RAID group number to be deleted, using either decimal or hexadecimal notation. For example, RAID group number 16 can be specified as "-raidgroup 16" in decimal notation or "-raidgroup 0x10" in hexadecimal notation.

-s

Processing continues without the output of a confirmation message.

-f

If there are volumes within the RAID group, the volumes will be deleted before the RAID group is deleted. However, the command will terminate with an error without deleting the volumes if any of the following conditions apply to the RAID group:

- The volumes in the RAID group have been mapped
- There are volumes other than open volumes
- There are LUN concatenated volumes
- There are ODX Buffer Volumes

Options of the info operand

-ipaddr *ipaddr*

Specify the IP address of the storage device.

-raidgroup *RAIDgroup_number*

Specify the RAID group number for which detailed information is to be displayed, using either decimal or hexadecimal notation. For example, RAID group number 16 can be specified as "-raidgroup 16" in decimal notation or "-raidgroup 0x10" in hexadecimal notation.

-remote *BOX-ID*

Specify a Box ID for the remote site ETERNUS Disk storage system. Specify it when you display the RAID group information of the remote site ETERNUS Disk storage system.

-csv

Displays the RAID group information in the CSV format.
If this option is omitted, it is displayed in the table format.

Options of the ecomode operand

-ipaddr *ipaddr*

Specify the IP address of the storage device.

-raidgroup *RAIDgroup_number*[,*RAIDgroup_number*,...]

Specify the RAID group number for which detailed information is to be displayed, using decimal and/or hexadecimal notations. For example, RAID group number 16 can be specified as "-raidgroup 16" in decimal notation or "-raidgroup 0x10" in hexadecimal notation.

The more than one RAID group number can be specified.

-on

Set the Eco-mode to ON for the specified RAID group.
This option cannot be specified at the same time as the -off option.
This option cannot be set if the Eco-mode cannot be set for any one of the specified RAID groups.

-off

Set the Eco-mode to OFF for the specified RAID group.
This option cannot be specified at the same time as the -on option.

-s

Continues processing without asking for confirmation.

EXAMPLES

- Creating a RAID group and displaying the created RAID group in the table format.

```
# /opt/FJSVssmgr/sbin/storageadm raid add -ipaddr 1.2.3.4 -disk 1:10,1:11,1:12,1:13,1:14,1:15 -
level raid5
<<< RAID ADD >>>
RGNO
-----
0x0000
-----
INFO:swsag0001:Command terminated normally.
```

- Creating a RAID group and displaying the created RAID group in the CSV format.

```
# /opt/FJSVssmgr/sbin/storageadm raid add -ipaddr 1.2.3.4 -disk 1:10,1:11,1:12,1:13,1:14,1:15 -
level raid5 -csv
RGNO
0x0000
```

- Deleting a RAID group.

```
# /opt/FJSVssmgr/sbin/storageadm raid delete -ipaddr 1.2.3.4 -raidgroup 16
Are you sure? [y/n]:y
INFO:swsag0001:Command terminated normally.
```

- Displaying the RAID group information in the table format.

```
# /opt/FJSVssmgr/sbin/storageadm raid info -ipaddr 1.2.3.4
<<< RAID Information >>>
RGNO  NAME  USAGE      LEVEL  STATUS  CM      TOTAL_CAPACITY  FREE_CAPACITY
-----
0x0000  Open, System RAID5  Available  CM0CPU0  407775  0
0x0001  Open, SDV   RAID5  Available  CM1CPU0  410880  285440
0x0002  Open      RAID1  Available  CM0CPU1  136960  345367
-----
INFO:swsag0001:Command terminated normally.
```

- Displaying the RAID group information in the CSV format.

```
# /opt/FJSVssmgr/sbin/storageadm raid info -ipaddr 1.2.3.4 -csv
RGNO,NAME,USAGE,LEVEL,STATUS,CM,TOTAL_CAPACITY,FREE_CAPACITY
0x0000,, "Open, System", RAID5, Available, CM0CPU0, 407775, 0
0x0001,, "Open, SDV", RAID5, Available, CM1CPU0, 410880, 285440
0x0002,, Open, RAID1, Available, CM0CPU1, 136960, 345367
```

- Displaying the RAID group detail information in the table format.

```
# /opt/FJSVssmgr/sbin/storageadm raid info -ipaddr 1.2.3.4 -raidgroup 0x0000
<<< RAID Information >>>
RGNO  NAME  USAGE      LEVEL  STATUS  CM      TOTAL_CAPACITY  FREE_CAPACITY
-----
0x0000  Open, System RAID5  Available  CM0CPU0  407775  0

NO      CONCATENATION NAME      TOTAL_CAPACITY  ALLOCATED      STATUS  TYPE
CAPACITY
```

```

-----
0x0001 1/3          sample      102400      102400      Available Open
0x0001 2/3          sample      1024        1024        Available Open
Free -             -           2048        2048
0x0004 -           -           1536        1536        Available Open
-----

```

INFO:swsag0001:Command terminated normally.

- Displaying the RAID group detail information in the CSV format.

```

# /opt/FJSVssmgr/sbin/storageadm raid info -ipaddr 1.2.3.4 -raidgroup 0x0000 -csv
RGNO,NAME,USAGE,LEVEL,STATUS,CM,TOTAL_CAPACITY,FREE_CAPACITY,NO,CONCATENATION,NAME,TOTAL_CAPACITY
,ALLOCATED_CAPACITY,STATUS,TYPE
0x0000,"Open,System",RAID5,Available,CM0CPU0,407775,0,0x0001,1/3,sample,
102400,102400,Available,Open
0x0000,"Open,System",RAID5,Available,CM0CPU0,407775,0,0x0001,2/3,sample,1024,1024,Available,Open
0x0000,"Open,System",RAID5,Available,CM0CPU0,407775,0,Free,-,,2048,2048,,
0x0000,"Open,System",RAID5,Available,CM0CPU0,407775,0,0x0004,-,,1536,1536,Available,Open

```

- RAID group Eco-mode set to ON.

```

# /opt/FJSVssmgr/sbin/storageadm raid ecomode -ipaddr 1.2.3.4 -raidgroup 0x0000 -on
Are you sure? [y/n]:y
INFO:swsag0001:Command terminated normally.

```

- RAID group Eco-mode set to OFF.

```

# /opt/FJSVssmgr/sbin/storageadm raid ecomode -ipaddr 1.2.3.4 -raidgroup 0x0000 -off
Are you sure? [y/n]:y
INFO:swsag0001:Command terminated normally.

```

NOTES

- The message below will be output if the -s option is not specified with the "delete" operand. Enter "y" to continue or "n" to cancel. This message can be suppressed by specifying the -s option.

```
Are you sure? [y/n]:
```

- Setting the Eco-mode for a RAID group with an Eco-mode schedule already set results in the following:
 - RAID group Eco-mode set to ON -> Eco-mode ON overwrites the RAID group eco-mode schedule.
 - RAID group Eco-mode set to OFF -> An error occurs (unless the Eco-mode schedule is software-controlled).
- If the Eco-mode operation is not possible for the specified RAID group, then the command terminates with an error. Refer to "[Uncontrollable RAID groups](#)" in "[1.2.5 Energy-saving operation for storage device](#)" for details of RAID groups for which the Eco-mode operation is not possible.
- You can use the -remote option only when using the Dynamic LUN Mirroring function of ServerView Resource Orchestrator.
- Temporary volumes are displayed as unknown volumes.
- You cannot create a new volume from RAID group with temporary volumes.
- ODX Buffer Volumes are not displayed.

12.1.2.3 storageadm volume (Volume management command)

NAME

storageadm volume - Manages volumes

SYNOPSIS

```
storageadm volume add -ipaddr ipaddr -size capacity -raidgroup RAIDgroup_number [-name alias_name] [-csv]
```

```
storageadm volume delete -ipaddr ipaddr [-volume volume_number[,volume_number,...]] [-remote BOX-ID -remote-volume volume_number [-remote-force]] [-s]
```

```
storageadm volume format -ipaddr ipaddr -volume volume_number[,volume_number,...] [-s]
```

```
storageadm volume info -ipaddr ipaddr [-volume volume_number,...] [-remote BOX-ID] [-csv]
```

```
storageadm volume nomapping -ipaddr ipaddr [-volume volume_number,...] [-remote BOX-ID] [-csv]
```

COMMAND PATH

Windows environment

```
$INS_DIR\ESC\Manager\opt\FJSVssmgr\sbin\storageadm volume
```

(\$INS_DIR means "Program Directory" specified at the ETERNUS SF Manager installation.)

Solaris or Linux environment

```
/opt/FJSVssmgr/sbin/storageadm volume
```

DESCRIPTION

This command is used to create/delete/format/display volumes in the ETERNUS Disk storage system that is registered with this software.

OPERANDS

add

Creates a volume.

delete

Deletes volumes.

format

Formats volumes.

info

Displays volume information.

nomapping

Displays the information of volumes that are not mapped to affinity group.

OPTIONS

Options of the add operand

-ipaddr *ipaddr*

Specify the IP address of the storage device.

-size *capacity*

Specify the size of the volume to be created in MB or GB. 1 GB is equivalent to 1024 MB. For example, 1024 MB is specified as "-size 1024MB" or "-size 1GB".

-raidgroup *RAIDgroup_number*

Specify the RAID group number for which a volume is to be created, using either decimal or hexadecimal notation. For example, RAID group number 16 can be specified as "-raidgroup 16" in decimal notation or "-raidgroup 0x10" in hexadecimal notation.

-name *alias_name*

Specify an alias for the volume to be created.

Only alphanumeric characters (a to z, A to Z and 0 to 9) and the following symbols can be used for aliases: !@#\$%^&*()-= ` _+|~[]{};:~"/.<>?. However, "?" is not supported for ETERNUS DX80 S2/DX90 S2/DX100 S3/DX200 S3, ETERNUS DX400 S2 series, ETERNUS DX500 S3/DX600 S3 and ETERNUS DX8000 S2 series. If the alias contains a space, enclose the entire alias in double quotes (e.g., -name "123 567").

If this option is omitted, the specification is as follows:

Storage Device	Specification when this option is omitted
ETERNUS DX60/DX60 S2 ETERNUS DX80/DX80 S2 ETERNUS DX90/DX90 S2 ETERNUS DX100 S3/DX200 S3 ETERNUS DX400 S2 series ETERNUS DX500 S3/DX600 S3 ETERNUS DX8000 S2 series	An alias name is set automatically.
ETERNUS DX400 series ETERNUS DX8000 series	An alias name is not set.

-csv

Displays the created volume number in the CSV format.
if this option is omitted, it is displayed in the table format.

Options of the delete operand or format operand

-ipaddr *ipaddr*

Specify the IP address of the storage device.

-volume *volume_number*[,*volume_number*,...]

Specify the numbers for the volumes to be deleted or formatted, using either decimal or hexadecimal notation.

If multiple volume numbers are specified, use commas (",") to separate volume numbers. For example, specify volumes 10 and 16 as either "-volume 10,16" in decimal notation or "-volume 0xa,0x10" in hexadecimal notation.

-remote *BOX-ID*

Specify a Box ID for the remote site ETERNUS Disk storage system. Specify it when you display the RAID group information of the remote site ETERNUS Disk storage system.

-remote-volume *volume_number*

Specify the number for the volume to be deleted from the remote site ETERNUS Disk storage system using either a decimal or hexadecimal number. Multiple volume numbers cannot be specified. If multiple volume numbers are specified, only the first one will be used.

Volumes which may be currently used cannot be deleted.

-remote-force

Specify this option to forcibly delete volumes, which may be currently used, from the remote site ETERNUS Disk storage system.

-s

Processing continues without the output of a confirmation message.

Options of the info operand or nomapping operand

-ipaddr *ipaddr*

Specify the IP address of the storage device.

`-volume volume_number[,volume_number,...]`

Specify the numbers for the volumes to be output for which information is to be output, using either decimal or hexadecimal notation. If multiple volume numbers are specified, use commas (",") to separate volume numbers. For example, specify volumes 10 and 16 as either "-volume 10,16" in decimal notation or "-volume 0xa,0x10" in hexadecimal notation.

If this option is omitted, information will be displayed for all target volumes.

`-remote BOX-ID`

Specify a Box ID for the remote site ETERNUS Disk storage system. Specify it when you display the RAID group information of the remote site ETERNUS Disk storage system.

`-CSV`

Displays the volume information in the CSV format.

If this option is omitted, it is displayed in the table format.

EXAMPLES

- Creating a volume and displaying the created volume in the table format.

```
> storageadm volume add -ipaddr 1.2.3.4 -size 1024MB -raidgroup 16
<<< Volume ADD >>>
NUMBER
-----
0x0001
-----
INFO:swsag0001:Command terminated normally.
```

- Creating a volume and displaying the created volume in the CSV format.

```
> storageadm volume add -ipaddr 1.2.3.4 -size 1024MB -raidgroup 16 -csv
NUMBER
0x0001
```

- Deleting a volume.

```
> storageadm volume delete -ipaddr 1.2.3.4 -volume 16
Are you sure? [y/n]: y
INFO:swsag0001:Command terminated normally.
```

- Formatting a volume.

```
> storageadm volume format -ipaddr 1.2.3.4 -volume 16
Are you sure? [y/n]: y
INFO:swsag0001:Command terminated normally.
```

- Displaying the volume information in the table format.

```
> storageadm volume info -ipaddr 1.2.3.4
<<< Volume Information >>>
NUMBER  NAME      TOTAL_CAPACITY STATUS   TYPE      CONCATENATION  RGNO  ENCRYPT
-----  -
Unknown  0          Available F6427G -      0x0001 -
0x0001   100        Available SDV     -      0x0000 -
0x0002   425        Available Open   -      0x0002 -
Unknown  1166       Available MVV(G) -      0x0001 -
Unknown  2332       Available MVV(G) 2      0x0001 -
0x0005   150        Available Open   -      0x0002 -
0x0006   4700       Available Open   3      0x0000,0x0002 -
-----
INFO:swsag0001:Command terminated normally.
```

- Displaying the volume information in the CSV format.

```
> storageadm volume info -ipaddr 1.2.3.4 -csv
NUMBER,NAME,TOTAL_CAPACITY,STATUS,TYPE,CONCATENATION,RGNO,ENCRYPT
Unknown,,0,Available,F6427G,-,0x0001,-
0x0001,,100,Available,SDV,-,0x0000,-
0x0002,,425,Available,Open,-,0x0002,-
Unknown,,1166,Available,MVV(G),-,0x0001,-
Unknown,,2332,Available,MVV(G),2,0x0001,-
0x0005,,150,Available,Open,-,0x0002,-
0x0006,,4700,Available,Open,3,"0x0000,0x0002",-
```

- Displaying the unused volume information in the table format.

```
> storageadm volume nomapping -ipaddr 1.2.3.4
<<< Volume Information >>>
NUMBER  NAME      TOTAL_CAPACITY STATUS    TYPE      CONCATENATION RGNO  ENCRYPT
-----  -
Unknown      0          Available F6427G -          0x0001 -
0x0001      100        Available SDV      -          0x0000 -
0x0002      425        Available Open    -          0x0002 -
Unknown      1166       Available MVV(G) -          0x0001 -
Unknown      2332       Available MVV(G) 2          0x0001 -
0x0005      150        Available Open  -          0x0002 -
0x0006      4700       Available Open  3          0x0000,0x0002 -
-----
INFO:swsag0001:Command terminated normally.
```

- Displaying the unused volume information in the CSV format.

```
> storageadm volume nomapping -ipaddr 1.2.3.4 -csv
NUMBER,NAME,TOTAL_CAPACITY,STATUS,TYPE,CONCATENATION,RGNO,ENCRYPT
Unknown,,0,Available,F6427G,-,0x0001,-
0x0001,,100,Available,SDV,-,0x0000,-
0x0002,,425,Available,Open,-,0x0002,-
Unknown,,1166,Available,MVV(G),-,0x0001,-
Unknown,,2332,Available,MVV(G),2,0x0001,-
0x0005,,150,Available,Open,-,0x0002,-
0x0006,,4700,Available,Open,3,"0x0000,0x0002",-
```

NOTES

- Only open volumes can be created.
- The volumes that are created are formatted automatically.
- The message below will be output if the -s option is not specified when either the "delete" operand or the "format" operand is specified.
Enter "y" to continue or "n" to cancel.
This message can be suppressed by specifying the -s option.

```
Are you sure? [y/n]:
```

- Volumes cannot be deleted by specifying the volume numbers for volumes that are not open volumes.
- Volumes cannot be deleted by specifying the volume numbers for LUN concatenated volumes.
- Volumes that have been mapped to an affinity group cannot be deleted.
- The Thin Provisioning Volume is not able to create. However, it possible to remove.
- You can use the -remote, the -remote-volume and the -remote-force options only when using the Dynamic LUN Mirroring function of ServerView Resource Orchestrator.
- Temporary volumes are displayed as unknown volumes.

- You cannot create a new volume from RAID group with temporary volumes.
- You cannot delete temporary volumes.
- You cannot create, delete, or format Wide Striping Volumes.
- You cannot create, delete, format, or display ODX Buffer Volumes.
- NAS Volumes will be displayed but will not be distinguished from other volumes. Confirm the NAS volumes by using the Web Console.
- A NAS volume on which a shared folder exists cannot be deleted.
- A NAS backup volume that is mounted cannot be deleted.
- Although NAS volumes and NAS backup volumes can be formatted, do not perform this process other than for the purpose of recovery when a volume malfunctions.
- A NAS system volume cannot be deleted or formatted.

12.1.2.4 storageadm affinity (AffinityGroup management command)

NAME

storageadm affinity - Manages affinity groups

SYNOPSIS

```
storageadm affinity add -ipaddr i paddr -volume vol ume_number[, vol ume_number, ...] [-lun LUN_number] [-affinitygroup affi ni tygroup_number] [-name ali as_name] [-csv]
```

```
storageadm affinity delete -ipaddr i paddr -affinitygroup affi ni tygroup_number [-s]
```

```
storageadm affinity update -ipaddr i paddr -affinitygroup affi ni tygroup_number {-add -volume vol ume_number[, vol ume_number, ...] [-lun LUN_number[, LUN_number, ...]] | -delete [-volume vol ume_number[, vol ume_number, ...] | -lun LUN_number[, LUN_number, ...]]} [-s]
```

```
storageadm affinity info -ipaddr i paddr [-affinitygroup affi ni tygroup_number] [-csv]
```

COMMAND PATH

Windows environment

```
$INS_DIR\ESC\Manager\opt\FJSVssmgr\sbin\storageadm affinity
```

(\$INS_DIR means "Program Directory" specified at the ETERNUS SF Manager installation.)

Solaris or Linux environment

```
/opt/FJSVssmgr/sbin/storageadm affinity
```

DESCRIPTION

This command is used to create/delete/modify/display affinity groups in the ETERNUS Disk storage system that is registered with this software.

OPERANDS

add

Creates an affinity group.

delete

Deletes an affinity group.

update

Updates the configuration of an affinity group.

info

Displays the affinity group information.

OPTIONS

Options of the add operand

-ipaddr *ipaddr*

Specify the IP address of the storage device.

-volume *volume_number*[,*volume_number*,...]

Specify the numbers of the volumes to be set to an affinity group, using either decimal or hexadecimal notation.

If multiple volume numbers are specified, use commas (",") to separate volume numbers. For example, specify volumes 16, 17 and 18 as either "-volume 16,17,18" in decimal notation or "-volume 0x10,0x11,0x12" in hexadecimal notation.

-lun *LUN_number*,...

Specify the LUN number to be allocated to the volume, using either decimal or hexadecimal notation. The number of LUN numbers specified must be the same as the number of volumes specified using the -volume option, and the LUN numbers must also be listed in the same order as their corresponding volume numbers.

If multiple LUN numbers are specified, use commas (",") to separate LUN numbers. For example, specify LUN numbers 16, 17 and 18 as either "-lun 16,17,18" in decimal notation or "-lun 0x10,0x11,0x12" in hexadecimal notation.

If this option is omitted, LUN numbers will be allocated in order, starting from 0.

-affinitygroup *affinitygroup_number*

Specify the affinity group number to be created, using either decimal or hexadecimal notation. For example, specify affinity group number 16 as either "-affinitygroup 16" in decimal or "-affinitygroup 0x10" in hexadecimal.

If this option is omitted, the affinity group numbers that can be created within the target storage device will be allocated automatically.

-name *alias_name*

Specify an alias for the AffinityGroup to be created.

Only alphanumeric characters (a to z, A to Z and 0 to 9) and the following symbols can be used for aliases: !@#%&^&*()-= ` _ + | ~[]{};:~"/<>?. However, "?" is not supported for ETERNUS DX80 S2/DX90 S2/DX100 S3/DX200 S3, ETERNUS DX400 S2 series, ETERNUS DX500 S3/DX600 S3 and ETERNUS DX8000 S2 series. If the alias contains a space, enclose the entire alias in double quotes (e.g., -name "123 567").

This option must be specified for ETERNUS DX60/DX60 S2/DX80/DX90.

This option can be omitted for ETERNUS DX80 S2/DX90 S2/DX100 S3/DX200 S3, ETERNUS DX400/DX400 S2 series, ETERNUS DX500 S3/DX600 S3 and ETERNUS DX8000/DX8000 S2 series.

If this option is omitted for ETERNUS DX400 series and ETERNUS DX8000 series, alias names are not set.

If this option is omitted for ETERNUS DX80 S2/DX90 S2/DX100 S3/DX200 S3, ETERNUS DX400 S2 series, ETERNUS DX500 S3/DX600 S3 and ETERNUS DX8000 S2 series, alias names are set automatically.

-csv

Displays the created affinity group number in the CSV format.

If this option is omitted, it is displayed in the table format.

Options of the delete operand

-ipaddr *ipaddr*

Specify the IP address of the storage device.

-affinitygroup *affinitygroup_number*

Specify the number of the affinity group to be deleted, using either decimal or hexadecimal notation. For example, specify affinity group number 16 as either "-affinitygroup 16" in decimal or "-affinitygroup 0x10" in hexadecimal.

-s

Processing continues without the output of a confirmation message.

Options of the update operand

-ipaddr *ipaddr*

Specify the IP address of the storage device.

-affinitygroup *affinitygroup_number*

Specify the number of the affinity group whose configuration is to be changed, using either decimal or hexadecimal notation. For example, specify affinity group number 16 as either "-affinitygroup 16" in decimal or "-affinitygroup 0x10" in hexadecimal.

-add

Adds volumes in the affinity group.

When the number for the allocated volume/LUN is specified, this command terminates abnormally.

-delete

Deletes volumes from an affinity group.

The command will terminate abnormally if a volume number or LUN number of a volume that has not been mapped is specified, or if deleting the specified mapping will mean that there are no more mappings.

-volume *volume_number[,volume_number,...]*

Specify the volume number of the volume to be added to or deleted from an affinity group, using either decimal or hexadecimal notation.

If multiple volume numbers are specified, use commas (",") to separate volume numbers. For example, specify volumes 16, 17 and 18 as either "-volume 16,17,18" in decimal notation or "-volume 0x10,0x11,0x12" in hexadecimal notation.

This option cannot be specified together with the **-lun** option when deleting volumes from an affinity group. Delete volumes by specifying either this option or the **-lun** option, not both together.

-lun *LUN_number[,LUN_number,...]*

Specify the LUN number to be allocated to a volume or released from a volume, using either decimal or hexadecimal notation. The number of LUN numbers specified must be the same as the number of volumes specified using the **-volume** option, and the LUN numbers must also be listed in the same order as their corresponding volume numbers.

If multiple LUN numbers are specified, use commas (",") to separate LUN numbers. For example, specify LUN numbers 16, 17 and 18 as either "-lun 16,17,18" in decimal notation or "-lun 0x10,0x11,0x12" in hexadecimal notation.

If this option is omitted when LUN numbers are being allocated, LUN numbers will be automatically allocated, starting with the smallest free LUN number.

When LUN numbers are being released from volumes, this option cannot be specified together with the **-volume** option. Release LUN numbers by specifying either this option or the **-volume** option, but not both together.

-s

Processing continues without the output of a confirmation message.

Options of the info operand

-ipaddr *ipaddr*

Specify the IP address of the storage device.

-affinitygroup *affinitygroup_number*

Specify the number of the affinity group for which detailed information is to be displayed, using either decimal or hexadecimal notation. For example, specify affinity group number 16 as either "-affinitygroup 16" in decimal or "-affinitygroup 0x10" in hexadecimal.

If this option is omitted, a list of affinity groups will be displayed.

-CSV

Displays the affinity group information in the CSV format.
If this option is omitted, it is displayed in the table format.

EXAMPLES

- Creating an affinity group and displaying the created affinity group in the table format.

```
> storageadm affinity add -ipaddr 1.2.3.4 -volume 16,17,18 -lun 0,1,2 -affinitygroup 16
<<< AffinityGroup ADD >>>
NUMBER
-----
0x0010
-----
INFO:swsag0001:Command terminated normally.
```

- Creating an affinity group and displaying the created affinity group in the CSV format.

```
> storageadm affinity add -ipaddr 1.2.3.4 -volume 16,17,18 -lun 0,1,2 -affinitygroup 16 -csv
NUMBER
0x0010
```

- Deleting an affinity group.

```
> storageadm affinity delete -ipaddr 1.2.3.4 -affinitygroup 16
Are you sure? [y/n]: y
INFO:swsag0001:Command terminated normally.
```

- Adding a LUN in the affinity group.

```
> storageadm affinity update -ipaddr 1.2.3.4 -affinitygroup 16 -add -volume 19 -lun 3
Are you sure? [y/n]: y
INFO:swsag0001:Command terminated normally.
```

- Deleting a LUN from the affinity group.

```
> storageadm affinity update -ipaddr 1.2.3.4 -affinitygroup 16 -delete -volume 19
Are you sure? [y/n]: y
INFO:swsag0001:Command terminated normally.
```

- Displaying the affinity group lists in the table format.

```
> storageadm affinity info -ipaddr 1.2.3.4
<<< AffinityGroup Information >>>
NUMBER NAME
-----
0x0000 AG00
0x0001 AG01
0x0002 AG02
0x0003 AG03
-----
INFO:swsag0001:Command terminated normally.
```

- Displaying the affinity group lists in the CSV format.

```
> storageadm affinity info -ipaddr 1.2.3.4 -csv
NUMBER,NAME
0x0000,AG00
0x0001,AG01
0x0002,AG02
0x0003,AG03
```


- Displaying the affinity group detail information (mapping) in the table format.

```
> storageadm affinity info -ipaddr 1.2.3.4 -affinitygroup 16
<<< AffinityGroup Information >>>
NUMBER NAME          LUN    VOLUME  VOLUME NAME
-----
0x0010 abcd          0x0000 0x0001  sample
                   0x0002 0x0004
-----
INFO:swsag0001:Command terminated normally.
```

- Displaying the affinity group detail information (mapping) in the CSV format.

```
> storageadm affinity info -ipaddr 1.2.3.4 -affinitygroup 16 -csv
NUMBER,NAME,LUN,VOLUME,VOLUME NAME
0x0010,abcd,0x0000,0x0001,sample
0x0010,abcd,0x0002,0x0004,
```

- Displaying the linked affinity group detail information (mapping) in the table format.

```
> storageadm affinity info -ipaddr 1.2.3.4 -affinitygroup 16
<<< AffinityGroup Information >>>
NUMBER NAME          LUN    VOLUME  VOLUME NAME
-----
0x0010,0x011 abcd    0x0000 0x0001  sample
                   0x0002 0x0004
-----
INFO:swsag0001:Command terminated normally.
```

- Displaying the linked affinity group detail information (mapping) in the CSV format.

```
> storageadm affinity info -ipaddr 1.2.3.4 -affinitygroup 16 -csv
NUMBER,NAME,LUN,VOLUME,VOLUME NAME
"0x0010,0x011",abcd,0x0000,0x0001,sample
"0x0010,0x011",abcd,0x0002,0x0004,
```

NOTES

- The message below will be output if the -s option is not specified when either the "delete" operand or the "update" operand is specified. Enter "y" to continue or "n" to cancel. This message can be suppressed by specifying the -s option.

```
Are you sure? [y/n]:
```

- The command will terminate abnormally if the -delete option is specified with the "update" operand in such a way that there are no items of mapping information for the affinity group.
- The command will terminate abnormally if the "add" operand or the "update" operand contains the number of a volume that cannot be set to an affinity group, such as:
 - Volume that does not exist in the storage device
 - Volume that is not open
 - LUN concatenated volume
 - ODX Buffer Volume
 - NAS volumes
- To display a concatenated affinity group when the "info" operand is specified, specify the the concatenated source affinity group in the -affinitygroup option.

12.1.2.5 storageadm ecomode (Eco-mode management command)

NAME

storageadm ecomode - Operates the Eco-mode

SYNOPSIS

```
storageadm ecomode on -ipaddr ipaddr
storageadm ecomode off -ipaddr ipaddr [-s]
storageadm ecomode info -ipaddr ipaddr [-csv]
```

COMMAND PATH

Windows environment

```
$INS_DIR\ESC\Manager\opt\FJSVssmgr\sbin\storageadm ecomode
```

(\$INS_DIR means "Program Directory" specified at the ETERNUS SF Manager installation.)

Solaris or Linux environment

```
/opt/FJSVssmgr/sbin/storageadm ecomode
```

DESCRIPTION

This command toggles and displays Eco-mode information for ETERNUS Disk storage systems registered with this product.

OPERANDS

on

Sets the Eco-mode to ON.

off

Sets the Eco-mode to OFF.

info

Displays the Eco-mode status.

OPTIONS

Options of the on operand

-ipaddr *ipaddr*

Specify the IP address of the storage device.

Options of the off operand

-ipaddr *ipaddr*

Specify the IP address of the storage device.

-s

Continues processing without asking for confirmation.

Options of the info operand

-ipaddr *ipaddr*

Specify the IP address of the storage device.

-csv

Displays the Eco-mode status of the ETERNUS Disk storage system in the CSV format.
if this option is omitted, it is displayed in the table format.

EXAMPLES

- Setting the Eco-mode to ON:

```
> storageadm ecomode on -ipaddr 1.2.3.4
INFO:swsag0001:Command terminated normally.
```

- Setting the Eco-mode to OFF:

```
> storageadm ecomode off -ipaddr 1.2.3.4
Are you sure? [y/n]:y
INFO:swsag0001:Command terminated normally.
```

- Displaying the Eco-mode information:

```
> storageadm ecomode info -ipaddr 1.2.3.4

<<< EcoMode Information>>
STATUS
-----
ON
-----
INFO:swsag0001:Command terminated normally.
```

- Displaying the Eco-mode information in CSV format:

```
> storageadm ecomode info -ipaddr 1.2.3.4 -csv
STATUS
ON
```

NOTES

- If the "off" operand is specified without the -s option, then the following message is displayed:
Enter "y" to continue or "n" to cancel.
This message can be suppressed by specifying the -s option.

```
Are you sure? [y/n]:
```

- If the device Eco-mode settings are as follows, the command terminates with an error:
 - The processing to switch Eco-mode on is executed when the Eco-mode is already on.

12.1.2.6 storageadm port (Port management command)

NAME

storageadm port - Collects a list of port information

SYNOPSIS

```
storageadm port info -ipaddr ipaddr [-csv]
```

COMMAND PATH

Windows environment

```
$INS_DIR\ESC\Manager\opt\FJSVssmgr\sbin\storageadm port
```

(\$INS_DIR means "Program Directory" specified at the ETERNUS SF Manager installation.)

Solaris or Linux environment

```
/opt/FJSVssmgr/sbin/storageadm port
```

DESCRIPTION

This command displays the port information of the ETERNUS Disk storage systems registered with this software.

OPERANDS

info

Displays a list of port information.

OPTIONS

Options of the info operand

-ipaddr *ipaddr*

Specify the IP address of the storage device.

-csv

Displays the port information in the CSV format.

If this option is omitted, it is displayed in the table format.

EXAMPLES

- Displaying port information in table format.

```
# /opt/FJSVssmgr/sbin/storageadm port info -ipaddr 1.2.3.4
<<< port Information >>>
PORT ID  PORT NAME  STATUS  TYPE      AFFINITY  PORT ADDRESS  SUPPLEMENT INFORMATION
-----
000  CM0CA0Port0  Online  FC-CA    On        1234567890ABCDEE -
001  CM0CA0Port1  Online  FC-CA    On        1234567890ABCDEF -
100  CM1CA0Port0  Online  iSCSI-CA On        192.168.1.1   iqn.iscsi.name
101  CM1CA0Port1  Online  iSCSI-CA On        192.168.1.2   iqn.iscsi.name
-----
INFO:swsag0001:Command terminated normally.
```

- Displaying port information in CSV format.

```
# /opt/FJSVssmgr/sbin/storageadm port info -ipaddr 1.2.3.4 -csv
PORT ID,PORT NAME,STATUS,TYPE,AFFINITY,PORT ADDRESS,SUPPLEMENT INFORMATION
000,CM0CA0Port0,Online,FC-CA,On,1234567890ABCDEE,-
001,CM0CA0Port1,Online,FC-CA,On,1234567890ABCDEF,-
100,CM1CA0Port0,Online,iSCSI-CA,On,192.168.1.1,iqn.iscsi.name
101,CM1CA0Port1,Online,iSCSI-CA,On,192.168.1.2,iqn.iscsi.name
```

NOTES

- SAS port information is not displayed.
- For SAS model devices of an ETERNUS DX60/DX60 S2/DX80, the command will end in an error.

12.1.2.7 storageadm iscsiport (iSCSI port management command)

NAME

storageadm iscsiport - Operates iSCSI ports

SYNOPSIS

```
storageadm iscsiport set -ipaddr ipaddr -port portID {[-portipaddr port_ipaddr] [-netmask  
port_netmask] [-gateway gateway_ipaddr] [-isns iSNS_server_ipaddr] [-iscsi iSCSI name] [-alias alias]  
[-affinity {on | off}] [-ipv4 {on | off}] [-ipv6localip local_ipaddr] [-ipv6connip connect_ipaddr] [-  
ipv6gateway v6gateway_ipaddr] [-ipv6 {on | off}]} [-s]
```

```
storageadm iscsiport info -ipaddr ipaddr [-port portID [-expand]] [-csv]
```

```
storageadm iscsiport ping -ipaddr ipaddr -port portID -target target_ipaddr [-count ping_count] [-csv]
```

COMMAND PATH

Windows environment

```
$INS_DIR\ESC\Manager\opt\FJSVssmgr\sbin\storageadm iscsiport
```

(*\$INS_DIR* means "Program Directory" specified at the ETERNUS SF Manager installation.)

Solaris or Linux environment

```
/opt/FJSVssmgr/sbin/storageadm iscsiport
```

DESCRIPTION

This command displays the iSCSI port settings and information of the ETERNUS Disk storage systems registered with this software.

Specify the storage device IP address and the iSCSI port setting information in the command parameters in order to set the iSCSI port settings and to display the set iSCSI port information and the IP reachability status of the iSCSI network to which the storage device is connected.

OPERANDS

set

Sets iSCSI port information.

info

Displays a list of iSCSI port information.

If -port is specified, detailed information concerning the specified iSCSI port is displayed.

If both -port option and -expand option are specified at the same time, the extended information for iSCSI port is displayed.

ping

Issues a ping to check the IP reachability status of the iSCSI network to which the storage device is connected and displays the result.

OPTIONS

Options of the set operand

-ipaddr *ipaddr*

Specify the IP address of the storage device.

-port *portID*

Specify the port ID of the iSCSI port.

For ETERNUS DX60/DX60 S2/DX80/DX90, the port ID is the CM number and the port number entered, and for ETERNUS DX80 S2/DX90 S2/DX100 S3/DX200 S3, ETERNUS DX400/DX400 S2 series, ETERNUS DX500 S3/DX600 S3 and ETERNUS DX8000/DX8000 S2 series, the port ID is the CM number, the CA number and the port number entered.

-portipaddr *port_ipaddr*

Specify the IP address of the iSCSI port.

-netmask *port_netmask*

Specify the subnet mask of the iSCSI port.

-gateway *gateway_ipaddr*

Specify the IP address of the gateway server for the iSCSI port.

Specify the following if delete the gateway server setting.

```
-gateway ""
```

-isns *iSNS_server_ipaddr*

Specify the IP address of the iSNS server for the iSCSI port.

Specify the following if delete the iSNS server settings.

```
-isns ""
```

If IPv4 configuration for the iSCSI port is invalid, IPv4 address cannot be specified.

If IPv6 configuration for the iSCSI port is invalid, IPv6 address cannot be specified.

-iscsi *iSCSI_name*

Specify the iSCSI name of the iSCSI port.

Specify the following if you want to set default iSCSI name.

```
-iscsi ""
```

-alias *alias_name*

Specify the alias of the iSCSI port.

-affinity {on | off}

Specify the security setting for the iSCSI port. If set to ON, specify as "-affinity on". If set to OFF, specify as "-affinity off".

-ipv4 {on | off}

Specify IPv4 setting for the iSCSI port. To enable IPv4 setting, specify "-ipv4 on" and to disable it, specify "-ipv4 off". If "-ipv4 off" is specified, IP address, subnet mask and gateway server settings are all deleted from the iSCSI port.

"-ipv4 off" cannot be specified together with the following options and their values:

- -portipaddr
- -netmask
- -gateway
- -ipv6 off

-ipv6localip *local_ipaddr*

Set the IPv6 link local address of the iSCSI port.

-ipv6connip *connect_ipaddr*

Specify the IPv6 connection IP address of the iSCSI port.

When deleting the IPv6 connection IP address setting, specify as below:

```
-ipv6connip " "
```

-ipv6gateway *v6gateway_ipaddr*

Specify the IPv6 gateway address of the iSCSI port.

When deleting the IPv6 gateway address setting, specify as below:

```
-ipv6gateway " "
```

-ipv6 {on | off}

Specify IPv6 settings of the iSCSI port. To enable IPv6 settings, specify "-ipv6 on" and to disable it, specify "-ipv6 off". If "-ipv6 off" is specified, IPv6 link local address, IPv6 connected IP address and IPv6 gateway address settings are all deleted from the iSCSI port.

"-ipv6 off" cannot be specified together with the following options and their values:

- -ipv6localip
- -ipv6connip
- -ipv6gateway
- -ipv4 off

-s

Causes processing to continue without output of a confirmation message.

Options of the info operand

-ipaddr *ipaddr*

Specify the IP address of the storage device.

-port *port ID*

Displays detailed information concerning the iSCSI ports. If this option is omitted, a list of iSCSI ports is displayed.

For ETERNUS DX60/DX60 S2/DX80/DX90, the port ID is the CM number and the port number entered, and for ETERNUS DX80 S2/DX90 S2/DX100 S3/DX200 S3, ETERNUS DX400/DX400 S2 series, ETERNUS DX500 S3/DX600 S3 and ETERNUS DX8000/DX8000 S2 series, the port ID is the CM number, the CA number and the port number entered.

-csv

Displays the port information in the CSV format.

If this option is omitted, it is displayed in the table format.

-expand

Add the following to iSCSI port information to display:

- IPv6 link local address
- IPv6 connection IP address
- IPv6 gateway

Added information depends on the version of the ETERNUS SF system. Upgrading the version of the ETERNUS SF system may increase displayed information.

This option can be specified only when the -port option is specified.

Options of the ping operand

-ipaddr *ipaddr*

Specify the IP address of the storage device.

-port *port ID*

Specify the port ID of the iSCSI port.

For ETERNUS DX60/DX60 S2/DX80/DX90, the port ID is the CM number and the port number entered, and for ETERNUS DX80 S2/DX90 S2/DX100 S3/DX200 S3, ETERNUS DX400/DX400 S2 series, ETERNUS DX500 S3/DX600 S3 and ETERNUS DX8000/DX8000 S2 series, the port ID is the CM number, the CA number and the port number entered.

-target *target_ipaddr*

Specify the IP address of the server that checks the IP reachability status.

-count *ping_count*

Specify a value between 1 and 10 for the number of pings issued to check the IP reachability status. A failure will be displayed if an error response is returned at least once. A success will be displayed if normal responses are returned for all pings.

If this option is omitted, the ping execution count is 1.

-csv

Displays the port information in the CSV format.

If this option is omitted, it is displayed in the table format.

EXAMPLES

- Setting iSCSI port information.

```
> storageadm iscsiport set -ipaddr 1.2.3.4 -port 000 -portipaddr 172.16.4.1
Are you sure? [y/n]: y
INFO:swsag0001:Command terminated normally.
```

- Displaying a list of iSCSI port information in table format.

```
> storageadm iscsiport info -ipaddr 1.2.3.4
<<< iSCSI Port Information >>>
PORT NAME          STATUS TYPE      AFFINITY ISCSI NAME          IP ADDRESS
ID
-----
00  CM0Port0      Online iSCSI-CA On          iqn.2000-09.com.fujitsu:storage-system.e2000:0000000029
172.16.4.38
01  CM0Port1      Online iSCSI-CA Off         iqn.2000-09.com.fujitsu:storage-system.e2000:0000000029
172.16.4.39
10  CM1Port0      Online iSCSI-CA On          iqn.2000-09.com.fujitsu:storage-system.e2000:0000000029
172.16.4.40
11  CM1Port1      Online iSCSI-CA On          iqn.2000-09.com.fujitsu:storage-system.e2000:0000000029
172.16.4.41
-----
INFO:swsag0001:Command terminated normally.
```

- Displaying a list of iSCSI port information in CSV format.

```
> storageadm iscsiport info -ipaddr 1.2.3.4 -csv
PORT ID,NAME,STATUS,TYPE,AFFINITY,ISCSI NAME,IP ADDRESS
00,CM0Port0,Online,iSCSI-CA,On,iqn.2000-09.com.fujitsu:storage-
system.e2000:0000000029,172.16.4.38
01,CM0Port1,Online,iSCSI-CA,Off,iqn.2000-09.com.fujitsu:storage-
system.e2000:0000000029,172.16.4.39
10,CM1Port0,Online,iSCSI-CA,On,iqn.2000-09.com.fujitsu:storage-
system.e2000:0000000029,172.16.4.40
```



```
11,CM1Port1,Online,iSCSI-CA,On,iqn.2000-09.com.fujitsu:storage-
system.e2000:0000000029,172.16.4.41
```

- Displaying detailed iSCSI port information in table format.

```
> storageadm iscsiport info -ipaddr 1.2.3.4 -port 00
<<< iSCSI Port Information >>>
PORT NAME          TYPE      IP ADDRESS      SUBNET          GATEWAY          ISNS   ISNS SERVER
ISCSI NAME ALIAS NAME TRANSFER BANDWIDTH MTU  AFFINITY HOST      HOST      HOST      RESET RESERVE
ID                                     MASK                                     SERVER IP
ADDRESS                                     RATE   LIMIT   SIZE MODE   RESPONSE  RESPONSE  SPECIFIC
SCOPE CANCEL AT

                                     NUMBER  NAME      MODE      CHIP RESET
-----
00  CM0Port0      iSCSI-CA 172.16.4.38    255.255.255.0  172.16.4.1      Off      -
iqn.2000-09.com.fujitsu:storage-system.e2000:0000000029 cm0port0 Auto - - Off 0x000F hresp00F
Normal Mode I_T_L Off
-----
INFO:swsag0001:Command terminated normally.
```

- Displaying detailed iSCSI port information in CSV format.

```
> storageadm iscsiport info -ipaddr 1.2.3.4 -port 00 -csv
PORT ID,NAME,TYPE,IP ADDRESS,SUBNET MASK,GATEWAY,ISNS SERVER,ISNS SERVER IP ADDRESS,ISCSI
NAME,ALIAS NAME,TRANSFER RATE,BANDWIDTH LIMIT,MTU SIZE,AFFINITY MODE,HOST RESPONSE NUMBER,HOST
RESPONSE NAME,HOST SPECIFIC MODE,RESET SCOPE,RESERVE CANCEL AT CHIP RESET
00,CM0Port0,iSCSI-CA,172.16.4.38,255.255.255.0,172.16.4.1,Off,-,iqn.2000-09.com.fujitsu:storage-
system.e2000:0000000029,cm0port0,Auto,-,-,Off,0x000F,hresp00F,Normal Mode,I_T_L,Off
```

- Displaying detailed iSCSI port information in table format including additional information.

```
> storageadm iscsiport info -ipaddr 1.2.3.4 -port 00 -expand
<<< iSCSI Port Information >>>
PORT NAME          TYPE      IP ADDRESS      SUBNET          GATEWAY          ISNS   ISNS SERVER
ISCSI NAME ALIAS NAME TRANSFER BANDWIDTH MTU  AFFINITY HOST      HOST      HOST      RESET RESERVE
LINK LOCAL IP ADDRESS                                     CONNECT IP ADDRESS                                     IPV6 GATEWAY
ADDRESS

ID                                     MASK                                     SERVER IP
ADDRESS                                     RATE   LIMIT   SIZE MODE   RESPONSE  RESPONSE  SPECIFIC
SCOPE CANCEL AT

                                     NUMBER  NAME      MODE      CHIP RESET
-----
00  CM0Port0      iSCSI-CA 172.16.4.38    255.255.255.0  172.16.4.1      Off      -
iqn.2000-09.com.fujitsu:storage-system.e2000:0000000029 cm0port0 Auto - - Off 0x000F hresp00F
Normal Mode I_T_L Off fe80::128c:24d8:3016:250a:56ff:fe67:a524
2001:100a:ab13:cd24:ef3f:db72:fe11:cd21 2001:1101:cfcl:b4d2:ef73:3f9c:2d11:ca34
-----
INFO:swsag0001:Command terminated normally.
```

- Displaying detailed iSCSI port information in CSV format including additional information.

```
> storageadm iscsiport info -ipaddr 1.2.3.4 -port 00 -expand -csv
PORT ID,NAME,TYPE,IP ADDRESS,SUBNET MASK,GATEWAY,ISNS SERVER,ISNS SERVER IP ADDRESS,ISCSI
NAME,ALIAS NAME,TRANSFER RATE,BANDWIDTH LIMIT,MTU SIZE,AFFINITY MODE,HOST RESPONSE NUMBER,HOST
RESPONSE NAME,HOST SPECIFIC MODE,RESET SCOPE,RESERVE CANCEL AT CHIP RESET,LINK LOCAL IP
ADDRESS,CONNECT IP ADDRESS,IPV6 GATEWAY ADDRESS
00,CM0Port0,iSCSI-CA,172.16.4.38,255.255.255.0,172.16.4.1,Off,-,iqn.2000-09.com.fujitsu:storage-
system.e2000:0000000029,cm0port0,Auto,-,-,Off,0x000F,hresp00F,Normal Mode,I_T_L,Off,fe80::128c:
24d8:3016:250a:
56ff:fe67:a524,2001:100a:ab13:cd24:ef3f:db72:fe11:cd21,2001:1101:cfc1:b4d2:ef73:3f9c:2d11:ca34
```

- Displaying the IP reachability status of the iSCSI network in table format.

```
> storageadm iscsiport ping -ipaddr 1.2.3.4 -port 00 -target 172.16.4.1
<<iSCSI Port Ping Status>>
PORT NAME          TARGET IP          RESULT
ID                ADDRESS
-----
000 CM0CA0Port0 172.16.4.38      Success
-----
INFO:swsag0001:Command terminated normally.
```

- Displaying the IP reachability status of the iSCSI network in CSV format.

```
> storageadm iscsiport ping -ipaddr 1.2.3.4 -port 00 -target 172.16.4.1 -csv
PORT ID,NAME,TARGET IP ADDRESS,RESULT
000,CM0CA0Port0,172.16.4.38,Success
```

NOTES

- The message below is displayed when the "set" operand is specified. Enter "y" to continue, or "n" to cancel. Note that this message is not displayed if the -s option is specified.

```
Are you sure? [y/n]:
```

- If you set BS2000 Mode to Host Specific Mode of Host Response when the iSCSI port is displayed in detail, it is displayed as "Normal Mode" to HOST SPECIFIC MODE.
- The IP address, link local IP address, connection IP address, iSCSI name, and iSCSI alias name of the iSCSI port might not be able to be registered by duplicating with other iSCSI port settings. Refer to [Note] in "[6.1.5 Connectivity Management](#)" for details.

12.1.2.8 storageadm progress (Progress display command)

NAME

storageadm progress - Displays progress information

SYNOPSIS

```
storageadm progress volumeformat -ipaddr ipaddr { [-volume volume_number[,volume_number...]] | [-all] } [-csv]
```

COMMAND PATH

Windows environment

```
$INS_DIR\ESC\Manager\opt\FJSVssmgr\sbin\storageadm progress
```

(\$INS_DIR means "Program Directory" specified at the ETERNUS SF Manager installation.)

Solaris or Linux environment

`/opt/FJSVssmgr/sbin/storageadm progress`

DESCRIPTION

This command displays progress information concerning the formatting of volumes on ETERNUS Disk storage systems registered with this software.

Specify the storage device IP address and the volume number in the command parameters in order to display volume formatting progress information.

OPERANDS

`volumeformat`

Displays the formatting progress.

OPTIONS

Options of the `volumeformat` operand

`-ipaddr ipaddr`

Specify the storage device IP address.

`-volume volume number[, volume number,...]`

Specify the numbers for the volumes to be output, using either decimal or hexadecimal notation.

If multiple volume numbers are specified, use commas (",") to separate volume numbers. For example, specify volumes 10 and 16 as either `"-volume 10,16"` in decimal notation or `"-volume 0xa,0x10"` in hexadecimal notation.

This displays formatting progress information (including format completion and formatting not yet being implemented) concerning the specified volume.

An error does not occur if the specified volume does not exist, but information is not displayed for that volume.

If this is omitted, progress information is displayed for all volumes for which formatting is in progress. However, if the `-all` option is specified, the progress information will include volumes not currently being formatted (formatting completed or not yet implemented).

This option cannot be specified at the same time as the `-all` option.

`-all`

Includes information concerning volumes not currently being formatted (formatting completed or not yet implemented) in the display.

If this option is omitted, progress information is displayed only for volumes for which formatting is in progress.

This option cannot be specified at the same time as the `-volume` option.

`-csv`

This option displays the formatting progress information in the CSV format.

If this option is omitted, it is displayed in the table format.

The table below shows the contents displayed when different combinations of `-volume` and `-all` options are specified.

-volume option	-all option	
	Specified	Not specified
Specified	(Cannot be specified.)	The display target is the specified volume, and volumes for which formatting is completed or not yet executed are included in the display.

-volume option	-all option	
	Specified	Not specified
Not specified	The display target is all volumes on the device, and volumes for which formatting is completed or not yet executed are included in the display.	The display target is all volumes on the device, but the display includes only the volumes for which formatting is in progress.

EXAMPLES

- Displaying the formatting progress information for all volumes in table format.

```
> storageadm progress volumeformat -ipaddr 1.2.3.4 -all
<<< Volume Format Progress Information >>>
NUMBER  NAME                TYPE  STATUS          PROGRESS
-----
0x0000  Volume0x0000        Open  Available       100
0x0001  ,Open,Available,70
0x0002  ,Open,Readying,0
0x0003  ,Open,Available,-
0x0004  ,SDV,Available,100
0x0005  ,SDPV,Available,100
-----
INFO:swsag0001:Command terminated normally.
```

- Displaying the formatting progress information for all volumes in CSV format.

```
> storageadm progress volumeformat -ipaddr 1.2.3.4 -all -csv
NUMBER,NAME,TYPE,STATUS,PROGRESS
0x0000,Volume0x0000,Open,Available,100
0x0001,,Open,Available,70
0x0002,,Open,Readying,0
0x0003,,Open,Available,-
0x0004,,SDV,Available,100
0x0005,,SDPV,Available,100
```

NOTES

- Formatting progress information is displayed for open volumes, SDV volumes, and SDPV volumes, but is not displayed for other volumes.
- If volume formatting fails, the "STATUS" field is as shown below, and 0 to 100 is displayed as the "PROGRESS" field.
 - Broken
 - Data Lost
 - Not Ready
- ODX Buffer Volumes are not displayed.

12.1.2.9 storageadm perfctl (Performance monitoring command)

NAME

storageadm perfctl - Performs monitoring operations

SYNOPSIS

```
storageadm perfctl start -ipaddr ipaddr [-interval time]
```

```
storageadm perfctl stop -ipaddr ipaddr
```

```
storageadm perfctl status -ipaddr ipaddr
```

COMMAND PATH

Windows environment

```
$INS_DIR\ESC\Manager\opt\FJSVssmgr\sbin\storageadm perfctl
```

(\$INS_DIR means "Program Directory" specified at the ETERNUS SF Manager installation.)

Solaris or Linux environment

```
/opt/FJSVssmgr/sbin/storageadm perfctl
```

DESCRIPTION

This command starts and stops performance monitoring for the NetApp FAS Series and displays the performance monitoring status.

OPERANDS

start

Starts performance monitoring.

stop

Stops performance monitoring.

status

Displays the performance monitoring status.

OPTIONS

Options of the start operand

-ipaddr *ipaddr*

Specify the IP address of the storage device.

-interval *time*

Specify either 10, 30, 60, or 300 (seconds unit) as the performance monitoring interval.

If a value other than 10, 30, 60, or 300 is set, the actual interval is set according to the table below (an error will occur if it is set to a negative value or a value greater than or equal to 2147483648):

Specified value	Monitoring interval (in secs)
<i>time</i> = 0	30
0 < <i>time</i> <= 10	10
10 < <i>time</i> <= 30	30
30 < <i>time</i> <= 60	60
60 < <i>time</i>	300

If this option is omitted, monitoring is performed at 30 second intervals.

Options of the stop operand

-ipaddr *ipaddr*

Specify the IP address of the storage device.

Options of the status operand

`-ipaddr ipaddr`

Specify the IP address of the storage device.

EXAMPLES

- Starting performance monitoring at 60-second intervals.

```
> storageadm perfctl start -ipaddr 1.2.3.4 -interval 60
```

- Stopping performance monitoring.

```
> storageadm perfctl stop -ipaddr 1.2.3.4
```

- Displaying the performance monitoring status.

```
> storageadm perfctl status -ipaddr 1.2.3.4
<<< Performance Monitor Status>>
DEVICE_NAME(IP_ADDRESS)          STATUS          INTERVAL[SEC]
-----
NR1000F(1.2.3.4)                 Monitoring     60
-----
```

```
INFO:swsag0001:Command terminated normally.
```

The explanation of the information displayed in each field is as follows.

Title	Explanation
DEVICE_NAME(IP_ADDRESS)	Displays the device name and its IP address.
STATUS	Displays the monitoring status. <ul style="list-style-type: none">- "Monitoring": Normal monitoring is in progress.- "Stop": Performance monitoring is stopped.- "Recovering": Retry is in progress, after communication was interrupted or an attempt failed.- "Error": Stopped with an error, after an unsuccessful retry. Collect the information required for troubleshooting and contact Fujitsu Technical Support. Refer to "B.1 Collecting the troubleshooting information" for details.
INTERVAL[sec]	Displays the performance monitoring interval (seconds).

NOTES

- The NetApp FAS Series must be registered with this product.

12.1.2.10 storageadm device (Device management command)

NAME

storageadm device - Operation of devices

SYNOPSIS

```
storageadm device unlock -ipaddr ipaddr [-s]
```

COMMAND PATH

Windows environment

```
$INS_DIR\ESC\Manager\opt\FJSVssmgr\sbin\storageadm device
```

(\$INS_DIR means "Program Directory" specified at the ETERNUS SF Manager installation.)

Solaris or Linux environment

```
/opt/FJSVssmgr/sbin/storageadm device
```

DESCRIPTION

This command unlocks the storage device.

OPERANDS

unlock

Unlocks the storage device.

OPTIONS

Options of the unlock operand

`-ipaddr ipaddr`

Specify the IP address of the storage device.

`-s`

Continues the processing without a confirmation message being output.

EXAMPLES

- Unlock the storage device.

```
> storageadm device unlock -ipaddr 1.2.3.4  
Are you sure? [y/n]: y
```

NOTES

- You can release only locks which are locked by using this software.
- If you release the lock, do not perform other operations by using this software.

12.2 Agent Commands

This section explains command operations on the Managed Server.

12.2.1 setagtip (Agent information change command)

NAME

setagtip - Changes the Storage Cruiser's agent information

SYNOPSIS

```
setagtip [-i ipaddr]
```

COMMAND PATH

Windows environment

```
$INS_DIR\ESC\Agent\bin\setagtip
```

(*\$INS_DIR* means "Program Directory" specified at the Storage Cruiser's agent installation.)

Solaris, Linux, HP-UX, or AIX environment

```
/opt/FJSSVssage/bin/setagtip
```

DESCRIPTION

This command sets Storage Cruiser's agent information.

In the Windows environment, only a user of the Administrators group can execute this command.

In the Solaris, Linux, HP-UX, or AIX environment, only OS administrator (root) user can execute this command.

To change the start IP address of Storage Cruiser's agent, specify an IP address to set the information.

OPTIONS

-i ipaddr

Specify the IP address of the server node that can communicate from the Management Server. The start IP address of the Storage Cruiser's agent is set to the specified IP address.

If this option is omitted, the current setting information is displayed.

When specifying IPv6 address, specify a global address.

As for IPv6 address display format, the Web Console displays IP addresses with reference to RFC5952. For this reason, they may be different from those specified by this command.

EXAMPLES

- Displaying the Storage Cruiser's agent information

```
> setagtip
```

- Setting the Storage Cruiser's agent IP address to 10.12.13.14

```
> setagtip -i 10.12.13.14
```

NOTES

If the host name cannot be resolved from the specified IP address, the messages shown below is displayed. Check for an error in the specified IP address or network definition (hosts, DNS, etc.), and re-execute the command.

```
IP Address = IP_address : Host's Name is not found.
```


12.2.2 traptest (SNMP Trap test for server node agent)

NAME

traptest - tests of SNMP Trap

SYNOPSIS

```
traptest [ipaddr]
```

COMMAND PATH

Windows environment

```
$INS_DIR\ESC\Agent\bin\traptest
```

(\$INS_DIR means "Program Directory" specified at the Storage Cruiser's agent installation.)

Solaris, Linux, HP-UX, or AIX environment

```
/opt/FJSVssage/bin/traptest
```

DESCRIPTION

This command checks whether SNMP Trap is correctly transmitted to the Management Server from a server node agent, display an event, and check the linkage with Shell/Bat. The Centric Manager linkage is not operated by this command.

If the action on SNMP Trap as a test is supposed to be changed, change the SNMP Trap XML definition file (1_3_6_1_4_1_211_4_1_3_21_2_2.xml) for the agent. In SNMP Trap as a test, 1 is used for Specific Trap Type number and the action can be changed by changing the definition of the Specific Trap Type number 1 defined in the SNMP Trap XML definition file. Refer to "[A.5 SNMP Trap XML Definition File](#)" for the SNMP Trap XML definition file.

OPERANDS

ipaddr

Only in the environment where the host holds two or more IP addresses (including loopback IP address, IPv4/IPv6 dual stack), specify a server node's IP address (start IP address of the Storage Cruiser's agent) which the Storage Cruiser's manager recognizes.

When specifying IPv6 address, specify a global address.

As for IPv6 address display format, the Web Console displays IP addresses with reference to RFC5952. For this reason, they may be different from those specified by this command.

OPTIONS

None.

EXAMPLES

- SNMP Trap is transmitted from the server node agent of IP address 11.11.11.11.

```
> traptest 11.11.11.11
```

NOTES

- If the SNMP Trap send destination address is not set to the server node when execute the command, the following results are output.

```
Target Host Nothing
SNMPTrap error
```

- If the server node that input in the command is not registered, re-execute the command after registering the server node.
- Execute the same action in case where the server node is not registered after deletion of the server node.
- The SNMP Trap community name that is issued using this command, is fixed to "public".
- If there is any error in the specified IP address format, the following result is output. Specify a valid IP address to re-execute the action.

```
Invalid parameter: speci fi edl pAddress
SNMPTrap error
```

12.2.3 agentsnap (Troubleshooting information collection of Agent)

NAME

agentsnap - Collects the troubleshooting information of Agent

SYNOPSIS

Windows environment

```
agentsnap -dir dirname [-all]
```

Solaris or Linux environment

```
agentsnap [-dir dirname] [-all]
```

COMMAND PATH

Windows environment

```
$INS_DIR\Agent\sbin\agentsnap
```

(\$INS_DIR means "Program Directory" specified at the Storage Cruiser's agent installation.)

Solaris or Linux environment

```
/opt/FJSSVssage/sys/agentsnap
```

DESCRIPTION

This command collects the troubleshooting information of the Storage Cruiser's agent.

In the Windows environment, only a user of the Administrators group can execute this command.

In the Solaris or Linux environment, only OS administrator (root) user can execute this command.

Execute this command to collect the troubleshooting information when a problem occurs on the Storage Cruiser's agent, and submit its information to Fujitsu Technical Support.

OPTIONS

-dir *dirname*

Corrects the troubleshooting information on *dirname* directory.

In the Windows environment, specify the full path name that starts from the drive letter for *dirname*. The maximum length that can be

specified for *dirname* is 100 bytes.

In the Solaris or Linux environment, specify the full path name for *dirname*. If this option is omitted, the troubleshooting information is stored on /tmp directory.

The collected information is gathered in the file that its name starts by "agentsnap_". Before executing this command, confirm that *dirname* directory has the following free space.

Collected information	Required free space
Initial investigation information	more than 10MB
All troubleshooting information	more than 30MB

-all

Collects all troubleshooting information on servers. Data includes lots of information, which will increase the size of the data. This option is not necessary for initial investigation.

EXAMPLES

Windows environment

- Collecting the troubleshooting information for initial investigation on D:\temp directory.

```
> agentsnap -dir D:\temp
```

Solaris or Linux environment

- Collecting the troubleshooting information for initial investigation.

```
> agentsnap
```

12.3 Starting and Stopping the Manager

This section explains how to start and stop the Storage Cruiser's manager.

12.3.1 Starting and stopping services (Windows environment)

This sub section explains how to start and stop the Storage Cruiser's manager in the Windows environment.

12.3.1.1 Starting and stopping the SNMP Trap monitoring service

- Starting the SNMP Trap monitoring service

1. Open the **Services** window.

- For Windows Server 2012

Click [Control Panel] - [System and Security] - [Administrative Tools] - [Services].

- For Windows environment other than above

Click [Control Panel] - [Administrative Tools] - [Services].

2. Select the SNMP Trap monitoring service, and click the [Start] button.

- Stopping the SNMP Trap monitoring service
 1. Open the **Services** window.
 - For Windows Server 2012
Click [Control Panel] - [System and Security] - [Administrative Tools] - [Services].
 - For Windows environment other than above
Click [Control Panel] - [Administrative Tools] - [Services].
 2. Select the SNMP Trap monitoring service, and click the [Stop] button.
- Checking the SNMP Trap monitoring service
 1. Open the **Services** window.
 - For Windows Server 2012
Click [Control Panel] - [System and Security] - [Administrative Tools] - [Services].
 - For Windows environment other than above
Click [Control Panel] - [Administrative Tools] - [Services].
 2. Check that the **Status** field of the SNMP Trap monitoring service status is "Started".



Note

The SNMP Trap monitoring service is an OS standard service. Do not stop the SNMP Trap monitoring service unless there is a special reason, because it will affect other products such as ServerView AlarmService and ServerView Resource Coordinator VE, etc.

12.3.1.2 Starting and stopping the service

- Starting the service
 1. Open the **Services** window.
 - For Windows Server 2012
Click [Control Panel] - [System and Security] - [Administrative Tools] - [Services].
 - For Windows environment other than above
Click [Control Panel] - [Administrative Tools] - [Services].
 2. Select the service "ETERNUS SF Manager Tomcat Service", and click the [Start] button.
- Stopping the service
 1. Open the **Services** window.
 - For Windows Server 2012
Click [Control Panel] - [System and Security] - [Administrative Tools] - [Services].
 - For Windows environment other than above
Click [Control Panel] - [Administrative Tools] - [Services].
 2. Select the service "ETERNUS SF Manager Tomcat Service", and click the [Stop] button.

12.3.2 Starting and stopping daemons (Solaris environment)

This sub section explains how to start and stop the Storage Cruiser's manager in the Solaris environment.

12.3.2.1 Starting and stopping the SNMP Trap monitoring daemon

Only OS administrator (root) user can execute following commands.

- Starting the SNMP Trap monitoring daemon

Execute the following command.

```
# /opt/FJSVswstt/bin/mpnm-trapd start
```

- Stopping the SNMP Trap monitoring daemon

Execute the following command.

```
# /opt/FJSVswstt/bin/mpnm-trapd stop
```

- Checking the SNMP Trap monitoring daemon

Execute the following command.

```
# /bin/ps -ef | grep nwsnmp-trapd | grep -v grep
```

12.3.2.2 Starting and stopping the daemons at specific times

Start or stop the following daemons in a batch operation:

- Management Server daemon
- SNMP Trap monitoring daemon

Only OS administrator (root) user can execute following commands.

- Starting daemons

Execute the following command.

```
# /opt/FJSVesfcm/bin/startesf.sh
```

- Stopping daemons

Execute the following command.

```
# /opt/FJSVesfcm/bin/stopesf.sh
```

Information

.....

In an environment in which the SAN administration manager in SystemWalker/StorageMGR-M V5.1/V10 or Softek SANView4.1 CD-ROM sub-directory is installed, the SNMP Trap monitoring daemon is controlled by SystemWalker/StorageMGR-M (SAN administration manager in Softek SANView4.1 CD-ROM sub-directory), so only the Management Server daemon is started and stopped by the above commands.

.....

Note

.....

When the batch stop is done, AdvancedCopy Manager cannot be operated from the Web Console.

.....

12.3.3 Starting and stopping daemons (Linux environment)

This sub section explains how to start and stop the Storage Cruiser's manager in the Linux environment.

12.3.3.1 Starting and stopping the SNMP Trap monitoring daemon

The procedure to start and stop the SNMP Trap daemon on the Management Server is different between when monitoring only IPv4 address assigned devices and when monitoring both IPv4 and IPv6 addresses assigned devices.

When monitoring only IPv4 address assigned devices

Only OS administrator (root) user can execute following commands.

- Starting the SNMP Trap monitoring daemon

Execute the following command.

```
# /etc/init.d/snmptrapd start
```



In an environment where the ServerView trap distributor program (SMAWtrpsv) is used, use the following procedure to start the daemon:

```
# /etc/init.d/trpsrvd stop  
# /etc/init.d/snmptrapd start  
# /etc/init.d/trpsrvd start
```

- Stopping the SNMP Trap monitoring daemon

Execute the following command.

```
# /etc/init.d/snmptrapd stop
```



Do not stop the daemon unless there is a special reason, because it affects other software using snmptrapd.

- Checking the SNMP Trap monitoring daemon

Execute the following command.

```
# /bin/ps -ef | grep snmptrapd | grep -v grep
```

When monitoring both IPv4 and IPv6 addresses assigned devices

If the settings are done in order to monitor IPv6 address assigned devices in the following sections in the *ETERNUS SF Installation and Setup Guide*, use the following procedure to start/stop the SNMP Trap daemon:

- "SNMP Trap setting (for Linux)" in "Setup of Storage Cruiser's manager"

Only OS administrator (root) user can execute following commands.

- Starting the SNMP Trap monitoring daemon

Execute the following command.

```
# /opt/FJSVswstt/bin/mpnm-trapd start
```

- Stopping the SNMP Trap monitoring daemon

Execute the following command.

```
# /opt/FJSVswstt/bin/mpnm-trapd stop
```

- Checking the SNMP Trap monitoring daemon

Execute the following command.

```
# /bin/ps -ef | grep nwsnmp-trapd | grep -v grep
```

12.3.3.2 Starting and stopping the daemon

Only OS administrator (root) user can execute following commands.

- Starting daemons

Execute the following command.

```
# /opt/FJSVesfcm/bin/startesf.sh
```

- Stopping daemons

Execute the following command.

```
# /opt/FJSVesfcm/bin/stopesf.sh
```

Information

If the settings are done in order to monitor IPv6 address assigned devices in the following sections in the *ETERNUS SF Installation and Setup Guide*, the SNMP Trap daemon is also started / stopped at the same time:

- "SNMP Trap setting (for Linux)" in "Setup of Storage Cruiser's manager"

Note

When the batch stop is done, AdvancedCopy Manager cannot be operated from the Web Console.

12.4 Starting and Stopping the Agent

This section explains how to start and stop the service/daemon of the Storage Cruiser's agent.

12.4.1 Starting and stopping services (Windows environment)

Start or stop the service of the Storage Cruiser's agent.

- Starting the service

1. Open the **Services** window.

- For Windows Server 2012

Click [Control Panel] - [System and Security] - [Administrative Tools] - [Services].

- For Windows environment other than above

Click [Control Panel] - [Administrative Tools] - [Services].

2. Select the service "ETERNUS SF Storage Cruiser Agent", and click the [Start] button.

- Stopping the service

1. Open the **Services** window.

- For Windows Server 2012

Click [Control Panel] - [System and Security] - [Administrative Tools] - [Services].

- For Windows environment other than above

Click [Control Panel] - [Administrative Tools] - [Services].

2. Select the service "ETERNUS SF Storage Cruiser Agent", and click the [Stop] button.

12.4.2 Starting and stopping daemons (Solaris, Linux, HP-UX, or AIX environment)

Only OS administrator (root) user can execute following commands.

- Starting the daemon

Execute the following command.

```
# /opt/FJSVssage/bin/sstorageagt
```

- Stopping the daemon

Execute the following command.

```
# /opt/FJSVssage/bin/pstorageagt
```

12.5 Commands for Reporting Function

The commands for Reporting function are as follows:

Command Name	Explanation
esfadm report collect	Information for the report will be collected.
esfadm report create	A report will be created.

The exclusive relationship of these commands is as follows.

	While executing the esfadm report collect command.	While executing the esfadm report create command.
When the esfadm report collect command has been executed	Not Available (Error. The same command cannot be executed at the same time, recover error.)	Available (Standby. Execute the esfadm report collect command after completing the esfadm report create command)
When the esfadm report create command has been executed	Available (Standby. Execute the esfadm report create command after completing the esfadm report collect command)	Not Available (Error. The same command cannot be executed at the same time, recover error.)

12.5.1 esfadm report collect (Report information collection command)

NAME

esfadm report collect - Collect the report information

SYNOPSIS

```
esfadm report collect -all [-test]
```


COMMAND PATH

Windows environment

```
$INS_DIR\Common\bin\esfadm report collect
```

(\$INS_DIR means "Program Directory" specified at the ETERNUS SF Manager installation.)

Solaris or Linux environment

```
/opt/FJSVesfcm/bin/esfadm report collect
```

DESCRIPTION

Collect the report information for the storage device for which the Reporting function is enabled on the Web Console to store in the information stack file.

In the Windows environment, only a user of the Administrators group can execute this command.

In the Solaris or Linux environment, only OS administrator (root) user can execute this command.

OPTIONS

-all

This option is required.

-test

In relation to the volume of which the report information will be collected, confirm whether the information collection command ends without errors. For this reason, the report information will not be accumulated in the information accumulation file.

Specify this option when confirming the storage of which information will be collected, or when confirming whether the process can be completed without error after dealing with an error that has occurred.

OUTPUT INFORMATION

- Accumulate the collected report information in the information stack file

The information regarding the volume will be output to the information stack file.

- Output the message to the command execution screen

The message including the name of the storage of which the report information was collected will be output.

- Operation History of ETERNUS SF

The following information in regard to operation will be output.

Output Items	Output Contents
Date	Date and time when the operation was executed
User ID	User name that performed the operation
Action	Collect Report Information (CLI)
State	Submit, Start, or Complete
Result	Success, Failed, or Warning
Target	-
Detail	Detailed information
Message	Error message

EXIT STATUS

=0: Completed successfully

>0: Terminated abnormally

EXAMPLES

- When the storages subject to collection are Storage1 and Storage2

```
> esfadm report collect -all
esrpt00002 The storage information was collected. Storage=Storage1,Storage2
```

- When the -test option is specified and the storages subject to collection are Storage1 and Storage2

```
> esfadm report collect -all -test
esrpt00005 The report data does not collect for test command.
esrpt00002 The storage information was collected. Storage=Storage1,Storage2
```

NOTES

- When this command is executed while the [esfadm report create command](#) is being executed, this command will be put in standby state. When the [esfadm report create command](#) executed earlier is completed, processing of this command will continue.
- This command cannot be executed again while the command is already executing. The command executed later will end in an error.
- In any of the following cases, this command collects only information-gathering time and ends normally:
 - There is no license existing on every storage device.
 - There is no storage device connected to server (host affinity is enabled).
 - There is no storage device for which the Reporting function is activated on the Web Console.
- When this command ends with an error, the report information that was partly collected is discarded. (The information accumulation file is returned to its state prior to execution of the command.)

12.5.2 esfadm report create (Report creation command)

NAME

esfadm report create - Create the Report

SYNOPSIS

```
esfadm report create -start YYYYMMDDhhmm -end YYYYMMDDhhmm [-outputfile fileName]
```

COMMAND PATH

Windows environment

```
$INS_DIR\Common\bin\esfadm report create
```

(\$INS_DIR means "Program Directory" specified at the ETERNUS SF Manager installation.)

Solaris or Linux environment

```
/opt/FJSVesfcm/bin/esfadm report create
```

DESCRIPTION

The report information of the period specified in the options will be output to the report file.

In addition, based on the save period configured with the policies, old report information that has exceeded the save period of the information accumulation file will be deleted.

(If there is report information in the information accumulation file, a report file will be output.)

In the Windows environment, only a user of the Administrators group can execute this command.

In the Solaris or Linux environment, only OS administrator (root) user can execute this command.

OPTIONS

-start YYYYMMDDhhmm -end YYYYMMDDhhmm

Specify the period of the report to be created in the form of YYYYMMDDhhmm (local time). The maximum period from start to end is 1 year (365 days, or 366 days when including a leap year). The number of seconds is counted as 0 second.

In addition, in a time period switching from summer time to winter time, there are winter local time and summer local time. This command considers that local time as winter local time.

- *YYYY* indicates the year and a value of 0000~9999 can be specified.
- *MM* indicates the month and a value of 01~12 can be specified.
- *DD* indicates the day and a value of 01~31 can be specified.
- *hh* indicates the hour, and a value of 00~23 can be specified.
- *mm* indicates the minute, and a value of 00~59 can be specified.

In the following cases, errors will occur:

- In the case the date and time later than the command executed date and time is specified at start or end.
- In the case the date and time earlier than the starting date and time is specified at end.
- In the case the date and time that does not exist is specified.

-outputfile *fileName*

Specify the file name for the report output. When a directory path is not included, the report will be stored in the current directory. The supported directory paths are an absolute path and a relative path.

When this option is omitted, the report will be created with the following file name under the current directory.

esfreport_manual_specified_YYYYMMDDhhmmSS.xml
 YYYYMMDDhhmmSS is the command execution date and time.

Use the local time for the execution time to output to the file name.

When a file or directory with the same name already exists on the output directory, an error will be displayed.

Only ASCII letters are supported for the output directory name and the output directory.

The date and time information is included in the file name to prevent file names from being identical.

Output Information

- Store the report information of the specified range in the report file
 Refer to "[8.4 Configuration of Report File](#)" for details on the report file.
- Output the message to the command execution screen
- Operation History of ETERNUS SF System

The following information will be output as operation history.

Output Items	Output Contents
Date	Date and time when the operation was executed
User ID	User name that performed the operation
Action	Create Report (CLI)
State	Submit, Start, or Complete
Result	Success, Failed, or Warning
Target	-
Detail	Detailed information
Message	Error message

EXIT STATUS

- =0: Completed successfully
- >0: Terminated abnormally

EXAMPLES

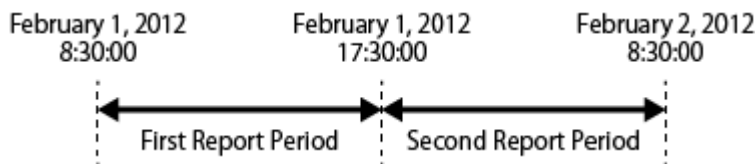
- A report from 8:30 on February 1, 2012 up to 17:30 of February 1, 2012 will be created.
(Report information up to 17:30:00 of February 1, 2012 will be subject to the report.)

```
> esfadm report create -start 201202010830 -end 201202011730 -outputfile C:\report\201202011730.xml  
esrpt00003 The report file was output. File=C:\report\201202011730.xml
```

NOTES

- When this command is executed while the [esfadm report collect command](#) is being executed, this command will be put in a stand-by state. When the [esfadm report collect command](#) executed earlier is completed, processing of this command will continue.
- This command cannot be executed again while the command is already executing. The command executed later will end in an error.
- When there is no report information within the period specified for the report, a report file with only header information will be output, and the process will end without displaying an error.
- When an error occurs while the report is being created, a report file is not be created.
- When a server error occurs while the report is being created, a report file will not be created and this command will end in an error.
- When configuration information has been changed during the period of the report being created, the report information will change from information before the configuration information was changed to information after the change.
- The date and time that is output to the report time is the local time of the ETERNUS SF system.
- The times that are specified for the -start option and the -end option will be handled as follows.
 - The time that is specified for the -start option (hhmm) will be handled at 0 seconds.
 - The time that is specified for the -end option (hhmm) will be handled at 0 seconds.

As shown in the following example, although the first end time of the period for the report specified with this command overlaps with 17:30:00 of February 1 specified as the second start time, the period of the start time subtracted from the end time is 9 hours and 15 hours respectively.



First Report Period (total 9 hours): From 8:30:00 of February 1, 2012 through to 17:30:00 of February 1, 2012

Second Report Period (total 15 hours): From 17:30:00 of February 1, 2012 through to 8:30:00 of February 2, 2012

Appendix A Customization

A.1 Overview

This software Manager and Agent control setting can be made by editing the appropriate definition files. Edit the files according to requirements. However, be sure not to edit values of parameters not discussed in this chapter.

sanma.conf (definition file)

Indicates a detailed setting file of the storage management.

ssmgr.conf (definition file for correlation management)

Indicates a detailed setting file of the storage management for the correlation management.

perf.conf (performance management definition file)

Indicates a detailed setting file of the storage performance management

SNMP Trap XML definition file (fault management definition file)

Creating this file enables detailed definitions of targets of fault monitoring using SNMP Traps and processing for the environment.

Correlation.ini (Agent definition file)

Indicates a detailed setting file of Agent.

policy.conf(reporting function definition file)

Indicates a detailed setting file of the reporting function.

A.2 sanma.conf Parameter

This file is saved at the following location as a detailed setting file of the storage management:

Platform of Manager	Location
Windows	\$ENV_DIR\ESC\Manager\etc\opt\FJSVssmgr\current\sanma.conf (\$ENV_DIR means "Environment Directory" specified at the Manager installation.)
Solaris OS, Linux	/etc/opt/FJSVssmgr/current/sanma.conf

Reflecting the contents of the setting file

If the setting file is changed, execute re-read definition file by using the Web Console, or reactivate the Manager. This reflects the settings on this software.

Customization

LOGICAL_MANAGER_IP

If the Management Server is clustered system which has physical IPs and logical IP, logical IP address must be specified in this parameter. For this parameter, specify only IPv4 format IP address.

```
Example:  
LOGICAL_MANAGER_IP="10.12.13.14";
```

This parameter is used to automatically configure a SNMP Trap send destination address for a fault monitoring device when adding devices. Refer to "[5.2.5 SNMP Trap transmission place automatic setting function](#)" for more information.

LOGICAL_MANAGER_V6IP

If the Management Server is clustered system which has physical IPs and logical IP, logical IP address must be specified in this parameter. For this parameter, specify only IPv6 format IP address.

```
Example:  
LOGICAL_MANAGER_V6IP="2001:db8::2:1";
```

This parameter is used to automatically configure a SNMP Trap send destination address for a fault monitoring device when adding devices. Refer to "[5.2.5 SNMP Trap transmission place automatic setting function](#)" for more information.

MANAGER_LAN_CARD_IP

This is specified if device detection and registration fail due to the environment having the Management Server which holds multiple IP addresses.

If specifying this parameter in a cluster environment, be sure to specify a logical IP address at the beginning.

For this parameter, specify only IPv4 format IP address.

```
Example:  
MANAGER_LAN_CARD_IP="10.12.13.14,100.101.102.103";
```

MANAGER_LAN_CARD_V6IP

This is specified if device detection and registration fail due to the environment having the Management Server which holds multiple IP addresses.

If specifying this parameter in a cluster environment, be sure to specify a logical IP address at the beginning.

For this parameter, specify only IPv6 format IP address.

```
Example:  
MANAGER_LAN_CARD_V6IP="2001:db8::2:1,2001:db8::2:2";
```

SET_SW_ZONING_ALWAYS

When an access path is set, if the zoning setting for the Fibre Channel switch need not be added because port zoning is set, this software does not generally set zoning for Fibre Channel. Specifying 1 in this parameter sets one-to-one WWPN zoning even in the above case (excluding cases in the No Security state):

```
Example:  
SET_SW_ZONING_ALWAYS=1; (Default: 0)
```

DISPLAY_SNMP_STANDARD_EVENT

Specify whether the SNMP Trap (Cold Start Trap etc.) common to devices from a device is indicated in the event log. Setting 1 for this parameter indicates the SNMP Trap common to devices. Setting 0 for this parameter does not indicate it. Default is 1 (indicate).

```
Example:  
DISPLAY_SNMP_STANDARD_EVENT = 0;
```

A.3 ssmgr.conf Parameter

This file is saved at the following location as a detailed setting file of the storage management for the correlation management:

Platform of Manager	Location
Windows	\$ENV_DIR\ESC\Manager\etc\opt\FJSVssmgr\current\ssmgr.conf (\$ENV_DIR means "Environment Directory" specified at the Manager installation.)
Solaris OS, Linux	/etc/opt/FJSVssmgr/current/ssmgr.conf

Reflecting the contents of the setting file

If the setting file is changed, execute re-read definition file by using the Web Console, or reactivate the Manager. This reflects the settings on this software.

Customization



Note

Note that the memory or the disk capacity may become insufficient when the number of generations or the maximum capacity of each log file is increased. Operation may stop when the memory or the disk capacity becomes insufficient.

Note when changing the number of generations or maximum capacity, secure the memory capacity and the disk capacity.

LOG_COUNT

The number of generations of log files (log.*) which is common to system is specified by an arbitrary decimal number.

Default is 4.

It circulates in the fourth generation (log.0, log.1, log.2 and log.3), when 4 is set.

```
Example for circulating in the fifth generation:  
LOG_COUNT = 5;
```

Location of the log file

Platform of Manager	Location
Windows	\$TMP_DIR\ESC\Manager\var\opt\FJSVssmgr\current (\$TMP_DIR means "Work Directory" specified at the Manager installation.)
Solaris OS, Linux	/var/opt/FJSVssmgr/current

LOG_LIMIT

The maximum capacity of log file (log.*) which is common to system is specified within the range of 0-2147483647 (KB).

Default capacity is 512 (KB).

When 0 or a minus value is specified, the log is not output. Moreover, when the value larger than the maximum value is specified, it becomes a default value.

```
Example for setting the maximum capacity to 2MB:  
LOG_LIMIT = 2048;
```

Refer to "[LOG_COUNT](#)" for location of the log files.

SYSTEMLOG_FACILITY (Valid only for Solaris OS Manager and Linux Manager)

Specify a facility name which has system log output destination information if a facility name is changed from the default ("daemon"). The facility name that is specified here must be defined by /etc/syslog.conf. Users can optionally change the system log output destination according to the specified facility name and the level.

Refer to online manuals of each operating system for syslog.conf definition.

A.4 perf.conf Parameter

This file is saved at the following location as a detailed setting file of the storage performance management:

Platform of Manager	Location
Windows	\$ENV_DIR\ESC\Manager\etc\opt\FJSVssmgr\current\perf.conf (\$ENV_DIR means "Environment Directory" specified at the Manager installation.)
Solaris OS, Linux	/etc/opt/FJSVssmgr/current/perf.conf

Reflecting the contents of the setting file

If the setting file is changed, execute re-read definition file by using the Web Console, or reactivate the Manager. This reflects the settings on this software.

Information

- In performance management, the setting file is referenced once every 4 hours so that changes are reflected even if the above procedure has not been performed.
- If the number of days to retain performance data is reduced, data retained that is older than the new number of days will be deleted. When you execute re-read definition file by using the Web Console, it may take a time to delete the performance data.

Customization

Note

- If the number of days performance data is kept is increased, the application may stop because of insufficient memory or disk space; therefore care must be taken to ensure space is sufficient. In particular, if 0 is set for PERF_DATA_KEEP_DAYS, processing to delete performance information stops, so check the memory or disk space regularly.
- If the number of generations of log files is increased, the application may stop because of insufficient memory or disk space, therefore care must be taken to ensure space is sufficient.
- When the performance management for number of active disks is performed, it may not be possible to obtain performance information inside the performance monitoring interval. Change the performance monitoring interval where necessary.

PERF_DATA_KEEP_DAYS

Specify the number of days during which performance management keeps performance data. The data is automatically deleted after the specified number of days elapse.

If 0 is specified, the data is not deleted. However, the number of days does not include the current day.

The default value is seven days and is defined as shown below. Change this value if necessary.

```
PERF_DATA_KEEP_DAYS = 7;
```

LOG_ROTATION

The number of generations of log files (perflog.*) related to performance is specified by an arbitrary decimal number. Default is 2. It circulates in the second generation of perflog.0 and perflog.1 when 2 is set.

```
Example for circulating in the fifth generation:  
LOG_ROTATION = 5;
```

Location of the log file

Platform of Manager	Location
Windows	\$TMP_DIR\ESC\Manager\var\opt\FJSVssmgr\log (\$TMP_DIR means "Work Directory" specified at the Manager installation.)

Platform of Manager	Location
Solaris OS, Linux	/var/opt/FJSVssmgr/log

ENABLED_ECO_MODE

Specify whether to use the performance management for the active disks, power consumption, and temperature. To use the performance management for them, specify "true". If you do not want to use it, specify "false". The default is "true".

Example: When the performance management for the number of active disks, power consumption, and temperature is used:
`ENABLED_ECO_MODE = true;`

ENABLED_PORT_ISCSI

Specify whether to use the performance management for iSCSI port on ETERNUS Disk storage system. To use the performance management for iSCSI port, specify "true". If you do not want to use it, specify "false". The default is "true".

Example: When the performance management for iSCSI port is used:
`ENABLED_PORT_ISCSI = true;`

A.5 SNMP Trap XML Definition File

Use of this file enables customization of the fault monitoring method. Define the file on the Manager and Agent sides.

SNMP Trap XML definition file on the Manager side

Event log messages and operations using linkage with Systemwalker Centric Manager, linkage with Shell/Bat and linkage with External Script can be defined for SNMP Traps received from individual device (including server node). Customize the contents of this file to change default values of this software on the Manager side according to the operating environment of the storage system used.

Creating this definition file enables a function equivalent to the fault monitoring function for support levels A and B to be implemented for a device of support level I.

The SNMP Trap XML definition file on the Agent side

It defines a fault monitoring method of an Agent server node. Customize its contents to change the monitoring method from default.

Reflecting the contents of the setting file

The setting file on the Manager side is dynamically read into this software and therefore no special reflection method is provided.

The setting file on the Agent side is read into this software statically and therefore the Agent needs to be restarted to reflect the contents of the setting file on this software.

Customization



Note

- If an error is detected in an XML definition file, a message in the format shown below is output to the event log. The fault level of notification is the information level. Linkage with Systemwalker Centric Manager and linkage with Shell/Bat are not used.

Message format: "XML parse error (detected trap: (SNMP Trap data character string))"

- Except for some devices, all swsag codes that are reported to Systemwalker Centric Manager are 4821.
- When customizing SNMP Trap processing, do not edit the definition file in the installation directory but edit the one in the customization directory.

Definition file names and storage location on the Manager side

The SNMP Trap XML definition file is created for each device. It is then stored in the following directory when Manager is installed or upgraded.

Platform of Manager	Location
Windows	\$INS_DIR\ESC\Manager\opt\FJSVssmgr\lib\snmpth (\$INS_DIR means "Program Directory" specified at the Manager installation.)
Solaris OS, Linux	/opt/FJSVssmgr/lib/snmpth

When customizing SNMP Trap processing of Manager, copy the SNMP Trap XML definition file in the above directory to the customization directory shown below, and edit the copy of the file.

Platform of Manager	Customization Directory
Windows	\$ENV_DIR\ESC\Manager\etc\opt\FJSVssmgr\current\snmpth (\$ENV_DIR means "Environment Directory" specified at the Manager installation.)
Solaris OS, Linux	/etc/opt/FJSVssmgr/current/snmpth

Manager operates as follows.

- When the SNMP Trap XML definition file exists in the customization directory
 Manager operates in accordance with its file.
- When the SNMP Trap XML definition file does not exist in the customization directory
 Manager operates in accordance with the definition file in the installation directory. (default)

In a trap of a device, the file name is enterprise code in which "." is replaced with "_".

Table A.1 Default SNMP Trap XML definition files on a system where this software is implemented with Manager

Device Type	File Name
ETERNUS SN200, Brocade, PRIMERGY Fibre Channel switch blade, Brocade VDX series, PRIMERGY BX Ethernet Fabric Switch	1_3_6_1_4_1_1588_2_1_1_1.xml
ETERNUS DX60/DX80/DX90	1_3_6_1_4_1_211_4_1_1_126_1_60.xml
ETERNUS DX80 S2/DX90 S2	1_3_6_1_4_1_211_4_1_1_126_1_100.xml
ETERNUS DX100 S3/DX200 S3	1_3_6_1_4_1_211_4_1_1_126_1_150.xml
ETERNUS DX60 S2	1_3_6_1_4_1_211_4_1_1_126_1_101.xml
ETERNUS DX400 series ETERNUS DX8000 series	1_3_6_1_4_1_211_4_1_1_126_1_50.xml
ETERNUS DX400 S2 series	1_3_6_1_4_1_211_4_1_1_126_1_100.xml
ETERNUS DX500 S3/DX600 S3	1_3_6_1_4_1_211_4_1_1_126_1_150.xml
ETERNUS DX8000 S2 series	1_3_6_1_4_1_211_4_1_1_126_1_102.xml
ETERNUS LT20(SCSI)	1_3_6_1_4_1_11_2_36_1.xml
ETERNUS LT200	1_3_6_1_4_1_119_1_83_1_21.xml
ETERNUS LT210, LT220, LT230	1_3_6_1_4_1_119_1_83_1_1.xml 1_3_6_1_4_1_119_1_83_1_2.xml
ETERNUS LT250	1_3_6_1_4_1_211_4_1_1_126_3_5.xml
ETERNUS LT270	1_3_6_1_4_1_211_4_1_1_126_3_2.xml

Device Type	File Name
ETERNUS LT270 S2	1_3_6_1_4_1_211_4_1_1_126_3_6.xml
Tape encryption device	1_3_6_1_4_1_2021_250_10.xml
Fibre Alliance MIB support device	1_3_6_1_3_94.xml
NetApp FAS Series and V-Series	1_3_6_1_4_1_789.xml
ETERNUS VS850	1_3_6_1_4_1_2_6_190.xml
ETERNUS LT20/LT20 S2/LT40/LT40 S2/LT60/LT60 S2 (SAS/FC model)	1_3_6_1_4_1_20884_10893_2_101_3.xml
ETERNUS CS2000	1_3_6_1_4_1_231_2_48_2_0.xml
Event from performance management	1_3_6_1_4_1_211_4_1_3_21_3.xml
Multipath-related event from Solaris OS Agent or Windows Agent	1_3_6_1_4_1_211_4_1_3_21_2.xml (*1)
Safe/PRIMECLUSTER GDS or GFS series event from Solaris OS Agent	1_3_6_1_4_1_211_4_1_3_21_2_2.xml (*1)(*2)
Multipath-related event from Solaris OS Agent	1_3_6_1_4_1_211_4_1_3_21_2_21.xml (*1)(*2)
Multipath-related event from Windows Agent	1_3_6_1_4_1_211_4_1_3_21_2_5.xml (*1)(*2)
MPIO event from Windows Agent	1_3_6_1_4_1_211_4_1_3_21_2_51.xml (*1)(*2)
ETERNUS multipath driver event from Linux Agent	1_3_6_1_4_1_211_4_1_3_21_2_3.xml (*1)(*2)
PRIMECLUSTER GDS or GFS series event from Linux Agent	1_3_6_1_4_1_211_4_1_3_21_2_31.xml (*1)(*2)
LVM(PV-Links) event from HP-UX Agent	1_3_6_1_4_1_211_4_1_3_21_2_4.xml (*1)(*2)
HBA driver event from HP-UX Agent	1_3_6_1_4_1_211_4_1_3_21_2_41.xml (*1)(*2)
Multipath-related event from AIX Agent	1_3_6_1_4_1_211_4_1_3_21_2_6.xml (*1)(*2)

*1: This file can be changed only concerning the on/off setting of "linkage with Systemwalker Centric Manager" (only Shell/Bat linkage control can be done and Systemwalker Centric Manager linkage cannot be.) and "external script linkage 1" and "external script linkage 2" in "Operation definition" (the flag attributes) in "Definition contents" of "Definition file format". For "Fault level" and "Message," this file cannot be changed.

*2: When this file is updated, the file with the same name on the Agent side must also be updated so that their contents are the same.

For devices excluding the above ones, SNMP Trap processing for each device is enabled by creating XML files according to the enterprise code of the device.

Definition file name and storage location on the Agent side

The XML definition file for customizing the fault monitoring method of an Agent server node is saved at the following location:

Platform of Agent	Location
Windows	\$ENV_DIR\ESC\Agent\etc\snmpth (\$ENV_DIR means "Environment Directory" specified at the Agent installation.)
Solaris OS, Linux, HP-UX, AIX	/etc/opt/FJSVssage/snmpth

The file is read and used when Agent starts. Therefore, the restart of Agent is needed to operate according to the modified contents when the file is modified.

The file name is the enterprise code in a trap issued from Agent to Manager and in which "." is replaced with "_".

Table A.2 Default SNMP Trap XML definition files on a system where this software is implemented with Agent

Server Node	File Name (*1)	Monitoring Target
Solaris OS	1_3_6_1_4_1_211_4_1_3_21_2_2.xml	Safe/PRIMECLUSTER GDS, GFS series
	1_3_6_1_4_1_211_4_1_3_21_2_21.xml	ETERNUS multipath driver
	1_3_6_1_4_1_211_4_1_3_21_2_22.xml	EMC PowerPath
	1_3_6_1_4_1_211_4_1_3_21_2_23.xml	HITACHI JP1/HiCommand Dynamic Link Manager
	1_3_6_1_4_1_211_4_1_3_21_2_24.xml	Sun MPxIO
Windows	1_3_6_1_4_1_211_4_1_3_21_2_5.xml	ETERNUS multipath driver
Linux	1_3_6_1_4_1_211_4_1_3_21_2_3.xml	ETERNUS multipath driver
	1_3_6_1_4_1_211_4_1_3_21_2_31.xml	PRIMECLUSTER GDS, GFS series
HP-UX	1_3_6_1_4_1_211_4_1_3_21_2_4.xml	PV-LINK (LVM function)
	1_3_6_1_4_1_211_4_1_3_21_2_41.xml	HBA driver
AIX	1_3_6_1_4_1_211_4_1_3_21_2_6.xml	MPIO

*1: When this file is updated, the file with the same name on the Manager side must also be updated so that their contents are the same.

Definition file format

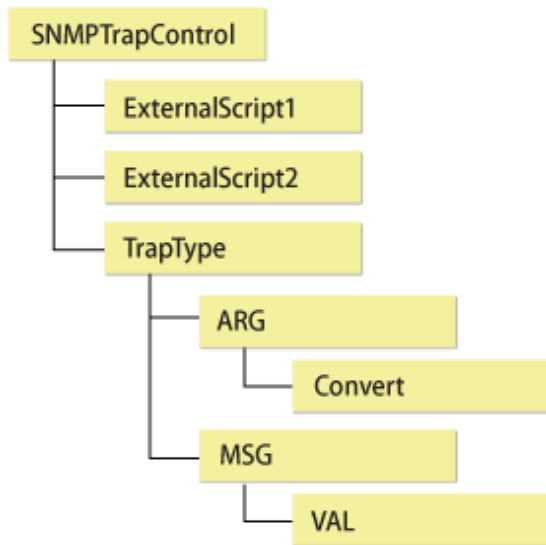
Definition contents

Operations are defined by the following items for the Specific Trap Type in the definition file:

Item	Description
Operation definition	Whether to post a status change to a window Whether to output the event log Whether to implement linkage with Systemwalker Centric Manager and linkage with Shell/Bat Whether to enable external script linkage 1 Whether to enable external script linkage 2
Fault level	Notification levels of individual events and linkage with Systemwalker Centric Manager (Information/Warning/Error)
Message	Message output for event and linkage with Systemwalker Centric Manager

Node hierarchy

The following figure shows the hierarchy of tag nodes:



Tags and attributes

SNMPTrapControl tag

Attribute Name	Description
name	Device name
ver	Version of this definition file

ExternalScript1, ExternalScript2 tag (option)

This tag defines the script name when using external script linkage. ExternalScript1 indicates external script linkage 1 and ExternalScript2 indicates external script linkage 2. A script defined here is executed when the corresponding linkage bit is set on in the flag attribute of the TrapType tag or the Convert tag.

ExternalScript1 and ExternalScript2 tag must be defined in a line above the TrapType tag definition.

Attribute Name	Description
name	Executed script name (using full path name)

TrapType tag

This tag defines trap analysis operations for each Specific Trap Type. Traps of types not defined by the TrapType tag are not analyzed and discarded.

Attribute Name	Description
type	"ST" + Specific Trap Type number (decimal)
flag	Control of event, linkage with Systemwalker Centric Manager, linkage with Script, and e-mail notification (in 7-bits binary) The "0" is interpreted as "off", the "1" is "on". bit6 ... e-mail notification of a information event (*1) bit5 ... external script linkage2 bit4 ... external script linkage1 bit3 ... Linkage with Systemwalker Centric Manager, Linkage with Shell/Bat (*2) bit2 ... Event log output bit1 ... (Cannot be changed) bit0 ... Status change notification

Attribute Name	Description
	For example, only linkage with Systemwalker Centric Manager is set to on flag="0001000". If you specify it only 4 bit length, the values of bit4, bit5, and bit6 are interpreted as "0". For example, flag="1111" is interpreted as flag="0001111".
level	Specify events and the levels that are posted to Systemwalker Centric Manager. (I: Information / W: Warning / E: Error)
msg	Messages displayed for events and linkage with Systemwalker Centric Manager, sending and linkage with Script. The following parameters can be included in messages: %d: Decimal number %x: Hexadecimal number %s: Character string As many ARG tags as the number of parameters included in a message must be defined as described in (4) below. If any character other than 'd', 'x', and 's' follows %, the % is handled as a character and displayed as is.

*1: Set it to on if you want to enable the e-mail notification of an information event or disable the e-mail notification of a warning event and an error event.

*2: Since events of the Agent are not reported to Systemwalker Centric Manager, only Shell/Bat linkage control can be done in the definition file of the Agent.

ARG tag

The ARG tag defines correspondence between a parameter specified in the msg attributes of the TrapType tag and a Variable Binding index in trap data. There are as many ARG tags as the number of parameters specified in the msg attributes must be defined.

Attribute Name	Description
index	Index number (0 or larger) of a parameter included in the msg attributes of the TrapType tag described in (3).
VBIndex	Index number (0 or larger) of Variable Binding in Trap data

Convert tag (option)

The Convert tag specifies how to express a character string for an INTEGER-type data value of a trap. Definition of this tag is optional. For example, to use Trap data value 0 to indicate the status of OK, specify <Convert val="0" name="OK"/> so that character string "OK" can be displayed instead of "0".

By specifying the flag attribute and level attribute (options), a fault level specified in the level attribute of the TrapType tag can be changed and posted. (If the msg attribute includes multiple ARGs and the flag or level attribute is specified in individual Convert tags, the values specified in the Convert tag of the last ARG are used.)

Attribute Name	Description
val	Numeric data value (decimal) of the INTEGER type in a Trap
flag (option)	Control of events, linkage with Systemwalker Centric Manager, linkage with Script, and e-mail notification (in 7-bit binary)

Attribute Name	Description
	Refer to " TrapType tag ". for values
level (option)	Fault level "I", "W", or "E" This tag is given a higher priority than the TrapType tag.
name	Character string corresponding to val

If an undefined value is received, the value is displayed as a numeric value as is.

MSG tag

The MSG tag defines a monitoring keyword for Server Node Agent monitoring. It is valid only for Server Node Agent.

Windows Agent: Monitors with the id, src, and type attributes (ignores the key attribute).

Another Agent: Monitors with the key attribute (ignores the id, src, and type attributes).

Attribute Name	Description
key	Monitoring keyword for monitoring (required for a non-Windows Agent)
id	Event ID of the event to be monitored (required for a Window Agent)
src	Source name of the event to be monitored (required for a Windows Agent)
line	When a VAL tag is used (a substring of a monitored event is added to notification information), specify the number of monitored event lines for the line attribute. The line attribute can be omitted for a single line or when a Windows Agent is used.
type	Specify the type of event logs to be monitored. (Valid only for windows Agent) System: Monitor the system log. (Default) Application: Monitor the application log.

To change the monitoring keyword, change this keyword.

A normal expression can be specified to the monitoring keyword.

To add a monitoring keyword for monitoring, add the TrapType tag and later shown below. Be sure not to specify a Specific Trap Type number that is already specified.

VAL tag (option)

The VAL tag is used to define the method of retrieving a character string from the monitored event and adding it to notification information. The VAL tag is valid only for Server Node Agent.

Attribute Name	Description
ref	Specify the value to be added to notification information. Specify the value in parentheses () in normal expression.

ID attribute specification by DTD

During SNMP Trap control, the type attribute of the TrapType tag is used as the ID attribute for searches, so DTD must be described as follows in the XML definition file:

```
<!DOCTYPE SNMPTrapControl[
<!ATTLIST TrapType type ID #REQUIRED>
]>
```

Definition file sample

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE SNMPTrapControl
<!ATTLIST TrapType type ID #REQUIRED>
]>
<SNMPTrapControl name="SW3800" ver="1.0">
  <TrapType type="ST1" flag="111111" level="E" msg="Faulty reason: %d">
    <ARG index="0" VBIndex="0">
      <Convert val="0" flag="000110" level="I" name="sw-ok"/>
      <Convert val="1" name="sw-faulty"/>
    </ARG>
  </TrapType>
  <TrapType type="ST2" flag="000111" level="E" msg="%s: is currently in state %d">
    <ARG index="0" VBIndex="4"/>
    <ARG index="1" VBIndex="0">
      <Convert val="1" name="unknown"/>
      <Convert val="2" name="faulty"/>
      <Convert val="3" name="below-min"/>
      <Convert val="4" flag="000110" level="I" name="nominal"/>
      <Convert val="5" name="above-max"/>
      <Convert val="6" name="absent"/>
    </ARG>
  </TrapType>
</SNMPTrapControl>
```



Example

Method of suppressing ETERNUS SN200 series, Brocade series FC port Online/Offline traps:

To suppress ETERNUS SN200 series, Brocade series FC port Online/Offline traps, change the following locations in the corresponding XML definition file.

The flag attribute is changed to "000000" in val="1" and val="2" of the Convert tag in <ARG index="1" VBIndex="0"> for which "ST3" is specified as the type attribute.

```
<Convert val="1" flag="000000" level="I" swsag="4203" name="Online" />
<Convert val="2" flag="000000" level="I" swsag="4203" name="Offline" />
```

A.6 Correlation.ini Parameter

This file is saved at the following location of the Server Node as a detailed setting file of Agent:

Platform of Agent	Location
Windows	\$ENV_DIR\ESC\Agent\etc\Correlation.ini (\$ENV_DIR means "Environment Directory" specified at the Agent installation.)
Solaris OS, Linux, HP-UX, AIX	/etc/opt/FJSVssage/Correlation.ini

Reflecting the contents of the setting file

The file is read and used when Agent starts.

To operate according to the contents of the file the restart of Agent is needed.

Customization

PollingTime

Specify a period of time in seconds during which system messages are monitored. The default value is 10.

0 (not monitored) to 3600 (one hour)

```
PollingTime=time
```

HBASStatus (HP-UX Agent does not support this parameter)

Specify this parameter to collect HBA's status. The default value is ON.

```
HBASStatus= ON or OFF
```

- ON (status of HBA is collected.)
- OFF (status of HBA is suppressed.)

To unite states of HBA in the environment where the Storage Cruiser's agent of Solaris OS and Windows exist together with SSC agent, turn HBASStatus to OFF.

HBAMask (HP-UX Agent does not support this parameter)

Use this parameter to make HBA port be non-displayed. Specify World Wide Port Name (WWPN) of HBA port non-displayed is specified. If multiple HBA ports are specified, specify as many parameters as the number of HBA ports.

```
HBAMask=WWPN-of-HBA-port
```

The Warning status is displayed for HBA port when FC cable is not connected with it. To suppress the status of HBA because of unused or similar reason, use this parameter.

If HBA displayed in the Web Console is specified, delete the relevant HBA in the Web Console. If not delete, the relevant HBA remains displayed in the Web Console.

A.7 Device Polling Setting File

Editing these setting files can customize the default behavior of the device polling function. Two setting files are provided: one file is for defining the polling function behavior and the other file is for defining event linkage control. These files are described in XML.

Reflecting the contents of the setting file

Changed contents are automatically reflected at the next polling operation. (Manager checks the file contents every 30 seconds even while polling is stopped.) Even if executing "Definition File Re-read" using the Web Console, be careful that the file may not be reflected.

Customization (Polling function behavior setting file)



- If an error is detected in an XML file, the event message shown below is output for each polling operation. In this event, the polling function operates with the default settings.

Message: "[Polling] XML File Format Error(XML file name)"

- Be sure not to delete the file itself even if no items are set. If the file is deleted, re-create the file according to the above sample.
- When customizing the polling function behavior setting file, do not edit the setting file in the installation directory but edit the one in the customization directory.

Setting file name and storage directory

The polling function behavior setting file is stored in the following location during Manager installation or upgrading:

Platform of Manager	Location
Windows	\$INS_DIR\ESC\Manager\opt\FJSVssmgr\lib\devicepolling\DP_config.xml (\$INS_DIR means "Program Directory" specified at the Manager installation.)
Solaris OS, Linux	/opt/FJSVssmgr/lib/devicepolling/DP_config.xml

When customizing the polling function behavior, copy the polling function behavior setting file in the above location to the customization location shown below, and edit the copy of the file.

Platform of Manager	Customization Location
Windows	\$ENV_DIR\ESC\Manager\etc\opt\FJSVssmgr\current\devicepolling\DP_config.xml (\$ENV_DIR means "Environment Directory" specified at the Manager installation.)
Solaris OS, Linux	/etc/opt/FJSVssmgr/current/devicepolling/DP_config.xml

If the polling function behavior setting file exists in the customization location, Manager operates in accordance with the setting file. If not, it operates in accordance with the default setting file in the installation directory.

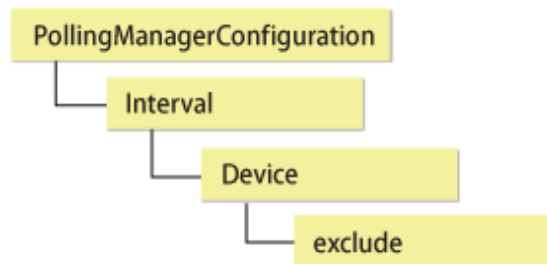
Setting file format

Setting contents

Item	Description
Polling interval	Polling operation interval (including during stoppage)
Device not subject to polling	Specify a device to exclude it from polling.

Node hierarchy

The tag node hierarchy is shown below.



Tags and attributes

Interval tag

Attribute Name	Description
value	A polling operation interval is set in seconds (decimal). The minimum interval is 30 seconds. If a value less than 30 is specified, 30 seconds is used for polling. Specifying 0 stops polling.

Device/exclude tag

No attributes can be set in the Device tag. As many exclude tags as required can be set.

exclude tag

Attribute Name	Description
address	Specify the IP address of a device to exclude it from polling operations. For IP address, IPv4 or IPv6 format can be specified.

Default value

The default values of the parameters are as follows:

Polling interval: 60 seconds

Device not subject to polling: None

Sample setting file

```
<?xml version="1.0" encoding="UTF-8" ?>
<PollingManagerConfiguration>
  <Interval value="60" />
  <Device>
    <exclude address="10.20.30.40" />
    <exclude address="10.20.30.50" />
  </Device>
</PollingManagerConfiguration>
```

Customization (Control Event Linkage setting file)



Note

- The portions that can be changed are the name attribute values of the ExternalScript1 and ExternalScript2 tags and the flag attribute value of the Convert tag only. The other portions may not be modified since the changes can possibly cause an abnormal behavior of the polling function.
- Events involving the server node agent are not posted to Systemwalker Centric Manager. Use the monitoring function of Systemwalker Centric Manager to monitor operating status.

Setting file name and storage directory

The setting file is stored in the following directory:

Platform of Manager	Location
Windows	\$INS_DIR\ESC\Manager\opt\FJSVssmgr\lib\snmpth\1_3_6_1_4_1_211_4_1_3_21_1.xml (\$INS_DIR means "Program Directory" specified at the Manager installation.)
Solaris OS, Linux	/opt/FJSVssmgr/lib/snmpth/1_3_6_1_4_1_211_4_1_3_21_1.xml

Setting file format

Setting contents

Item	Description
External script name definition	Define the script name when using external script linkage.
Operation definition	Whether to display a posted status change Whether to output the event log Whether to implement linkage with Systemwalker Centric Manager and linkage with Shell/Bat

Item	Description
	Whether to implement external script linkage 1
	Whether to implement external script linkage 2

Setting method

- External Script name definition

When using external script linkage, define the script name in the name attribute of following definition lines (in full path specification).

Item	Definition Line
external script linkage 1	<ExternalScript1 name="c:\somedir\script1.bat" />
external script linkage 2	<ExternalScript2 name="c:\somedir\script2.bat" />

- Event linkage behavior definition

In the configuration file, there are following definition lines according to the events. To define Event linkage behavior, set in the flag attribute of each definition line.

Event	Definition Line
When the status becomes normal	<Convert val="0" name="" level="I" flag="001111" />
When the status becomes warning	<Convert val="1" name="" level="W" flag="001111" />
When the status becomes error	<Convert val="2" name="" level="E" flag="001111" />
When the status becomes timeout	<Convert val="3" name="" level="WT" flag="001111" />
When communication has been recovered	<Convert val="10" name="" level="IR" flag="001111" />

Flag Attribute is shown below.

Attribute Name	Description
flag	<p>Control of event, linkage with Systemwalker Centric Manager, and linkage with Script (in 6-bits in binary)</p> <p>The "0" is interpreted as "off", the "1" is "on".</p> <p>bit5 ... External script linkage 2 bit4 ... External script linkage 1 bit3 ... Linkage with Systemwalker Centric Manager, Linkage with Shell/Bat bit2 ... Event log output bit1 ... (Cannot be changed) bit0 ... Status change notification</p> <p>For example, only linkage with Systemwalker Centric Manager is set to on "001000".</p>

A.8 Polling Service Setting File

The default operation of the polling service can be customized by editing its XML configuration file.

Reflecting the file

If the setting file is changed, execute re-read definition file by using the Web Console, or reactivate the Manager. This reflects the settings on this software.

Customization



- Do not delete the file, even if no items are specified.
- To customize the polling service, edit the file in the customization directory (not the one in the installation directory).

File path and name

When the Manager is installed or upgraded, the configuration file is stored in the directory below:

Manager OS	Absolute Path Name
Windows	\$INS_DIR\ESC\Manager\opt\FJSVssmgr\lib\polling\pollingService.xml, where \$INS_DIR is the "executable directory" specified during Manager installation.
Solaris OS, Linux	/opt/FJSVssmgr/lib/polling/pollingService.xml

To customize the polling service, copy the configuration file in the directory above to the customization directory below, then edit it:

Manager OS	Absolute Path Name (for customization)
Windows	\$ENV_DIR\ESC\Manager\etc\opt\FJSVssmgr\current\polling\pollingService.xml, where \$ENV_DIR is the "environment directory" specified during Manager installation.
Solaris OS, Linux	/etc/opt/FJSVssmgr/current/polling/pollingService.xml

If there is a configuration file in the customization directory, then the Manager uses it, otherwise it uses the default configuration file in the installation directory.

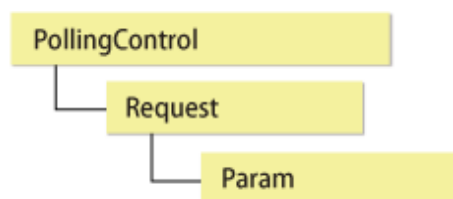
File format

Contents

Item	Content
Polling interval	Polling operation interval (including stopping).
Polling execution time specification	Polling execution time.

Node hierarchy

The tag node hierarchy for is displayed below:



Tags and attribute types

Request tag

Attribute Name	Content
interval	<p>Polling interval in seconds (in decimal format).</p> <p>The minimum value is 30 - specifying shorter values will result in this value being used.</p> <p>The maximum value is 9223372036854775 - specifying larger values will result in this value being used.</p> <p>Note that values larger than 9223372036854775807 will cause an error.</p> <p>Specifying 0 will cause the polling service to not be executed.</p> <p>If both interval attribute and exectime attribute exist, interval attribute "interval" is given a higher priority than exectime attribute.</p>
exectime	<p>Polling execution time (in hh:mm:ss format - example: 21:15:00)</p> <p>hh has a valid range of 0 to 23, and mm and ss have a range of 0 to 59.</p> <p>If both interval attribute and exectime attribute exist, interval attribute "interval" is given a higher priority than exectime attribute.</p>

Param tag

None.

Default value

The default values of the parameters are as follows:

Polling interval: 3600 seconds

Polling execution time: 01:00:00

Sample configuration file

```
<?xml version="1.0" encoding="UTF-8" ?>
<PollingControl name="Default" ver="1.0">
  <Request name="WatchAlarm"
className="com.fujitsu.storagesoft.services.polling.method.WatchPoolAlarm" interval="3600">
    <param key="Warning" value="pool status changed: Warning" />
    <param key="Caution" value="pool status changed: Caution" />
    <param key="Normal" value="pool status changed: Normal" />
  <Request name="WatchCapacity"
className="com.fujitsu.storagesoft.services.polling.method.WatchPoolCapacity"
exectime="01:00:00" />
</PollingControl>
```



Example

Modification Method at intervals that observes threshold of Thin Provisioning Pool

Change the following part when you change the threshold watch interval of Thin Provisioning Pool.

The name attribute changes the interval attribute of the Request tag of "WatchAlarm". It specifies it at the second. Interval attribute is changed to "1800" when changing every 30 minutes.

```
<Request name="WatchAlarm"
className="com.fujitsu.storagesoft.services.polling.method.WatchPoolAlarm" interval="1800">
```

Example

Modification method at acquisition time of capacity information on Thin Provisioning Pool

Change the following part when you change acquisition time of capacity information on Thin Provisioning Pool.

The name attribute changes the exectime attribute of the Request tag of "WatchCapacity". The value is time (hh):(mm): It specifies it by second (ss). The exectime attribute is changed to "12:00:00" when changing at 12:00.

```
<Request name="WatchCapacity"
className="com.fujitsu.storagesoft.services.polling.method.WatchPoolCapacity" exectime="12:00:00" />
```

A.9 Explanation of the Configuration Settings File

The configuration file of devices targeted by the performance management function can be configured by editing the configuration settings file.

The following devices can be customized:

- Fibre Channel switches and Fibre Channel switch blades that support performance monitoring

Reflecting the file

If the file has been changed, then either start performance monitoring of targeted devices, or reactivate the Manager. This will reflect the contents of the file to this product.

Customization

Note

To restore the contents, the configuration file must be updated. Refer to ["7.2.9 Updating configuration information"](#) for details.

File path and name

A separate configuration settings file must be created for each device for which you want to change the configuration file.

Manager OS	Absolute Path Name
Windows	\$ENV_DIR\ESC\Manager\etc\opt\FJSVssmgr\current\perfconf\IP address.xml where \$ENV_DIR is the "environment directory" specified during Manager installation.
Solaris OS Linux	/etc/opt/FJSVssmgr/current/perfconf/IP address.xml

Specify the following for file name:

IP Address Set to Device	File Name
IPv4 address	"." in the IP address set to device is replaced with "_".
IPv6 address	":" in the IP address displayed in FC switch list is replaced with "_". Refer to "Display FC Switch List" in the <i>ETERNUS SF Web Console Guide</i> for the procedure to display FC switch list.

Example

If the IPv4 address is 10.20.30.40:

```
10_20_30_40.xml
```

If the IPv6 address displayed in FC switch list is 2001:0:0:1::1:

```
2001_0_0_1__1.xml
```

port-baud-rate-X

Specify the port number in the X part of the property name (port-baud-rate-X).

Specify a port transfer rate value between 0 and 25 (Unit: Gbps).

Note

- Performance monitoring and threshold value monitoring cannot be used if 0 is set as the transfer rate of the port.
- The graph display function cannot be used if 0 is set as the transfer rate of the port.
- When the performance values are displayed as a graph, 0 is displayed as the performance value for intervals in which 0 is set as the transfer rate.
- If the specified transfer rate is invalid range, then the following values are displayed:

Transfer Rate	Explanation
Less than 0	0Gbps is set.
Greater than 25	25Gbps is set.

Example

Setting 8Gbps as the transfer rate for Ports 1 and 2

```
port-baud-rate-1=8  
port-baud-rate-2=8
```

Point

The maximum transfer rate for the VE port of the Fibre Channel switch is set to the default of 1Gbps.

If the FCIP trunking function or the FCIP data compression function are enabled and a transfer quantity of 1Gbps or more occurs for the VE port, then you must change the VE port transfer rate.

Use the formula below to calculate the transfer rate:

```
Transfer rate = Compression ratio set for the VE port * Total bandwidth set for the VE port
```

Example

Method for calculating the transfer rate of VE ports

For the environment below:

- Compression ratio (4:1)
- Four FCIP circuits each with a bandwidth of 0.5Gbps set for the VE port

```
Transfer rate = Compression ratio (4:1) * Total bandwidth (0.5Gbps * 4 circuits)  
              = 4 * (0.5 * 4)  
              = 8 (Gbps)
```


A.10 snmptrapd.conf Configuration File

In order for the Linux Manager to use SNMP Traps for fault monitoring, customize snmptrapd.conf (the configuration file included in the OS standard net-snmp package).

Manager OS	Location
Linux	/etc/snmp/snmptrapd.conf
	/usr/share/snmp/snmptrapd.conf

Reflecting the file

If the file has been changed, then restart snmptrapd:

```
# /etc/init.d/snmptrapd stop
# /etc/init.d/snmptrapd start
```



In an environment where a ServerView trap distributor program (SMAWtrpsv) is being used, follow the steps below to restart it:

```
# /etc/init.d/snmptrapd stop
# /etc/init.d/trpsrvd stop
# /etc/init.d/snmptrapd start
# /etc/init.d/trpsrvd start
```

Customization

disableAuthorization

Set as shown below if you want to disable access control.

If not set, access control is enabled.

```
disableAuthorization yes
```



- Check both /etc/snmp/snmptrapd.conf and /usr/share/snmp/snmptrapd.conf.
- If there are no requests from other products, then disable access control by setting this parameter to "yes".

authCommunity

This parameter can be customized if access control is enabled.

The format is displayed below:

```
authCommunity TYPES COMMUNITY [SOURCE [OID | -v VIEW ]]

TYPES: log, execute, net
COMMUNITY: Community name of monitoring target SNMP trap
```

TYPES can be set to log, execute, or net. COMMUNITY must be set to the SNMP Trap community name of the monitoring target device. Do not set SOURCE, OID, or VIEW.

Set as shown below.

```
Example:
authCommunity net public
authCommunity net SANMA
```

If a device with an SNMP Trap community name other than "public" or "SANMA" is to be monitored, add an authCommunity entry. For example, if the device to be monitored has the community name "common", set this parameter as below. Note that the "public" and "SANMA" entries are mandatory.

```
Example:
authCommunity net public
authCommunity net SANMA
authCommunity net common
```

If authCommunity log or authCommunity execute has already been set by another product, in the TYPES field, then add "net", preceded by a comma. For example, set as shown below if authCommunity execute public is already set:

```
Example:
authCommunity execute,net public
```

Note

Check /etc/snmp and /usr/share/snmp, and edit snmptrapd.conf in the file that already has authCommunity set by another product. If there is no setting in either file, then edit /etc/snmp/snmptrapd.conf.

forward

Make sure that the following is set in /etc/snmp/snmptrapd.conf:

```
forward default unix:/var/opt/FJSVssmgr/trap_socket
```

Examples

If access control is disabled

```
disableAuthorization yes
forward default unix:/var/opt/FJSVssmgr/trap_socket
```

If access control is enabled

```
authCommunity net public
authCommunity net SANMA
forward default unix:/var/opt/FJSVssmgr/trap_socket
```

Monitoring a device that has the SNMP Trap community name "common"

```
authCommunity net public
authCommunity net SANMA
authCommunity net common
forward default unix:/var/opt/FJSVssmgr/trap_socket
```

If authCommunity execute public has already been set

```
authCommunity execute,net public
authCommunity net SANMA
forward default unix:/var/opt/FJSVssmgr/trap_socket
```

Note

After snmptrapd.conf is customized, if an application (such as ServerView AlarmService) that uses snmptrapd is installed or uninstalled, or if settings are changed, then make sure that the customized contents of snmptrapd.conf have not been changed.

A.11 policy.conf Parameter

It is a detailed configuration file of the Reporting function, and is stored in the following location.

Platform of Manager	Absolute Path Name
Windows	\$INS_DIR\Common\etc\report (<i>\$INS_DIR</i> means "Program Directory" specified at the ETERNUS SF Manager installation.)
Solaris OS, Linux	/etc/opt/FJSVesfcm/conf/report

Reflecting the contents of the setting file

There is no special reflection method because of being read when the [esfadm report create command](#) is executed.

Customization

Format of set item

The preservation period of collected report information is specified.

Initialization is three months (retention_period =0000-03-00).

The date when the [esfadm report create command](#) was executed is the starting point, and the preservation period is specified in the form of "YYYY-MM-DD". Only one of YYYY, MM, and DD can be specified.

- YYYY: The preservation period is specified in number of years. Years that can be specified are from 0000 to 0010.
- MM: The preservation period is specified in number of months. Months that can be specified are from 00 to 12.
- DD: The preservation period is specified in number of days. Days that can be specified are from 00 to 31.

The message esrpt00221 is output when two or more are specified, and the command terminates abnormally.

Examples

Preservation periods

- Policy setting
 - Example 1: retention_period =0001-00-00
 - Example 2: retention_period =0000-01-00
 - Example 3: retention_period =0000-00-01
- Execution date and time of command
 - 8:00 on March 31, 2012
- Handling at preservation period
 - Example 1: The preservation period is one year from 8:00 on March 31, 2011 to 8:00 on March 31, 2012.
 - Example 2: The preservation period is one month from 8:00 on February 29, 2012 to 8:00 on March 31, 2012.
 - Example 3: The preservation period is one day from 8:00 on March 30, 2012 to 8:00 on March 31, 2012.

Appendix B Troubleshooting

This appendix explains the most common problems that might be encountered during ETERNUS SF Storage Cruiser operation. Further, it explains basic troubleshooting and also provides information on where to find further help.

B.1 Collecting the troubleshooting information

If a failure occurs in this software, the following troubleshooting information will be required:

Information for initial investigation

It is the information required for the initial analysis of problems.

The size of data should be small so that it can easily be sent by email.

Collect troubleshooting information immediately when a problem occurs. Sometimes, important information is lost over time.

Information for further investigation

The information for initial investigation can sometimes determine the cause of problems. However, some problems might require further, detailed troubleshooting information. Therefore, in case the cause of a problem cannot be determined from an initial investigation alone, it is required to collect more detailed information.

Collect information for further investigation and submit it to Fujitsu technical staff if requested.



- Sometimes, important information is lost over time. Collect troubleshooting information immediately when a problem occurs.
- When using the following to store the collected information, check if there is enough space in the filesystem to ensure system resources are not depleted or any effect is had on system operation.

Platform	Filesystem Which Attention is Necessary for Use
Windows	filesystem configured in the environment variable TEMP
Solaris OS, Linux, HP-UX, AIX	"/", "/var", and "/tmp"

Also, be careful about space when a different directory is specified with the command option. Ensure there is sufficient space in the directory.

- As a material for investigation, the information will reach 200KB - 5 MB (the maximum size is 30MB with "-all" option). Also, it is necessary to reserve 5 - 30MB (30 - 80 MB with the "-all" option) for a temporary directory to store the information. The space required varies depending on operating environment, and the data described above is for reference.

B.2 Information for initial investigation

When a system failure occurs, determine and analyze the cause of the problem as soon as possible.

This section explains information required for initial investigation.

Advantage

The information used for initial problem analysis can be acquired immediately, and is small enough to be sent by email.

B.2.1 Collecting information from the Management Server (Solaris OS)

Export the initial investigation information by using the Web Console.

If the export fails or the Web Console cannot be used, collect the information as follows. Submit the information to the Fujitsu technical staff.

Point

In cluster configurations, collect information on both the primary and secondary nodes of the Management Server.

1. Make a note of the error code (swsagXXXX), if an error dialog box is displayed.

2. Login to the server where you perform the operation.

Perform the operation with OS administrator permissions (root) after login.

3. Execute the esfsnap command.

```
# /opt/FJSVesfcm/bin/esfsnap -dir directory
```

Specify the directory to save the information with -dir option (The -dir option cannot be omitted).

B.2.2 Collecting information from the Management Server (Linux)

Export the initial investigation information by using the Web Console.

If the export fails or the Web Console cannot be used, collect the information as follows. Submit the information to the Fujitsu technical staff.

Point

In cluster configurations, collect information on both the primary and secondary nodes of the Management Server.

1. Make a note of the error code (swsagXXXX), if an error dialog box is displayed.

2. Login to the Management Server with OS administrator permissions (root).

OS administrator permissions are required to collect the information.

3. Execute the esfsnap command.

```
# /opt/FJSVesfcm/bin/esfsnap -dir directory
```

Specify the directory to save the information with -dir option (The -dir option cannot be omitted).

B.2.3 Collecting information from the Management Server (Windows)

Export the initial investigation information by using the Web Console.

If the export fails or the Web Console cannot be used, collect the information as follows. Submit the information to the Fujitsu technical staff.

1. Make a note of the error code (swsagXXXX), if an error dialog box is displayed.

2. Login to the Management Server with the user of an Administrators group.

OS administrator permissions are required to collect the information.

3. Execute the esfsnap command. The \$INS_DIR means "Program Directory" specified at the Manager installation.

```
C:\> $INS_DIR\Common\bin\esfsnap -dir directory
```

Specify the directory to save the information with `-dir` option (The `-dir` option cannot be omitted).

B.2.4 Collecting information on the Managed Server node (Solaris OS)

The method for collecting information is as follows. Submit the information to the Fujitsu technical staff.

1. Login to the server where you perform the operation.

Perform the operation with OS administrator permissions (root) after login.

2. Execute the `agentsnap` command.

```
# /opt/FJSVssage/sys/agentsnap [-dir directory]
```

It is possible to change a directory to save the information by specifying `-dir` option. If the option is omitted, information will be saved in `/tmp`.

B.2.5 Collecting information on the Managed Server node (Windows)

The method for collecting information is as follows. Submit the information to the Fujitsu technical staff.

1. Login to the server node with the user of an Administrators group.

OS administrator permissions are required to collect the information.

2. Execute the `agentsnap` command. The `$INS_DIR` means "Program Directory" specified at the Agent installation.

```
C:\> $INS_DIR\ESC\Agent\sbin\agentsnap -dir directory
```

Specify the directory to save the information with `-dir` option (The `-dir` option cannot be omitted).

3. Collect event log of Windows by Event Viewer which is a standard application of Windows.

Run "Event Viewer", select [Action] - [Save Log File As], and save the following event log files.

- System files
- Application files

B.2.6 Collecting information on the Managed Server node (Linux)

The method for collecting information is as follows. Submit the information to the Fujitsu technical staff.

1. Login to the server node with OS administrator permissions (root).

OS administrator permissions are required to collect the information.

2. Execute the `agentsnap` command.

```
# /opt/FJSVssage/sys/agentsnap [-dir directory]
```

It is possible to change a directory to save the information by specifying `-dir` option. If the option is omitted, information will be saved in `/tmp`.

B.2.7 Collecting information on the Managed Server node (HP-UX)

The method for collecting information is as follows. Submit the information to the Fujitsu technical staff.

Collect information directly by `cp` command.

1. Collect system log files.
Collect all files from the directory below.
 - /var/adm/syslog/syslog.log
 - /var/adm/syslog/OLDsyslog.log (If exists)
2. Collect trace log files.
Collect all files from /var/opt/FJSVssage directory. (including sub-directories)
3. Collecting setting files.
Collect all files from /etc/opt/FJSVssage directory. (including sub-directories)
4. Collect core file, if it exists on the root directory "/".

B.2.8 Collecting information on the Managed Server node (AIX)

The method for collecting information is as follows. Submit the information to the Fujitsu technical staff.

Collect information directly by cp command.

1. Collect trace log files.
Collect all files from /var/opt/FJSVssage directory. (including sub-directories)
2. Collecting setting files.
Collect all files from /etc/opt/FJSVssage directory. (including sub-directories)
3. Collect core file, if it exists on the root directory "/".
4. Collect the files specified as a error log file.
Example: /var/adm/ras/errlog
5. Collect syslog files when you make settings so that syslog messages are displayed.

B.3 Information for further investigation

If it is not possible to determine the cause of the problem in the initial investigation, further detailed information may be needed.

This section explains how to collect required information to resolve the problem.

Data feature

As there is various information required in order to determine the cause of the problem, the size of the data will be greater than that used for the initial investigation.

B.3.1 Collecting information from the Management Server (Solaris OS)

Export the initial investigation information by using the Web Console.

If the export fails or the Web Console cannot be used, collect the information as follows. Submit the information to the Fujitsu technical staff.



Point

.....
In cluster configurations, collect information on both the primary and secondary nodes of the Management Server.
.....

1. Login to the server where you perform the operation.

Perform the operation with OS administrator permissions (root) after login.

2. Execute the fjsnap command or esfsnap command.

Usually, use the fjsnap command. If fjsnap command cannot be executed for some reason, use the esfsnap command.

- fjsnap command

```
# /opt/FJSVsnap/bin/fjsnap -a output
```

Replace the variable *output* with the name of the output medium or specific file name to save the collected information.

- esfsnap command

```
# /opt/FJSVesfcm/bin/esfsnap -dir directory -all
```

Specify the directory to save the information with -dir option (The -dir option cannot be omitted).

B.3.2 Collecting information from the Management Server (Linux)

Export the initial investigation information by using the Web Console.

If the export fails or the Web Console cannot be used, collect the information as follows. Submit the information to the Fujitsu technical staff.

Point

.....
In cluster configurations, collect information on both the primary and secondary nodes of the Management Server.
.....

1. Login to the Management Server with OS administrator permissions (root).

OS administrator permissions are required to collect the information.

2. Execute the fjsnap command and esfsnap command.

Execute both commands. If the fjsnap command cannot be executed for some reason, use only the esfsnap command.

- fjsnap command

```
# /opt/FJSVsnap/bin/fjsnap -a output
```

Replace the variable *output* with the name of the output medium or specific file name to save the collected information.

- esfsnap command

```
# /opt/FJSVesfcm/bin/esfsnap -dir directory -all
```

Specify the directory to save the information with -dir option (The -dir option cannot be omitted).

B.3.3 Collecting information from the Management Server (Windows)

Export the initial investigation information by using the Web Console.

If the export fails or the Web Console cannot be used, collect the information as follows. Submit the information to the Fujitsu technical staff.

1. Login to the Management Server with the user of an Administrators group.

OS administrator permissions are required to collect the information.

2. Execute the esfsnap command. The \$INS_DIR means "Program Directory" specified at the Manager installation.

```
C:\> $INS_DIR\Common\bin\esfsnap -dir directory -all
```


Specify the directory to save the information with `-dir` option (The `-dir` option cannot be omitted).

B.3.4 Collecting information on the Managed Server node (Solaris OS)

The method for collecting information is as follows. Submit the information to the Fujitsu technical staff.

1. Login to the server where you perform the operation.

Perform the operation with OS administrator permissions (root) after login.

2. Execute the `agentsnap` command.

```
# /opt/FJSVssage/sys/agentsnap [-dir directory] -all
```

It is possible to change a directory to save the information by specifying `-dir` option. If the option is omitted, information will be saved in `/tmp`.

B.3.5 Collecting information on the Managed Server node (Windows)

The method for collecting information is as follows. Submit the information to the Fujitsu technical staff.

1. Login to the server node with the user of an Administrators group.

OS administrator permissions are required to collect the information.

2. Execute the `agentsnap` command. The `$INS_DIR` means "Program Directory" specified at the Agent installation.

```
C:\> $INS_DIR\ESC\Agent\sbin\agentsnap -dir directory -all
```

Specify the directory to save the information with `-dir` option (The `-dir` option cannot be omitted).

B.3.6 Collecting information on the Managed Server node (Linux)

The method for collecting information is as follows. Submit the information to the Fujitsu technical staff.

1. Login to the server node with OS administrator permissions (root).

OS administrator permissions are required to collect the information.

2. Execute the `agentsnap` command.

```
# /opt/FJSVssage/sys/agentsnap [-dir directory] -all
```

It is possible to change a directory to save the information by specifying `-dir` option. If the option is omitted, information will be saved in `/tmp`.

B.3.7 Collecting information on the Managed Server node (HP-UX)

Collect the information which is required by Fujitsu technical staff, and submit the file to them.

B.3.8 Collecting information on the Managed Server node (AIX)

Collect the information which is required by Fujitsu technical staff, and submit the file to them.

Appendix C How to check product version

This appendix describes how to check version of installed ETERNUS SF Storage Cruiser.

Point

- ETERNUS SF Storage Cruiser can be operated even if a different version of the agent and manager. Therefore, ETERNUS SF Storage Cruiser to determine the exact use of the environment, you must determine the version of each component.
- How to check version is different for each platform. ETERNUS SF Storage Cruiser check from the platform of the system components are installed, read how to determine the appropriate platform.
- Although the ETERNUS SF Storage Cruiser manager is compatible with some lower version agents, not all ETERNUS SF Storage Cruiser features maybe available.

C.1 To check the product version in Windows operating system

Check the product version according to the procedure shown below.

1. Logon to Windows operating system, ETERNUS SF Storage Cruiser component is installed.
2. Open the window that can add or remove programs.
 - For Windows Server 2003
From the Control Panel, open the [Add or Remove Programs] screen.
 - For Windows Server 2008 or later
From the Control Panel, open the [Programs and Features] screen.
3. Select ETERNUS SF Storage Cruiser component on "Add or Remove Programs" window.
The following is ETERNUS SF Storage Cruiser component and program name.

Component Name	Program Name
Manager	ETERNUS SF Manager
Agent	ETERNUS SF Storage Cruiser Agent

4. A screen is displayed to confirm the version information.
 - For Windows Server 2003
Click "Click here for support information." in step 3.
 - For Windows Server 2008 or later
Continue with step 5.
5. Confirm the version information.
 - For Windows Server 2003
Confirm the version information in "Support information" dialog.
 - For Windows Server 2008 or later
Confirm the version information, displayed in the [Programs and Features] screen.

C.2 To check the product version in Solaris OS

Check the product version according to the procedure shown below.

1. Logon to Solaris OS, ETERNUS SF Storage Cruiser component is installed.
The root(superuser) privileges are not required.
2. Perform the check version according to the command shown below.
 - To check Manager version

```
# pkginfo -l FJSVssmge
```
 - To check agent version

```
# pkginfo -l FJSVssage
```
3. pkginfo command output that results from, VERSION verify information.
ETERNUS SF Storage Cruiser VERSION component information, xx.y.z format (x, y and z are numbers) will be output. Of these, xx.y is part of the specified components and versions.
For example, it is output as 16.0.0.

C.3 To check the product version in Linux

Check the product version according to the procedure shown below.

1. Logon to Linux, ETERNUS SF Storage Cruiser component is installed.
The root(superuser) privileges are not required.
2. Perform the check version according to the command shown below.
 - To check Manager version

```
# rpm -qi FJSVssmge
```
 - To check agent version

```
# rpm -qi FJSVssage
```
3. rpm command output that results from, VERSION verify information.
ETERNUS SF Storage Cruiser VERSION component information, xx.y.z format (x, y and z are numbers) will be output. Of these, xx.y is part of the specified components and versions.
For example, it is output as 16.0.0.

Information

.....
Depending on your version of the product, Version 14.0.0_40I32 may be output and so on. However, if you please 14.x version is part of the decision.
.....

C.4 To check the product version in HP-UX

Check the product version according to the procedure shown below.

In addition, HP-UX running on ETERNUS SF Storage Cruiser is the only component of the agent and explained to the agent.

1. Logon to HP-UX, ETERNUS SF Storage Cruiser component is installed.
The root(superuser) privileges are not required.

2. Perform the check version according to the command shown below.

```
# /usr/sbin/swlist | grep FJSVssage
```

3. The result of command execution, output is as follows.

```
# /usr/sbin/swlist | grep FJSVssage
FJSVssage      13.4.0      ETERNUS SF Storage Cruiser Agent
#
```

Version information is output in the second column. If the value in the second column is 13.4.n (n is an arbitrary number), it is the most up-to-date version.

C.5 To check the product version in AIX

Check the product version according to the procedure shown below.

In addition, AIX running on ETERNUS SF Storage Cruiser is the only component of the agent and explained to the agent.

1. Logon to AIX, ETERNUS SF Storage Cruiser component is installed.
The root(superuser) privileges are not required.
2. Perform the check version according to the command shown below.

```
# /usr/bin/cat /etc/opt/FJSVssage/version.dat
```

3. The result of command execution, output is as follows.

```
# /usr/bin/cat /etc/opt/FJSVssage/version.dat
version=15.1.0
#
```

Version information is output in the form of "x.y.z" (x, y, and z are digit).

Index

[A]

Accounting Application.....	117
Active-Active connection.....	82,91
Active-Standby connection.....	82,91
Active Directory.....	92
Authentication Method using LDAP.....	83

[C]

CIFS.....	82,93
Common Control Repository.....	117
Copy group.....	81,89,96
Copy pair.....	82,90,97

[I]

Information Stack File.....	117
-----------------------------	-----

[K]

Kerberos Authentication Method with Active Directory.....	83
---	----

[L]

LDAP.....	92
-----------	----

[N]

NAS backup volume.....	81
NAS system volume.....	81
NAS volume.....	81
NFS.....	82,93

[P]

Policy File.....	117
------------------	-----

[R]

Report File.....	117
Report Information.....	117

[S]

Single connection.....	82,91
------------------------	-------