



PRIMECLUSTER™

Installation and Administration Guide 4.1

(for Solaris™ Operating Environment)

Edition April, 2003

Preface

This manual serves as your starting point for using PRIMECLUSTER. It explains the workflow of the series of operations from installation to operation management of the PRIMECLUSTER system. Since the PRIMECLUSTER system comprises multiple features, there are several other manuals beside this one for each feature. However, by reading this manual first, you will be able to perform the series of operations because this manual refers readers to other manuals that contain feature-specific information that is necessary for the operations.

This manual also provides a functional overview of products that are supported by the PRIMECLUSTER system and describes operation procedures.

This manual only covers the basic operation of PRIMECLUSTER. For operations using different hardware and software configurations, see "Related Documentation".

The table below shows the operation flow from PRIMECLUSTER installation to the start of operation management and indicates the reference location in this manual for each operation.

Flow from PRIMECLUSTER system installation to operation management

PRIMECLUSTER system operation flow	Reference location in this manual
1. Understanding the flow of PRIMECLUSTER system building and designing the PRIMECLUSTER system	Part 1 Planning
2. Installing the PRIMECLUSTER system	Part 2 Installation
3. Monitoring the operation status of the PRIMECLUSTER system	Part 3 Operations
4. Changing the PRIMECLUSTER system configuration after system operation has been started	Part 4 System Configuration Modifications
5. Backing up and restoring the operation environment of the PRIMECLUSTER system	Part 5 Maintenance
6. Installing products for the PRIMECLUSTER system	Part 6 PRIMECLUSTER Products

For detailed procedural explanations, refer to the reference manuals that are indicated in the target location of each part.

◆ Target Readers

This manual is intended for all users who use PRIMECLUSTER 4.1 and perform cluster system installation and operation management. It is also intended for programmers who develop applications that operate on PRIMECLUSTER.

◆ Configuration of This Documentation

This manual consists of five parts, appendixes, and a glossary. The contents of each part are described below.

Part 1 Planning

Audience: System administrators who build PRIMECLUSTER systems

Contents: This part describes the overall workflow from installation to operation of the PRIMECLUSTER system.

Part 2 Installation

Audience: System administrators who build PRIMECLUSTER systems

Contents: This part describes operations for software installation, cluster building, and application building.

Part 3 Operations

Audience: System administrators who manage system operations.

Contents: This part describes operation methods for operations such as monitoring the PRIMECLUSTER system and investigating failure causes.

Part 4 System Configuration Modifications

Audience: System administrators who build PRIMECLUSTER systems

Contents: This part describes necessary work items for additions, modifications, and deletions to the PRIMECLUSTER system configuration.

Part 5 Maintenance

Audience: System administrators who build PRIMECLUSTER systems

Contents: This part describes the necessary work items for maintaining the operation environment of the PRIMECLUSTER system.

Part 6 PRIMECLUSTER Products

Audience: Users who operate PRIMECLUSTER products on PRIMECLUSTER systems

Contents: This part describes the versions and levels of products that are supported by the PRIMECLUSTER system and provides a functional overview of those products.

Appendix A PRIMECLUSTER System Design Worksheets

Audience: Users who design PRIMECLUSTER systems

Contents: This appendix contains the PRIMECLUSTER System Design Worksheet.

Appendix B Manual Pages

Audience: All users who use PRIMECLUSTER systems

Contents: This appendix describes the online manual pages that are used by the individual features of the PRIMECLUSTER system.

Appendix C Troubleshooting

Audience: All users who use PRIMECLUSTER systems

Contents: This appendix describes corrective actions for problems that may occur in the PRIMECLUSTER system. It also explains how to collect data when requesting a problem investigation.

Appendix D Messages

Audience: All users who use PRIMECLUSTER systems

Contents: This appendix describes the contents and actions for messages output by the userApplication Configuration Wizard GUI and messages output by procedure resources in PRIMECLUSTER systems. For other messages, this manual indicates the reference locations in other manuals.

Appendix E Using SynfinityCluster Products in PRIMECLUSTER

Audience: All users who used the SynfinityCluster system

Contents: This appendix describes feature differences and terminology differences between SynfinityCluster and PRIMECLUSTER.

Appendix F Registering, Changing, and Deleting State Transition Procedure Resources for SynfinityCluster Compatibility

Audience: All users who use SynfinityCluster-compatible resources

Contents: This appendix describes procedures for registering, changing, and deleting procedure resources when the cluster applications use procedure resources.

Appendix G Registering SynfinityCluster-compatible Resources

Audience: All users who use SynfinityCluster-compatible resources

Contents: This appendix describes the procedure for registering SynfinityCluster-compatible resources.

Appendix H Supplemental Information

Audience: All users who use PRIMECLUSTER systems
Contents: This appendix describes the feature supplied with the Supplement CD of the PRIMECLUSTER product.

Glossary

Audience: All users who use PRIMECLUSTER systems

Contents: This section explains terms used to describe the PRIMECLUSTER system.
Abbreviations

Audience: All users who use PRIMECLUSTER systems

Contents: This section explains abbreviations of the PRIMECLUSTER system.

◆ Related Documentation

Refer to the following manuals as necessary when setting up the cluster:

- *PRIMECLUSTER Concepts Guide*
- *PRIMECLUSTER Cluster Foundation Configuration and Administration Guide*
- *PRIMECLUSTER RMS Configuration and Administration Guide*
- *PRIMECLUSTER Global Disk Services Configuration and Administration Guide*
- *PRIMECLUSTER Global File Services Configuration and Administration Guide*
- *PRIMECLUSTER Global Link Services Configuration and Administration Guide: Redundant Line Control Function*
- *PRIMECLUSTER Global Link Services Configuration and Administration Guide: Multipath Function*
- *PRIMECLUSTER Web-Based Admin View Operation Guide*
- *PRIMECLUSTER Scalable Internet Services (SIS) Configuration and Administration Guide*
- *RC2000 User's Guide*

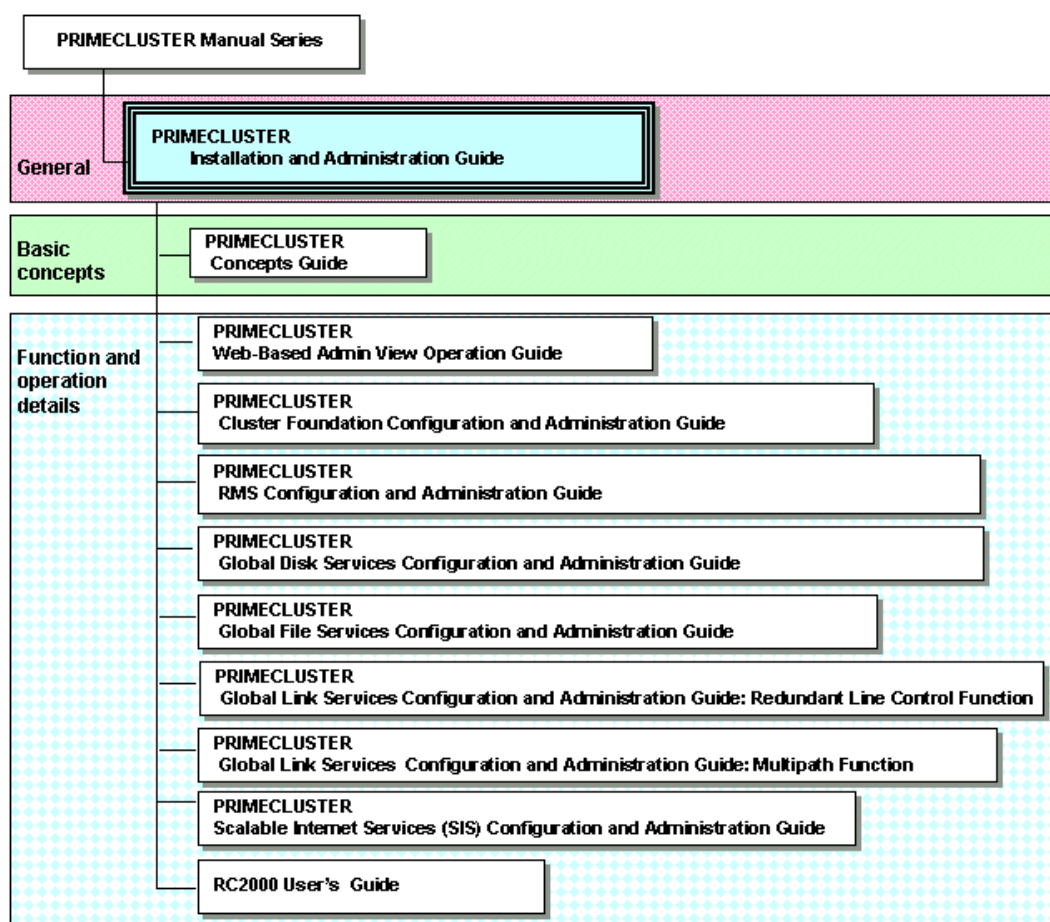


Note

The PRIMECLUSTER documentations include the following documentation in addition to those listed above:

- *PRIMECLUSTER Installation Guide*
This printed installation guide is included with each PRIMECLUSTER product.

◆ Manual Series



◆ Manual Printing

If you want to print a manual, use the PDF file found on the CD-ROM for the PRIMECLUSTER product. The correspondences between the PDF file names and manuals are described in the PRIMECLUSTER Installation Guide that comes with the product.

You will need Adobe Acrobat Reader to read and print the PDF file. Use Adobe Acrobat Reader Version 4.0 or higher.

◆ Online Manuals

To allow users to view the online manuals, use the Cluster management server to register each user name to one of the user groups (wvroot, clroot, cladmin, or clmon).

For information on user group registration procedures and user group definitions, see 4.1.1 "Assigning Users to Manage the Cluster."

◆ Conventions

Notation

Prompts

Command line examples that require system administrator (or root) rights to execute are preceded by the system administrator prompt, the hash sign (#). Entries that do not require system administrator rights are preceded by a dollar sign (\$).

Manual page section numbers

References to the UNIX operating system commands are followed by their manual page section numbers in parentheses – for example, cp(1)

The keyboard

Keystrokes that represent nonprintable characters are displayed as key icons such as [Enter] or [F1]. For example, [Enter] means press the key labeled Enter; [Ctrl-b] means hold down the key labeled Ctrl or Control and then press the [B] key.

Typefaces

The following typefaces highlight specific elements in this manual.

Typeface	Usage
Constant Width	Computer output and program listings; commands, file names, manual page names and other literal programming elements in the main body of text.
<i>Italic</i>	Variables that you must replace with an actual value.
Bold	Items in a command line that you must type exactly as shown.

Example 1

Several entries from an /etc/passwd file are shown below:

```
root:x:0:1:0000-Admin(0000):/:  
sysadm:x:0:0:System Admin.:/usr/admin:/usr/sbin/sysadm  
setup:x:0:0:System Setup:/usr/admin:/usr/sbin/setup  
daemon:x:1:1:0000-Admin(0000):/:
```







Example 2

To use the cat(1) command to display the contents of a file, enter the following command line:

```
$ cat file
```

Notation symbols

Material of particular interest is preceded by the following symbols in this manual:

-  ● **Point** Contains important information about the subject at hand.
-  ● **Note** Describes an item to be noted.
-  ● **Example** Describes operation using an example.
-  ● **Information** Describes reference information.
-  ● **See** Provides the names of manuals to be referenced.
-  ● **Conclusion** Summarizes the contents described in the parts and chapters.

Abbreviations

- Microsoft(R) Windows(R) 98 operating system and Microsoft(R) Windows(R) 98 Second Edition operating system are abbreviated as Windows(R) 98.
- Microsoft(R) Windows NT(R) Server operating system Version 4.0, and Microsoft(R) Windows NT(R) Server Workstation System Version 4.0 are abbreviated as Windows NT(R).
- Microsoft(R) Windows(R) 2000 operating system is abbreviated as Windows(R) 2000.

-
- Microsoft(R) Windows(R) Millennium Edition is abbreviated as Windows(R) Me.
 - Microsoft(R) Windows(R) XP operating system is abbreviated as Windows(R) XP.
 - Windows(R) 98, Windows NT(R), Windows(R) 2000, Windows(R) Me, and Windows(R) XP are generically referred to as Microsoft(R) Windows.
 - If "Solaris X" is indicated in the reference manual name of the Solaris(TM) operating environment (Solaris OE) manual, replace "Solaris X" with "Solaris 8 operating environment (Solaris 8 OE)" or the "Solaris 9 operating environment (Solaris 9 OE)".

April 2003

◆ Trademarks

UNIX is a registered trademark of Open Group in the United States and other countries.

Sun, Sun Microsystems, Sun logos, Solaris, and all trademarks and logos related to Solaris are trademarks or registered trademarks of Sun Microsystems, Inc. in the United States and other countries. A license from Sun Microsystems, Inc. has been received for using these trademarks and registered trademarks.

NFS and NFS Client are trademarks of Sun Microsystems, Inc.

Java and all Java-related products and logos are trademarks or registered trademarks of Sun Microsystems, Inc. in the United States and other countries.

Netscape and Netscape Navigator are trademarks or registered trademarks of Netscape Communications Corporation in the United States and other countries.

Microsoft Internet Explorer is a registered trademark of Microsoft Corporation in the United States and other countries.

Microsoft, Windows, Windows NT, and Windows NT Server are registered trademarks of Microsoft Corporation in the United States and other countries.

ORACLE and Oracle Applications are trademarks or registered trademarks of Oracle Corporation.

CORBA, OMG, and ORB are registered trademarks of Object Management Group (OMG).

NetWorker is a registered trademark of Legato Systems, Inc.

Symfoware is a registered trademark of Fujitsu Limited.

PRIMECLUSTER is a trademark of Fujitsu Limited.

Other product names are product names, trademarks, or registered trademarks of these companies.

Copyright (c) 1986-1997 Sun Microsystems, Inc.

Copyright (c) 1983-1989 Portions may be derived from Berkeley BSD system, licensed from the University of California.

(C) 1990-2000 Legato Systems, Inc. All Rights Reserved.

Requests

- No part of this documentation may be reproduced or copied without permission of FUJITSU LIMITED.
- The contents of this documentation may be revised without prior notice.

Copyright(C) 2003 Fujitsu LIMITED.

All Rights Reserved.

Copyright (C) 2003 Fujitsu Siemens Computers GmbH.

All Rights Reserved.

Contents

Part 1	Planning	1
Chapter 1	Build Flow	3
1.1	Planning.....	4
1.2	Installation.....	5
1.3	Development.....	8
1.4	Test	9
1.5	Operation and Maintenance	13
1.6	Operation Mode Change	14
Chapter 2	Site Preparation	15
2.1	PRIMECLUSTER Product Selection	16
2.1.1	PRIMECLUSTER Product Selection	16
2.1.2	PRIMECLUSTER Function Selection.....	17
2.2	System Design.....	18
2.3	Determining the Cluster System Operation Mode	19
2.3.1	Standby Operation.....	19
2.4	Determining the Web-Based Admin View Operation Mode.....	25
2.5	Setting the Failover Range of a Cluster Application	29
Part 2	Installation	31
Chapter 3	Software Installation	33
3.1	PRIMECLUSTER Installation	34
3.2	Installation and Setup of Related Software	35
3.2.1	Setting Up the Network.....	36
3.2.2	Setting Up Disk Units.....	36
3.2.3	Checking the Kernel Parameters.....	38
3.3	Installation and Environment Setup of Applications.....	39
Chapter 4	Starting the Web-Based Admin View Screen	41
4.1	Preparations for Starting the Web-Based Admin View Screen.....	42
4.1.1	Assigning Users to Manage the Cluster	42
4.1.2	Preparing the Client Environment.....	43
4.1.3	Initial Setup of Web-Based Admin View	45
4.1.4	Setting Up the Browser	47
4.1.5	Setting Up the Java Plug-in	47
4.2	Starting the Web-Based Admin View Screen.....	48

4.3	Web-Based Admin View Screen	50
4.3.1	Operation Menu Functions	50
4.3.2	Global Cluster Services Menu Functions	53
4.3.3	Cluster Admin Functions.....	54
4.3.4	userApplication Configuration Wizard Functions.....	55
4.4	Exiting the Screen	57
Chapter 5 Building a Cluster.....		59
5.1	Preparations	61
5.1.1	Checking the Cluster Worksheet.....	61
5.1.2	Preparations for Starting the Web-Based Admin View Screen	61
5.1.3	Setting Up the Operating System Console.....	61
5.2	Initial Cluster Setup	63
5.2.1	Setting Up CF and CIP	63
5.2.2	Setting Up the Shutdown Facility.....	65
5.2.3	Initial Setup of the Cluster Resource Management Facility	68
5.3	Setting Up Power Supply Linkage.....	76
5.4	Setting Up Shared Disk Connection Confirmation	77
5.5	Setting Up Fault Resource Identification and Operator Intervention Request.....	79
Chapter 6 Building Cluster Applications		81
6.1	Initial GLS Setup.....	83
6.1.1	GLS Setup.....	83
6.1.2	Setting Up Web-Based Admin View When GLS Is Used.....	85
6.2	Initial GDS Setup	86
6.2.1	Automatic Configuration of Shared Disks.....	86
6.2.2	GDS Configuration Setup	86
6.3	Initial GFS Setup	98
6.4	Setting Up the Application Environment.....	100
6.5	Setting Up Online/Offline Scripts.....	101
6.6	Setting Up Cluster Applications.....	104
6.6.1	Setting Up Resources.....	106
6.6.2	Creating Cluster Applications	166
6.6.3	Setting Up Dependency Relationships Between Cluster Applications	171
6.6.4	Editing global settings in Configuration	176
6.6.5	Attributes.....	179
6.6.6	Changing the RMS Configuration Name	182
6.7	Setting Up Patrol Diagnosis	183
Part 3 Operations		187
Chapter 7 Operations		189

7.1	Viewing the PRIMECLUSTER System Operation Management Screens.....	190
7.1.1	CF Main Window.....	190
7.1.2	CRM Main Window.....	191
7.1.3	RMS Main Window.....	197
7.2	Operating the PRIMECLUSTER System.....	202
7.2.1	RMS Operation.....	202
7.2.2	Cluster Application Operations.....	203
7.3	Monitoring the PRIMECLUSTER System.....	205
7.3.1	Monitoring the State of a Node.....	205
7.3.2	Monitoring the State of a Cluster Application.....	205
7.3.3	Concurrent Viewing of Node and Cluster Application States.....	206
7.3.4	Viewing Logs Created by the PRIMECLUSTER System.....	207
7.3.5	Viewing Detailed Resource Information.....	209
7.3.6	Displaying environment variables.....	210
7.3.7	Monitoring Cluster Control Messages.....	211
7.4	Corrective Actions for Resource Failures.....	212
7.4.1	Corrective Action when the resource state is Faulted.....	212
7.4.2	Corrective Action when Patrol Diagnosis Detects a Fault.....	214
Part 4	System Configuration Modification.....	217
Chapter 8	Changing the Operation Configuration.....	219
8.1	Changing the Cluster Configuration.....	220
8.1.1	Changing the Cluster Application Configuration.....	220
8.1.2	Changing the Operation Attributes of a Cluster Application.....	221
8.1.3	Changing Resources.....	224
8.2	Changing an IP Address on the Public LAN.....	235
8.3	Changing a CIP Address.....	238
8.4	Changing Settings for the Shared Device Connection Confirmation Feature.....	239
8.5	Changing the Operation Environment for Patrol Diagnosis.....	240
8.6	Changing a Node Name.....	241
8.7	Changing the Operation Attributes of a userApplication.....	242
8.7.1	Operation Attribute Types.....	242
8.7.2	Changing Environment Variables.....	243
8.8	Changing PRIMECLUSTER Operation Attributes.....	244
8.9	Deleting a Cluster Application.....	245
8.9.1	Deleting a userApplication.....	245
8.9.2	Deleting a Resource.....	246
8.9.3	Supplement on Cluster Application and Resource Deletion.....	248
Chapter 9	Expanding the Operation Configuration.....	253
9.1	Adding a Node.....	254

9.1.1	Setting Up a New Node	255
9.1.2	Preparing the Existing Nodes	255
9.1.3	Connecting a Node	256
9.1.4	Setting Up Web-Based Admin View	257
9.1.5	Setting Up CF and SF	257
9.1.6	Setting Up CRM (Resource Database)	258
9.1.7	Setting Up RMS	260
9.1.8	GFS Shared Settings	262
9.2	Recovering the Original Cluster Configuration at Node Expansion	263
Part 5 Maintenance		265
Chapter 10 Backing Up and Restoring a PRIMECLUSTER System		267
10.1	Backing Up the PRIMECLUSTER Operation Environment	269
10.2	Restoring the PRIMECLUSTER Operation Environment	270
10.3	Environment Setup File	272
Part 6 PRIMECLUSTER Products.....		275
Chapter 11 PRIMECLUSTER Product List.....		277
11.1	What Are the PRIMECLUSTER Operation Modes?	278
Chapter 12 PRIMECLUSTER Wizard for NetWorker		281
12.1	Functional Overview	282
12.1.1	Client Cluster	282
12.1.2	Storage Node Cluster	284
12.1.3	Server Cluster	285
12.1.4	Suspending NetWorker Monitoring.....	288
12.1.5	Standby Operation	288
12.2	Operation Environment.....	289
12.2.1	System Configuration	289
12.2.2	Supported Modes.....	291
12.2.3	Overview of Cluster System Support.....	291
12.3	Notes	292
Chapter 13 PRIMECLUSTER Wizard for Oracle.....		293
13.1	Functional Overview	294
13.2	Operation Environment.....	295
13.2.1	System Configuration	295
13.2.2	Supported Modes.....	296

13.2.3	Overview of Cluster System Support.....	296
13.3	Notes	297
Chapter 14	Interstage Application Server Enterprise Edition	299
14.1	Functional Overview	300
14.1.1	Overview of Cluster System Support.....	300
14.1.2	Supported Modes.....	300
14.2	Registering a SynfinityCluster-compatible State Transition Procedure	301
14.2.1	Setting Resource Information	301
14.2.2	Setting State Transition Instruction Timings	301
14.2.3	Registering a State Transition Procedure to a userApplication.....	301
Chapter 15	Softek AdvancedCopy Manager.....	305
15.1	Functional Overview	306
15.1.1	Overview of Cluster System Support.....	306
15.1.2	Supported Modes.....	306
15.2	Standby Classes.....	307
15.2.1	System Configuration	307
15.2.2	Setting Up the Environment.....	308
Chapter 16	Symfaware Server Hot-Standby Option.....	309
16.1	Functional Overview	310
16.1.1	Overview of Cluster System Support.....	310
16.1.2	Supported Modes.....	310
16.2	Standby Classes.....	311
16.2.1	System Configuration	311
16.2.2	Design and Development	311
16.2.3	Setting Up the Environment.....	311
16.2.4	Operation	312
16.2.5	Operation at Startup.....	312
16.2.6	Operation at Shutdown	312
16.2.7	Operation at Switchover	312
16.2.8	Performance	312
Chapter 17	Symfaware (Standby).....	313
17.1	Hot Standby Operation and Environment Setup Procedure.....	314
17.2	Preparation Prior to Environment Setup	315
17.3	Setting Up Symfaware and the Cluster System Environment	316
17.3.1	Creating Raw Devices	316
17.3.2	Editing RDB Configuration Parameter Files	316
17.3.3	Editing Operation Environment Files.....	317

17.3.4	Setting Up Environment Variables	318
17.3.5	Activating Gds Resources	318
17.3.6	Creating the RDB Environment	320
17.3.7	Declaring Hot Standby	322
17.3.8	Deactivating Gds Resources	322
17.3.9	Registering RDB Resources	323
17.3.10	Creating a Cluster Application	325
17.3.11	Setting Up Exclusive Relationships Between Cluster Applications.....	336
17.3.12	Starting a Cluster Application	338
17.3.13	Checking the Operation	339
17.4	Failover Maintenance and Management.....	340
17.4.1	Changing System Files.....	340
17.4.2	Changing to Scalable Log Operation.....	353
17.4.3	Changing the Scalable Log Environment	354
Chapter 18	Systemwalker CentricMGR.....	357
18.1	Functional Overview	358
18.1.1	Overview of Cluster System Support.....	359
18.1.2	Supported Modes.....	359
18.2	Standby class	360
18.2.1	System Configuration	360
18.2.2	Environment Setup	361
Chapter 19	Systemwalker OperationMGR	363
19.1	Functional Overview	364
19.1.1	Overview of Cluster System Support.....	365
19.1.2	Supported Modes.....	365
19.2	Standby Classes.....	366
19.2.1	System Configuration	366
19.2.2	Environment Setup	368
Chapter 20	Systemwalker WebMGR.....	369
20.1	Functional Overview	370
20.1.1	Overview of Cluster System Support.....	370
20.1.2	Supported Modes.....	370
20.1.3	Notes.....	370
20.2	Standby Classes.....	371
20.2.1	System Configuration	371
20.2.2	Notes.....	371
Appendix A	PRIMECLUSTER System Design Worksheets	373

A.1	Worksheet Purpose	373
A.2	Notes on Worksheet Creation	374
A.3	Overall Design Worksheet.....	374
A.4	CE(FE for North America) Instruction Worksheet	376
A.5	Cluster Installation Environment Worksheet	380
A.6	Kernel Parameter Worksheet	381
A.6.1	CF Configuration	382
A.6.2	RMS Configuration.....	383
A.6.3	Using GFS	384
A.6.4	Using GLS	384
A.7	Cluster Configuration Worksheet	384
A.8	Cluster Application Configuration Worksheets.....	386
A.8.1	GFS Local File System Setup Worksheet.....	386
A.8.2	GLS Configuration Worksheet	387
A.9	GDS Setup Worksheets	390
A.9.1	System Disk Mirror Setup Worksheet.....	390
A.9.2	Shared Disk Setup Worksheet.....	391
A.10	Cluster Application Worksheets	395
A.10.1	Cmdline Resource Worksheet	395
A.10.2	Fsystem Resource Worksheet.....	397
A.10.3	Gds Resource Worksheet.....	398
A.10.4	Gls Resource Worksheet	399
A.10.5	Takeover Network Resource Worksheet.....	400
A.10.6	Procedure Resource Worksheet.....	401
A.10.7	Process Monitoring Resource Worksheet.....	402
A.10.8	Line Switching Unit Resource Worksheet.....	403
A.10.9	Cluster Application Worksheet.....	404
A.10.10	Cluster Application Exclusion Worksheet.....	405
A.10.11	Configuration Global Settings Worksheet.....	406
A.11	System Design Examples	407
A.11.1	Cluster Building Worksheet.....	409
A.11.2	GFS Local File System Setup Worksheet.....	411
A.11.3	GLS Setup Worksheet.....	411
A.11.4	System Disk Mirror Setup Worksheet	412
A.11.5	GDS Configuration Worksheet.....	412
Appendix B Manual Pages		419
B.1	CCBR.....	419
B.2	CF	419
B.3	CIP	419
B.4	Operator Intervention.....	420
B.5	PAS	420
B.6	Cluster Resource Management Facility	420

B.7	RMS	421
B.8	Shutdown Facility (SF)	421
B.9	Monitoring Agent (MA)	421
B.10	SIS	422
B.11	Tracing Failed Resource	422
B.12	Web-Based Admin View	422
B.13	Procedure Resource	422
B.14	Process Monitoring Feature	422
B.15	RMS Wizards	423
Appendix C Troubleshooting		425
C.1	Collecting Troubleshooting Information	425
C.1.1	Executing the fjsnap Command	425
C.1.2	System dump	426
C.1.3	SCF Dump	426
C.2	Troubleshooting	427
C.2.1	GUI in General	427
C.3	Detecting a Failed Resource	427
C.3.1	Failed Resource Message	428
C.3.2	Resource Fault History	429
C.3.3	Fault Resource List	431
Appendix D Messages		433
D.1	Messages Related to CF	433
D.2	Messages Related to RMS	436
D.3	Messages Related to CRM View	439
D.4	Messages Related to Line Switching Unit	439
D.4.1	Warning Message	439
D.4.2	Error Messages	440
D.5	Failed Resource and Operator Intervention Messages (GUI)	446
D.5.1	Information Messages	446
D.5.2	Error Messages	446
D.6	Failed Resource and Operator Intervention Messages (CLI)	448
D.6.1	Operator Intervention Messages	448
D.6.2	Information Messages	450
D.6.3	Error Messages	451
D.7	Shared Disk Connection Confirmation Messages	454
D.7.1	Information Message	455
D.7.2	Error Messages	455
D.8	Patrol Diagnosis Messages	456
D.8.1	Information Messages	456
D.8.2	Error Messages	457

D.9	userApplication Configuration Wizard GUI Messages	458
D.9.1	Information messages.....	459
D.9.2	Warning Messages	460
D.9.3	Error messages.....	463
D.9.4	Messages of the wgcncfclient Command.....	465
D.10	Procedure Resource Messages	466
D.10.1	Error Messages.....	466
D.11	Process Monitoring Messages	469
 Appendix E Using SynfinityCluster Products in PRIMECLUSTER		473
E.1	Terminology	473
E.2	Manual Series.....	474
E.3	Building Procedure	475
E.3.1	Software Installation	475
E.3.2	Initial Cluster Setup	475
E.3.3	Application Setup	476
E.3.4	Operations	477
 Appendix F Registering, Changing, and Deleting State Transition Procedure Resources for SynfinityCluster Compatibility		479
F.1	Registering a Procedure Resource	479
F.2	Changing a Procedure Resource	480
F.3	Deleting a Procedure Resource	481
 Appendix G Registering SynfinityCluster-compatible Resources		483
G.1	Registering a Cluster Service.....	483
G.2	Associating Resources to a Cluster Service Instance	485
G.3	Deleting a Cluster Service.....	488
 Appendix H Supplemental Information		491
H.1	Setting Up the Resource Database from the CRM Main Window	491
H.2	Setting Up the SF Configuration.....	491
H.2.1	SF Preparations	491
H.2.2	SF Configuration Files	492
H.3	Setting Up the Alternate Keyboard Abort Sequence.....	492
H.4	SCF Dump	492
H.5	Cluster Resource Management Facility Messages.....	493
H.5.1	GUI (Cluster Resource Management Facility).....	493
H.5.2	Error Messages.....	495
H.6	Monitoring Agent Messages.....	498
H.6.1	Information Messages	498

H.6.2	Warning Messages	499
H.6.3	Error Messages.....	499
H.7	Setting Up the Shutdown Facility	501
H.7.1	Starting Configuration Wizard.....	502
H.7.2	Simple configuration (recommended).....	503
H.7.3	Detailed configuration	509
Glossary		519
Abbreviations.....		545
Index		549

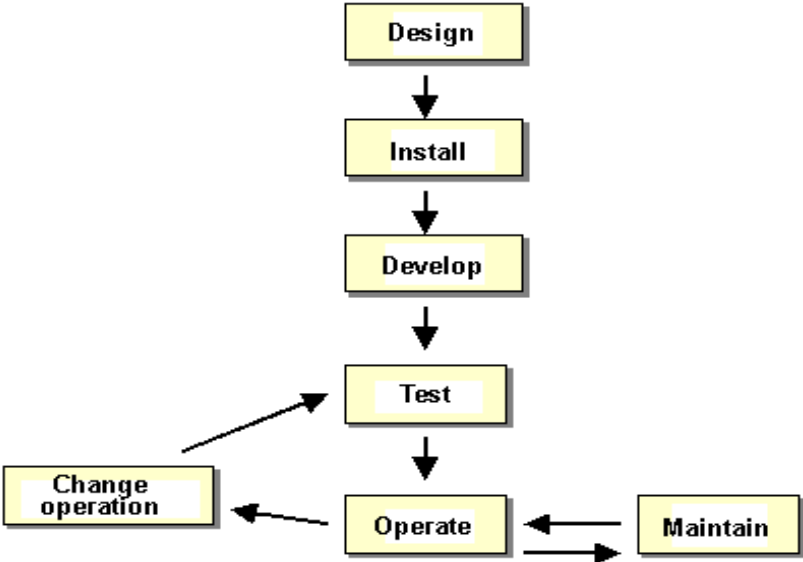
Part 1 Planning

Part 1 describes the workflow from PRIMECLUSTER design to installation and operation management. Users who are installing a PRIMECLUSTER system for the first time need to read this part.

Chapter 1 Build Flow

This chapter describes the workflow for building a PRIMECLUSTER system. To build a PRIMECLUSTER system, follow the procedure described below.

Flow of building a PRIMECLUSTER system



1.1 Planning

Before building a PRIMECLUSTER system, you must first design the system.

■ Designing a PRIMECLUSTER system

1. Select the PRIMECLUSTER products.

Select the PRIMECLUSTER products required for the system you want to build.

For details, see 2.1 "PRIMECLUSTER Product Selection".

2. Design the system.

Determine the operation environment for building the PRIMECLUSTER system. This includes selecting the applications to be used and determining the required hardware resources, such as the number of hosts, networks, and disk size.

For details, see 2.2 "System Design".

3. Determine the cluster system operation mode.

Determine the number of nodes and the operation mode of the cluster system.

For details, see 2.3 "Determining the Cluster System Operation Mode".

4. Determine the operation mode for using Web-Based Admin View.

Determine the operation mode for running Web-Based Admin View. Web-Based Admin View can manage up to 16 nodes.

For details, see 2.4 "Determining the Web-Based Admin View Operation Mode".



Note

In multi-node (3 or more nodes) operation, the 3-tier model, in which the cluster management server is installed separately, is recommended.

5. Determine the cluster applications.

Determine the number of cluster applications. Also determine which nodes are to be used for each application.

6. Determine the resources required for each cluster application.

Determine the resources required for each cluster application.

— Determine the switchover network type (IP address takeover, MAC address takeover, or node name takeover) and the takeover address.

— Determine whether a user-defined RMS configuration script is to be used. Determine whether there are other items (for example, line switching units) to be used as resources.

— Determine the cluster interconnect paths and quantity. Two or more cluster interconnects are recommended.

— For a disk device, determine which nodes will be sharing the device, whether the device is to be used as a RAW device (database system), whether the device is to be used as a file system (general files), and whether the device is to be grouped.

7. Determine the failover range of the cluster application.

Determine the trigger for cluster application failover.

For details, see 2.5 "Setting the Failover Range of a Cluster Application."



See

For details on designing the system, see Chapter 2 "Site Preparation".

1.2 Installation

After completing the design of the PRIMECLUSTER system and determining the configuration of the PRIMECLUSTER system to be built, install the PRIMECLUSTER system.

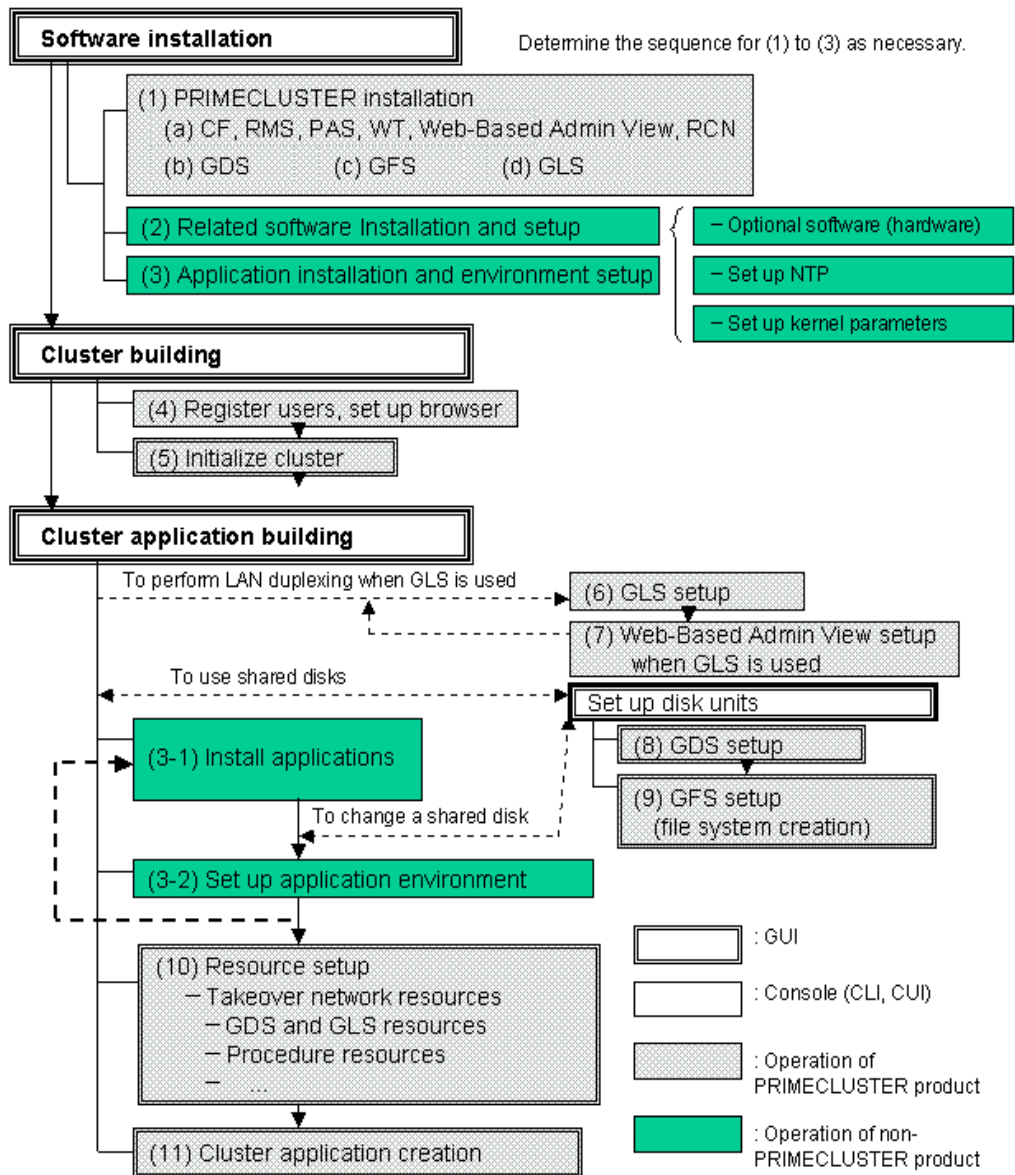
Since the work will be performed based on the PRIMECLUSTER system design worksheet that was created, check that all items on the design worksheet have been entered.

Install the PRIMECLUSTER system by performing the following procedure in sequence from (1). Perform the operations described in the dotted line sections if the system design matches the described conditions.

If you are installing applications after you install the PRIMECLUSTER system, go back to the operations from the Application environment setup to the Application installation.

The screens to be used differ according to the operation. The work procedures to be performed with GUI from Web-Based Admin View and the work procedures to be performed with CLI and CUI from console screens are shown in separate boxes.

Flow of PRIMECLUSTER system installation



The abbreviations in the flowchart for PRIMECLUSTER system installation are explained below.

- CF: Cluster Foundation
- RMS: Reliant Monitor Services
- PAS: Parallel Application Services
- WT: Wizard Tools
- RCN: RC2000
- GDS: Global Disk Services
- GFS: Global File Services
- GLS: Global Link Services

For detailed information on each item, refer as necessary to the corresponding manual reference section mentioned in the table below.

Installation procedure and manual reference sections

Work items	Manual reference section	Required/ optional
System design	Chapter 2 "Site Preparation"	Required
Software installation		
(1) PRIMECLUSTER installation	3.1 "PRIMECLUSTER Installation"	Required
(2) Related software Installation and setup	3.2 "Installation and Setup of Related Software"	Optional
(3) Application installation and environment setup	3.3 "Installation and Environment Setup of Applications"	Optional
Cluster building		
(4) User registration/browser setup	5.1 "Preparations"	Required
(5) Initial cluster setup	5.2 "Initial Cluster Setup"	Required
Cluster application building		
(6) GLS setup	6.1 "Initial GLS Setup"	Optional
(7) Web-Based Admin View setup when GLS is used		(required to use GLS)
(8) GDS setup	6.2 "Initial GDS Setup"	Optional
		(required to use GDS)
(9) GFS setup (file system creation)	6.3 "Initial GFS Setup"	Optional
		(required to use GFS)
(10) Resource setup	6.6.1 "Setting Up Resources"	Optional
(11) Cluster application creation	6.6 "Setting Up Cluster Applications"	Required

1.3 Development

To configure a user application to be monitored by PRIMECLUSTER, you need to create an RMS configuration script.

- Online script
This script executes a process that sets the resources to Online or Standby.
- Offline script
This script executes a process that sets the resources to Offline.



[See](#)

For details on the online/offline script settings, see 6.5 "Setting Up Online/Offline Scripts."

1.4 Test

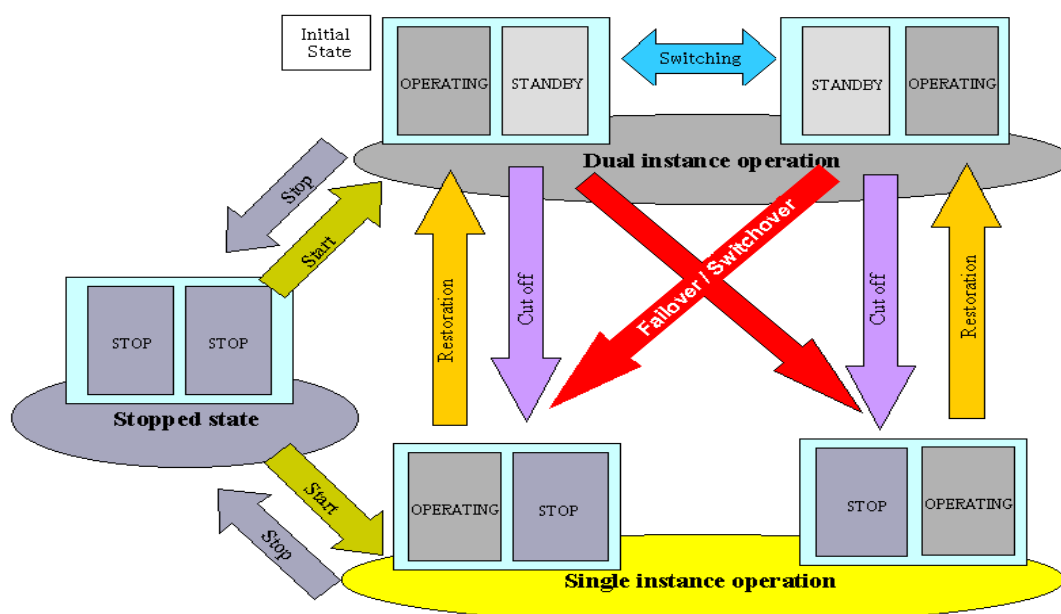
■ Purpose

When you build a cluster system using PRIMECLUSTER, you need to confirm before starting production operations that the entire system will operate normally and cluster applications will continue to run in the event of failures.

For 1:1 standby operation, the PRIMECLUSTER system takes an operation mode like the one shown in the figure below.

The PRIMECLUSTER system switches to different operation modes according to the state transitions shown in the figure below. To check that the system operates normally, you must test all operation modes and each state transition that switches to an operation mode.

State transitions of the PRIMECLUSTER system



◆ PRIMECLUSTER System State

	Description
Dual instance operation	A cluster application is running, and it can switch to the other instance in the event of a failure (failover). Two types of the dual instance operation are OPERATING and STANDBY. Even if an error occurs while the system is operating, the standby system takes over ongoing operations as an operating system. This operation ensures the availability of the cluster application even after failover.
Single instance operation	A cluster application is running, but failover is disabled. Two types of the single instance operation are OPERATING and STOP. Since the standby system is not supported in this operation, a cluster application cannot switch to other instance in the event of a failure. So, ongoing operations are disrupted.
Stopped state	A cluster application is stopped.

The above-mentioned "OPERATING", "STANDBY", and "STOP" are defined by the state of RMS and cluster application as follows;

	RMS state	Cluster application state	Remark
OPERATING	Operating	Online	
STANDBY	Operating	Offline or Standby	
STOP	Stopped	Unknown *	Sysnode is Offline

* RMS determines the cluster application state. When RMS is stopped, the cluster application state is unknown.

■ Main tests for PRIMECLUSTER system operation

◆ Startup test

Conduct a startup test and confirm the following:

- View the Cluster Admin screen of Web-Based Admin View, and check that the cluster system starts as designed when the startup operation is executed.
- If an RMS configuration script was created, check that the commands written in the script are executed properly as follows.
 - For a command that outputs a message when it is executed, check that a message indicating that the command was executed properly is displayed on the console.
 - Check that the command has been executed properly by executing the “ps(1)” command.
- A new cluster application is not started automatically during the PRIMECLUSTER system startup. To start the cluster application automatically, you must set "AutoStartUp" for that cluster application. The AutoStartUp setting must be specified as a userApplication attribute when the application is created. For details, see 6.6.2 "Creating Cluster Applications."

◆ Clear fault

If a failure occurs in a cluster application, the state of that application changes to Faulted. To build and run this application in a cluster system again, you need to execute "Clear Fault" and clear the Fault state.

Conduct a clear-fault test and confirm the following:

- Check that the Faulted state of a failed application can be cleared without disrupting ongoing operations.
- If an RMS configuration script was created, check that the commands written in the script are executed properly as follows.
 - For a command that outputs a message when it is executed, check that a message indicating that the command was executed properly is displayed on the console.
 - Check that the command has been executed properly by executing the “ps(1)” command.

◆ Switchover

Conduct a failover or switchover test and confirm the following:

- Check that failover is triggered by the following event:
 - When an application failure occurs
- Check that switchover is triggered by the following events:
 - When the OPERATING node is shut down
 - When an application is terminated by the exit operation
 - When an OPERATING cluster application is stopped
- Check that failover or switchover is normally done for the followings:
 - Disk switchover
 - Check that the disk can be accessed from the OPERATING node.
 - For a switchover disk, you need to check whether a file system is mounted on the

- disk by executing the “df(1M)” command.
- If the Cmdline resources are to be used, check that the commands written in the Start and Stop scripts for the Cmdline resources are executed properly.
 - For a command that outputs a message when it is executed, check that a message indicating that the command was executed properly is displayed on the console.
 - Check that the command has been executed properly by executing the “ps(1)” command.
- If IP address takeover is set, check that the process takes place normally by executing the “ifconfig(1M)” command.
- If MAC address takeover is set, check that the process takes place normally by executing the “ifconfig(1M)” command.
- If node name takeover is set, check that both the OPERATING and STANDBY nodes have the same node name after network takeover.
- If a line switching unit is set up, check that line switching takes place correctly.
- Check that an application is switched to other node.

You need to know the operation downtime in the event of a failure, so measure the switching time for each failure detection cause and check the recovery time.

◆ Replacement test

Conduct a replacement and confirm the followings:

- Check that the OPERATING and STANDBY instances of the OPERATING business application occurs normally when the cluster application replacement is executed. Check the followings:
 - If disk switchover is to be used, check that the disk can be accessed from the OPERATING node but not from the STANDBY node.
For a switchover disk, you need to check whether a file system is mounted on the disk by executing the “df(1M)” command.
 - If Cmdline resources are to be used, check that the commands written in the Start and Stop scripts for the Cmdline resources are executed properly.
 - For a command that outputs a message when it is executed, check that a message indicating that the command was executed properly is displayed on the console.
 - Check that the command has been executed properly by executing the “ps(1)” command.
 - If IP address takeover is to be used, check that IP address takeover takes place normally.
 - Check that an application is switched to other node.

◆ Stop

Conduct a stop test and confirm the followings:

- Check that an OPERATING work process can be stopped normally by the stop operation.
- Check that work processes can be started by restarting all nodes simultaneously.
- If Cmdline resources are to be used, check that the commands written in the Start and Stop scripts for the Cmdline resources are executed properly.
 - For a command that outputs a message when it is executed, check that a message indicating that the command was executed properly is displayed on the console.
 - Check that the command has been executed properly by executing the “ps(1)” command.

◆ **Work process continuity**

Conduct work process continuity and confirm the followings:

- Generating some state transitions in a cluster system, check that the application operates normally without triggering inconsistencies in the application data in the event of a failure.
- For systems in which work processes are built as server/client systems, check that while a state transition is generated in the cluster system, work process services can continue to be used by clients, according to the specifications.



[See](#)

- For information on the operation procedures for start, clear fault, failover, switchover, and stop, see 7.2 "Operating the PRIMECLUSTER System".
- For descriptions of IP address takeover and node name takeover, see 6.6.1.5 "Creating Takeover Network Resources".

1.5 Operation and Maintenance

After confirming that work processes can be continued no matter what state the cluster system lapses into, you can begin actual operations.



Note

The cluster system can continue work processes even if a failure occurs. However, work processes cannot be continued if another failure occurs during single node operation before the first failure is corrected. To enhance reliability, you need to eliminate the cause of the failure immediately and recover the dual node operation.



See

For details for collecting information required for an investigation, see Appendix C "Troubleshooting".

1.6 Operation Mode Change

Change the operation of the PRIMECLUSTER system when it becomes necessary to change the system configuration while the PRIMECLUSTER system is operating. The system configuration must be changed, for example, when a cluster application is added.



[See](#)

For details on changing the operation mode, see Chapter 8 "Changing the Operation Configuration".

Chapter 2 Site Preparation

You must plan the items listed below before building the PRIMECLUSTER system.

Planning items

- PRIMECLUSTER product selection
- System design
- Cluster system operation mode
- Operation mode for using Web-Based Admin View
- Cluster applications and resources to be used by the cluster applications



Point

An overview of each PRIMECLUSTER product is described in the "*PRIMECLUSTER Concepts Guide*." Be sure to read the guide before designing the PRIMECLUSTER system.

2.1 PRIMECLUSTER Product Selection

The sequence for selecting PRIMECLUSTER products is as follows:

1. Select the products to be used.
For details, see 2.1.1 "PRIMECLUSTER Product Selection".
2. Select the functions to be used.
For details, see 2.1.2 "PRIMECLUSTER Function Selection".

2.1.1 PRIMECLUSTER Product Selection

The product sets described below have been prepared for PRIMECLUSTER. Select the necessary products according to how the system will be used.

- **PRIMECLUSTER Enterprise Edition (EE)**
All-in-one cluster product that comprises a switchover-type cluster and parallel database functions.
This product is used for scalable operations, such as RAC and Symfaware.
- **PRIMECLUSTER HA Server (HA)**
Switchover-type cluster system that features HA (switchover) cluster functions, volume management functions, system functions, and network multiplexing functions.

The following table shows the components (modules) that are included in each product.

Components		Products	
Names	Features	EE	HA
Cluster Foundation (CF)	Basic cluster services	○	○
Reliant Monitor Services (RMS)	Local recovery – Attempt to bring back to Online on the current node without switching. Remote recovery – The application is switched to other node.	○	○
Wizard Tools	Configuration definition tools for RMS	○	○
Web-Based Admin View	GUI common framework and cluster administration GUI	○	○
One Shot Installer	One-time batch installer for OS and PRIMECLUSTER products	○	○
System Information Output Tool	Collects system information required for failure investigation	○	○
Cluster Configuration Backup/Restore	Backup and restoration for cluster configuration	○	○
Global Link Services (GLS)	Provides highly reliable transmission routes by setting up redundant network	○	○
Global File Services (GFS)	Simultaneous access from two or more nodes to a shared disk	○	○
Global Disk Services (GDS)	Cluster volume management functions	○	○
Netcompo BASE	Online trace function (for GLS)	○	○
Scalable Internet Services (SIS)	Network load balancing	○	—
Parallel Application Services (PAS)	Foundation for parallel databases	○	—

2.1.2 PRIMECLUSTER Function Selection

Check that the functions to be used for the selected product are included, using the following manuals:

- PRIMECLUSTER basic functions
For information on the basic functions, see "3.3 PRIMECLUSTER modules" in the *"PRIMECLUSTER Concepts Guide."*
- Other feature
In addition to the PRIMECLUSTER basic functions, the following function is also provided:
 - Process monitoring function
This function monitors the live state of applications and other processes.
For details, see 6.6.1.7.1 "What Is the Process Monitoring Function."

2.2 System Design

Use the "PRIMECLUSTER System Design Worksheet" to design the system.

The installation of the PRIMECLUSTER system is based on the completed Appendix A "PRIMECLUSTER System Design Worksheets."



See

For details on the operation environment, see "3. Operating Environment" in the "PRIMECLUSTER Installation Guide."



Information

When designing the system it may be helpful to see A.11 "System Design Examples."

2.3 Determining the Cluster System Operation Mode

To ensure that the cluster system to be built operates efficiently, you need to determine the number of nodes and an appropriate operation mode.

PRIMECLUSTER allows you to configure multiple cluster applications. The operation mode is determined depending on how you set up the cluster applications in the cluster system.

The main operation modes are listed below:

Classification	Operation mode	Number of cluster applications	Number of nodes
Standby operation	1:1 standby	1	2
	N:1 standby	2 to (number of nodes – 1)	3 to (number of supported nodes)
	Mutual standby	2 to (number of nodes)	2 to (number of supported nodes)
	Cascade	1 to 16	3 to (number of supported nodes)



Note

Note that failover does not occur when a node is switched off. When designing the system, consider using an uninterruptible power supply (USP).

2.3.1 Standby Operation

Standby operation has the following operation modes.

■ 1:1 standby

◆ Definition

- It is an operation mode in which a cluster system consists of 2 nodes. One is operating, and the other is standby. When a failure occurs in the operating node, a cluster application switches to the standby node. This does not disrupt ongoing operation.

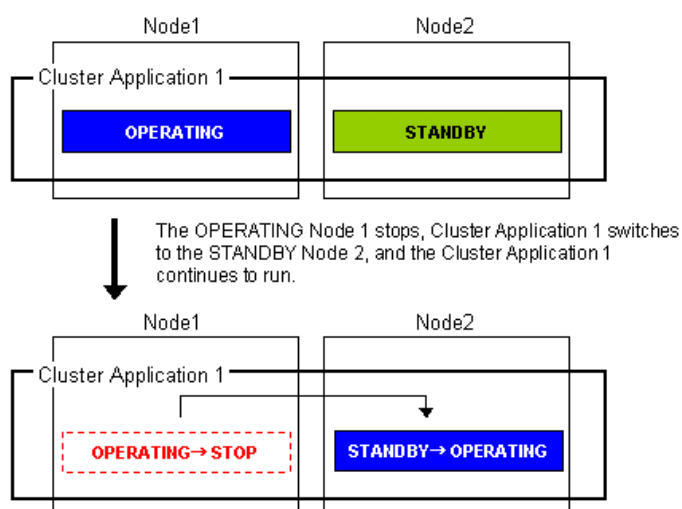
Advantage

- This operation mode ensures the availability of the cluster application even after failover.

Disadvantage

- Nodes cannot be used efficiently because of a redundant configuration.

◆ **Failover image**



■ **N:1 standby**

◆ **Definition**

- It is an operation mode in which a cluster system consists of 3 or more nodes. One is standby, and the others are operating. When a failure occurs in one of the operating nodes, a cluster application switches to the standby node. If a failure occurs in two or more operating nodes at the same time, the cluster applications switch to the standby node.

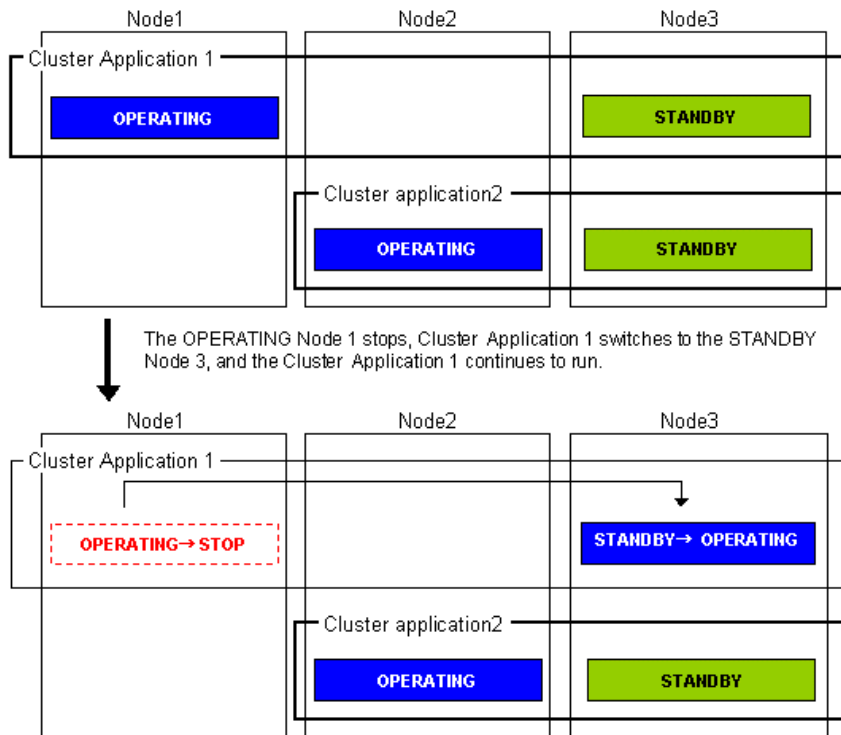
Advantages

- This operation mode ensures the availability of the cluster application even after failover.
- Since one node serves as the STANDBY node for multiple applications, the STANDBY cost can be reduced when the number of applications is large.

Disadvantages

- If failover occurs for multiple applications, the performance of the applications is reduced because multiple applications will be operating in one node.
- Since one node becomes the STANDBY node for multiple applications, performance drops if the number of application is large.

◆ Failover image



■ Mutual standby

◆ Definition

- It is an operation mode in which a cluster system consists of 2 or more nodes. Normally, 2 nodes are used in this operation mode. Each node has one operating and one standby application. The operating cluster application has its own standby in each other's node.

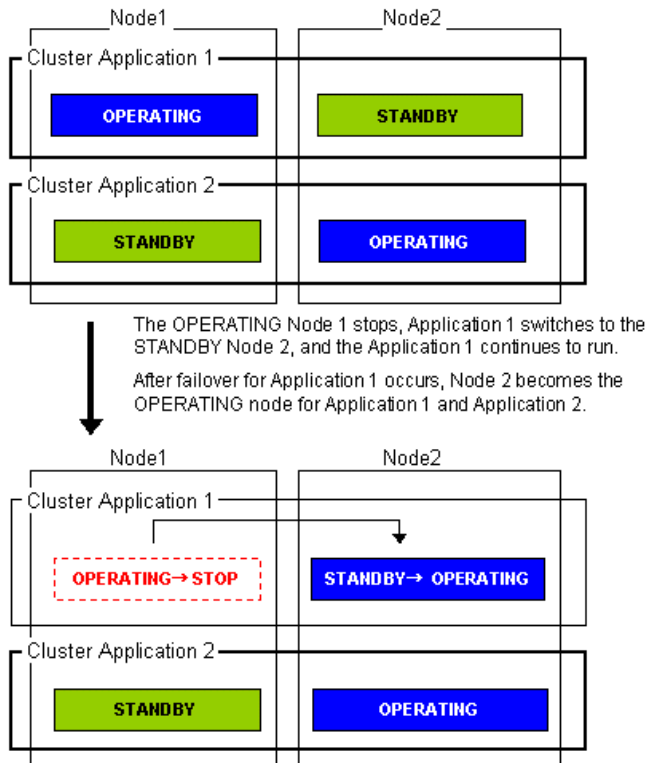
Advantages

- Since all nodes are used for cluster application operation, the nodes can be used efficiently.

Disadvantages

- If failover occurs for any of the cluster applications, the performance of the cluster applications may drop because two or more cluster applications will be operating in the failover node. For this operation mode, you need to estimate adequate resources.

◆ **Failover image**



■ **Cascade(using one cluster application)**

◆ **Definition**

- It is an operation mode in which a cluster system consists of 3 or more nodes: one is operating, and the others are standby. When a failure occurs in the operating node, a cluster application switches to one of the standby nodes. When a failover is even failed, this application switches to other standby node.

Advantages

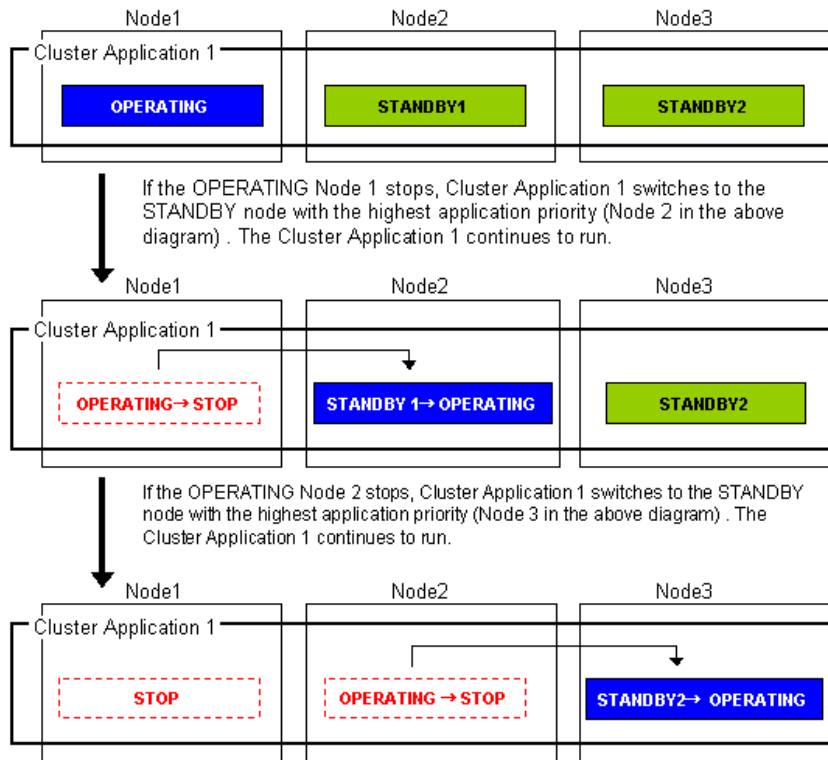
- Even after one node is stopped, the redundant configuration of the cluster application can be maintained by using other nodes. The availability is guaranteed during system maintenance.
- This operation mode ensures the availability of cluster applications even after failover.

Disadvantages

- As the system has a redundant configuration, nodes cannot normally be used efficiently.

◆ **Failover image**

In this example, the nodes are defined in the sequence Node 1, Node 2, and Node 3 starting from the node with the highest cluster application priority. These nodes are defined when the cluster application is set up.



■ Cascade (using two or more cluster applications)

◆ Definition

- It is an operation mode in which a cluster system consists of 3 or more nodes. If three nodes and two cluster applications are used, the 1st and 2nd node have one operating and one standby cluster applications. The operating cluster applications have standby in each other's node. The 3rd node has standby applications of the operating applications on the 1st and 2nd node. If a failure occurs in the operating application, it switches to the 3rd node.

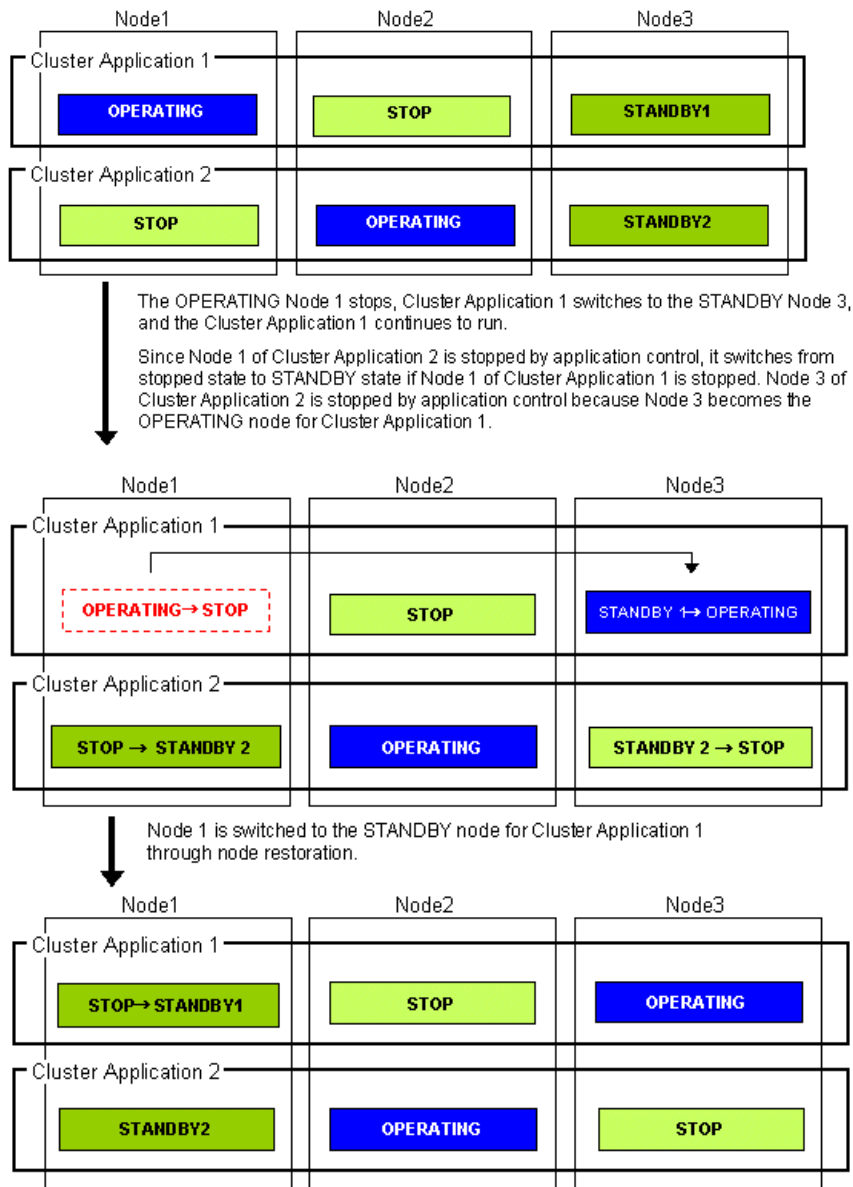
Advantage

- The OPERATING node for a cluster application does not become the OPERATING or STANDBY node for the other cluster applications.
- This operation mode ensures the availability of the cluster applications even after failover.
- Switching back of the cluster application is unnecessary during cluster application recovery.
- Since one node serves as the exclusive STANDBY node for multiple cluster applications, the STANDBY cost can be reduced when the number of cluster applications is large.

Disadvantage

- Since one node becomes the dedicated STANDBY node for multiple cluster applications, the availability drops when the number of cluster application is high.

◆ **Failover image**



◆ **Active node shutdown in cascade mode**

In cascade mode, the OPERATING node can be shut down because of control process of the cluster application as well as a failure or operator intervention.

Cluster application-controlled shutdown means that an OPERATING node is shut down by cluster application control. Among the applications in cascade operation, the OPERATING node cannot become the STANDBY node for other cluster application in the event of a failover. The OPERATING node that is shut down by application control is automatically started by cluster application control and becomes the STANDBY node when the OPERATING node of other cluster application is switched to STANDBY or is shut down.

For the transition image, see “Failover image” above.

2.4 Determining the Web-Based Admin View Operation Mode

Determine the operation mode of Web-Based Admin View according to your PRIMECLUSTER configuration. Consider system performance and RC2000 that controls the OS console. This section describes operation modes and typical models of PRIMECLUSTER systems that run Web-Based Admin View, and provides a guideline for adopting models.



See

- For information on the operation modes of Web-Based Admin View, see "1.2 Web-Based Admin View topology" in the *"PRIMECLUSTER Web-Based Admin View Operation Guide."*
- RC2000 supports integrated management of the operating system consoles of multiple nodes. It is used to log into the console of a node to install software on the node or modify configuration. For details on the RC2000, see the *"RC2000 User's Manual."*



Note

When a cluster contains 3 or more nodes, the 3-tier model, in which the cluster management server is not in the cluster, is recommended.

■ Roles of individual nodes

Web-Based Admin View adopts a logical 3-tier architecture, which consists of clients, a cluster management server, and cluster nodes. It has the following functions.

◆ Clients

A client is a computer with which a user manages operations. Basically, the computer is a personal computer that uses a Web browser or Solaris OE Workstation.

◆ Management server

The cluster management server manages cluster operation and features web server functions. The server can be as a cluster node. The cluster management server can be duplexed. In this case the system will have a two-server configuration, consisting of a primary management server and a secondary management server.

Set up both primary and secondary management servers for redundancy.

You can dynamically move the secondary management server depending on the operation mode. The cluster management servers run Solaris OE.

◆ Cluster nodes

Cluster nodes construct the PRIMECLUSTER system. The cluster nodes run Solaris OE.

■ Logical 3-tier architecture and operation models

Web-Based Admin View adopts a logical 3-tier architecture consisting of clients, management servers, and monitored nodes. Physically, the system can adopt a 2-tier architecture.

Typical operation modes that run Web-Based Admin View are introduced below.

◆ 2-tier model

In the 2-tier model, the cluster management server and the cluster node are used together on the same machine, and the client is on a machine other than the nodes and the management servers.

This model is used for a configuration where the number of nodes is relatively small.

Normally, this model is used for an operation mode such as 1:1 standby or mutual standby in a 2-node configuration.

If the RC2000 is used with this model, you need to adopt local operation.

In the local operation, RC2000 supports integrated management of the OS consoles of multiple nodes without linking to the cluster management server.



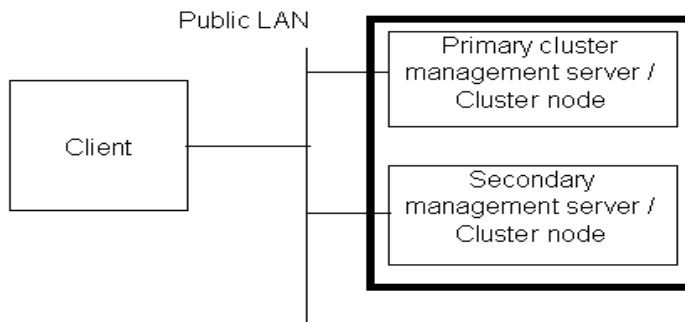
See

For details on the RC2000 operation mode, see the "RC2000 User's Guide."

This model supports 2 types of topology, which are described below.

- **Topology where a network is shared**

In this topology, the public LAN and the LAN that is connected to the management client are used together. You can adopt this topology if the network users and network range are limited for security. This is the default Web-Based Admin View configuration after PRIMECLUSTER installation.

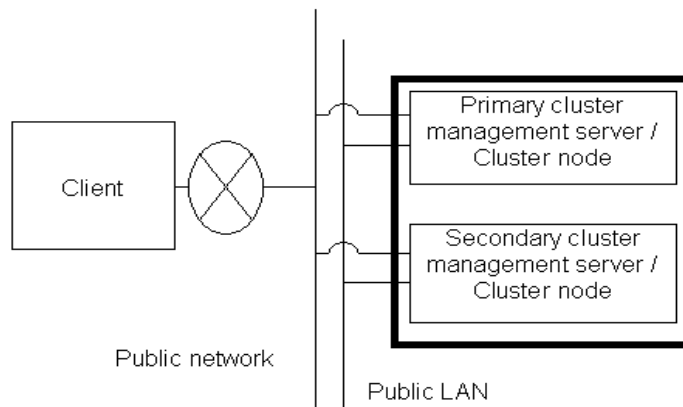


The cluster system is working in

- **Topology where separate LANs are used**

In this topology, the public LAN and the LAN that is connected to the management client are separate. When using a management client from a public network, this topology is recommended for security. After the PRIMECLUSTER installation is done, you will need to modify the Web-Based Admin View configuration.

Specify IP addresses used for a cluster node and a client respectively. For details, see 5.2.1 "Setting Up CF and CIP."



The cluster system is working in

◆ 3-tier model

In the 3-tier model, clients, cluster management servers, and cluster nodes are set up separately.

This model is adopted for configurations where the number of nodes is relatively large.

Normally, this model is used for integrated management of the PRIMECLUSTER system. You can also use this mode when you do not want to impose the load of running the management server on the cluster node or when you want to perform the integrated management of the PRIMECLUSTER system.

To maintain operation continuity and availability, Fujitsu recommends this 3-tier model for a configuration with 3 or more nodes.

When the RC2000 is used with this model, you need to adopt server/client operation.

In the server/client operation, RC2000 supports integrated management of the OS consoles of multiple nodes, and can be operated on the cluster management server as well as on the client.



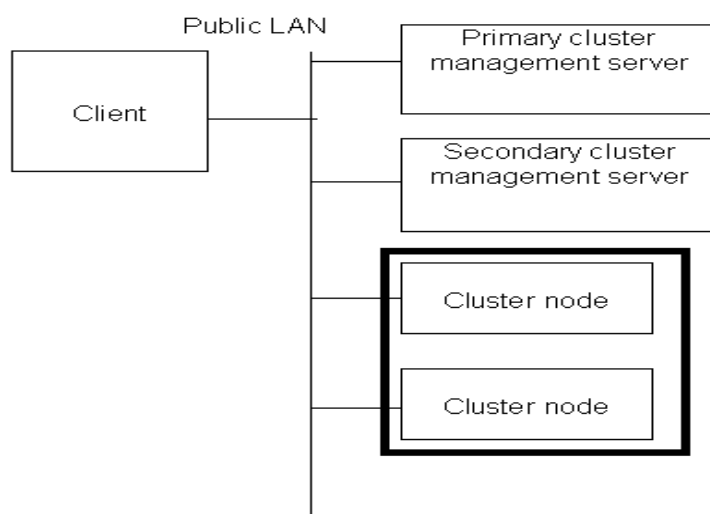
See

For details on the RC2000 operation modes, see the *"RC2000 User's Manual."*

This model supports 2 types of topology, which are described below.

● Topology where a network is shared

In this topology, the public LAN and the LAN that is connected to the management client are the same. You can adopt this topology if the network users and network range are limited for security. This is the default Web-Based Admin View configuration after PRIMECLUSTER installation.

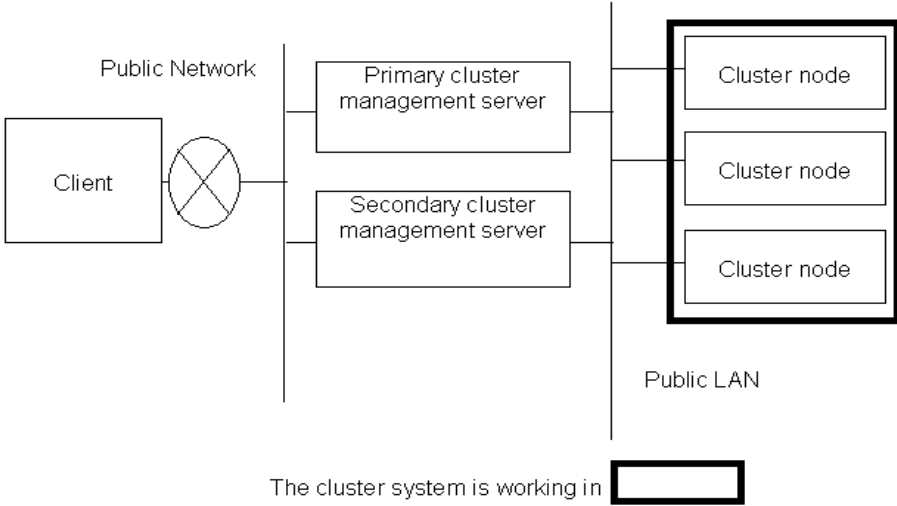


The cluster system is working in

● Topology where separate LANs are used

In this topology, the public LAN and the LAN that is connected to the management client are separate. When using a management client from a public network, this topology is recommended for security. After PRIMECLUSTER installation is done, you will need to modify the Web-Based Admin View configuration.

Specify IP addresses used for a cluster node and a client respectively. For details, see 5.2.1 "Setting Up CF and CIP."



2.5 Setting the Failover Range of a Cluster Application

Determine the trigger for cluster application failover. You can choose from the followings:

1. The cluster application does not automatically switch to other host.
2. The cluster application switches to other host in the event of a node failure or a resource failure.
3. The cluster application switches to other host in the event of a node failure, a resource failure, or RMS shutdown.

Part 2 Installation

This part describes procedures for installing the PRIMECLUSTER system and running Web-Based Admin View.

The work operations include the procedures up to installing a new PRIMECLUSTER system.

For procedures on changing the PRIMESYSTEM configuration after the system is installed, see Chapter 8 "Changing the Operation Configuration".

Chapter 3 Software Installation

Install Solaris OE and other software products related to PRIMECLUSTER on each node.

This chapter describes the following topics:

- PRIMECLUSTER installation (overview)
- Installation and setup of related software
- Application installation and environment setup

3.1 PRIMECLUSTER Installation

The two methods of installing PRIMECLUSTER Enterprise Edition, HA server, Parallel Server, and Scalability Server are installation scripts or One Shot Installer as follows:

- One Shot Installer

The One Shot Installer tool is used to set up Solaris custom JumpStart. Using this JumpStart, you can also install Solaris software, PRIMECLUSTER, and related software products on multiple nodes at the same time.

- Installation script

The installation script is also called the CLI Installer. It is used to install PRIMECLUSTER on a system in which Solaris software and related Fujitsu software have been installed. This method is also used for installation on the cluster management server.



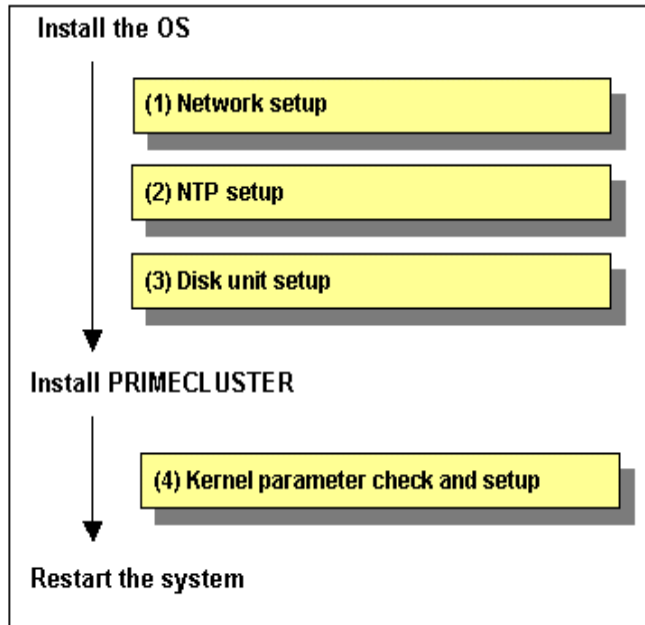
[See](#)

For details on the installation procedures, see the "*PRIMECLUSTER Installation Guide*."

3.2 Installation and Setup of Related Software

After installation of the software products related to PRIMECLUSTER is done, you need to set up the OS and hardware for installing and operating PRIMECLUSTER.

Set up the followings if necessary.



- Network setup
If a network adapter for a public LAN has been installed, you need to configure the IP addresses after installing the OS.
Perform this setup after installing the operating system.
For details, see 3.2.1 "Setting Up the Network".
- NTP setup
This setup synchronizes the time in all of the nodes of the cluster system. This NTP setup needs to be done before installing PRIMECLUSTER.
- Disk unit setup
When using a shared disk unit, you need to install and set up the software product. This disk unit setup should be done after installing the OS.
For details, see 3.2.2 "Setting Up Disk Units."
- Kernel parameter check and setup
When operating the software products related to PRIMECLUSTER, you need to adjust kernel parameters according to the hardware configuration and applications. This kernel parameter setup should be done before operating PRIMECLUSTER.
For details, see 3.2.3 "Checking the Kernel Parameters."

3.2.1 Setting Up the Network

If a network adapter for a public LAN has been installed, the IP address setup is required. You need to create the `/etc/hostname.interface` file for the interface.



See

For details, see the *"Solaris X AnswerBook2 System Administrator Collection."*

Also set a local MAC address in each node if the following conditions apply:

- If MAC address takeover is to be performed and network interfaces for multiple LANs are connected to the same transmission path
- If MAC address takeover is to be performed in the network interface for an expansion LAN that Web-Based Admin View does not use

Determine one local MAC address between the interfaces for takeover, and set the address in the `/etc/opt/FSUNnet/mactool/macaddr.conf` file of each node. If a local MAC address is set, the LAN network interface is not activated until the cluster application is started. The interface in which the local MAC address is set cannot be used for Web-Based Admin View. You cannot set up an IP address in this interface. Also, this interface cannot be connected to power control box 4.



See

- For details, see *the "Netcompo FNA-LAN User's Guide."*
- For information on changing the public LAN that the PRIMECLUSTER system uses, see 8.2 "Changing the IP Address of a Public LAN".



Information

Web-Based Admin View automatically sets up an interface that was assigned the IP address of the host name corresponding to the node on which PRIMECLUSTER was installed. This interface will be used as a transmission path between cluster nodes and cluster management server, and between cluster management servers and clients.

3.2.2 Setting Up Disk Units

■ Installation and Setup of Related Software

Install and set up the software products required for using shared disk units. See the installation guides and manuals of each software product.



Point

- If the disk unit uses a Fibre Channel interface, a Fibre Channel driver for the card needs to be installed and set up. For installation details, see "Installation Procedures" in *"FUJITSU PCI Fibre Channel x.x Guide for Solaris(TM) Environment."*
- If the disk array unit is used with a multipath configuration, refer to the following manuals for instructions on installing and setting up the software.
 - When the GR multipath driver (GRMPD) is used
 - *"GR Multipath Driver 1.0 User's Guide"*
 - When the multipath disk control load balance option (MPLB) is used
 - *"INSTALLATION GUIDE - Multipath Disk Control load balance option x.x for*

Solaris(TM) Environment"

- *"Multipath Disk Control Load Balance option x.x Guide"*
- When multipath disk control (MPHD) is used
 - *"INSTALLATION GUIDE - Multipath Disk Control x.x for Solaris(TM) Environment "*
 - *"Multipath Disk Control x,x Guide"*

- If an ETERNUS3000 or GR700 series disk array is used with a single-path configuration, you need to install and setup a hard disk driver (HDDV).
For details on installing HDDV, see the *"Hard Disk Driver x.x Guide."*

■ Preparation for automatic shared disk configuration

◆ Multipath disk

Before executing automatic shared disk configuration, format the logical units and assign labels to the units.



See

- For information on the procedures, refer to the manual (*"Multipath Disk Control x,x Guide," "Multipath Disk Control load balance option,"* or *"GR Multipath Driver 1.0 User's Guide"*) of the software product to be used.
- For information on automatic configuration of shared disks, see 5.2.3 "Initial Setup of the Cluster Resource Management Facility" and 6.2.1 "Automatic Configuration of Shared Disks."



Note

At this stage, do not create logical paths for MPHD, MPLB, and GRMPD.

If MPLB or GRMPD is installed and the disk unit supports load balancing, the automatic shared disk configuration process automatically creates the MPLB logical path and automatically registers the MPLB resources. To create the MPHD logical path automatically and register the MPHD resources automatically, you need to set up the parameters beforehand by executing the `clsetacparam(1M)` command.



See

For details on the `clsetacparam(1M)` command, see the *"PRIMECLUSTER Global Disk Services Configuration and Administration Guide."*

◆ If the disk is not a multipath disk

Before executing automatic shared disk configuration, you need to assign a label to the disk by executing the `format(1M)` command.



See

For information on automatic configuration of shared disks, see 5.2.3 "Initial Setup of the Cluster Resource Management Facility" and 6.2.1 "Automatic Configuration of Shared Disks."

3.2.3 Checking the Kernel Parameters

You need to edit the values for the kernel parameters according to the environment.

Target node:

All nodes in which PRIMECLUSTER is to be installed

The kernel parameters differ according to the products and components to be used.

Check the Kernel Parameter Worksheet, and edit the value if necessary.



See

For information on the kernel parameters, see the A.6 "Kernel Parameter Worksheet".



Note

To enable modifications, you need to restart the system after installation.

3.3 Installation and Environment Setup of Applications

Install software products to be operated on the PRIMECLUSTER system and configure the environment as necessary.

To bring about application switchover in the event of a failure, you need to register the resources of software application to RMS. RMS will monitor these resources. For details, see Chapter 6 "Building Cluster Applications".



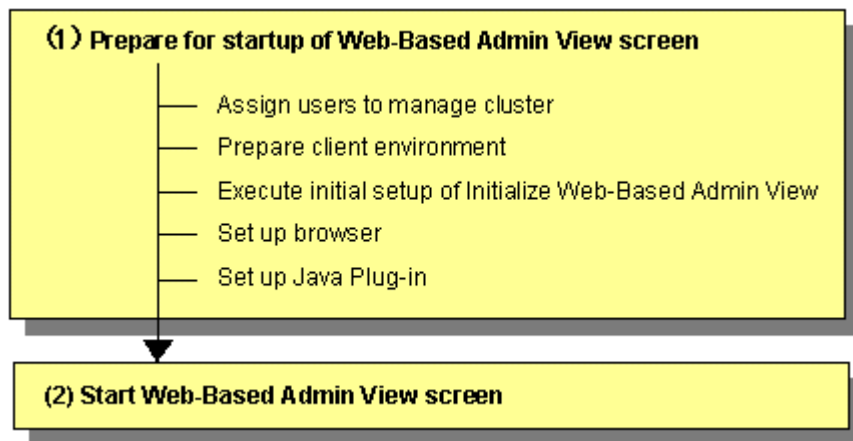
[See](#)

- For information on products supported by the PRIMECLUSTER system, see Table 11-1 "PRIMECLUSTER Product List".
- For details on installing applications, see the manuals and installation guides for the individual applications.

Chapter 4 Starting the Web-Based Admin View Screen

This chapter explains how to start and exit the Web-Based Admin View screen. It also describes the windows that are displayed from the Web-Based Admin View screen.

The procedure for starting the Web-Based Admin View screen is shown below.



Operation procedure and manual reference location for starting the Web-Based Admin View screen

	Work item	Execution Node	Required/Optional	Manual reference location*
(1)	4.1.1 Assigning Users to Manage the Cluster	Cluster node	Required	
	4.1.2 Preparing the Client Environment	Client	Required	WEB "3.1.2 Prerequisite client environment"
	4.1.3 Initial Setup of Web-Based Admin View	Cluster node	Required	
	4.1.4 Setting Up the Browser	Client	Required	WEB "3.1.3.1 Preparing the Web browser"
	4.1.5 Setting Up the Java Plug-in	Client	Required	WEB "3.1.3.2 Required for the Web Browser Environment"
(2)	4.2 Starting the Web-Based Admin View screen	Client	Required	WEB "3.2 Screen startup"

* The PRIMECLUSTER manual name is abbreviated as follows:

- **WEB**: PRIMECLUSTER Web-Based Admin View Operations Guide

4.1 Preparations for Starting the Web-Based Admin View Screen

Take the following steps for starting the GUI screen of Web-Based Admin View:

1. Environment setup

You can set up the following in no special order:

 - 4.1.1 Assigning Users to Manage the Cluster
 - 4.1.2 Preparing the Client Environment
 - 4.1.3 Initial setup of Web-Based Admin View
2. Web environment preparation

You need to set up the browser first.

 - 4.1.4 Setting Up the Browser
 - 4.1.5 Setting Up the Java Plug-in

4.1.1 Assigning Users to Manage the Cluster

Web-Based Admin View restricts access to specific operation management GUIs by using user groups in the management server.

The table below shows the groups used for operation management GUIs of PRIMECLUSTER.

Operation management GUIs of Web-Based Admin View and authorized user groups

GUI name	UNIX user group name	Privileges
All GUIs	wvroot	Root authority. This group can execute all operations.
Cluster Admin	clroot	Root authority. This group can specify settings, execute management commands, and display information.
	cladmin	Administrator authority. This group cannot specify settings. It can execute management commands and display information.
	clmon	User authority. This group cannot specify settings and cannot execute management commands. It can only display information.
GDS (Global Disk Services)	sdxroot	Root authority.

The groups for the operation management GUIs are defined as shown in the above table.

wvroot is a special user group, and is used for Web-Based Admin View and GUIs. Users belonging to this group are granted the highest access privileges for Web-Based Admin View and all kinds of operation management GUIs.

The system administrator can grant different access privileges to users according to the products that the users need to use.

For example, a user who belongs to the "clroot" group but not to "sdxroot" is granted all access privileges when opening the Cluster Admin screen but no access privileges when opening the Global Disk Services (GDS) GUIs.

You need to create the above UNIX groups for both the primary and secondary management servers as necessary, and assign users to these groups. The Web-Based Admin View group membership should maintain consistency among all management servers associated with a specific cluster system. To set a user group, execute the "useradd(1M)" command as follows:

```
# useradd -g wvroot usrname
```

The root user is granted the highest access privilege regardless of which group the root user belongs to.

For details about user groups, see "3.1.1 User group determination" in the *"PRIMECLUSTER Web-Based Admin View Operations Guide."*

4.1.2 Preparing the Client Environment

Prepare hardware, operating systems, and Web browsers of the clients supported by Web-Based Admin View.

- **PC client**

- CPU

- Equivalent to Pentium II 233 MHz or faster

- Memory

- 128 MB or more installed

- Operating system

- Windows(R) 98, Windows NT(R), Windows(R) 2000, Windows(R) Me, Windows(R)

- XP



- Note**

- There are restrictions on the Japanese display environment. For details, see "Notes" below.

- Web browser

- Netscape(R) Communicator 4.5 to 4.7X, Netscape(R) 6.2, Microsoft(R) Internet Explorer 5.0 or later (Java Plug-in is required.)
(Netscape(R) 7 is not supported.)

- Java Plug-in

- Java(TM) 2 Runtime Environment Standard Edition Version 1.3.1

- Display unit

- Unit that supports 800×600 pixels or more and can display High Color (16 bits, 65,536 colors).

- **Solaris Workstation**

- Memory

- 128 MB or more installed (256 MB or more are recommended if multiple browsers are to be started or if an individual operation management screen is to be started more than once concurrently)

- OE

- Solaris8 OE 01/01 or later, Solaris9 OE

- Web browser

- Netscape(R) Communicator 4.72 to 4.7X

- Java Plug-in

- 20.1.2.2,REV=1999.10.14.18.04 or later

- 20.1.2.2,REV=2001.05.01.15.36 or later

- Java(TM) 2 Runtime Environment Standard Edition Version 1.2.2

- Java(TM) 2 Runtime Environment Standard Edition Version 1.3.1

The System Management Console that comes with PRIMEPOWER

800/900/1000/1500/2000/2500 can also be used as a client. However, the above OE must be used.



Note

- For Japanese to be displayed in Web-Based Admin View, the operating system environment must satisfy the following conditions:
 - Japanese Windows(R) is installed, and the language environment being used by Windows(R) is set to Japanese.
 - The Japanese package is installed in the Solaris Workstation, and the language environment to be used is set to Japanese.
- If Java(TM) 2 Runtime Environment Standard Edition Version 1.3.1 is used in the Japanese environment of the Solaris 8 OE, the top menu of Web-Based Admin View is sometimes not displayed because of a JVM problem. If the top menu is not displayed, use Java(TM) 2 Runtime Environment Standard Edition Version 1.2.2.
- For details on the Java Plug-in settings, see "3.1.3.2 Required for the Web Browser Environment" in *"PRIMECLUSTER Web-Based Admin View Operations Guide."*
- For details on the operation environments of the Web-Based Admin View management server and the monitoring nodes, see "2.1 Prerequisite server environment" in the *"PRIMECLUSTER Web-Based Admin View Operations Guide."*
- If you are using a 3-layer configuration and operating Web-Based Admin View separately from the cluster system, the operating system of the server in which Web-Based Admin View and the GUI packages are installed must be Solaris8 OE 1/01 or later, or Solaris9 OE.
- In clients that are supported by Web-Based Admin View, the following color depth problems may exist.

- **Solaris**

When Sun's PGX32 PCI graphics card is set to 8-bit color, the GUI screen of Web-Based Admin View is sometimes not displayed correctly. This problem is present if the password field and other GUI fields are displayed as a single-color blue block when the GUI screen of Web-Based Admin View is displayed. If the problem exists, use the following commands to check the color depth of the display:

```
$ xwininfo
```

The color depth of the window is displayed in the Depth output parameter.

If the GUI screen of Web-Based Admin View is not displayed correctly and the color depth is 8 bits, you can use the `pgxconfig` command to set the color depth to 24 bits (Use the "24" bit color depth setting, not the "8 & 24" bit setting.)

```
# pgxconfig -i
```

For information on using the `pgxconfig` command, see the Sun manual *"Sun PGX32 PCI Graphics Card Installation Guide."*

- **Windows(R)**

When the GUI screen of Web-Based Admin View is displayed with Windows(R), the 16-bit or 32-bit color mode must be used. The 24-bit color mode does not properly support an alpha component (transparency) that is required for RMS graphs. If 24-bit color is used, RMS graphs may not be displayed properly.

Whether problems will occur in 24-bit color mode depends on the graphics card and video driver being used.

4.1.3 Initial Setup of Web-Based Admin View

4.1.3.1 Initial setup of the operation management server

When using Web-Based Admin View for the first time, you need to initialize the management server on each node. Take the following steps in the order listed below.



Note

You do not have to initialize the server on the node on which PRIMECLUSTER was installed using the One Shot Installer tool

◆ Operation Procedure:

1. Stop Web-Based Admin View.

```
# /etc/init.d/fjsvwvcnf stop
# /etc/init.d/fjsvwvbs stop
```

2. Set the IP addresses of the primary management server and secondary management server.

```
# /etc/opt/FJSVwvbs/etc/bin/wvSetparam primary-server
<primary-management-server-IP-address>
# /etc/opt/FJSVwvbs/etc/bin/wvSetparam secondary-server
<secondary-management-server-IP-address>
```

Example: Set the "primary cluster management server IP" and "secondary cluster management server IP" of the "operation management mode" found on the cluster building worksheet.

```
# /etc/opt/FJSVwvbs/etc/bin/wvSetparam primary-server 10.34.214.181
# /etc/opt/FJSVwvbs/etc/bin/wvSetparam secondary-server
10.34.214.182
```

3. Restart Web-Based Admin View.

```
# /etc/opt/FJSVwvbs/etc/bin/wvCntl restart
# /etc/init.d/fjsvwvcnf restart
```



See

Web-Based Admin View has some different operation management modes. For further details, see "1.2.2 System topology" and "Chapter 7 Web-Based Admin View setup modification" in the *"PRIMECLUSTER Web-Based Admin View Operations Guide."*

4.1.3.2 Confirming Web-Based Admin View Startup

This section describes the procedure for confirming whether Web-Based Admin View has been started.

◆ Confirmation Procedure

Check that all node information is output by executing the "wvstat(1M)" command on the connected management server.

[Example]

In a two-node configuration consisting of node1(10.20.30.40) and node2(10.20.30.41), node1 is the primary management server and node2 is the secondary management server.

```
# /etc/opt/FJSVwvbs/etc/bin/wvstat
primaryServer 10.20.30.40 node1 http=10.20.30.40 Run 1d+7h36m
```



```

primaryServer Sessions: 0
primaryServer Nodes: 2
    10.20.30.40 node1 SunOS-5.8 1d+7h36m
    10.20.30.41 node2 SunOS-5.8 1d+7h36m
secondaryServer 10.20.30.41 node2 http=10.20.30.41 Run 1d+7h36m
secondaryServer Sessions: 0
secondaryServer Nodes: 2
    10.20.30.41 node2 SunOS-5.8 1d+7h36m
    10.20.30.40 node1 SunOS-5.8 1d+7h36m
#

```

If the information is not displayed, Web-Based Admin View has not been started or there may be an error in the Web-Based Admin View settings. Restart Web-Based Admin View and execute the operation again. If node information is still not displayed, refer to the "PRIMECLUSTER Web-Based Admin View Operations Guide" and check the parameter settings.

For details on the `wvstat(1M)` command, see the manual page.

4.1.3.3 Setting the Web-Based Admin View Language

The language environment Web-Based Admin View operates is set to English as default. Even though the client has a Japanese environment, the text of cluster resource management facility messages that are sent from the cluster node is displayed in English.

If you want to display the messages in Japanese, take the following steps to set up environment variables of Web-Based Admin View. You need to set up the variables using a system administrator access privilege on all nodes and the cluster management servers that construct a cluster system.

This operation must be executed with the system administrator authority for all cluster nodes and the cluster management server that make up the cluster system.

Environment variable for the operation language of Web-Based Admin View

Attribute	Variable	Possible values	Meaning
sys	lang	C, ja	Language environment in which Web-Based Admin View operates. C: Operates in English. ja: Operates in Japanese. If this variable is not set, Web-Based Admin View operates in the English environment.

◆ Operation Procedure:

1. Stop Web-Based Admin View.

```
# /etc/init.d/fjsvwvcnf stop
# /etc/init.d/fjsvwvbs stop
```

2. Add the environment variable to the definition file (`/etc/opt/FJSVwvbs/etc/webview.cnf`) of Web-Based Admin View, and set the language.

```
# /etc/opt/FJSVwvbs/etc/bin/wvSetparam -add <attribute>
<environment-variable> <set-value>
```

Example: Add the environment variable and set the operation language to Japanese.

```
# /etc/opt/FJSVwvbs/etc/bin/wvSetparam -add sys lang ja
```

3. Restart Web-Based Admin View.

```
# /etc/opt/FJSVwvbs/etc/bin/wvCntl restart
# /etc/init.d/fjsvwvcnf start
```



Note

- For Web-Based Admin View to display messages in Japanese, the language environment of the personal computers and Solaris OE workstations that are being used as clients must be set to Japanese. If a client has an English environment, the message contents turn into garbled characters by the above setting change.
- To change the environment variable again after it is added by the above procedure, execute the following command:

```
# /etc/opt/FJSVwvbs/etc/bin/wvSetparam <operation_environment_variable>  
<setting_value>
```

For details on the command, see "4.5.3 Environment variable modification" in the *"PRIMECLUSTER Web-Based Admin View Operations Guide."*

4.1.4 Setting Up the Browser

Set up a Web browser on the clients.



See

See "3.1.3.1 Preparing the Web browser" in the *"PRIMECLUSTER Web-Based Admin View Operations Guide."*

4.1.5 Setting Up the Java Plug-in

Install the Java Plug-in on the clients.



See

For details on the supported Java Plug-in versions, see 4.1.2 "Preparing the Client Environment." For instructions on setting up the Java Plug-in, see "3.1.3.2 Required for the Web Browser Environment" in the *"PRIMECLUSTER Web-Based Admin View Operations Guide."*

4.2 Starting the Web-Based Admin View Screen

After completing the all preparations, start the Web-Based Admin View GUI screen.

◆ **Operation Procedure:**

1. Start the Web browser in the client.
2. Specify the URL in the following format, and access the cluster management server:

http://<host-name>:<port-number>/Plugin.cgi

<host-name>

IP address or host name (**httpip**) that clients use to access the primary or secondary cluster management server.

The default value of **httpip** is the IP address that is assigned to the node name that is output when "uname -n" is executed.

<port-number>

Specify "8081."

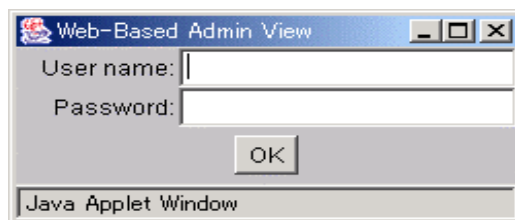
If the port number has been changed, specify the up-to-date number.

For instructions on changing the http port number, see "7.2.1 http port number" in the *"PRIMECLUSTER Web-Based Admin View Operations Guide."*



Note

- If the Web-Based Admin View screen cannot be started when the host name is specified in **<host-name>**, specify the IP address directly that corresponds to the host name.
 - Note that the access method may be different depending on the operation management product. To use operation management products that have different access methods at the same time, see "3.3.4 Concurrent use of operation management products with different access methods" in the *"PRIMECLUSTER Web-Based Admin View Operations Guide."*
 - For information on the IP address or host name (**httpip**) used by clients, see the *"PRIMECLUSTER Web-Based Admin View Operations Guide."*
3. When the Web-Based Admin View is started, the following window appears.
Enter a user name and password that have been registered to the cluster management server, and click OK.



Note

You cannot close this window by clicking "x" at the top right corner.

4. When authentication ends, you can use Web-Based Admin View.

**Note**

- After starting the Web-Based Admin View screen, do not change the page by pressing the *Forward/Next*, *Back*, or *Reread/Refresh* buttons.
- The screen of some browsers may hang.
 - If the browser is terminated, restart the browser and display Web-Based Admin View.
 - Reread the URL or restart the browser if the browser does not work (no response).
 - The operation can be continued after the Web-Based Admin View is started by moving the mouse on the browser if the page switches to a black screen.
- If the URL of the Java Plug-in is read with Netscape Communicator or Netscape Navigator, a message stating “Click here to get the plugin” may appear. In this case, the Java Plug-in may not be installed or an older Java Plug-in version that is not supported may be installed. See the *“PRIMECLUSTER Web-Based Admin View Operations Guide”* and install the Java Plug-in. Note that if you click the “Click here to get the plugin” icon, a dialog box indicating “Plug-in is not read” appears. Select *Cancel*.
- If “Welcome to Web-Based Admin View” does not appear after you read the URL of the Java Plug-in with Internet Explorer, an appropriate Java Plug-in may not be installed. Confirm that an appropriate Java Plug-in is installed by using “Add/Remove Programs” in the control panel. If the Java Plug-in is not be installed or if an older Java Plug-in version that is not supported is installed, see the *“PRIMECLUSTER Web-Based Admin View Operations Guide”* and install the Java Plug-in. Also, if the “security warning” dialog box appears, and prompts you to specify whether the “Java Plug-in” is to be installed and executed, select *No*.
- If the secondary cluster management server is set to operate dynamically, there is a function that connects automatically to the primary or secondary cluster management server that is operating at that time even if the URL of a specific monitoring node is specified. For details, see “7.4 Secondary management server automatic migration” in the *“PRIMECLUSTER Web-Based Admin View Operations Guide.”*
- If repeated errors occur during the authentication of Step 3, the message 0016 may be displayed and you may not be able to log in. For the action to take if this happens, see “Symptom 17” in “Appendix B Troubleshooting” of the *“PRIMECLUSTER Web-Based Admin View Operations Guide.”*
- If Netscape 6.X is used, URL input may become disabled. This condition is a Netscape problem and Netscape is currently working to correct the problem.

If this condition occurs, minimize the Netscape window and then return it to its original size, or restart the Netscape Web browser.
- If some problems occur while you are using Web-Based Admin View, see “Appendix A Message” and “Appendix B Troubleshooting” of the *“PRIMECLUSTER Web-Based Admin View Operations Guide.”*

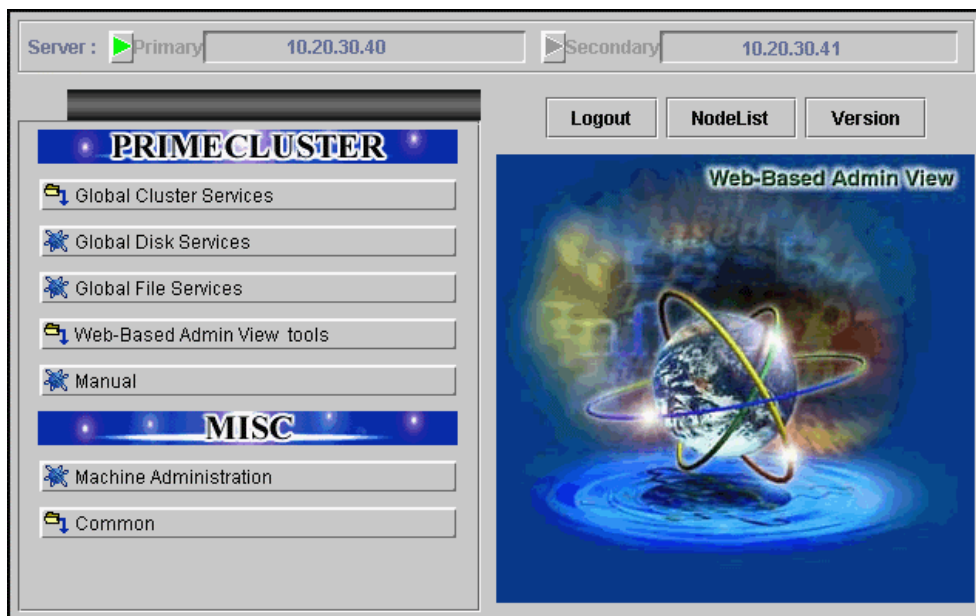
4.3 Web-Based Admin View Screen

When you start Web-Based Admin View, the Web-Based Admin View screen is displayed. The left area of the Web-Based Admin View screen displays the currently supported functions as **operation menus**.

4.3.1 Operation Menu Functions

Web-Based Admin View screen supports the functions shown below. See "Menu Outline."

Web-Based Admin View screen



■ Menu Outline

The operation menus are divided into the following two categories:

1. **PRIMECLUSTER category**

Management screens and manuals of operation management products that are presented by PRIMECLUSTER

2. **MISC category**

Management screens and manuals of operation management products that are presented by a software product other than PRIMECLUSTER, such as the Enhanced Support Facility (ESF)

The following operations are enabled for each category:

- **PRIMECLUSTER**

- **Operation management product name**

You can operate the screen of the operation management product.

For details, see the manual provided with each operation management product.

- Global Cluster Services (CF, CRM, RMS, SIS)
- Global Disk Services (PRIMECLUSTER GDS)
- Global File Services (PRIMECLUSTER GFS)

If the 3-tier model is used and an RC2000 is set, the following menu is displayed in addition to those listed above:

- RC2000

- **Web-Based Admin View tools**

These tools display the Web-Based Admin View log and allow you to set the operation environment. For details, see "Part 3 Web-Based Admin View tools menu" in the *"PRIMECLUSTER Web-Based Admin View Operations Guide."*

- **Manual**

The PRIMECLUSTER online manual is displayed.

- **MISC**

Buttons for starting the management screens of installed operation management products other than the PRIMECLUSTER products are displayed. In this system, this menu category is displayed because Enhanced Support Facility (ESF) is installed.

For details, see the manual provided with each operation management product.

- **Operation management product name**

You can operate the management screens of installed operation management products other than the PRIMECLUSTER products.

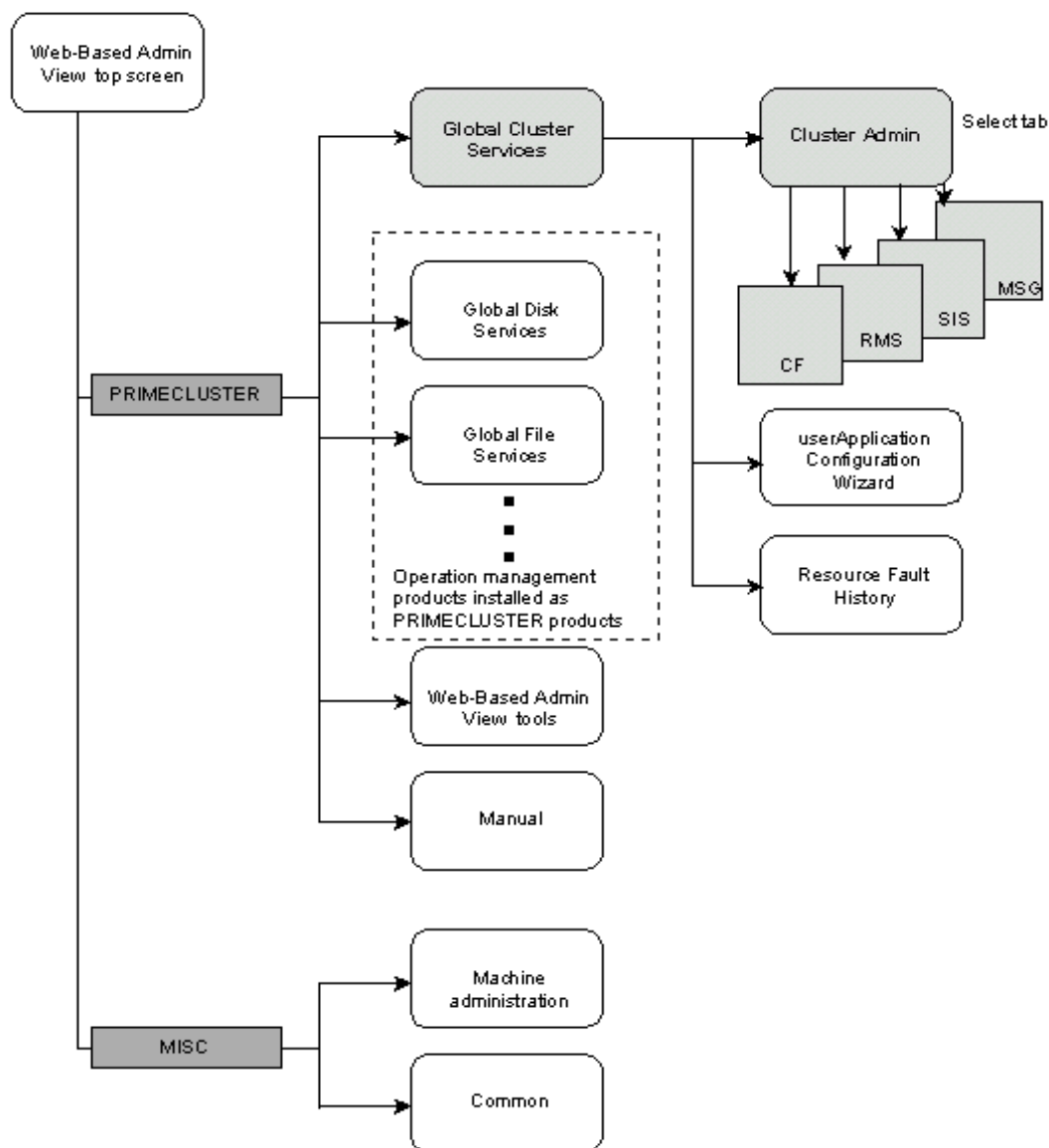
- Machine Administration
- MultiPathDisk view

- **Common**

You can refer to manuals that are available as online manuals. For details, see the *"PRIMECLUSTER Web-Based Admin View Operations Guide."*

- **Operation menu transition diagram**

Shown below are the transitions from the top screen of Web-Based Admin View to the other screens.



At the Cluster Admin screen, you can switch the window by clicking the following tabs:

- CF: Cluster Foundation
- CRM: Cluster Resource Management
- RMS: Reliant Monitor Services
- SIS: Scalable Internet Services
- MSG: Message

The following sections describe the screens found after the Global Cluster Services menu.

4.3.2 Global Cluster Services Menu Functions

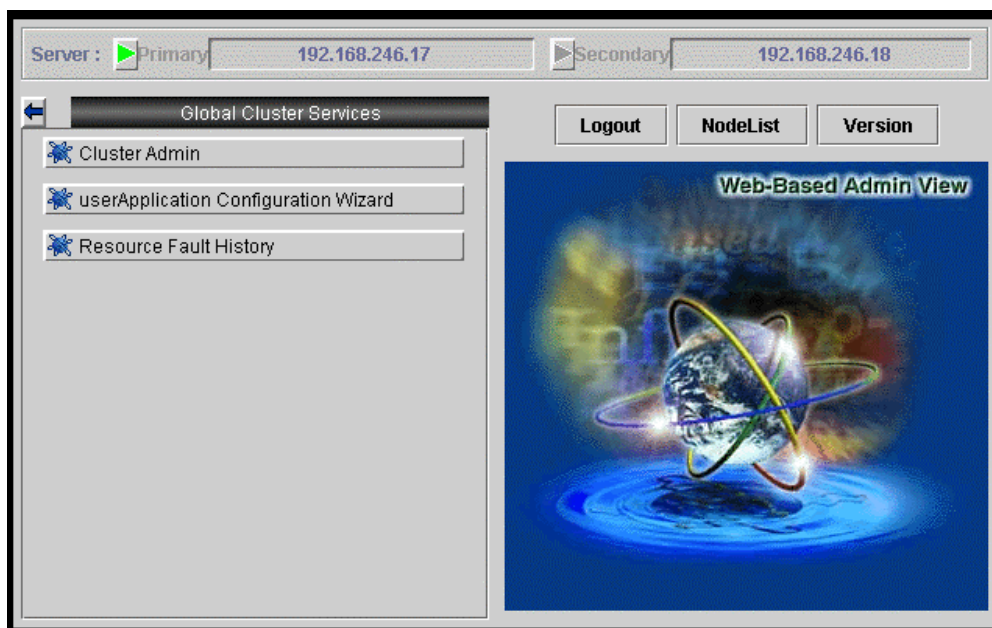
Display procedure

Web-Based Admin View screen -> Global Cluster Services

Exit procedure

To return to the Web-Based Admin View screen, click the arrow next to *the Global Cluster Services*.

Web-Based Admin View screen (Global Cluster Services menu)



Overview of the Global Cluster Services menu

- **Cluster Admin**
This function allows you to monitor the status of the PRIMECLUSTER system and operate the system.
- **userApplication Configuration Wizard**
This function allows you to create cluster applications.
- **Resource Fault History**
This function allows you to display the resource fault history.

4.3.3 Cluster Admin Functions

Display procedure

Web-Based Admin View screen -> Select *Global Cluster Services*. -> Select *Cluster Admin*. -> Node selection screen -> Select the node.

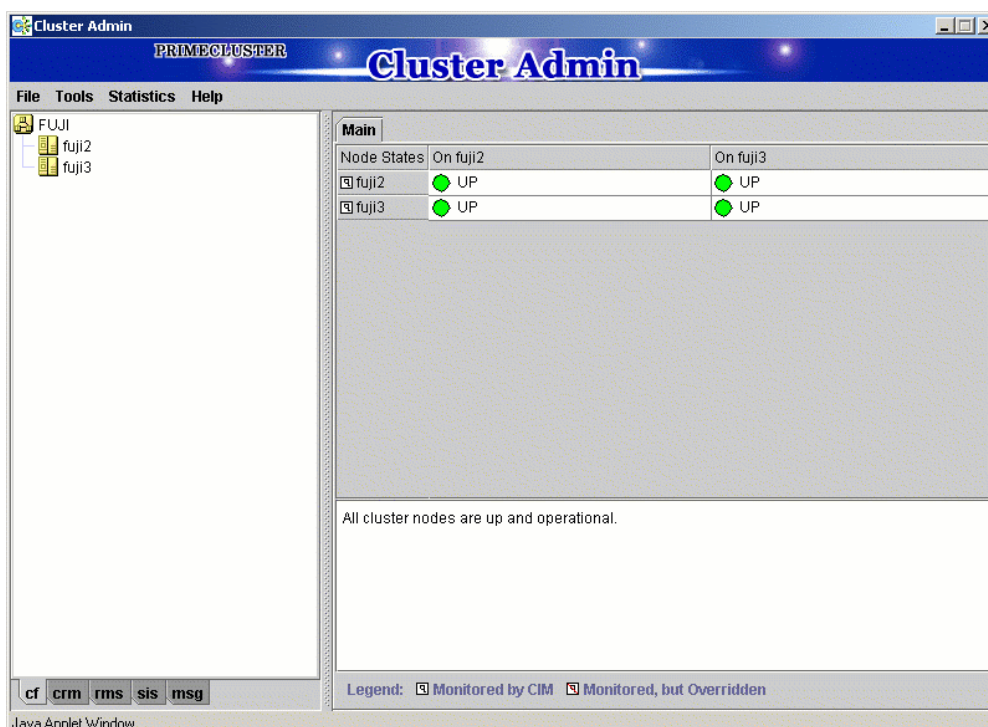
Exit procedure

Select the *Exit* in the *File* menu. -> Confirmation screen -> Select the *Yes*. -> *Global Cluster Services* menu

Cluster Admin supports the functions described below.

The manual reference locations are indicated in "Overview of Cluster Admin."

Web-Based Admin View screen (Cluster Admin)



Overview of Cluster Admin

- **cf (CF: Cluster Foundation)**
This function allows you to manage, build, monitor, and diagnose the cluster.
Reference location: 5.2 "Initial Cluster Setup", Chapter 7 "Operations"
- **crm (CRM: Cluster resource management facility)**
This function manages the resource database, which contains information about the hardware devices (including shared disks, line switching units, and network interface cards).
Reference location: 5.2.3 "Initial Setup of the Cluster Resource Management Facility", Chapter 7 "Operations"
- **rms (RMS: Reliant Monitor Services)**
This function monitors the status of the cluster system and manages applications and resources.
Reference location: Chapter 7 "Operations"
- **sis (SIS: Scalable Internet Services)**
This function enables PRIMECLUSTER to act as a scalable, reliable, and easily managed network system.

Reference location: PRIMECLUSTER Scalable Internet Services (SIS) Configuration and Administration Guide

- **msg (Message)**

Cluster control messages are displayed.

Reference location: Chapter 7 "Operations"

4.3.4 userApplication Configuration Wizard Functions

Display procedure

Web-Based Admin View screen -> *Global Cluster Services* -> *userApplication Configuration Wizard*

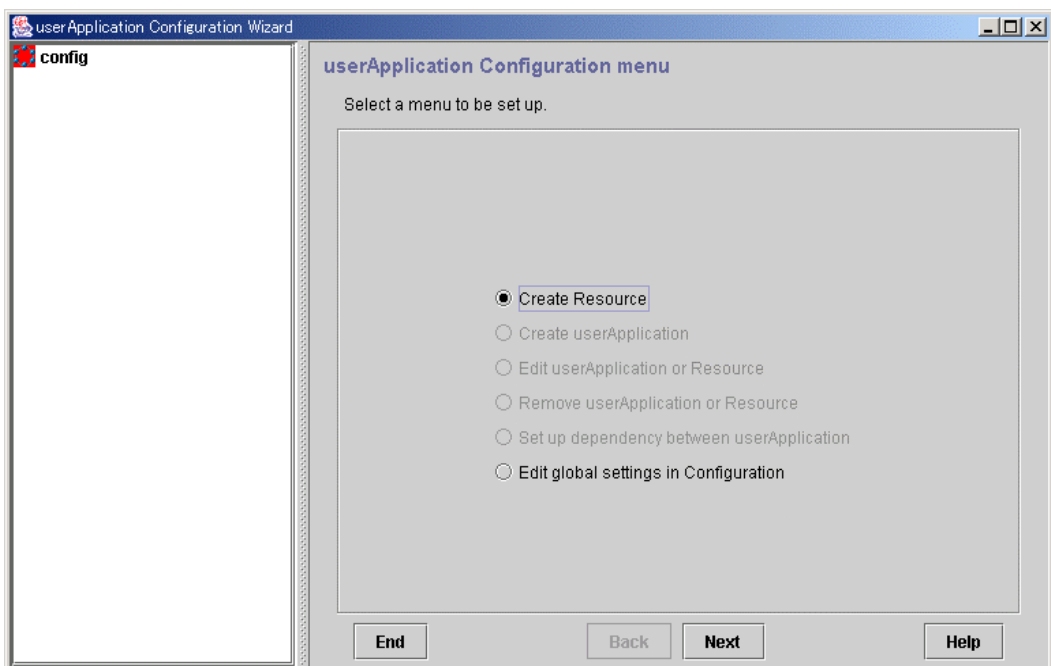
Exit procedure

Click *the End* button. -> Global Cluster Services menu

userApplication Configuration Wizard supports the functions described below.

The manual reference locations are indicated in "Overview of userApplication Configuration Wizard."

Web-Based Admin View screen (userApplication Configuration Wizard)



Overview of userApplication Configuration Wizard

- **Create Resource**

This function creates a new resource.

Reference location: 6.6.1 "Setting Up Resources"

- **Create userApplication**

This function monitors the cluster system status, and manages cluster applications and resources.

Reference location: 6.6.2 "Creating Cluster Applications"

- **Edit userApplication or Resource**

This function edits the attributes of cluster applications or resources.

Reference locations: 8.1.2 "Changing the Operation Attributes of a Cluster Application" and 8.1.3.2 "Changing the Attributes Used by a Resource or a Resource Interface"

- **Remove userApplication or Resource**

This function removes cluster applications or resources.

Reference location: 8.9 "Deleting a Cluster Application"

- **Set up dependency between userApplication**

This function sets up dependency between cluster applications.

Reference location: 6.6.3 "Setting Up Dependency Relationships Between Cluster Applications"

- **Edit global settings in Configuration**

This function edits global settings in configuration.

Reference location: 6.6.4 "Editing global settings in Configuration."

4.4 Exiting the Screen

To exit the Web-Based Admin View screen, carry out the procedure described below.

◆ Logging out of the screen

To log out of the Web-Based Admin View screen, follow the procedure below.

1. Close all screens if the management screen of the operation management product is displayed.
2. When only the Web-Based Admin View screen is displayed, select *the Logout*.

◆ Exiting the screen

To exit the Web-Based Admin View screen, carry out the procedure described below.

1. Log out from the Web-Based Admin View screen according to "Logging out of the screen" described above.
2. The login screen will be displayed. To exit the Web-Based Admin View screen, execute one of the following operations while the login screen is still displayed:
 - Terminate the Web browser.
 - Specify another URL in the Web browser to switch the screen. (Enter a new URL or specify a bookmark.)
 - Select the *Back* button of the browser.

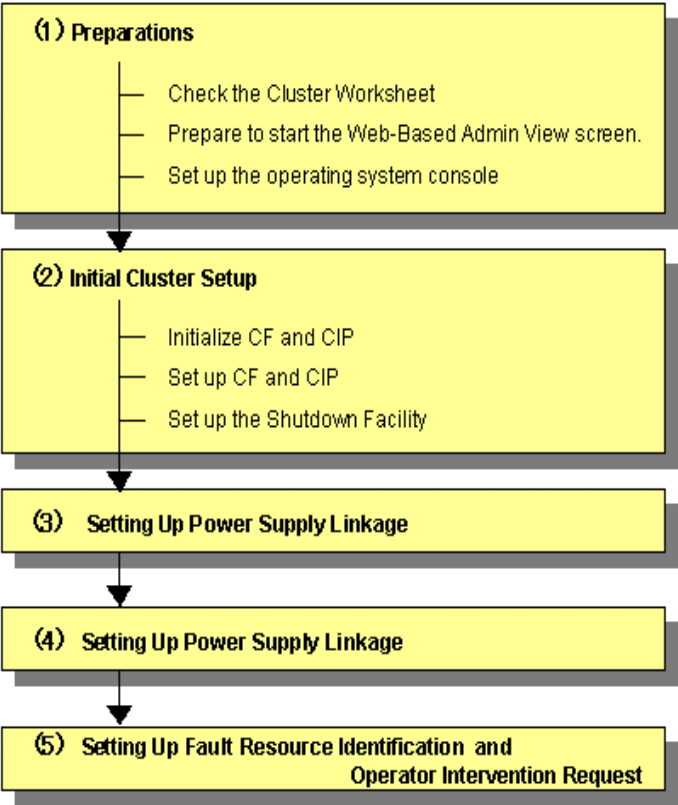


Note

- To terminate the Web browser, select the *Close* in the *File* menu, or click the "x" at the top right corner of the screen.
Note that if you are using Netscape, selecting the *Exit* in the *File* menu will terminate all browser screens.
- At the login screen, clicking the "x" at the top right corner of the screen will not terminate the screen.
- The login screen will remain temporarily after exiting the browser.

Chapter 5 Building a Cluster

The procedure for building a PRIMECLUSTER cluster is shown below.



Cluster building procedure and manual reference locations

	Work item	Execution Node	Required/Optional	Manual reference location*
(1)	5.1 Preparations	All nodes	Required	ING "3 Operating Environment"
	5.1.1 Checking the cluster worksheet	—	Required	This manual: Appendix A
	5.1.2 Preparations for starting the Web-Based Admin View screen	All nodes	Required	This manual: "4.1 Preparations for Starting the Web-Based Admin View Screen"
	5.1.3 Setting up the operating system console	All nodes	Optional	
(2)	5.2 Initial Cluster Setup			
	5.2.1 Setting up CF and CIP	All nodes	Required	CF "2.1 CF, CIP and CIM configuration"
	5.2.2 Setting Up the Shutdown Facility	All nodes	Required	CF "8 Shutdown Facility (SF)"
	5.2.3 Initial Setup of the Cluster Resource Management Facility	All nodes	Required	CF "4.3 Resource database configuration"
(3)	5.3 Setting Up Power Supply Linkage	All nodes	Optional	"Machine Administration Guide"
(4)	5.4 Setting up shared disk connection confirmation	All nodes	Required	
(5)	5.5 Setting Up Fault Resource Identification and Operator Intervention Request	1 node	Required	

* The PRIMECLUSTER manual names are abbreviated as follows:

- **ING:** PRIMECLUSTER Installation Guide
- **CF:** PRIMECLUSTER Cluster Foundation Configuration and Administration

5.1 Preparations

As preparation for building the cluster, check the operation environment. See "3 Operating Environment" in the "PRIMECLUSTER Installation Guide."

5.1.1 Checking the Cluster Worksheet

Make certain of filling the worksheet. If there is missing information, you should specify values and complete the sheet.



See

For information on the worksheet, see Appendix A "PRIMECLUSTER System Design Worksheet".

5.1.2 Preparations for Starting the Web-Based Admin View Screen

For information on the preparations before starting the Web-Based Admin View screen, see 4.1 "Preparations for Starting the Web-Based Admin View Screen".

5.1.3 Setting Up the Operating System Console

In the PRIMECLUSTER system, it is recommended that XON/XOFF flow control of the operating system console be disabled.

In the environment immediately after the Solaris OE is installed, XON/XOFF flow control is enabled for console messages that are output from the operating system.

Although this setting allows you to stop screen display by pressing the [Ctrl] + [S], it might affect the system by disturbing ongoing operations in the event of a console failure.

To avoid this, you need to disable XON/XOFF flow control for output from the server to the console terminal.

Change the settings in the server and the terminal (remote console connection unit) according to the procedure described below.

◆ Operation Procedure:

1. Setting up the server

Take the following steps on all servers in the cluster system.

- 1) Log in using a system administrator access privilege.
- 2) Edit the "/etc/ttydefs" file.

Change all lines that begin with "console:" to the following:

```
console:9600 hupcl opost onlcr -ixon:9600::console
```

- 3) Restart the machine.

```
# shutdown -g0 -i6 -y
```

2. Setting the remote console connection unit

If a remote console connection unit (RCCU) is connected to each server in the cluster system, perform the following.

- 1) Log into the RCCU.

```
% telnet <RCCU-IP-address> 8010 <-- Enter "telnet RCCU-IP-address 8010"
```


and press the [Return] key

```
Trying <RCCU-IP-address>...  
Connected to <RCCU-IP-address>.  
Escape character is '^]'.  
  
login :somebody <-- Enter "somebody" and press the [Return] key  
passwd: <-- Press the [Return] key  
cs >su <-- Enter "su" and press the [Return] key  
passwd: <-- Press the [Return] key
```

2) Edit the rs232c.def file.

```
# edit rs232c.def <-- Enter "edit rs232c.def" and press the [Return] key  
0001 #  
Press the [M] key 5 times.  
0002 baud 9600  
0003 parity none  
0004 stop 1  
0005 bichar 8  
0006 flow xon  
Press the [C] key.  
0006> flow xon  
0006< flow rxon <-- Enter "flow rxon" and press the [Return] key  
0006 flow rxon  
Press the [E] key.  
# write <-- Enter "write" and press the [Return] key  
writing configuration to flash ROM . done.
```

3) Reboot the RCCU.

```
# reboot <-- Enter "reboot" and press the [Return] key  
Do you really want to reboot [y/n] ? y <-- Enter "y" and  
press the [Return] key
```

3. Confirmation of modified settings

Log in again to the console of each server. While executing the command such as "ls -l", press [Ctrl] + [S] and check that the output does not stop.

If the data output stops, review the settings for Step 1 and Step 2 again.

5.2 Initial Cluster Setup

This section describes the initial setup of the PRIMECLUSTER cluster.

For details on the setup methods, see the reference locations indicated in the table below.

	Contents	Manual reference location*
1	5.2.1 Setting up CIF and CIP (setting up cluster configuration information and IP addresses)	CF "2.1 CF, CIP and CIM configuration"
2	5.2.2 Setting up the shutdown facility	CF "8 Shutdown Facility (SF)"
3	5.2.3 Initial Setup of the Cluster Resource Management Facility	CF "4.3 Resource database configuration"

* The PRIMECLUSTER manual names are abbreviated as follows:

- **CF:** PRIMECLUSTER Cluster Foundation Configuration and Administration

5.2.1 Setting Up CF and CIP

Set up Cluster Foundation (CF) and CIP using the CF Wizard of Cluster Admin. Enter the information described in the table below. The worksheet for the CF and CIP setup is the A.7 "Cluster Configuration Worksheet."

Setup item	Description	Described in worksheet
Cluster name	Define the name of the cluster systems. Use up to 31 printable ASCII characters (except space, line feed, and tab characters) for each name. Cluster names are always processed as uppercase characters.	"Cluster name"
Cluster nodes	Select the nodes that will construct a cluster system.	"Node name (uname-n)" for "Node 1" and "Node 2"
CF node names	Set the names of the nodes that construct the cluster. Use up to 31 printable ASCII characters (except space, line feed, and tab characters) for each node name. CF node names are always processed as lowercase characters. In the setup screen, the same names as the "Cluster nodes" above are displayed by default.	"CF node name" for "Node 1" and "Node 2"
Cluster interconnects	In each node of the cluster, determine the network interface to be used in CF inter-node communication. A representative network interface is the Ethernet device. Set the network interfaces to be used for CF inter-node communication so that they are activated when the system is started. However, IP addresses must not be assigned to the interfaces.	"Path 0 NIC name" and "Path 1 NIC name" for "Node 1" and "Node 2"
IP interconnects	Optional. This setup allows you to operate CF over IP.	"IP interconnect setup"

Setup item	Description	Described in worksheet
CIP subnets	Set the following items, and set the IP address used by CF: <ul style="list-style-type: none"> ● CIP subnet count ● Host suffix ● Subnet number ● Subnet mask 	"Subnet count," "Subnet IP," and "Netmask" for "CIP"
Usage confirmation of CF remote services	Check whether the following functions are to be enabled: <ul style="list-style-type: none"> ● Remote file copy (cfcp) ● Remote command execution (cfsh) <p>With the default settings, these services are "Not selected." To use RMS, you need to select at least one function.</p>	"Usage status of CF remote services"
Cluster Integrity Monitor (CIM) configuration	Set the nodes to be monitored by CIM.	"Is a node in the CF quorum set" for "Node 1" and "Node 2"



Note

- If you enable any one of the CF remote services, do not connect the following systems in the same cluster interconnect:
 - Systems that have a security problem
 - Systems in which cluster interconnects are not secured
- If you used the userApplication Configuration Wizard (GUI), the two remote services, "remote file copy" and "remote command execution," will be enabled automatically. If the cluster interconnects are not secured, comment out the following two lines in the "/etc/default/cluster.config" file for all cluster nodes after you build userApplication:

```
CFCP    "cfcp"
CFSH    "cfsh"
```

The results are as follows:

```
#CFCP    "cfcp"
#CFSH    "cfsh"
```

5.2.2 Setting Up the Shutdown Facility

The procedure for setting up the shutdown facility differs according to the type of machine to be used. Check the hardware type, and configure the appropriate shutdown agent.

- For PRIMEPOWER 200, 400, 600, 650, and 850:
Select all RCI monitoring agent (Panic, Reset) and console monitoring agent (RCCU).
- For PRIMEPOWER 800, 900, 1000, 1500, 2000, and 2500:
Select RCI monitoring agent (Panic, Reset).

Please refer to other FSC manual according to the SCON.



See

For details on the setup procedures and functions of the shutdown facility and monitoring agent, see the following manuals:

- "3.3.1.6 PRIMECLUSTER SF" in the "*PRIMECLUSTER Concept Guide*"
- "8. Shutdown Facility (SF)" in "*PRIMECLUSTER Cluster Foundation Configuration and Administration*"

Live priority

If cluster partitioning occurs as a result of a cluster interconnect failure, all nodes can still access the user resources.

To ensure the data consistency, you must determine which node groups are to be left alive and which node groups are to be eliminated (forcibly shut down).

In PRIMECLUSTER, the weight assigned to each node group is called the "live priority."

If the weight of a node is large, the live priority is high. Conversely, if the weight becomes smaller, the live priority becomes lower. If the weight is the same between node groups, the following node remains alive:

- the number of characters for a node name is smallest, and
- first comes when sorted alphabetically by name

The live priority is calculated from the following equation:

Live priority = SF node weight + userApplication ShutdownPriority

SF node weight (weight):

Node weight. Default value = 1. This value is specified when the shutdown function is set.

Shutdown Priority of userApplication:

Specify this setting in the attribute setup when userApplication is created. For instructions on how to change the setting value, see 8.7 "Changing the Operation Attributes of a userApplication".



See

For details on the ShutdownPriority attribute of userApplication, see 6.6.5 "Attributes."

Design guide for the live priority

The design guide for the live priority is described below based on frequently used cases.

[To keep the most number of nodes alive]

- Set the weight of all nodes to 1 (default value).
- Set the ShutdownPriority attribute of all user applications to 0 (default value).

	Node group1			Node group2
	node1	node2	node3	node4
weight of node	1	1	1	1
ShutdownPriority of app1 = 0				0
ShutdownPriority of app2 = 0				0
ShutdownPriority of app3 = 0				0
Live priority	3			1

[To keep a specific node alive]

- Set the weight of the node to be kept alive to a value that is at least twice the total weights of the other nodes.
- For all use applications, set the ShutdownPriority attribute to 0 (default value).

In the example below, the values are set to keep node1 alive.

	Node group1	Node group2		
	node1	node2	node3	node4
weight of node	10	1	1	1
ShutdownPriority of app1 = 0		0		
ShutdownPriority of app2 = 0			0	
ShutdownPriority of app3 = 0				0
Live priority	10	3		

[To keep the nodes in which a specific application is operating alive]

- For all nodes, set the weight to 1 (default value).
- For the application to be kept operating, set the ShutdownPriority attribute to a value that is at least twice the total of the ShutdownPriority values of the other applications and the weights of all nodes.

In the example below, the nodes in which app1 is operating are kept alive.

	Node group1	Node group2		
	node1	node2	node3	node4
weight of node	1	1	1	1
ShutdownPriority of app1 =20	20			
ShutdownPriority of app2 =1			1	
ShutdownPriority of app3 =1				1
Live priority	21	5		

5.2.3 Initial Setup of the Cluster Resource Management Facility

This section explains how to set up the resource database that the cluster resource management facility (CRM) manages.

Set up the CRM resource database according to the following procedure:

1. Initial setup
 - Set up the resource database that CRM manages.
2. Automatic configure
 - Register the connected hardware devices (shared disks, line switching units, and network interface cards) to the resource database that CRM manages.



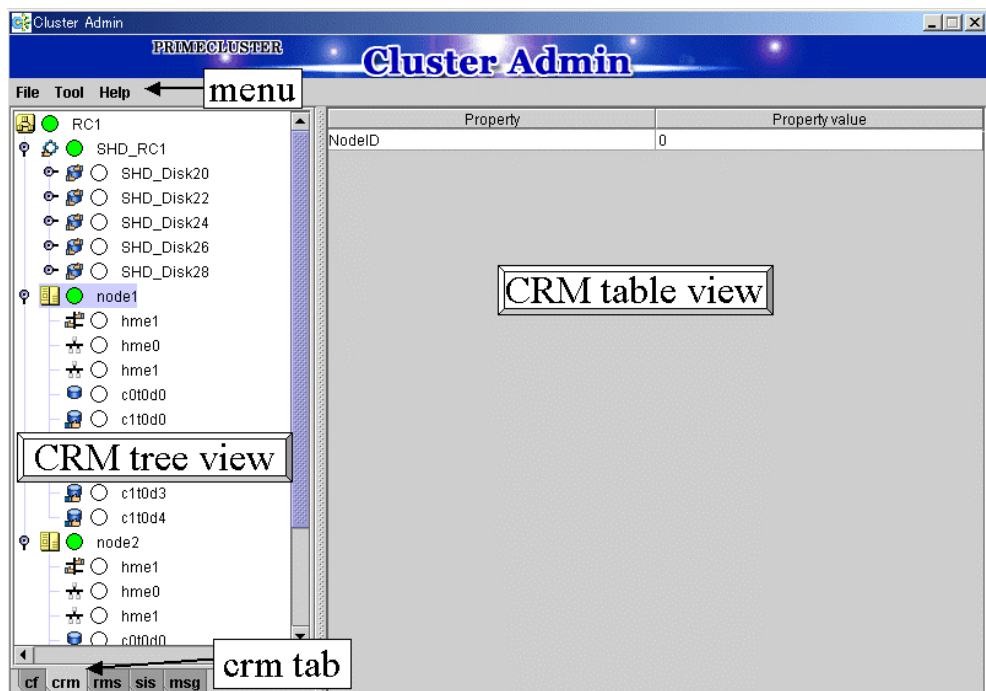
Note

You can check the NIC (network interface card) to be registered by executing the “ifconfig(1M)” command in the plumb up state.

Set up the CRM resource database from the CRM main window. Use the CRM main window as follows:

◆ Operation procedure

1. Select *PRIMECLUSTER -> Global Cluster Services -> Cluster Admin* in the *Web-Based Admin View operation menu*.
2. When the “Cluster Admin” screen is displayed, select the *crm* tab.



The areas shown in the screen are described below.

Menu bar

This area displays the menu. See 7.1.2.1.3 “Operations_”

CRM tree view

This area displays the resources registered to CRM. The resources are displayed

in a tree structure.

For details on the colors and status of the icons displayed in the tree, see 7.1.2.1 "Displayed Resource Types."

CRM table view

This area displays attribute information for the resource selected in the CRM tree view. For information on the displayed information, see 7.1.2.2 "Detailed Resource Information."

5.2.3.1 Initial Configuration Setup

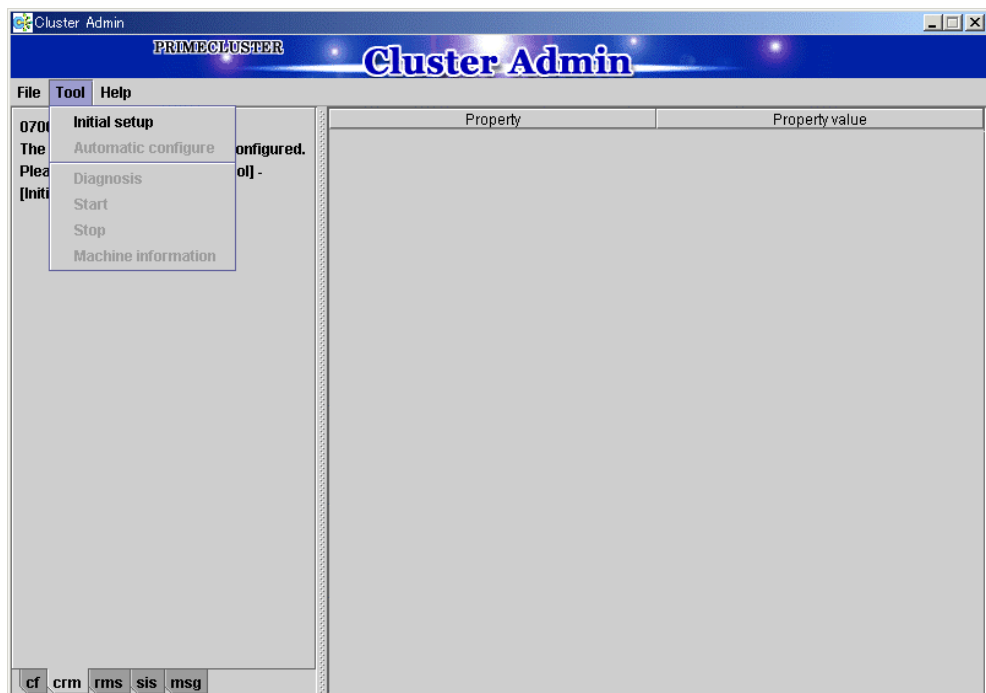
Set up the resource database that CRM manages.

When setting up the initial configuration, make sure that all nodes in the cluster have been started and that CF configuration is completed.

◆ Operation procedure

1. Select the *Initial setup* in the *Tool* menu.

Screen for cluster resource management facility

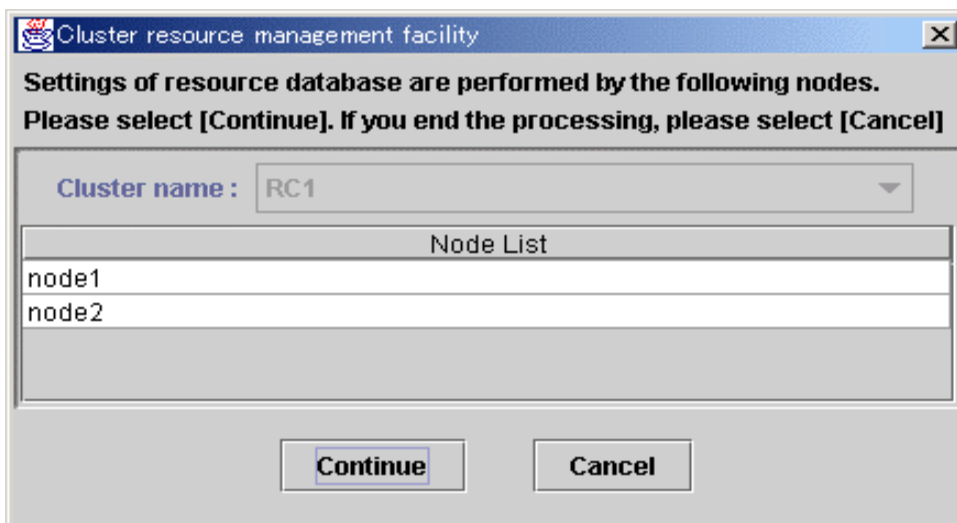


Note

The *Initial setup* can be selected only if the resource database has not been set.

2. The screen for initial setup is displayed.

Screen for initial setup



Cluster name

This area displays the names of the clusters that make up the resource database. The cluster names displayed here were defined during CF configuration.

Node List

This area displays a list of the nodes in the cluster named in the Cluster name pulldown.



Note

Check that the nodes that were configured in the cluster built with CF and the nodes displayed here are the same.

If the nodes do not match, check the following:

- Whether all nodes displayed by selecting the *cf* tab in the Cluster Admin screen are Online.
- Whether Web-Based Admin View is operating in all nodes.

For instructions on checking this, see 4.1.3.2 "Confirming Web-Based Admin View Startup."

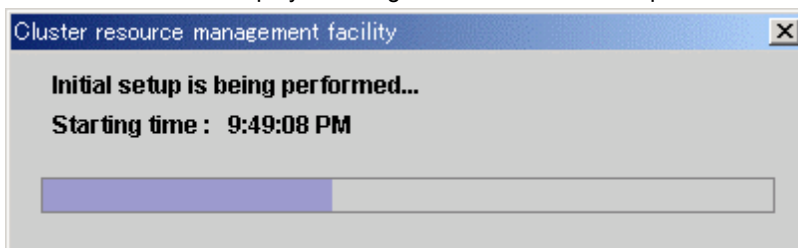
Continue button

Click this button to set up the resource database for the displayed cluster. Initial setup is executed on all nodes displayed in the Node list.

Cancel button

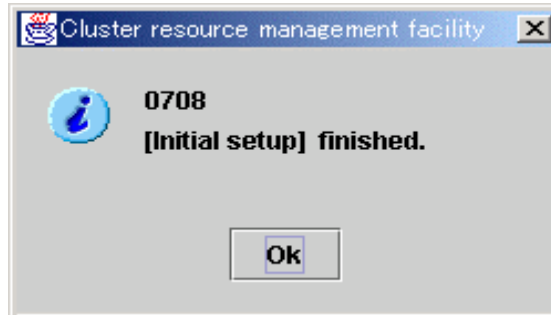
Click this button to cancel processing and exit the screen.

3. Check the displayed contents, and click the *Continue* to start initial setup.
4. The screen below is displayed during execution of initial setup.



5. When initial setup ends, the following message is displayed. If *Ok* is selected, the automatic configure screen is displayed. For details on automatic

configure, see 5.2.3.2 "Automatic Configure."



Note

- If a message appears during operation at the CRM main window, or if the frame title of the message dialog says "Cluster resource management facility" appears, refer to the following:
 - H.5 "Cluster Resource Management Facility Messages"
 - D.5 "Failed Resource and Operator Intervention Messages (GUI)"
 - D.7 "Shared Disk Connection Confirmation Messages"
 - D.8 "Patrol Diagnosis Messages"
- If you want to add, delete, or rename a disk class from the *Global Disk Services* screen after executing automatic configuration from the CRM main window, close the *Cluster Admin* screen.

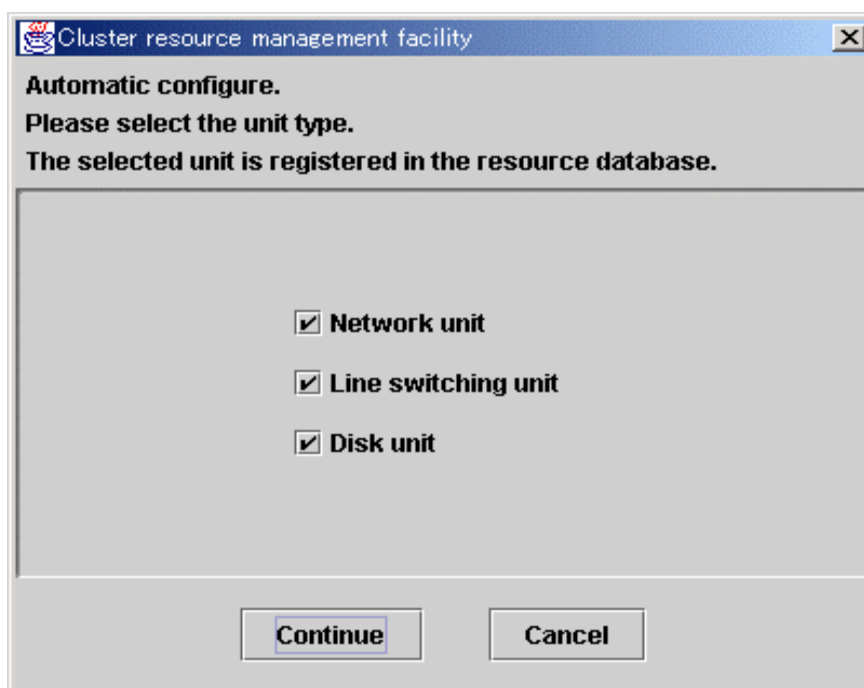
5.2.3.2 Automatic Configure

The automatic configure process registers the connected hardware devices (shared disks, line switching units, and network interface cards) to the resource database.

◆ Operation Procedure

1. Display the automatic configure screen by one of the following methods:
 - Respond to the "0708 [Initial setup] finished." message, which is displayed after initial setup is completed.
 - Select *Tool -> Automatic configure* from the CRM main window of Cluster Admin.

Screen for automatic configure

**Network unit**

Select this item to detect network interfaces automatically and register them to the resource database.

You must select this item to use public LAN takeover.

Line switching unit

Select this item to detect connected line switching units automatically and register them to the resource database.

You must select this item to use the line takeover function.

Disk unit

Select this item to detect connected shared disk units automatically and register them to the resource database. You must select this item to use system disk mirroring or to use Global Disk Services (GDS) and Global File Services (GFS) in shared disk unit takeover.

**Note**

When you use the multipath disk control function to set shared disk units, the following messages may be displayed on the console, depending on the configuration:

```
WARNING: mphd2048: paths setup information of command is reverse against device one.
```

```
WARNING: mphd2049: paths setup information of command is reverse against device one.
```

You can ignore these messages. These messages indicate that the multipath that is stored in multipath disk control and actual connection of multipath disk is not identical. But multipath disk control automatically reconfigures the multipath according to the actual connection.

Continue button

Click this button to detect the selected device type automatically and register it to

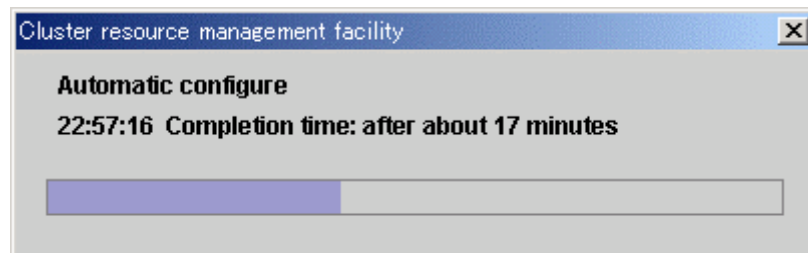
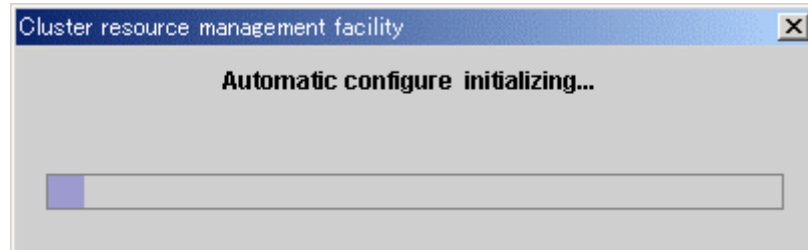
the resource database.

Cancel button

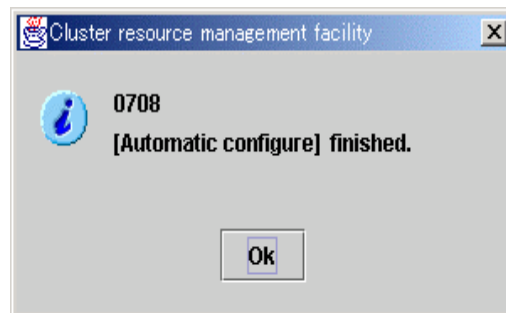
Click this button to cancel processing and exit the screen.

2. Select the device type, and click the *Continue*.

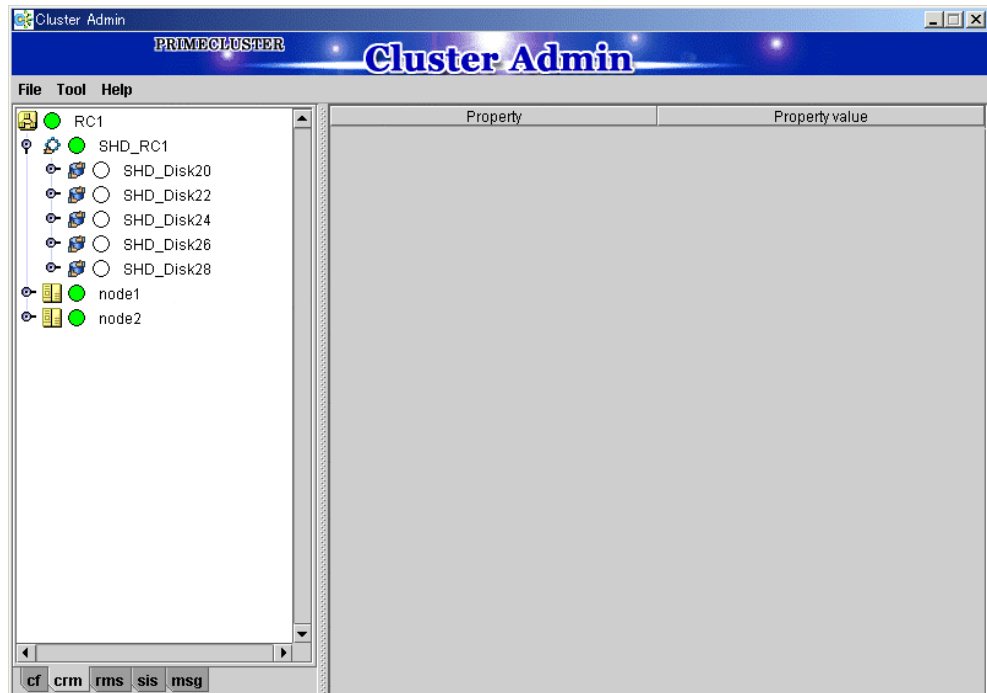
Processing is executed according to the following flow:



3. When automatic configure is completed, the following message is displayed:



4. When the initial setup and automatic configure are completed, the following screen appears.



5. When automatic configuration is completed, go to the CRM main window and confirm that the resource registration is completed by checking the following.
 - Whether the disk configuration is different among the nodes.
 - Whether the number of disks in each node differs from the number of shared disk units.
 - Whether the number of shared disk unit resources is less than the actual device configuration.
 - Whether any disks other than shared disk unit is registered as shared disk unit.
 - Whether the number of public LAN resources is less than the actual device configuration.
 - Whether all connected line switching units are displayed.

If the actual device configuration and the resources do not match each other as described above, automatic detection may have been disabled because of one of the following causes:

- There is a connection path failure between a host device and a disk array unit.
- A disk array unit is not ready.
- A network adapter failed.
- A network adapter driver failed.
- A line switching unit is not connected properly.
- A line switching unit is not turned on.

If the resources are not registered correctly, first review the above causes. Then in the CRM main window, select the *Automatic configure* in the *Tool* to re-register the resources.



Note

If a message is displayed in the CRM main window during operation or a message is displayed in the message dialog box entitled "Cluster resource management facility," see the following manuals for details:

- H.5 "Cluster Resource Management Facility Messages"
- D.5 "Failed Resource and Operator Intervention Messages (GUI)"

- D.7 "Shared Disk Connection Confirmation Messages"
- D.8 "Patrol Diagnosis Messages"
- If you want to add, delete, or rename a disk class from the *Global Disk Services* screen after executing automatic configuration from the CRM main window, close the *Cluster Admin* screen.

5.3 Setting Up Power Supply Linkage

If you want to set up power supply linkage, see the "*Machine Administration Guide*."

5.4 Setting Up Shared Disk Connection Confirmation

Shared disk connection confirmation is a function that performs the followings:

- Check that the shared disk is powered.
- Check that the cable is properly connected.
- Detect new shared disks.



Note

If the paths of a disk array unit are multiplexed, and the paths are controlled by a multipath disk control function, shared disk connection confirmation will not detect an error even if an error occurs in part of the multiplexed paths.

If an error is detected in a shared disk unit or if a new shared disk unit is detected, shared disk connection confirmation outputs a message to syslogd(1M) and the CRM main window.

This function allows you to specify whether or not RMS activation is to be suppressed in the node in which the failure was detected. If a failure is detected in a shared disk unit, the userApplication might not operate normally and user resources in that shared disk unit might become damaged. It is therefore recommended that you specify that RMS activation should be suppressed if a failure is detected. After PRIMECLUSTER is installed, shared disk connection confirmation is initially disabled by default. To change this, follow the procedures described below.



Note

- Set up shared disk connection confirmation after the initial setup of the Cluster Resource Management facility is completed.
- To view the manual pages of each command, add "/etc/opt/FJSVcluster/man" to the MANPATH variable.

■ Enabling shared disk connection confirmation

Take the following steps on each node. Shared disk connection confirmation will be executed from the next node startup.

◆ RMS activation is to be suppressed if a failure is detected

1. Add the following to the "RELIANT_INITSCRIPT" environment variable of RMS:

```
/etc/opt/FJSVcluster/bin/clinitscript
```

Example: Add the following to /usr/opt/reliant/bin/hvenv.local.

```
export RELIANT_INITSCRIPT=/etc/opt/FJSVcluster/bin/clinitscript
```
2. Execute the clsetacparam(1M) command.

Example:

```
# /etc/opt/FJSVcluster/bin/clsetacparam -p auto
```

◆ RMS activation is not to be suppressed if a failure is detected

1. Execute the clsetacparam(1M) command.

Example:

```
# /etc/opt/FJSVcluster/bin/clsetacparam -p auto
```


■ **Disabling shared disk connection confirmation**

Take the following steps on each node. Shared disk connection confirmation will not be executed from the next node startup.

◆ **"Suppress RMS activation if an error is detected" was previously configured**

1. Delete the following from the RELIANT_INITSCRIPT environment variable of RMS.

```
/etc/opt/FJSVcluster/bin/clinitscript
```

Example: Delete the following from /usr/opt/reliant/bin/hvenc.local.

```
export RELIANT_INITSCRIPT=/etc/opt/FJSVcluster/bin/clinitscript
```

2. Execute the "clsetacparam(1M)" command.

Example:

```
# /etc/opt/FJSVcluster/bin/clsetacparam -p none
```

◆ **"Do not suppress RMS activation if an error is detected" was specified**

1. Execute the "clsetacparam(1M)" command.

Example:

```
# /etc/opt/FJSVcluster/bin/clsetacparam -p none
```



[See](#)

- For details on the RMS environment variables, see "8. Appendix – Environment Variables" in the "*PRIMECLUSTER RMS Configuration and Administration*."
- For details on the "clsetacparam(1M)" command, see the manual page for clsetacparam(1M).

5.5 Setting Up Fault Resource Identification and Operator Intervention Request

The fault resource identification is a function that displays a message to syslogd(1M) and ClusterAdmin if a failure occurs in a resource or node that is registered to a cluster application. After setting the initial configuration of the resource database, specify the settings for enabling fault resource identification and operator intervention request. An example of a message displayed by fault resource identification is shown below.

```
6750 A resource failure occurred.   SysNode:node1RMS  userApplication:app0
Resource:apl1
```

The operator intervention request function displays a query-format message to the operator if a failed resource or a node in which RMS has not been started is found when a cluster application is started. The messages for operator intervention requests are displayed to syslogd(1M) and ClusterAdmin.

```
1421 userApplication "app0" was not started automatically because all SysNodes that
make up userApplication were not started within the prescribed time.
Forcibly start userApplication in SysNode "node1RMS"? (no/yes)
Message number: 1001
Warning: When userApplication is forcibly started, the safety check becomes disabled.
If the operation is used incorrectly, data may be damaged and the consistency may be
lost. Check that userApplication to be forcibly started is not online in the cluster before
executing the forced startup.
```



See

For details on the messages displayed by the fault resource identification function and the messages displayed by the operator intervention request function, see D.5 “Failed Resource and Operator Intervention Messages (GUI)” and D.6 “Failed Resource and Operator Intervention Messages (CLI).”

This section describes procedures for operating fault resource identification and operator intervention request.



Note

- After PRIMECLUSTER is installed, fault resource identification and operator intervention request are initially disabled. The following ClusterAdmin functions are also disabled:
 - Messages for fault resource identification and operator intervention request are not displayed to ClusterAdmin.
 - The list of resources that are currently affected by faults is not displayed in the Resource Fault History screen of ClusterAdmin.
 - The fault history of the resources is not displayed in the Resource Fault History screen of ClusterAdmin.
- To view the manual pages of each command, add "/etc/opt/FJSVcluster/man" to the MANPATH variable.

■ **Enabling the operation of fault resource identification and operator intervention request**

1. Execute the “clsetparam(1M)” command and specify the settings for enabling the fault resource identification and operator intervention request. Execute this procedure in any node that is part of the cluster system.

```
# /etc/opt/FJSVcluster/bin/clsetparam -p AppWatch ON
```

2. Execute the “clsetparam(1M)” command, and check that the parameters are set so that the operation of fault resource identification and operator intervention request is enabled. Execute this procedure on any node that is part of the cluster system.

```
# /etc/opt/FJSVcluster/bin/clsetparam -p AppWatch  
ON
```

3. Restart all the operating nodes.
If a node is stopped, the fault resource identification and operator intervention request begin operating in that node from the next node reboot.

■ **Disabling the operation of fault resource identification and operator intervention request**

1. Execute the “clsetparam(1M)” command and specify the settings for disabling the fault resource identification and operator intervention request. Execute this procedure in any node that is part of the cluster system.

```
# /etc/opt/FJSVcluster/bin/clsetparam -p AppWatch OFF
```

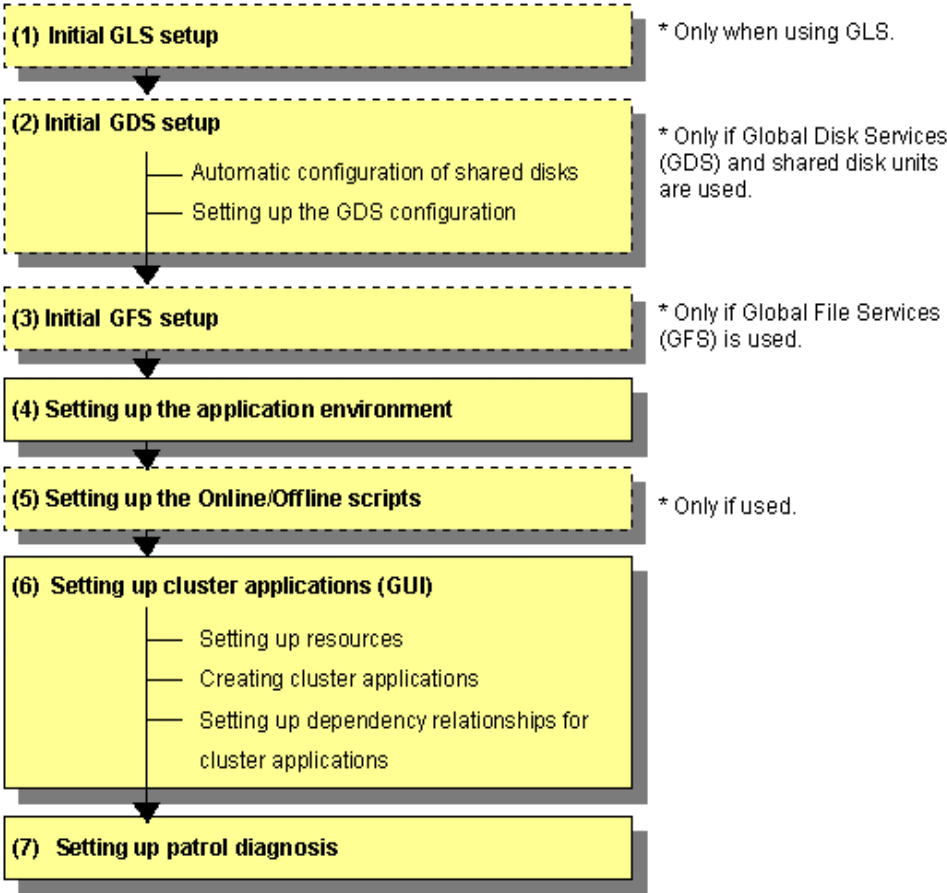
2. Execute the “clsetparam(1M)” command, and check that the parameters are set so that the operation of fault resource identification and operator intervention request is disabled. Execute this procedure on any node that is part of the cluster system.

```
# /etc/opt/FJSVcluster/bin/clsetparam -p AppWatch  
OFF
```

3. Restart all the operating nodes.
If a node is stopped, the fault resource identification and operator intervention request stop operating in that node from the next node reboot.

Chapter 6 Building Cluster Applications

The procedure for building a cluster application is shown below.



Application building procedure and manual reference locations

	Work item	Execution Nodes	Required/optional	Manual reference location*
(1)	6.1 Initial GLS Setup	All nodes	Optional (required when GLS is used)	GLSR GLSM
(2)	6.2 Initial GDS Setup	All nodes	Optional (required when GDS is used)	
	6.2.1 Automatic Configuration of Shared Disks	All nodes	Optional	CF "4.3.1 Automatic resource registration"
	6.2.2 GDS Configuration Setup	All nodes	Optional	GDSG "Chapter 5 Operations"
(3)	6.3 Initial GFS Setup	All nodes	Optional (required when GFS is used)	GFSG
(4)	6.4 Setting Up the Application Environment	All nodes	Required	Manuals for each application
(5)	6.5 Setting up Online/Offline Scripts	All nodes	Optional	RMS "2.8 Environment Setup", "8 Appendix – Environment Variables"
(6)	6.6 Setting Up Cluster Applications	All nodes	Required	"Solaris X Reference Manual Collection," "Solaris Answer Book"
	6.6.1 Setting Up Resources			
	6.6.2 Creating Cluster Applications			
	6.6.3 Setting up Dependency Relationships Between Cluster Applications			
(7)	6.7 Setting Up Patrol Diagnosis	All nodes	Required	

* The names of the reference PRIMECLUSTER manuals are abbreviated as follows:

- **RMS:** PRIMECLUSTER RMS Configuration and Administration
- **CF:** PRIMECLUSTER Cluster Foundation Configuration and Administration
- **GDSG:** PRIMECLUSTER Global Disk Services Configuration and Administration Guide
- **GFSG:** PRIMECLUSTER Global File Services Configuration and Administration Guide
- **GLSR:** PRIMECLUSTER Global Link Services Configuration and Administration Guide: Redundant Line Control Function
- **GLSM:** PRIMECLUSTER Global Link Services Configuration and Administration Guide: Multipath Function

6.1 Initial GLS Setup

This section outlines the steps for configuring Global Link Services (GLS).

6.1.1 GLS Setup

For information on the initial GLS setup, see "Chapter 5 Operation on Cluster System" in the *"PRIMECLUSTER Global Link Services Configuration and Administration Guide: Redundant Line Control Function"* and "Chapter 7 Administration on a Cluster System" in the *"PRIMECLUSTER Global Link Services Configuration and Administration Guide: Multipath Function."*

This section describes how to set up "logical IP takeover of the NIC switching mode" that GLS (redundant line control function) provides. This procedure is described based in the example below.

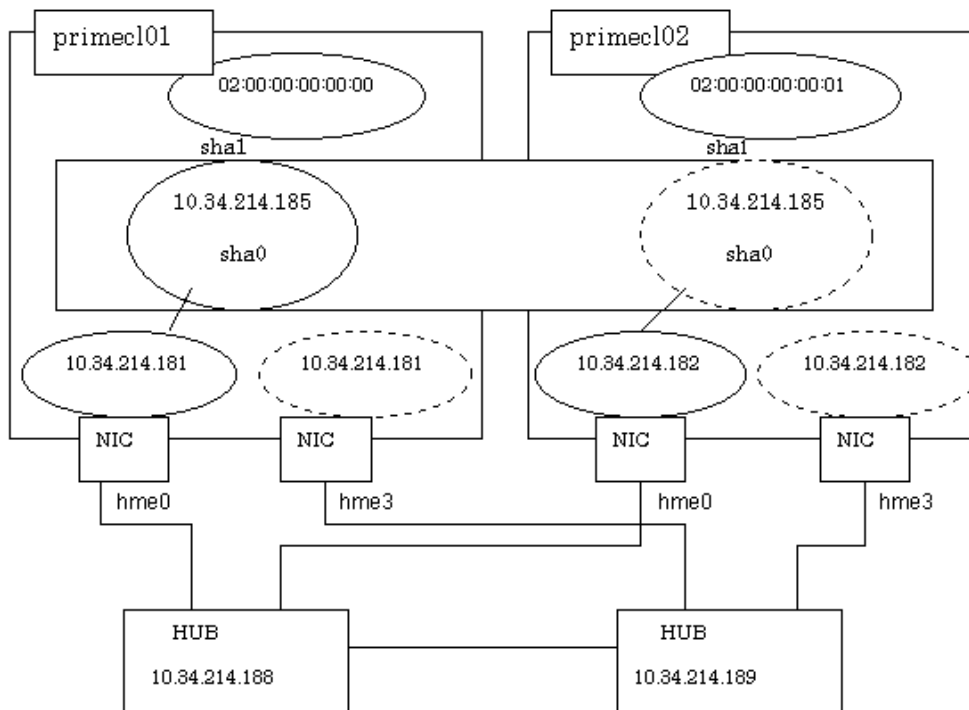


Note

You can use PRIMECLUSTER "takeover network" and GLS "IP address takeover" together in a same cluster system; however, you cannot configure them on the same interface. If this occurs, communication using takeover IP addresses is disabled.

For example, if you select hme1 as the interface when you set up the PRIMECLUSTER "takeover network," do not set hme1 in the GSL environment settings (do not specify hme1 using "-t" option of the "hanetconfig create" command).

The setup values correspond to those on the A.8.2 "GLS Configuration Worksheet."



◆ Operation Procedure:

- If the OPERATING node is [HOST-primecl01]
 1. Set up the virtual interface.

In the underlined parameter, specify the physical IP address of the node.

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m d -i
10.34.214.185 -e 10.34.214.181 -t hme0,hme3
```

Check that the virtual interface has been set up correctly.

```
# /opt/FJSVhanet/usr/sbin/hanetconfig print
```

2. Set up the inter-hub monitoring facility.

In the underlined parameter, specify the IP addresses of the hubs to be monitored.

```
# /opt/FJSVhanet/usr/sbin/hanetpoll create -n sha0 -p
10.34.214.188,10.34.214.189 -b off
```

Check that the facility has been set up correctly.

```
# /opt/FJSVhanet/usr/sbin/hanetpoll print
```

3. Set up the standby patrol function.

In the underlined parameter, specify the MAC address using the format 02:xx:xx:xx:xx:xx. Specify the address so that the values of the two nodes are not the same.

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha1 -m p -a_
02:00:00:00:00:00 -t sha0
```

Check that the facility has been set up correctly.

```
# /opt/FJSVhanet/usr/sbin/hanetconfig print
```

4. Register the node to the cluster resources.

```
# /opt/FJSVhanet/usr/sbin/hanethvrsc create -n sha0
```

Check that the registration has been set up correctly.

```
# /opt/FJSVhanet/usr/sbin/hanethvrsc print
```

- **If the standby node is [HOST-primecl02]**

1. Set up the virtual interface.

In the underlined parameter, specify the physical IP address of the node.

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m d -i
10.34.214.185 -e 10.34.214.182 -t hme0,hme3
```

Check that the virtual interface has been set up correctly.

```
# /opt/FJSVhanet/usr/sbin/hanetconfig print
```

2. Set up the inter-hub monitoring facility.

In the underlined parameter, specify the IP addresses of the hubs to be monitored.

```
# /opt/FJSVhanet/usr/sbin/hanetpoll create -n sha0 -p
10.34.214.188,10.34.214.189 -b off
```

Check that the facility has been set up correctly.

```
# /opt/FJSVhanet/usr/sbin/hanetpoll print
```

3. Set up the standby patrol function.

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha1 -m -a
02:00:00:00:00:01 -t sha0
```

Check that the facility has been set up correctly.

```
# /opt/FJSVhanet/usr/sbin/hanetconfig print
```

4. Register the cluster resources.

```
# /opt/FJSVhanet/usr/sbin/hanethvrsc create -n sha0
```

Check that the resources have been set up correctly.

```
# /opt/FJSVhanet/usr/sbin/hanethvrsc print
```

◆ Post-setup processing

After the OPERATING and STANDBY node setup is done, create the GLS resources, and register them to the cluster application.

For details, see 6.6.1.4 "Creating GLS Resources" and 6.6.2 "Creating Cluster Applications."



See

For information on GLS (redundant line control function) and other operation modes, see "Appendix B Examples of Setting Up" in the *"PRIMECLUSTER Global Link Services Configuration and Administration Guide: Redundant Line Control Function."*

6.1.2 Setting Up Web-Based Admin View When GLS Is Used

To use Web-Based Admin View in a network that was made redundant with GLS, you must set up Web-Based Admin View after setting up the NIC switching mode or the fast switching mode.



See

For setup details, see "2.3 Setup with GLS" in the *"PRIMECLUSTER Web-Based Admin View Operation Guide."*

6.2 Initial GDS Setup

Take Use the following steps to configure Global Disk Services (GDS). If shared disk units are to be used, you are recommended to use GDS to manage the shared disk units.



Note

If you plan to add, delete, or rename a disk cluster from the Global Cluster Services screen, close the ClusterAdmin screen before starting the operation.

6.2.1 Automatic Configuration of Shared Disks

Before setting up GDS, you must have configured the shared disks using automatic configuration. If the disk units were already configured with automatic configuration in 5.2.3.2 "Automatic Configuration," skip this operation.



Note

If disk units are not set up for automatic configuration during the initial setup or if a shared disk unit was added after the initial configuration setup, execute automatic configuration of disk units before the GDS setup.

6.2.1.1 Executing Automatic Configuration

After setting up the disk units according to the procedure described in 3.2.2 "Setting Up Disk Units," either execute *Automatic configure* from the Tools menu of the CRM main window in ClusterAdmin, or execute the following command in any one of the nodes in the cluster system:

```
# /etc/opt/FJSVcluster/bin/clautoconfig -r
```



Note

If disk units were specified during automatic resource registration in 5.2.3.1 "Initial Configuration Setup," the resources have already been created. If you want to check whether the disk units were registered as resources, you can reexecute automatic resource registration.



See

For details, see the manual page for the "clautoconfig(1M)" command or "4.3.1 Automatic resource registration" in the *"PRIMECLUSTER Cluster Foundation Configuration and Administration."*

6.2.2 GDS Configuration Setup

The GDS setup operations are described below.

These setup operations can be performed in any sequence.

- 6.2.2.1 "Setting Up System Disk Mirroring"
Set up system disk mirroring in both nodes, and then restart both nodes.
- 6.2.2.2 "Setting Up Shared Disks"

Set up the shared disk volumes.

6.2.2.1 Setting Up System Disk Mirroring

Take the following setup procedures to enable system disk mirroring.

The setup values correspond to the values that were specified in the A.9.1 "System Disk Mirror Setup Worksheet." In the operation procedure, the "System Disk Mirror Setup Worksheet" is abbreviated as "worksheet."



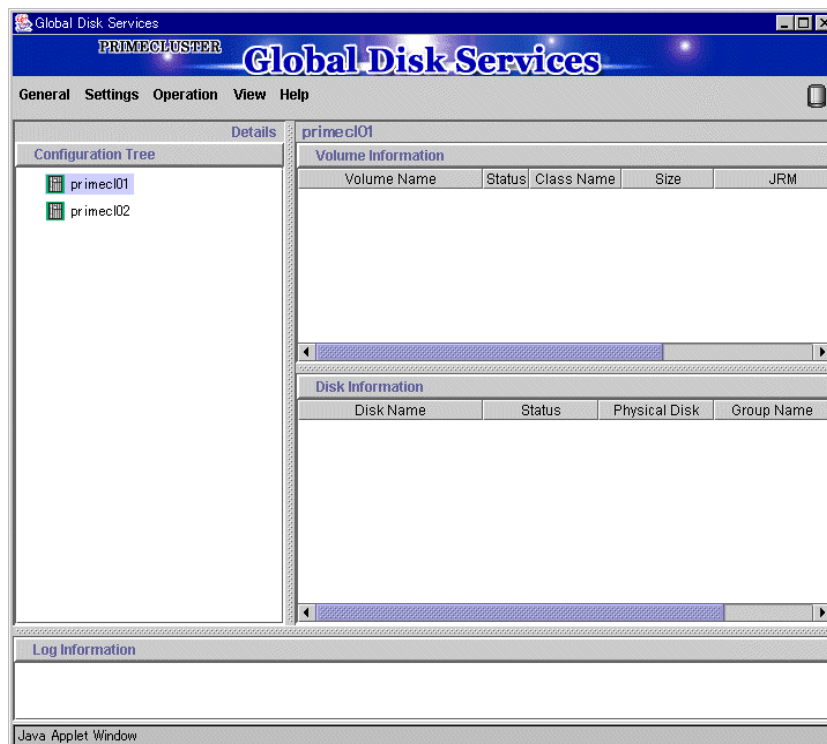
See

For setup details, see "5.2.1 System Disk Settings" in the "*PRIMECLUSTER Global Disk Services Configuration and Administration Guide*."

- **Operation Procedure:**

1. Select *Global Disk Services* at the Web-Based Admin View top screen.

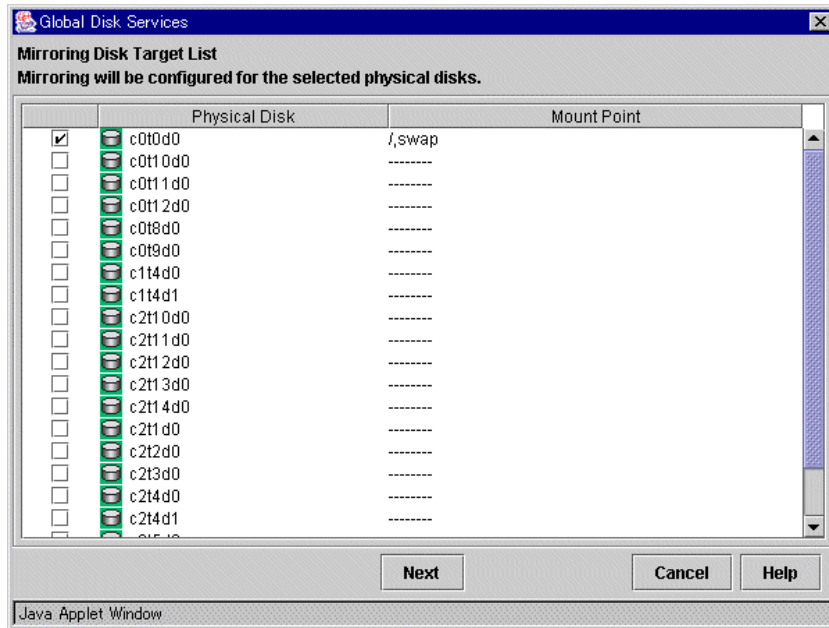
The GDS window is displayed.



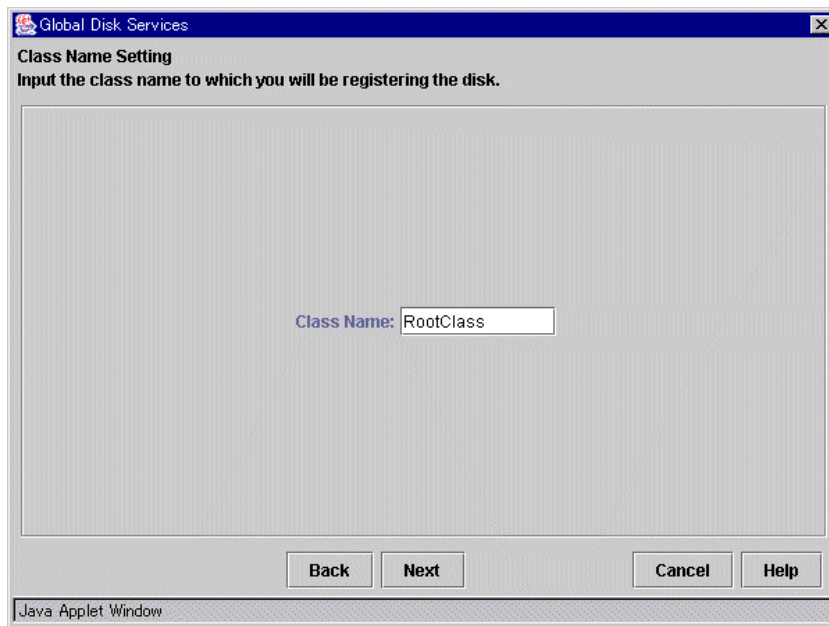
2. Select the host name, click the *Settings* menu, and select *System Disk Configuration*.

A list of disks that can be used for mirrored disks for the specified host is displayed.

Select the system disk ("Physical disk name" on the worksheet), and click *Next*.



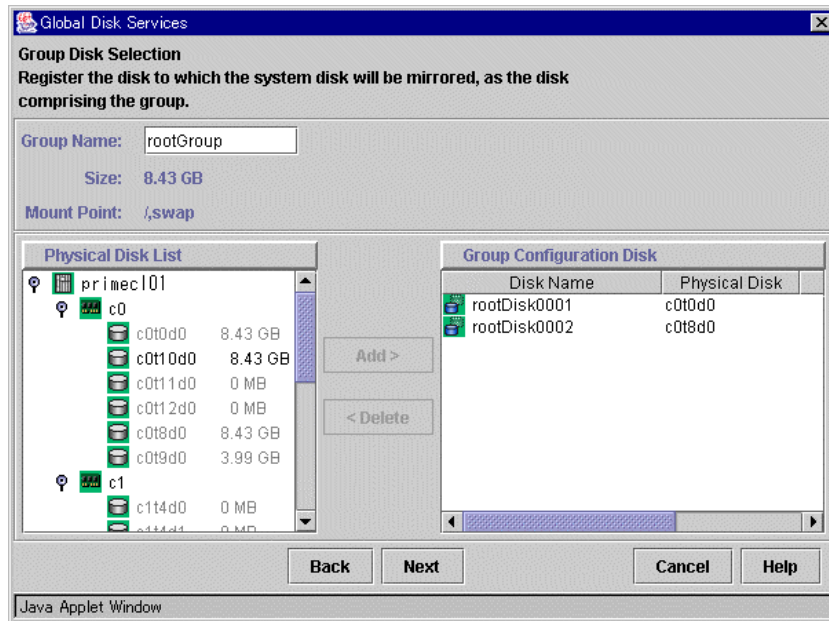
3. Configure class name of the root class.
Enter the class name ("Class name" on the worksheet) of the root class, and click *Next*.



Note

Specify the class name so that the class name of the root class is not duplicated in any cluster node.

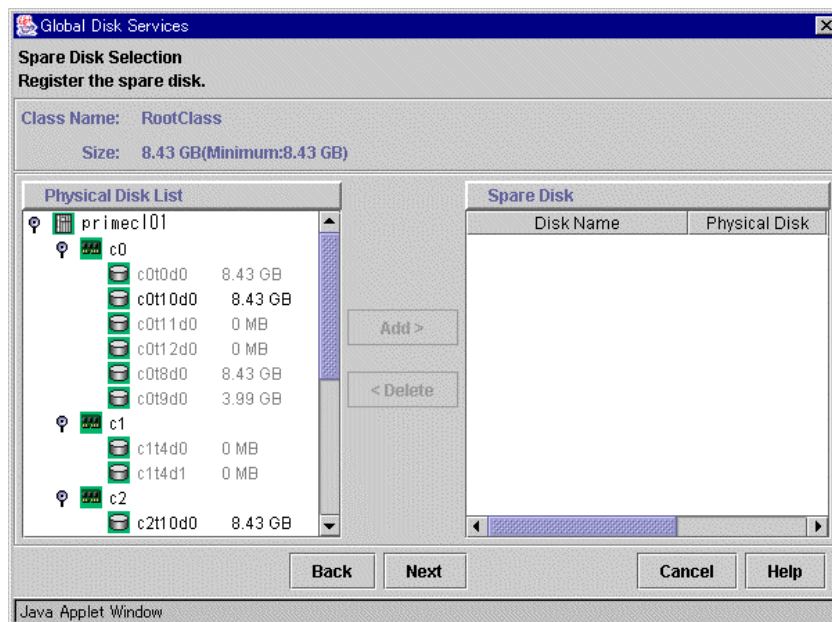
4. Add a mirror disk to the group.
Enter the "group name" ("Group name" on the worksheet), then from the "Physical disk list," select the "mirror disk" ("Mirror disk name" on the worksheet) for the system disk, and click *Add*.
Check that the "mirror disk" that was selected is displayed in "Group Configuration Disk," and then click *Next*.



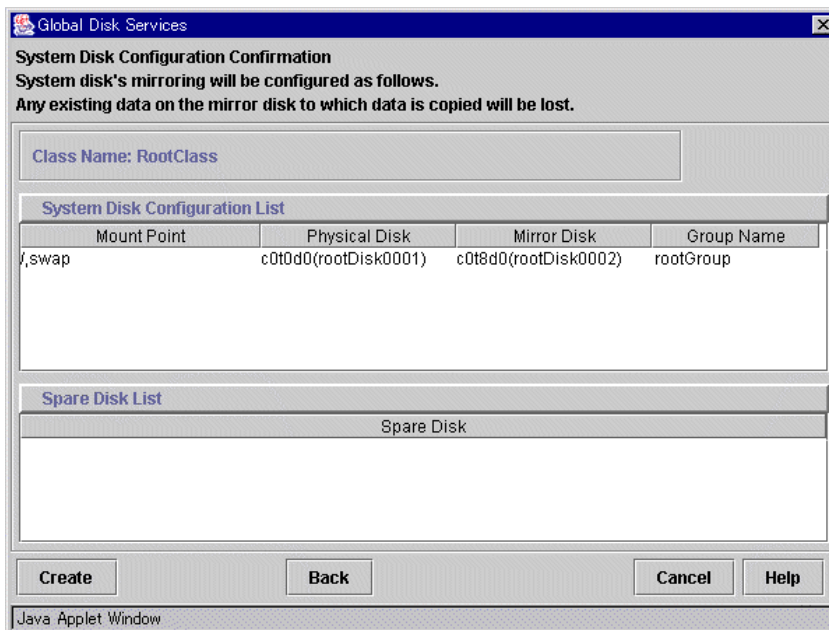
5. Select a spare disk ("Spare disk" on the worksheet) from the physical disk list, and click *Add*.

Check that the spare disk that was selected is registered to "Spare disk," and then click *Next*.

If a spare disk is unnecessary, go to Step 6.



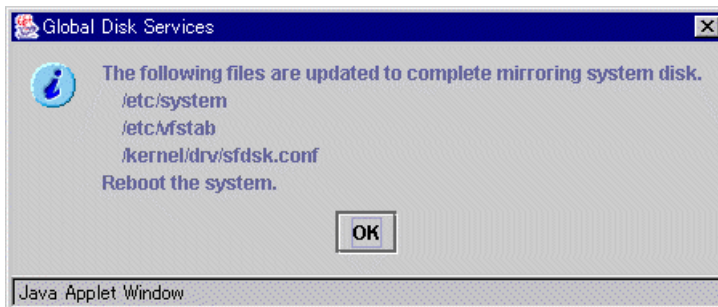
6. Check the system disk configuration.
Check the physical disk name and the mirror disk name, and then click *Create*.



After creation of the system disk is completed, the following screen is displayed.

Check the screen contents, and then click *OK*.

Set up mirroring for the system disk of primecl02 on each node, and then, restart all the nodes.



You must start the system in multiuser mode.

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



Note

GFS partition in the system disk

If a GFS local file system is using a partition in the system disk, you need to change the following for the partition after the system disk setup is completed but before the system is restarted.

- Configuration changes in the partition information
For information on the setup change procedure, see the "PRIMECLUSTER Global File Services Configuration and Administration Guide" or the manual page for the "sfxadm(1M)" command.
- /etc/vfstab file modification
Change the device special file names from special file names of the physical slices to special file names of the logical volumes.

The GFS local file system cannot be used as /(root), /usr, /var, or /opt. Also partitions in the system disk cannot be used by a GFS shared file system. For details, see the "PRIMECLUSTER Global File Services Configuration and Administration Guide."

6.2.2.2 Setting Up Shared Disks

Set up the shared disks according to the following procedures:

- Volume setup
- File system setup

■ Volume setup

There are four types of volumes:

- a. Single volume
- b. Mirror volume
- c. Striped volume
- d. Volume created in a concatenation group

This section separately describes the volume setup procedures for a single volume (a) and for other volumes (b, c, d). For details, see "Chapter 5 Operations" in the "*PRIMECLUSTER Global Disk Services Configuration and Administration Guide*."

The values to be set for the individual items correspond to the values in the A.9.2 "GDS Configuration Worksheet."



Note

If you plan to add, delete, or rename a disk cluster from the GDS window, close the ClusterAdmin screen before starting the operation.

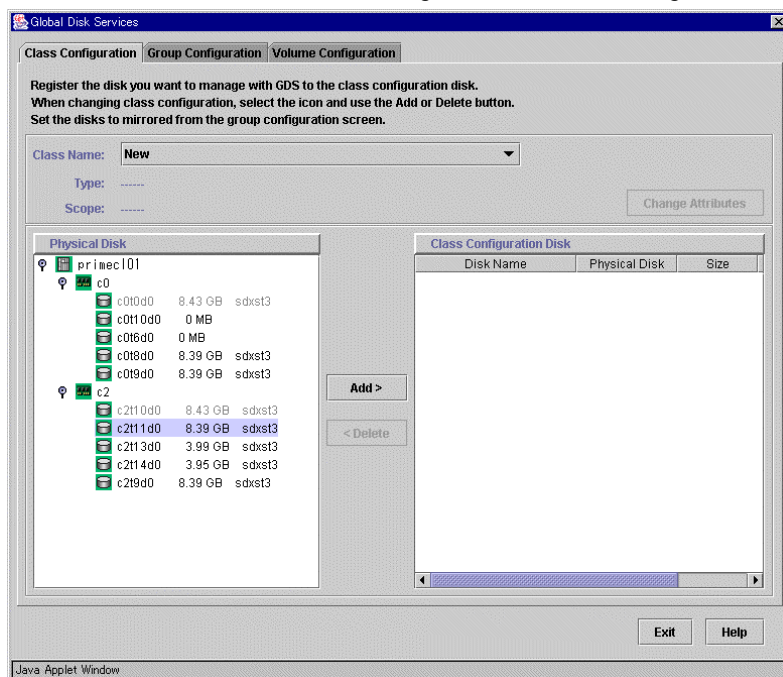
◆ Single volume setup

If you are not using a single volume, this setup is unnecessary.

● Operation Procedure:

1. Disk class creation and physical disk registration

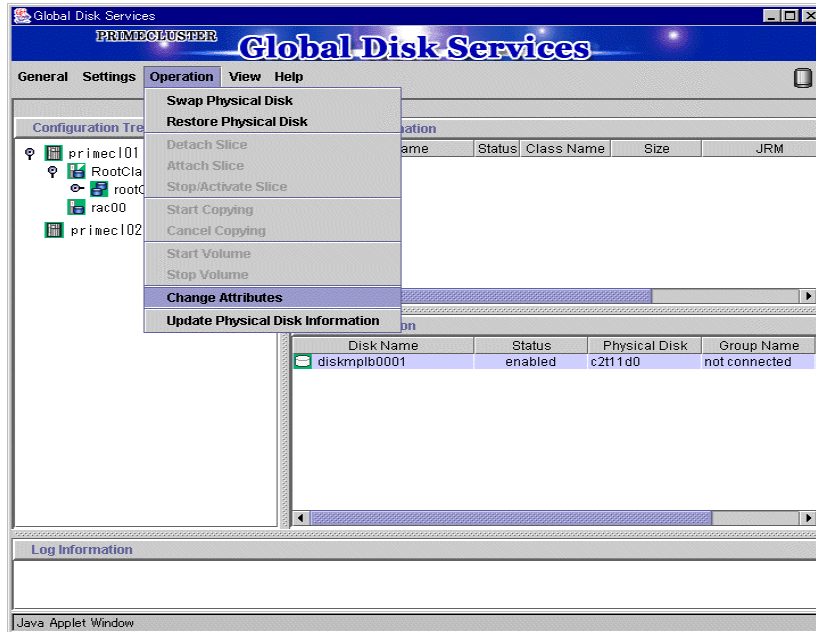
At the GDS window, select *Class Configuration* from the *Settings* menu.



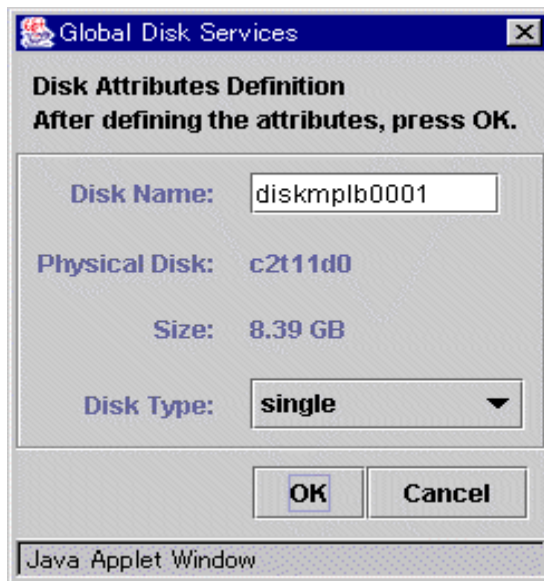
At the above screen, select the physical disk to be registered from the "*Physical Disk*" list, and then click *Add*. When *Add* is clicked, the class attribute definition screen opens. Enter the *Class name* but do not change the *Type* value (leave the value as "shared"). Then click *Exit*.

2. Disk type attribute setup

At the GDS window, select the disk that was registered in Step 1 from the disk information field, and select *Operation -> Change Attributes* from the menu bar.



Set *Disk Type* to "single," and then click *OK*.

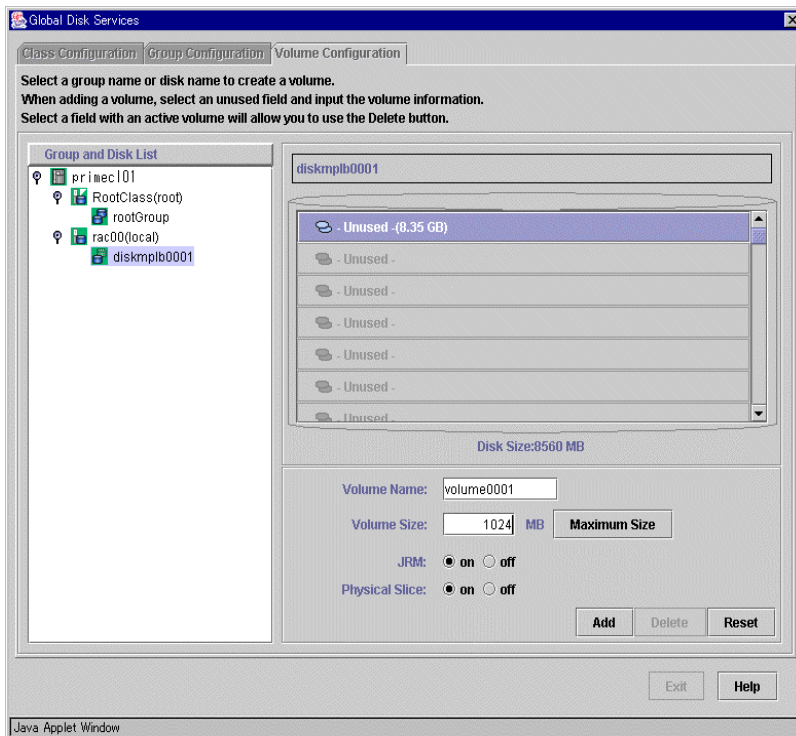


3. Volume creation

Select *Settings -> Volume Configuration*, and then select the disk that was registered in Step 1 from the *Group and Disk List*. Select "Unused" in the volume diagram, and enter the "Volume Name," the "Volume Size," and the volume attributes.

Click *Add* to enable the settings.

Check the settings, and then click *Exit*.



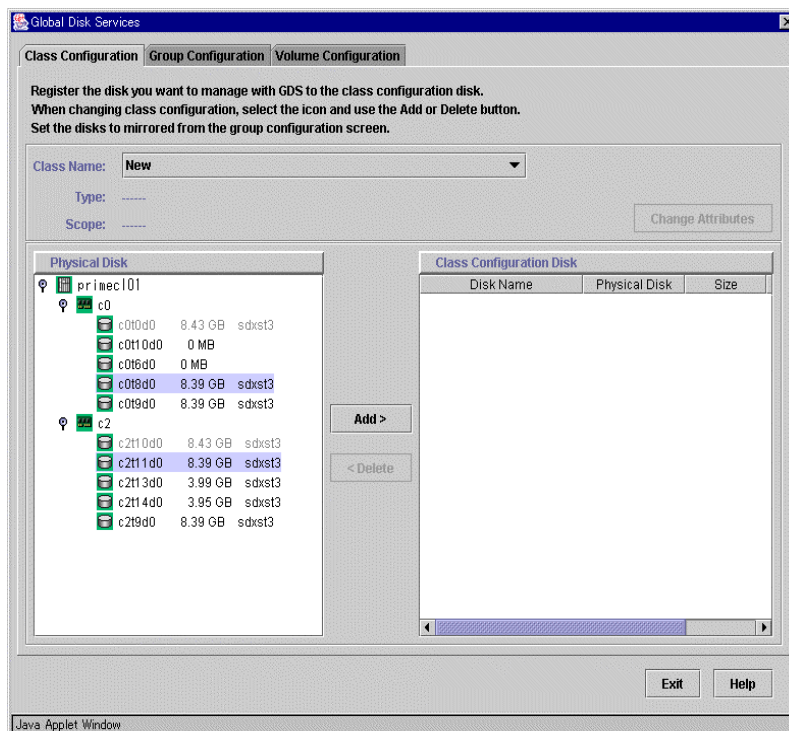
◆ **Setup for other volumes**

If you are using only a single volume, this setup is unnecessary.

● **Operation Procedure:**

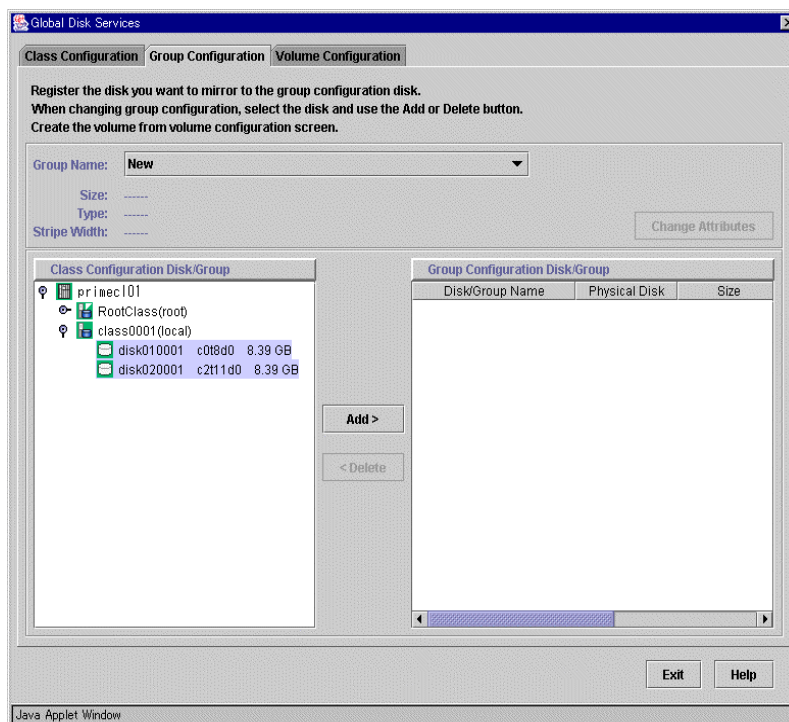
1. Creating disk classes and registering physical disks

At the GDS window, select *Class Configuration* from the *Settings* menu.



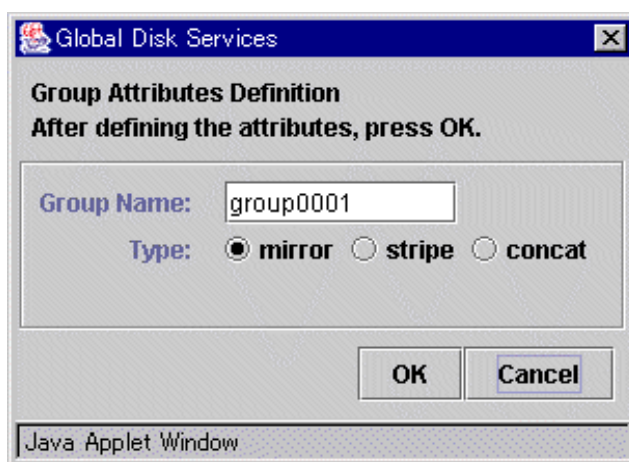
At the above screen, select the physical disk to be registered from the *Physical Disk* list, and then click *Add*. When *Add* is clicked, the class attribute definition screen opens. Enter the "Class name" but do not change the "Type" value (leave the value as "shared"). Then click *Exit*.

2. Setting up the disk group configuration
Click the *Group Configuration* tab.



At the above screen, select the disk to be added to the group from the *Class Configuration Disk/Group* list, and then click *Add*.

Enter the "Group Name" and "Type" in the group attribute definition screen, and then click *Exit*.

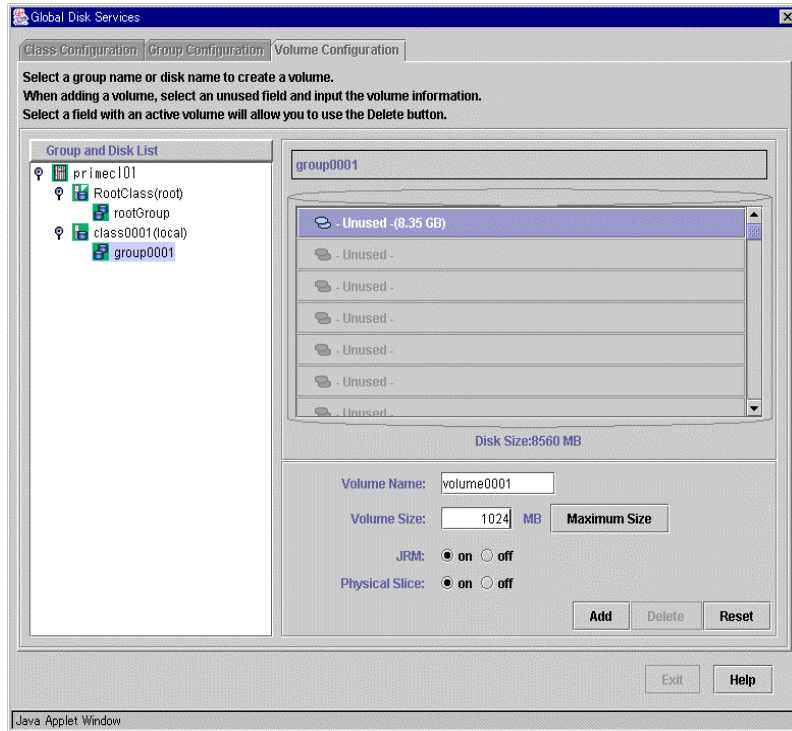


3. Creating a volume

Click the *Volume Configuration* tab, and select the group that was created in Step 2 from the *Group and Disk List*. Select *Unused* in the volume diagram, and enter the "Volume Name," the "Volume Size," and the volume attributes.

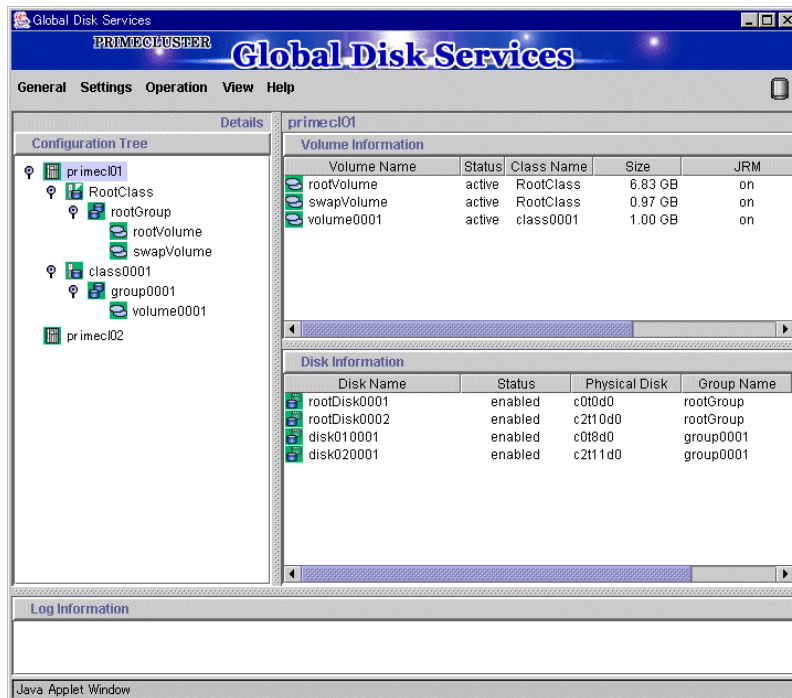
Click *Add* to enable the settings.

Check the setup information, and then click *Exit*.



4. Checking the configuration

The disk configuration is displayed as shown below.



■ File system setup

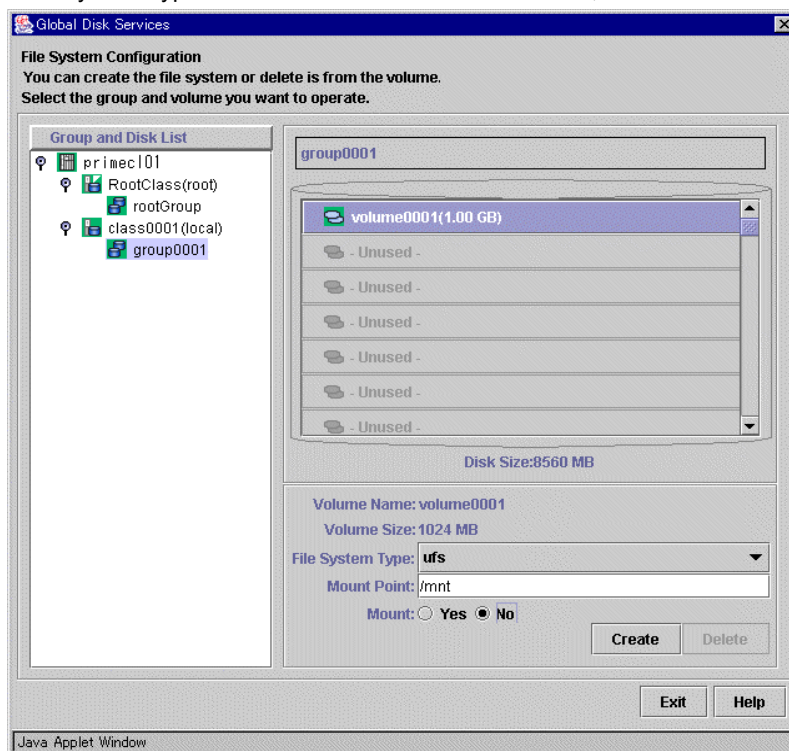
If you are using a volume as a "ufs" file system or a GFS local file system, you can set up the file system from the file system configuration screen. For details, see "5.2.4 File System Configuration" in the "PRIMECLUSTER Global Disk Services Configuration and Administration Guide."

**Note**

If you set up a file system according to this procedure, the entries of the created file system are added to the `/etc/vfstab` file. To use the created file system as an Fsystem resource, you must modify the entries that were added to the `/etc/vfstab` file. For details, see 6.6.1.2 "Creating Fsystem Resources."

- **Operation Procedure:**

1. At the GDS window, select *File System Configuration* from the *Settings* menu, enter the "File System Type" of the volume and other information, and then click *Create*.



2. To exit the *File System Configuration*, click *Exit*.

6.3 Initial GFS Setup

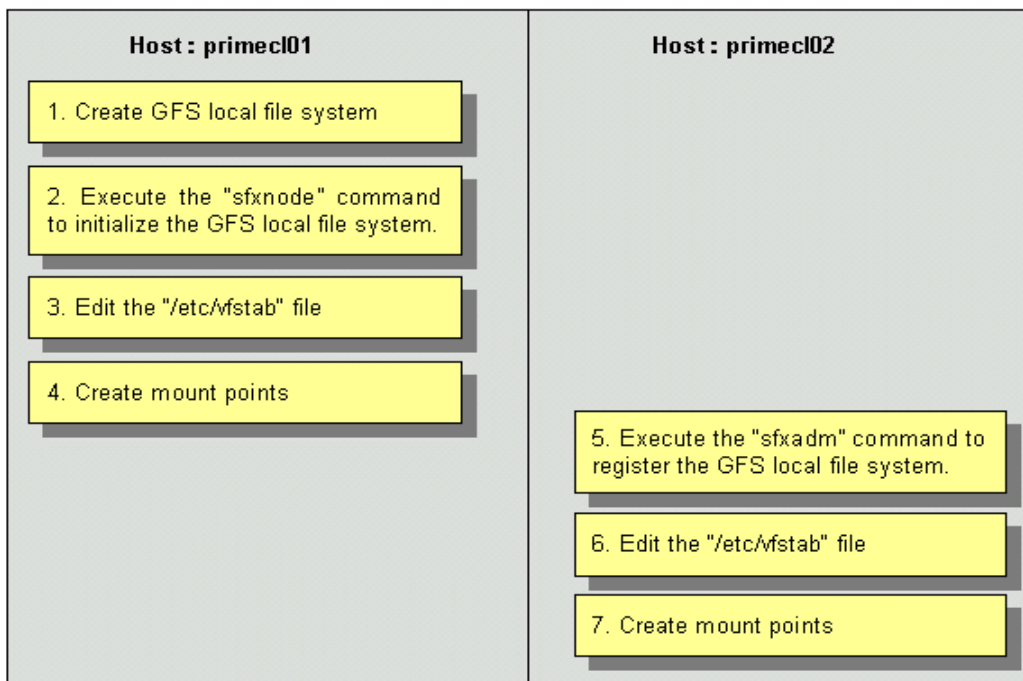
For a Global File Services (GFS) local file system to be created on the Global Disk Services (GDS) volume, there must be a GDS volume and that volume must be active. If the volume is stopped, start the volume.



See

For information on the volume startup procedure, see "4.2.3 Operation" or "D.4 sdxvolume - Volume operations" in the "*PRIMECLUSTER Global Disk Services Configuration and Administration Guide*."

To use the GFS Local File System in standby operation, set up GFS according to the flow shown below.



The device name and mount points that are specified here correspond to the values on the A.8.1 "GFS Local File System Setup Worksheet."

- **Operation Procedure:**

1. Create the GFS Local File System. [Execute on the primecl01 host.]
Create a Local File System of the file system type supported by GFS. (The file system can also be created from the GDS screen.)

```
# sfxnewfs /dev/sfdsk/class0001/rdsk/volume0001
# sfxnewfs /dev/sfdsk/class0001/rdsk/volume0002
```

Get the hostid in primecl02.

```
# hostid
80f175ca
```

2. Execute initial setup of the GFS Local File System according to the following procedure. [Execute on the primecl01 host.]

```
# sfxnode -a -n primecl02 -i 80f175ca
/dev/sfdsk/class0001/rdsk/volume0001

# sfxnode -a -n primecl02 -i 80f175ca
/dev/sfdsk/class0001/rdsk/volume0002
```

3. Edit the /etc/vfstab file. [Execute on the primecl01 host.]
Using a text editor like vi, add the GFS local file system entries to the /etc/vfstab file.
Make sure that each line begins with "#RMS#".

```
#RMS#/dev/sfdsk/class0001/dsk/volume0001
/dev/sfdsk/class0001/rdsk/volume0001 /disk1 sfxfs - no -

#RMS#/dev/sfdsk/class0001/dsk/volume0002
/dev/sfdsk/class0001/rdsk/volume0002 /disk2 sfxfs - no -
```

4. Create the mount points. [Execute on the primecl01 host.]

```
# mkdir /disk1

# mkdir /disk2
```

5. Register the GFS Local File System. [Execute on the primecl02 host.]

```
# sfxadm -A /dev/sfdsk/class0001/rdsk/volume0001

# sfxadm -A /dev/sfdsk/class0001/rdsk/volume0002
```

6. Edit the /etc/vfstab file. [Execute on the primecl02 host.]
Using a text editor like vi, add the GFS local file system entries to the /etc/vfstab file.
Check that each line begins with "#RMS#".

```
#RMS#/dev/sfdsk/class0001/dsk/volume0001
/dev/sfdsk/class0001/rdsk/volume0001 /disk1 sfxfs - no -

#RMS#/dev/sfdsk/class0001/dsk/volume0002
/dev/sfdsk/class0001/rdsk/volume0002 /disk2 sfxfs - no -
```

7. Create the mount points. [Execute on the primecl02 host.]

```
# mkdir /disk1

# mkdir /disk2
```

6.4 Setting Up the Application Environment

Configure an environment for the applications to be used in the PRIMECLUSTER system.

The environment configuration for the individual applications may involve registering resources to the PRIMECLUSTER system.

There are also products that require you to set up an environment that uses the shared disk units and takeover networks that were set in this chapter.



[See](#)

See the manuals for the individual applications.

6.5 Setting Up Online/Offline Scripts

Create Online and Offline scripts to start and stop ISV applications and user applications in line with the userApplication state transition.

Set the created scripts as Cmdline resources and set those resources in userApplication.

An Online script is started when userApplication is switched to Online.

An Offline script is started when userApplication is switched to Offline.

This section presents script examples and describes notes on script creation.

■ Sample scripts

This section shows samples of the online and offline scripts, which are set as Cmdline resources.

```
#!/bin/ksh
#
# Script.sample
#   Sample of Online/Offline Script
#
# Copyright(c) 2002 FUJITSU LIMITED.
# All rights reserved.
#
# $1 -c : OnlineScript
#   -u : OfflineScript

if [[ $1 = "-c" ]]; then
    # Start your application
elif [[ $1 = "-u" ]]; then
    # Stop your application
else
    # Default operation
    exit 1 # Error
fi
exit 0
```

The above Script sample covers both the Start script and the Stop script.

- Start script \$FULL_PATH/Script.sample -c
- Stop script \$FULL_PATH/Script.sample -u

■ Notes on script creation

● Exit codes

The userApplication state transition occurs according to the exit code of the script.

0: Normal termination of the script

The system assumes that state transition of the Cmdline resource was processed normally, and then the userApplication state transition occurs. If all resources that were set to the userApplication are processed normally, the userApplication state transition is processed normally.

Other than 0: Abnormal termination of the script

The system assumes that an error occurred during state transition of the Cmdline

resources, and discontinues the userApplication state transition processing.

- **Timeout**

If script processing is not completed within the specified time, a timeout occurs, script processing is interrupted by the SIGTERM signal, and state transition ends with an error.

Default: 300 seconds

The timeout value can be specified with the TIMEOUT flag value of the Cmdline resources.

When creating the Cmdline resource, you need to set up a timeout value in "Setting up Cmdline Flags" of 6.6.1.1 "Creating Cmdline Resources." If a timeout occurs when a Cmdline resource is used, change the timeout value to an appropriate value according to the instructions in 8.1.3 "Changing Resources."

- **Environment variables**

When the script is executed, the environment variables shown in the table below are set.

Environment variable	Outline
HV_APPLICATION	This variable sets the userApplication name that the resource belongs to. Example) APP0
HV_AUTORECOVER	This variable sets the AUTORECOVER value. For details on AUTORECOVER, see "Setting up Cmdline flags." 0: No is set. 1: Yes is set.
HV_FORCED_REQUEST	This variable sets a value that indicates whether or not forced failover was requested by operator intervention. 0: Forced failover was not requested. 1: Forced failover was requested.
HV_NODENAME	This variable contains the resource name. Example) Cmdline0
HV_OFFLINE_REASON	This variable sets the trigger for bringing the resource Offline. SWITCH: The resource was set to Offline because of a userApplication switchover request (hvswitch). STOP: The resource was set to Offline because of a userApplication stop request (hvutil -f) FAULT: The resource was set to Offline because of a resource fault. DEACT: The resource was set to Offline because of a userApplication deactivate request (hvutil -d) SHUT: The resource was set to Offline because of an RMS stop request (hvshut)
HV_SCRIPT_TYPE	This variable sets the type of script that was executed. Online: Online script Offline: Offline script
HV_LAST_DET_REPORT	This variable sets the state of the current resources. Online: Online state Offline: Offline state Standby: Standby state Faulted: Faulted state Warning: Warning state
HV_INTENDED_STATE	This variable sets the resource state that is expected after state transition is completed. Online: Online state Offline: Offline state Standby: Standby state Faulted: Faulted state Warning: Warning state
NODE_SCRIPTS_TIME_OUT	This variable sets the timeout duration (seconds) of the script. Example) 300

RMS also has other environment variables. For information on the other environment variables, see the files below.

File Names	Contents
hvenv	Environment variable file to be defined in the entire cluster system
hvenv.local	Environment variable file to be defined only in that node



[See](#)

- For details on the RMS environment variable files (hvenv and hvenv.local), see "2.8 Environment Variables" in "*PRIMECLUSTER RMS Configuration and Administration*."
- For details on the RMS environment variables, see "8 Appendix – Environment Variables" in "*PRIMECLUSTER RMS Configuration and Administration*."

6.6 Setting Up Cluster Applications

This section explains how to set up a cluster application by using the cluster application GUI. The terms "userApplication" and "Resource" that appear on the setup screen refer to "cluster application" and "resource," respectively.



Information

- After you finish setting up the cluster application, start the cluster applications. For instructions on starting the application, see 7.2.2.1 "Starting a Cluster Application."
- For instructions on changing a cluster application, see 8.1 "Changing the Cluster Application." For instructions on deleting a cluster application, see 8.9 "Deleting a Cluster Application."

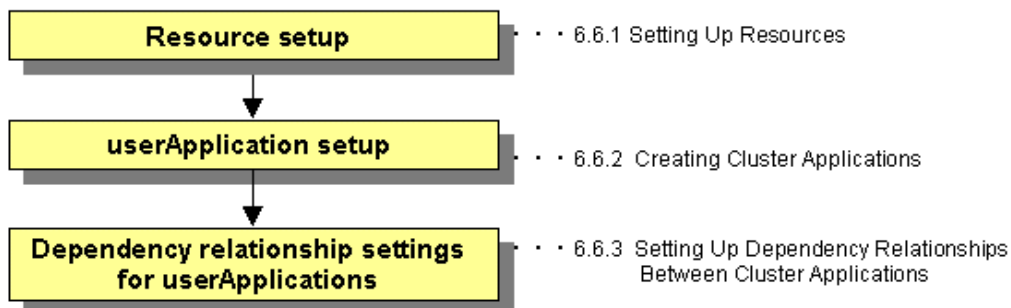


Note

- Set up the cluster application and resources based on the cluster application and resource information in the A.10 "Cluster Application Worksheet," which was created in the planning stage. If you need to change the cluster application after it is created, the worksheet is helpful.
- If you use userApplication Configuration Wizard, the CF remote services (remote file copy and remove command execution) are enabled automatically. For instructions disabling these definitions, see Notes in 5.2.1 "Setting Up CF and CIP."

■ Setting up cluster applications by using GUIs

- **Operation Procedure:**



1. Resource setup
Create all resources that make up the userApplication.
2. userApplication setup
Use all the resources and create the userApplication.



Note

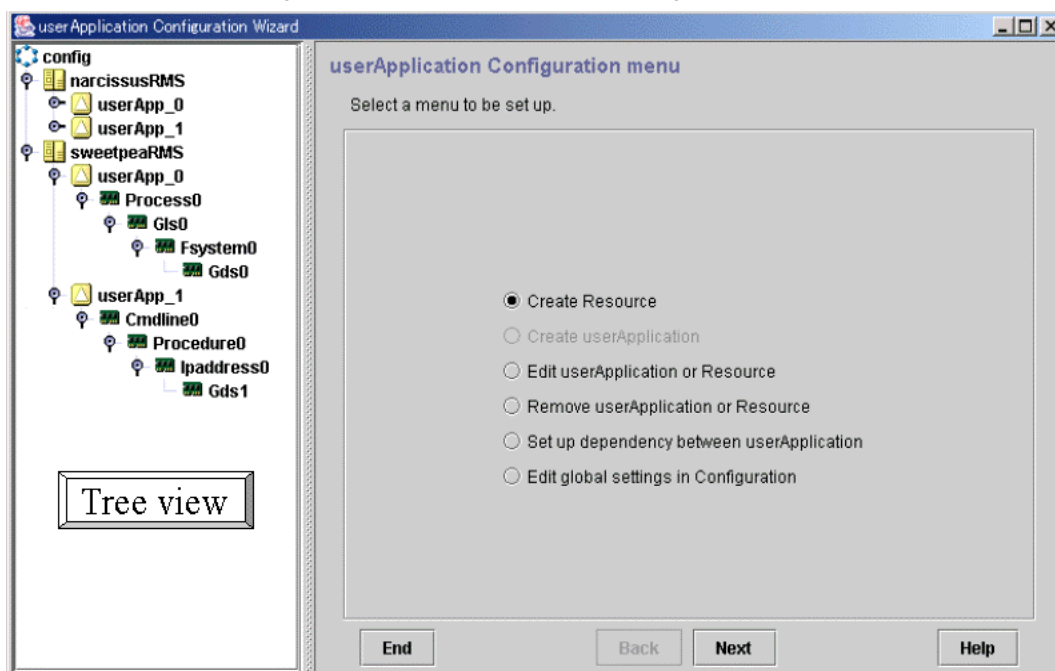
- RMS will not start if there is any remaining resource that is not part of userApplication. Delete unnecessary resources.
 - To create multiple userApplication, repeat steps 1) and 2).
3. Dependency relationship settings for userApplication
Dependency relationship settings are enabled when two or more userApplication are created.
These settings define how each userApplication is controlled on the same cluster node.

◆ **Starting the userApplication Configuration Wizard**

1. At the Web-Based Admin View top screen, select *Global Cluster Services*.
2. At the Global Cluster Services screen, select *userApplication Configuration Wizard*.

● **Explanation of GUI screen and icons**

The userApplication Configuration Wizard screen has the configuration shown below.



The following table shows the icons that are displayed in the tree view of the userApplication Configuration Wizard.

Icon	Description
	Indicates the configuration.
	Indicates that a discrepancy was found in the configuration information. A resource that does not belong to any userApplication or userApplication with no resources was found.
	Indicates SysNode.
	Indicates userApplication.
	Indicates userApplication that was created with the TURNKEY Wizard. The userApplication Configuration Wizard does not allow change and deletion operations for this userApplication and its Resources.
	Indicates a controller. Currently, this icon is not supported.
	Indicates a resource.

6.6.1 Setting Up Resources

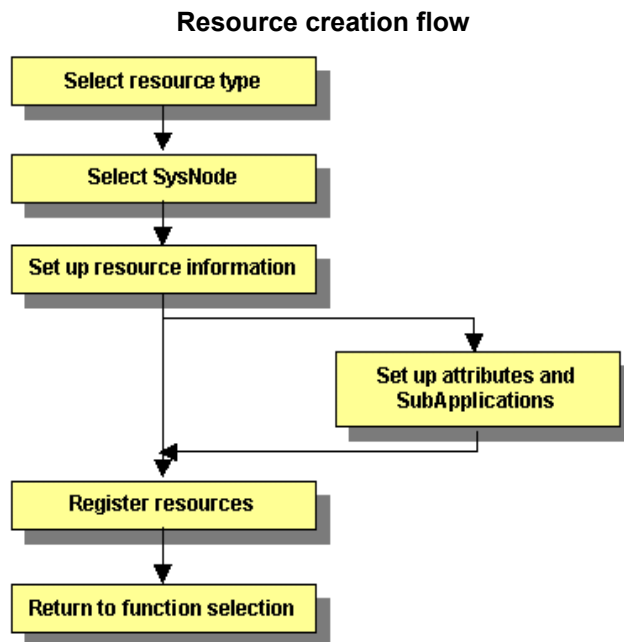
This section explains how to register resources to RMS using the "userApplication Configuration Wizard" screen.

The resources include the following:

- Cmdline resources
- Fsystem resources
- Gds resources
- GlS resources
- Takeover network resources
- Procedure resources
- Process monitoring resources
- Line switching resources (used simultaneously with Netcompo WAN control or Netcompo BCDR)
- Independent software vendor (ISV) resources

CUI (hww) cannot display or operate any configuration that was created by using resources other than those listed above.

The flow of resource creation is shown below.



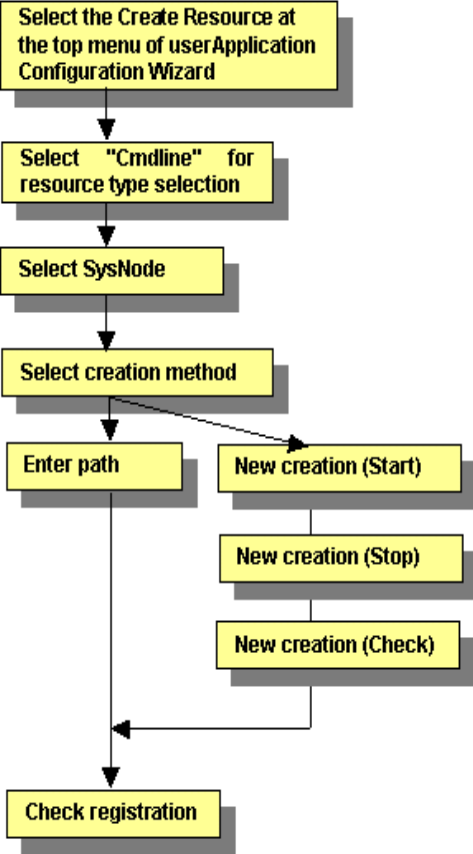
Note

When specifying an association (priority setting) between resources of the same type, create the resource starting from the one with the higher priority.

6.6.1.1 Creating Cmdline Resources

This section describes the procedure for creating Cmdline resources.

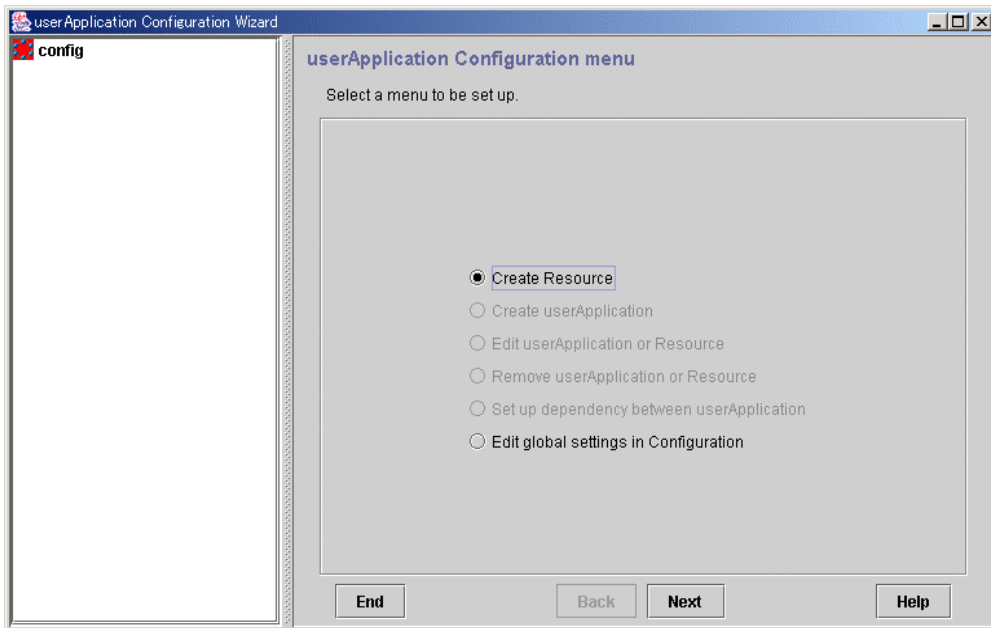
Flow of Cmdline resource creation



■ **Creating resources**

At the top menu of the "userApplication Configuration Wizard," select *Create Resource*.

Top menu of the userApplication Configuration Wizard

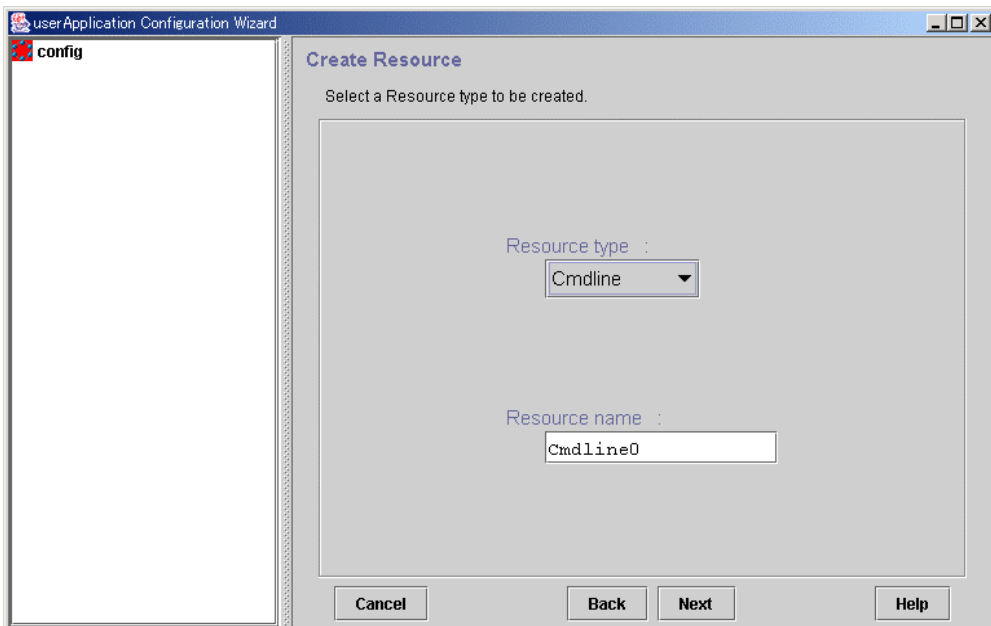


Click Next to go to the "Create Resource" screen.

■ **Selecting the resource type**

Select the type of resource that you want to create.

Create Resource



Resource Type

Select the type of resource to be created from the types described in the table below.

Resource type	Outline
Cmdline	Use this type to set a user-created script file or command as a resource. The resource is required to start or stop the ISV application or application in line with the userApplication state transition, and in the same way, to cause the state transition with the application stop.

Resource type	Outline
Fsystem	Mounts a file system at userApplication startup.
Gds	Sets up a disk class in userApplication. The disk class is defined in Global Disk Services.
Gls	Sets up a takeover IP address in userApplication. The Ipaddress is defined in Global Link Services (network redundancy).
Ipaddress	Sets up a takeover network in userApplication. <ul style="list-style-type: none"> The two types of takeover addresses are takeover IP address and takeover node name.
Procedure	Sets up a state transition procedure in userApplication.
Process	Sets up a user-created program to be monitored by the process monitoring function in userApplication.
Oracle, Nwcl, Nwsv, Nwst	Sets up an ISV application in userApplication.
SH_SWLine	Sets up a line switching unit in userApplication.

Resource Name

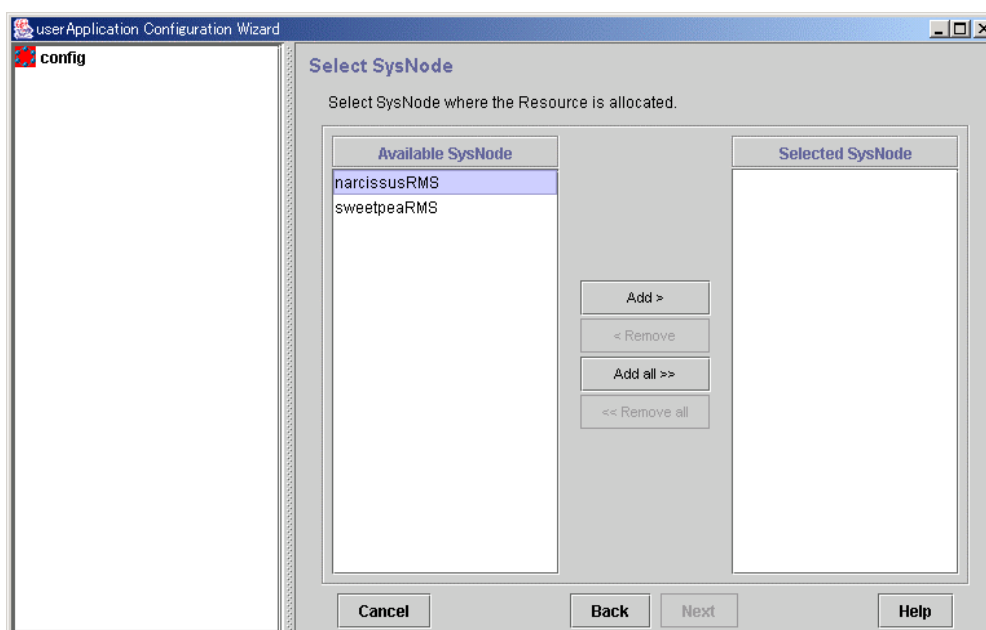
Specify the name of the resource to be created. The input character string must be specified with **up to 18 characters**, starting with an alphabet letter and consisting of only alphanumeric characters and "_" (underscore). If you use a name that has 19 or more characters for the resource name, RMS will not start. Do not use the same name as the Configuration name (config).

Click *Next* to go to the "Select SysNode" screen.

■ Selecting the SysNode

Select the SysNode in which the resource is to exist. SysNode refers to the CIP node name used by RMS.

Select SysNode



Available SysNode

Of the nodes in a cluster system, only the names accessible through Web-Based Admin View are displayed.

Selected SysNode

The SysNode name in which the resource is to exist is displayed. This information is used as filtering information for the interfaces used by each resource.

From the *Available SysNode*, select the SysNode, and then click *Add*. To add all the listed SysNodes, click *Add all*.

To delete a SysNode, select the SysNode to be deleted from *Selected SysNodes*, and then click *Remove*. To delete all listed SysNodes, click *Remove all*.

Click *Next* to go to the "Set up each resource" page.

■ **Selecting the Cmdline creation method**

Cmdline resources are general-purpose resources. By defining three scripts for starting, stopping, and monitoring the user application (program) to be monitored, you can create a resource that matches the purpose.

The scripts correspond to the following processes in RMS

Start script

It starts a program in Online processing.

Stop script

It stops a program in Offline processing.

Check script

This script is started periodically.

It notifies the user program state.

◆ **Exit codes, timeout values, and environment variables of scripts**

When creating a script, note the items described below.

● **Exit codes**

Start/Stop scripts

0: Normal exit

Other than 0: Abnormal exit. The Online or Offline processing fails, and this brings the resource Faulted state.

Check script

It returns the state of userApplication as follows:

0: Online

Value other than 0: Offline

If ALLEXITCODES is set to "Yes," exit codes 2 to 6 indicate a detailed program status other than Offline. For details, see "Setting up Cmdline flags."

● **Timeout**

When script processing does not complete within the specified time, a timeout error occurs.

The Online or Offline processing fails, and this brings the resource state to Faulted.

Default: 300 seconds

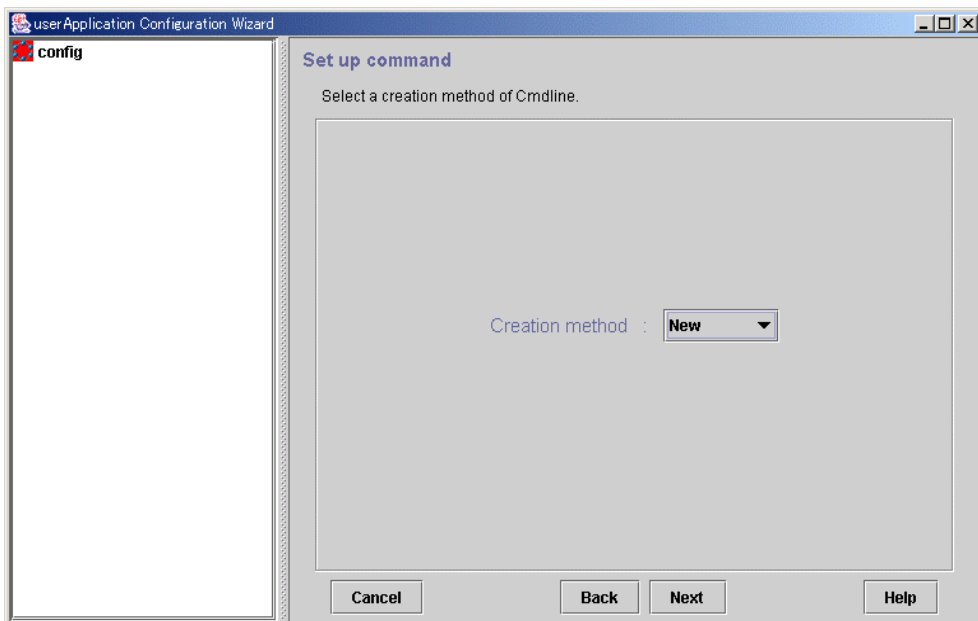
You can change the timeout value by changing the TIMEOUT value. For details, see "Setting Up Cmdline Flags."

● **Environment variables**

For information on environment variables that are set during script execution, see "Environment Variables" in 6.5 "Setting Up Online and Offline Scripts."

Select a method of configuring the script files and commands as the resource.

Cmdline creation



Creation methods

Select the creation method from the following:

- New
You can create a new script file.
- Path Input
You can specify the existing script or command.
Click *Next*.

After completing the setup, click *Next*. This will lead you to the following operation according to the selected item:

- New: "Creating new script files"
- Path input: "Creating scripts by pass input"

◆ Creating new script files

Create new script files.



Note

- The created script files are stored in the "/opt/FJSVwvcuw/scripts/start" directory.
- These script files are not removed even when processing is cancelled during Cmdline creation, or the Cmdline resource or GUI package (FJSVwvcuw) is removed. If you want to remove the files, you need to remove the "/opt/FJSVwvcuw/scripts/start" directory. For example, execute the "rm(1)" command to remove one script file as follows:

```
# rm /opt/FJSVwvcuw/scripts/start/XXXXXXXX
```

To remove the directory, specify "/opt/FJSVwvcuw/scripts/start" or "/opt/FJSVwvcuw."

● Start script creation

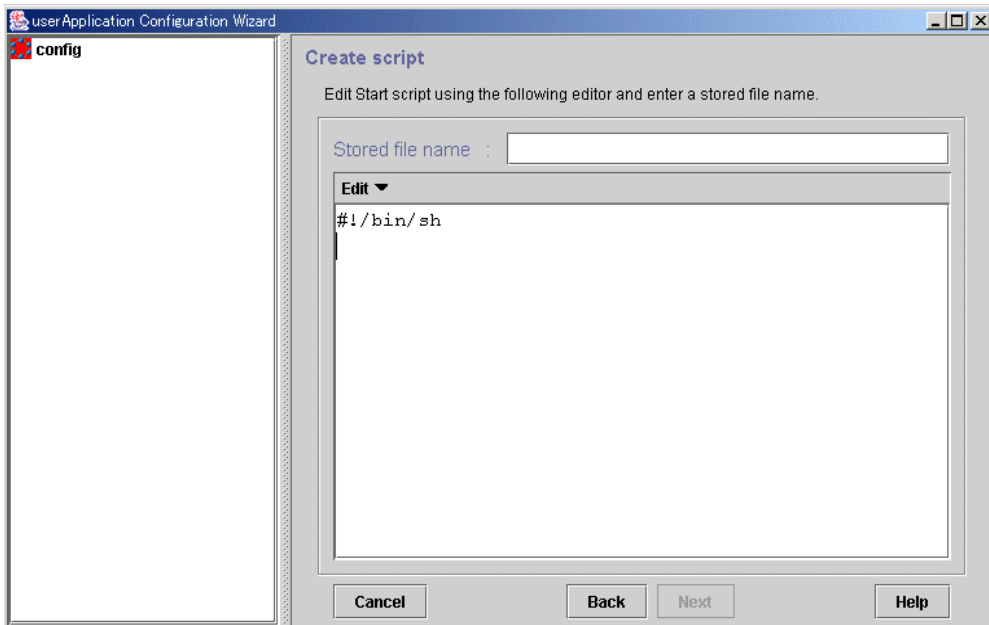
The Cmdline contents can be input directly into the editing area.



Note

- The text copy, cut, and paste operations are enabled only in the editing area. For information on how to edit text, see "Edit area operations," which is described later.
- For information on the exit codes for Start scripts, see "Exit codes, timeout values, and environment variables of scripts."

Start script creation



Stored file name

Specify the file name to be saved.

The following characters cannot be used in the file name or the arguments: back slash ("¥"), tilde ("~"), percent sign ("%"), ampersand ("&"), and at sign ("@").

Even though processing is cancelled or the screen is closed during Cmdline creation, the script files are still stored in the "/opt/FJSV/wvucw/scripts/start" directory. Therefore the scripts can be reused when the Cmdline resources are re-created.



Note

When specifying arguments, separate the arguments with "blank" characters. Since the scripts that can be created in this screen are Bourne shell by default, the following string is displayed at the beginning of the editing area:

```
#!/bin/sh
```

Edit

You can edit scripts from the simplified menu. See "Edit area operations."

Click *Next* to go to "Stop script creation."

- **Example of Start script creation**

In this example, the start command is executed to start the user program.

The command starts the program and then ends.

To ensure that the Start script is not affected by timeout, end the script after startup processing is

executed, as shown in this example.

```
#!/bin/sh
#-----
# Sample
#   Start-script
#
#-----
PATH=/usr/bin:/usr/sbin

# Exit codes for RMS
e_normal=0
e_error=1

CmdPath=/opt/FJSVxxxx/bin/start

if [ ! -x $CmdPath ];then
    exit $e_error
fi

#
# Start the program.
#
$CmdPath
if [ $? -eq 0 ]; then
    Status=$e_normal
else
    Status=$e_error
fi

exit $Status
```

- **Stop script creation**

The Cmdline contents can be input directly into the editing area.

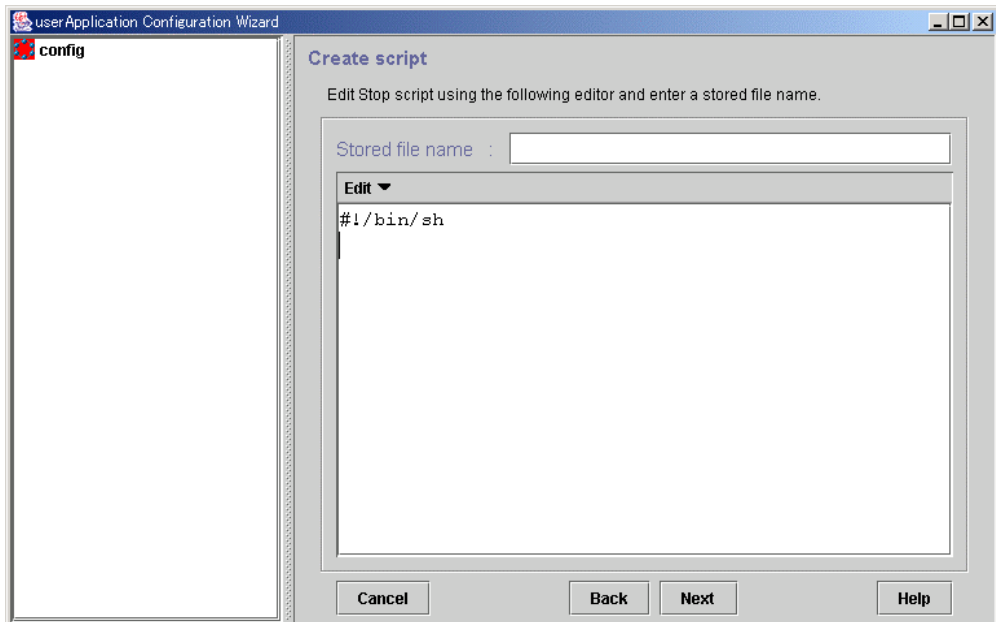


Note

- The created script files are stored in the “/opt/FJSVwvcuw/scripts/stop” directory.
- You can omit setup of this script file. Just click *Next*.
- These script files are not removed even when processing is cancelled during Cmdline creation, or the Cmdline resource or GUI package (FJSVwvcuw) is removed. If you want to remove the files, you need to remove the “/opt/FJSVwvcuw/scripts/stop” directory. For example, execute the “rm(1)” command to remove one script file as follows:


```
# rm /opt/FJSVwvcuw/scripts/stop/XXXXXXXX
```
- For information on the exit codes for Stop scripts, see “Exit codes, timeout values, and environment variables of scripts.”

Stop script creation



Stored file name

Specify the file name to be saved.

The following characters cannot be used in the file name or the arguments: back slash ("¥"), tilde ("~"), percent sign ("%"), ampersand ("&"), and at sign ("@").

Even though processing is cancelled or the screen is closed during Cmdline creation, the script files are still stored in the "/opt/FJSVwwucw/scripts/stop" directory. Therefore the scripts can be reused when the Cmdline resources are re-created.



Note

When specifying arguments, separate the arguments with "blank" characters. Since the scripts that can be created in this screen are Bourne shell by default, the following string is displayed at the beginning of the editing area:

```
#!/bin/sh
```

Edit

You can edit scripts from the simplified menu. See "*Edit area operations*," for details.

Click *Next* to go to "Check script creation."

- **Example of Stop script creation**

In this example, the stop command is executed to stop the user program. The command stops the active program and then ends.

```

#!/bin/sh
#-----
# Sample
# Stop-script
#
#-----
PATH=/usr/bin:/usr/sbin

# Exit codes for RMS
e_normal=0
e_error=1

CmdPath=/opt/FJSVxxxx/bin/stop

if [ ! -x $CmdPath ];then
    exit $e_error
fi

#
# Stop the program.
#
$CmdPath
if [ $? -eq 0 ]; then
    Status=$e_normal
else
    Status=$e_error
fi

exit $Status

```

- **Check script creation**

The Cmdline contents can be input directly into the editing area.

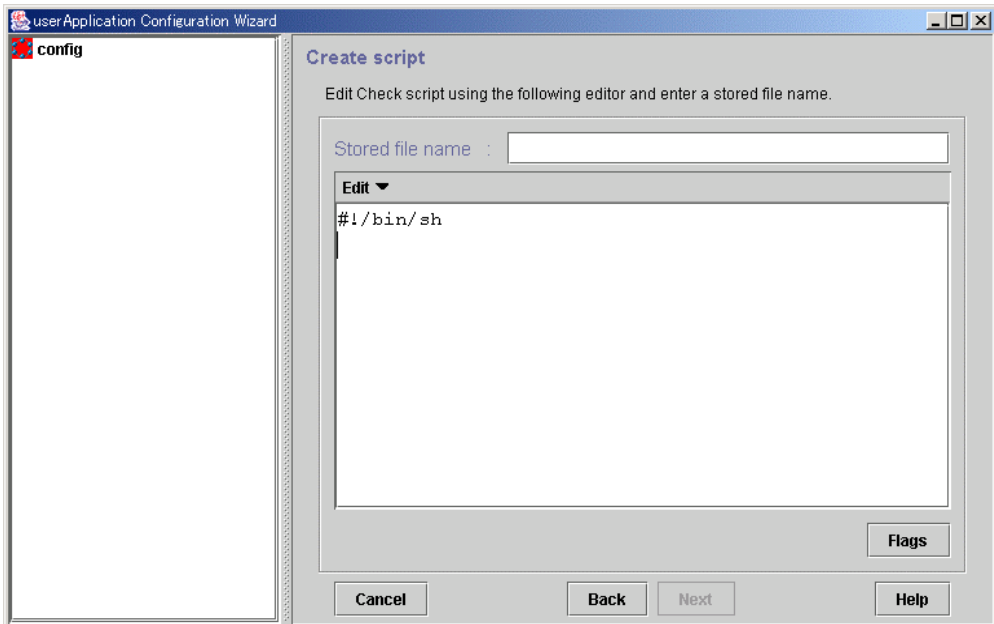


Note

- The created script files are stored in the “/opt/FJSVwvcuw/scripts/check” directory.
- These script files are not removed even when processing is cancelled during Cmdline creation, or the Cmdline resource or GUI package (FJSVwvcuw) is removed. If you want to remove the files, you need to remove the “/opt/FJSVwvcuw/scripts/check” directory. For example, execute the “rm(1)” command to remove one script file as follows:


```
# rm /opt/FJSVwvcuw/scripts/check/XXXXXXXX
```
- For information on the exit codes for Check scripts, see “Exit codes, timeout values, and environment variables of scripts.”

Check script creation

**Stored file name**

Specify the file name to be saved.

The following characters cannot be used in the file name or the arguments: back slash ("¥"), tilde ("~"), percent sign ("%"), ampersand ("&"), and at sign ("@").

Even though processing is cancelled or the screen is closed during Cmdline creation, the script files are still stored in the "/opt/FJSVwvucw/scripts/check" directory. Therefore the scripts can be reused when the Cmdline resources are re-created.

**Note**

- When specifying arguments, separate the arguments with "blank" characters. Since the scripts that can be created in this screen are Bourne shell by default, the following string is displayed at the beginning of the editing area:

```
#!/bin/sh
```

- If "NULLDETECTOR" was set to "Yes" at the "Set Cmdline Flag" screen, a Check script does not need to be configured. In this case, the Check script is not configured as resource information because the Check script is not started from RMS.

Edit

You can edit scripts from the simplified menu. See "*Edit area operations*," for details.

Flags button

You can set script attributes from a dialog box. See "*Setting up Cmdline flags*," for details.

- **Example of Check script creation**

In this example, the processing in the command name of the user program is considered to be the Online processing.

**Note**

This script has an extremely simple structure because it is presented only for reference

purposes.

```
#!/bin/sh
#-----
# Sample
#   Check-script
#
#-----
PATH=/usr/bin:/usr/sbin

# Exit codes for RMS
e_online=0
e_offline=1

# Target Command name
CmdName=appl

pgrep $CmdName >/dev/null
if [ $? -eq 0 ];then
    Status=$e_online
else
    Status=$e_offline
fi
exit $Status
```

- **Edit area operations**

The operations for the script editing area are described below.

Item	Operation
Move cursor	You can move the cursor to any position by placing the mouse pointer at the target position and single-clicking the mouse pointer or by operating the arrow keys on the keyboard in the top, bottom, left, or right directions.
Insert text	You can input characters at the cursor position.
Delete text	<ul style="list-style-type: none"> ● To delete 1 character <ul style="list-style-type: none"> — Press the <i>[Delete]</i> key to delete the character at the cursor position. — Press the <i>[Backspace]</i> key to delete the character positioned directly before the cursor position. ● To delete a string with one or more characters, use the following keys: <ul style="list-style-type: none"> — <i>[Delete]</i> key — <i>[Backspace]</i> key — <i>Edit -> Delete</i> from the menu bar
Cut text	Select a string with one or more characters in the editing area and go to <i>Edit -> Cut</i> .
Copy text	Select a string with one or more characters in the editing area and go to <i>Edit -> Copy</i> .
Paste text	Position the cursor at the position where the character string that was previously cut or copied within the editing area is to be pasted, and then select <i>Edit -> Paste</i> .

- ◆ **Creating scripts by path input**

If a script already exists, you can enter a path to select the script.

**Note**

The following characters cannot be used in the file path or the arguments: back slash ("¥"), tilde ("~"), percent sign ("%"), ampersand ("&"), and at sign ("@").

Cmdline setup
Start script

Enter the path of the Start script. If you are specifying arguments, separate the arguments with "blanks."

The Start script is always a required script. The script must be entered with a full path name.

Stop script

Enter the path of the Stop script. If you are specifying arguments, separate the arguments with "blanks."

The Stop script is not required information. The script must be entered with a full path name.

Check script

Enter the path of the Check script. If you are specifying arguments, separate the arguments with "blanks." The script must be entered with a full path name.

Although the Check script is always a required script, it does not have to be specified if NULLDETECTOR was set to "Yes" in the "Set Cmdline Flag" screen. Even if the script is setup, the information is deleted during resource registration because the Check script is not started from RMS.

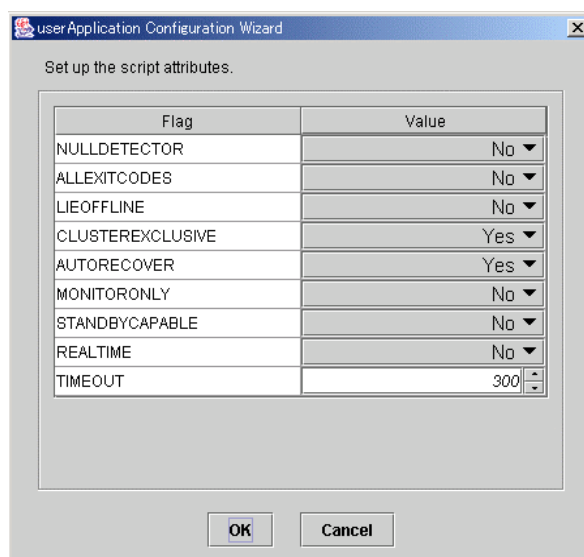
Flags button

Set the script attributes. For information, see "Setting up Cmdline flags," which is described later.

- **Setting up Cmdline flags**

The method of a controlling a script defined to a Cmdline resource can be adjusted by changing the flag values.

Set up Cmdline flags



After completing the setup, click *OK* to return to the "Set up Cmdline" screen.

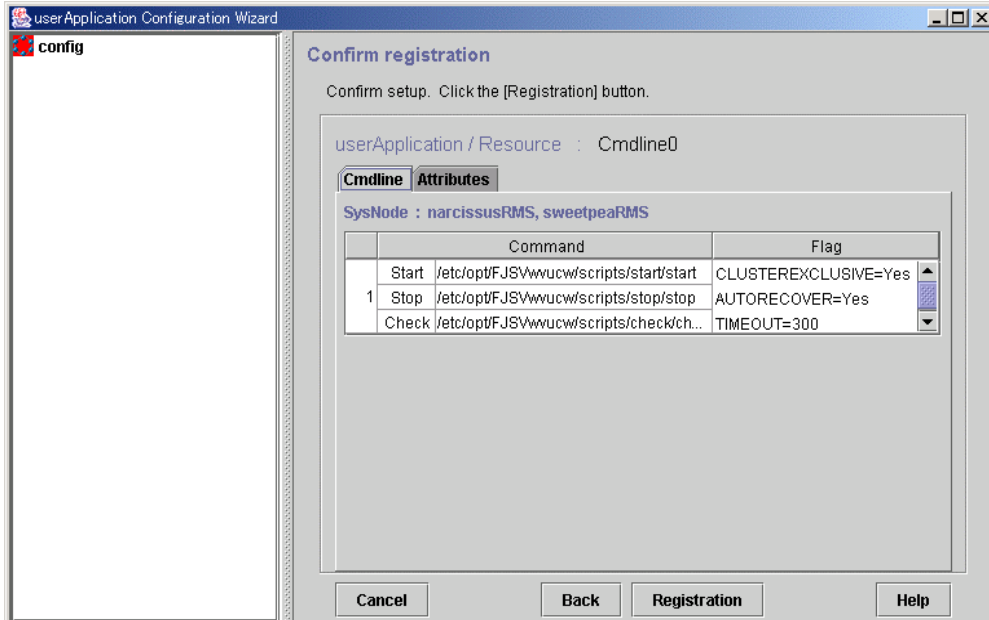
Flag	Outline
NULLDETECTOR	<p>If this flag is set to "Yes," the Check script that was specified for determining the resource state becomes disabled. Instead, RMS assumes that the resource is Online during Online processing and Offline during Offline processing. When RMS is restarted, this resource becomes Offline.</p> <p>This flag is used to register the program that starts or stops in line with Online or Offline processing as a resource.</p> <p>[Note] The Start and Stop scripts are executed by the Online or Offline processing regardless of the resource state. The resource is given a name beginning with "RunScriptsAlways" in RMS.</p>
ALLEXITCODES	<p>With the default setting, the exit codes are interpreted as follows:</p> <ul style="list-style-type: none"> 0: Online Other than 0: Offline <p>If this flag is set to "Yes," the exit codes are interpreted through the values that are set by the Return Codes. The ReturnCodes are as follows:</p> <ul style="list-style-type: none"> 0: Online 1: Offline 2: Faulted 3: Unknown 4: Standby 5: Online warning 6: Offline faulted
LIEOFFLINE	<p>If this flag is set to "Yes," the resource is notified as being Offline if a Stop script is not specified. If a Stop script is specified, the failure of the script triggers fault processing.</p>
CLUSTEREXCLUSIVE	<p>If this flag is set to "Yes", the resource becomes Online only on one node in a cluster system. If the resource becomes Online on two or more nodes at the same time because of a script problem, the state of userApplication to which this resource belongs becomes Inconsistent.</p>
AUTORECOVER	<p>If this flag is set to "Yes," RMS tries to recover the resource if it becomes faulted. In this way, RMS tries to prevent the userApplication from being switched to another host</p> <p>This recovery is tried only once.</p>

Flag	Outline
MONITORONLY	This flag controls whether the "faulted" condition in the resource makes the userApplication Faulted. If this flag is set to yes, the resource becomes Faulted, but this does not make the userApplication Faulted. The system does not allow this value to be set to "Yes" for Cmdline resources that can be created from the GUI. If you use this flag, keep the "No" setting because RMS startup will be disabled if the flag value is set to "Yes."
STANDBYCAPABLE	If this flag is set to "Yes," RMS sets the StandbyCapable attribute to 1 for this resource. For detailed information regarding this attribute, see "7. Appendix –Attributes" in "PRIMECLUSTER RMS Configuration and Administration."
REALTIME	The Check script is started with the TS class (time-sharing scheduling) by default. If this flag is set to "Yes," the Check script is started with the RT class (real time mode). Note that since the operating system assigns the highest priority to processes that are started with the RT class, any bugs in the script or commands may have a large effect on system performance.
TIMEOUT	This flag sets the timeout interval (seconds) for program start and stop processing.

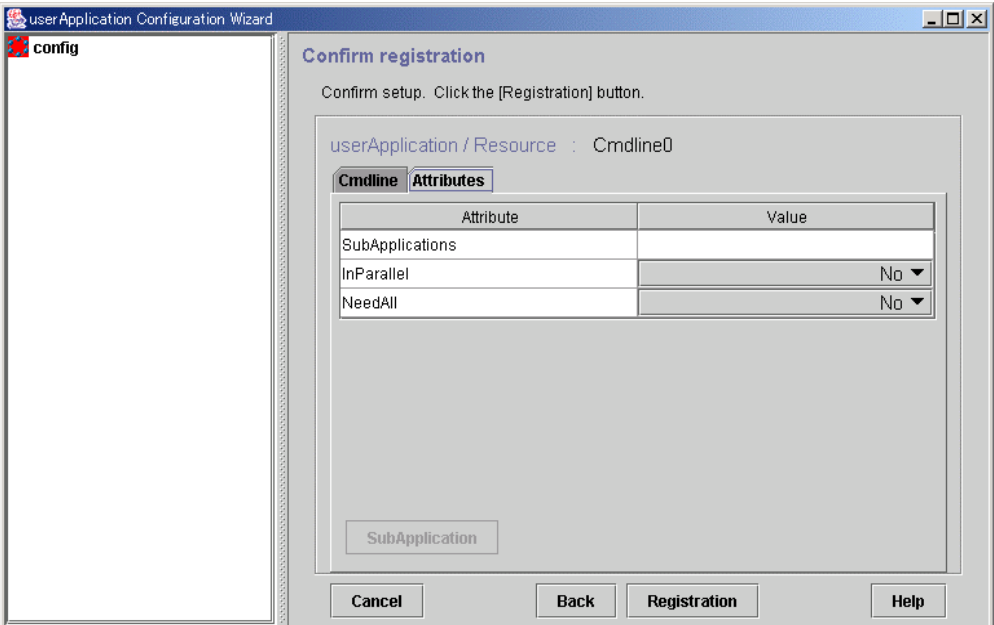
■ **Check Cmdline registration information**

You can check a list of the scripts that has been set up previously. You can also configure resource attributes by selecting the *Attributes* tab and switching the screen. For information on the resource attributes, see 6.6.5 "Attributes."

Confirmation of registration information



The attributes that are displayed in the "Flag" column are only those Resource attributes for which a value has been set. For example, if *No* is set for the AUTORECOVER attribute, then it means that AUTORECOVER attribute has not been set, and it is not displayed in the Flag column.



SubApplication button

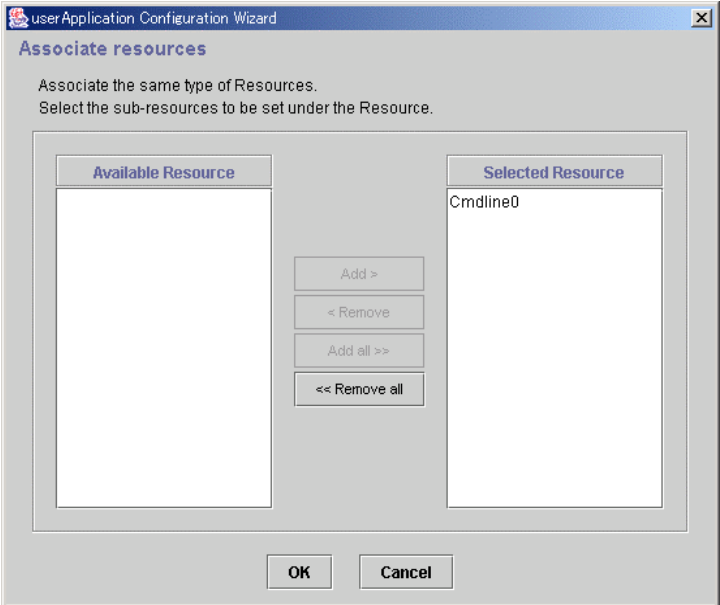
Associate the other Cmdline resources or process monitoring resources with the Cmdline resource that has been created above. See "Resource association."

After checking the registration information, click *Registration*.

◆ **Resource association**

- Use this function to configure a startup sequence among resources of the same type. By assigning startup priorities to resources, you can clarify the order in which the resources are to be switched to Online or Offline. In Online processing, resources that have a high startup priority are switched to Online before resources that have a low startup priority. Conversely in Offline processing, resources that have a low startup priority are switched to Offline before resources that have a high startup priority. If a startup priority is not assigned or if resources have the same priority, the sequence is undefined.

Associate resources



Available Resource

Available resource is referred to as the resource of the same type that can be associated, and satisfies the following conditions.

- The resource is of the same type as the resource that was called.
- The resource is not being used by another cluster application.

Note: Cmdline and process monitoring resources are considered the same type of resources.

Selected Resource

Resources to be set under the current resource being created.

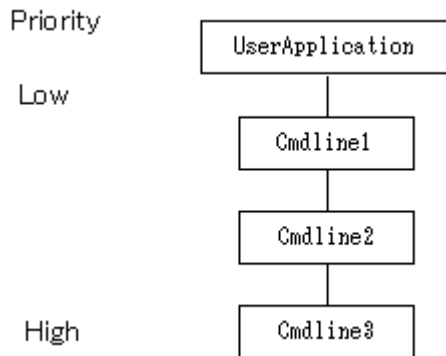
From *Available Resource* select the resource to be configured under the current resource, and then click *Add*. To add all listed resources, click *Add all*. To delete a resource from under the current resource, select the resource to be deleted from the *Selected Resource*, and then click *Remove*. To delete all listed resources, click *Remove all*.

After completing the setup, click *OK*, and return to the “Confirm Registration Information” screen.



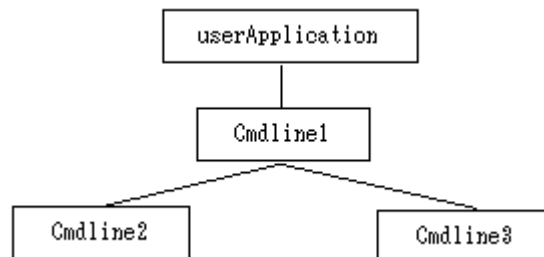
In the configuration shown below, the startup priority has been set to resources of the same type.

To build this configuration, build the resources according to the procedure shown below.



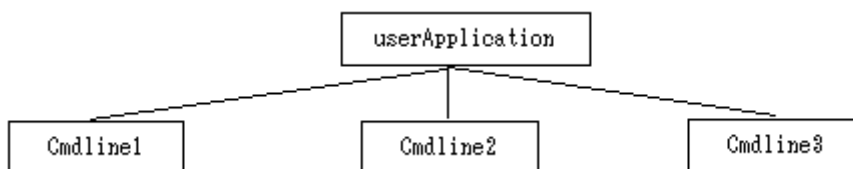
- 1) Create Cmdline3.
- 2) Create Cmdline2, and set Cmdline3 as subApplication.
- 3) Create Cmdline1, and set Cmdline2 as subApplication.
- 4) Create userApplication, and set Cmdline1 as subApplication.

The procedure for building the following configuration is shown below.



- 1) Create Cmdline3.
- 2) Create Cmdline2.
- 3) Create Cmdline1, and set Cmdline2 and Cmdline3 as subApplication.
- 4) Create userApplication, and set Cmdline1 as subApplication.

In the configuration shown below, the other resources were not set as subApplication during the creation of resource.



6.6.1.2 Creating Fsystem Resources

Set up an Fsystem resource if you want to mount a file system when userApplication is started. To control multiple mount points in parent-child relationships, create the file system as one Fsystem resource.

You need to work on the following prerequisites to create an Fsystem resource.

Mount point characteristics

- Mount points are used to mount UFS and other local file systems.
- The file system can be shared as an NFS file system in the network. The file system can also be set up so that it is not shared.
- When a file system is shared in the network, the NFS Lock Failover function becomes enabled.

6.6.1.2.1 Prerequisites

This section describes operations that must be performed before the file system is set up with the GUI. Although not mentioned in the procedure, editor commands such as those featured by vi(1) are generally used in file editing.

■ Editing the /etc/vfstab file

Define the mount point in the "/etc/vfstab" file on all nodes where userApplication is configured to use Fsystem.

```
#RMS#/dev/sfdsk/class0001/dsk/volume0001
/dev/sfdsk/class0001/rdsk/volume0001 /disk1 ufs - no -

#RMS#/dev/sfdsk/class0001/dsk/volume0002
/dev/sfdsk/class0001/rdsk/volume0002 /disk2 sfxfs - no -
```



Note

Lines must begin with "#RMS#".

■ Preparations for sharing (NFS) a file system in a network

● 1) Create laddress or GIs resources.

Since a takeover network is necessary when an NFS service is used as a cluster application, create an laddress or a GIs resource.

For details on the setup procedure, see 6.6.1.5 "Creating Takeover Network Resources" and 6.6.1.4 "Creating GIs Resources."

Set this resource to the same userApplication as the Fsystem resource.

- **2) Carry out preparations for enabling NFS Lock Failover.**

Select the "Edit global settings in Configuration" command from the menu, and specify the settings for enabling NFS Lock Failover.

For details on the setup procedure, see 6.6.4 "Editing global settings in Configuration."

- **3) Set up the NFS service.**

3-1) Create a directory for dummy entries.

Dummy entries are necessary to ensure that the NFS service is started when Solaris OE is started.

Execute the command below to create a blank directory.

```
# mkdir /var/opt/SMAWRrms/nfsshare
```

3-2) Edit the /etc/dfs/dfstab file.

Add the entries shown below to the file in all nodes that make up userApplication. The first entry is a dummy entry, and the subsequent entries are entries of the file system to be shared.

```
share -F nfs -o ro=fuji2 -d "dummy directory for NFS sharing on
PRIMECLUSTER" /var/opt/SMAWRrms/nfsshare
#RMS# share -F nfs /disk1
#RMS# share -F nfs /disk2
```



Note

- Be sure to start each line with "#RMS#" (except for the dummy entry).
- In the dummy entry, set the "o" option to ensure that network clients cannot see the entry.

Example) `share -F nfs -o ro=hostname_of_local_node`

3-3) Start the NFS service.

To start the daemon without rebooting the system, execute the following command:

```
# /etc/init.d/nfs.server start
```

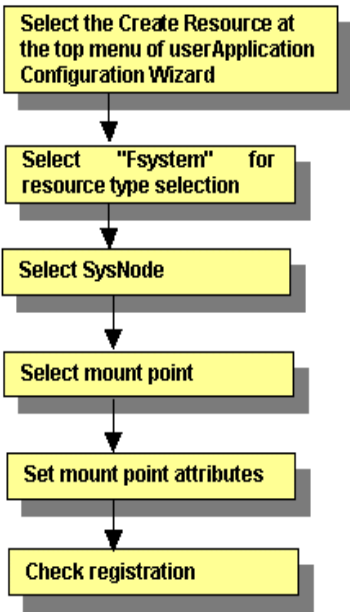
- **If another file system is used**

The disk must be formatted and the file system must be created beforehand. For information on formatting and file system commands, see the "Solaris X Reference Manual Collection." If you plan to use GFS as the file system, see 6.3 "Initial GFS Setup" when you build the file system.

6.6.1.2.2 Setup Method

This section describes how to create Fsystem resources.

Flow of Fsystem resource creation

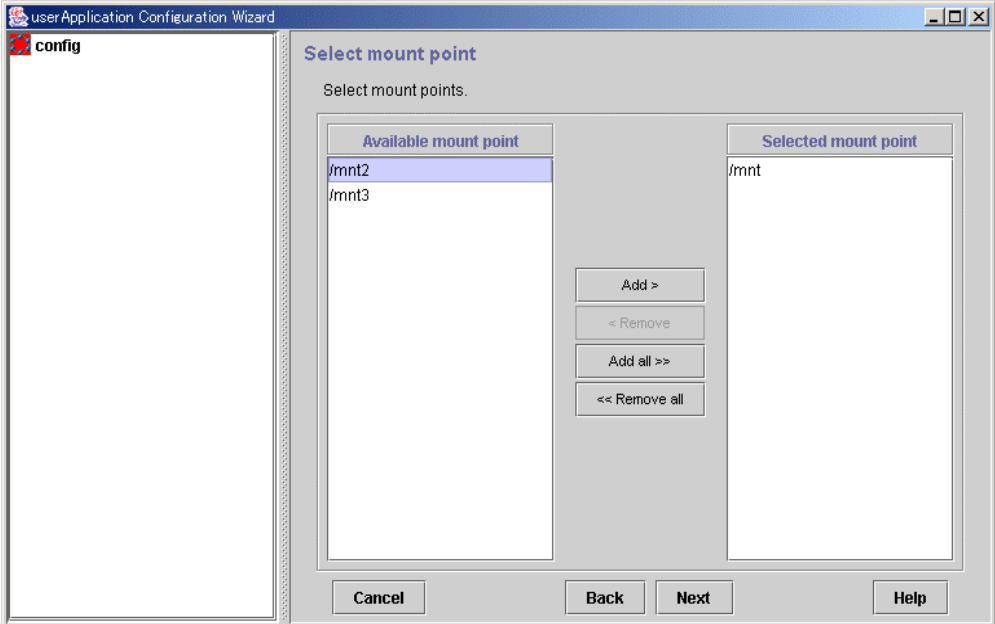


For information on the above operations up to "Select SysNode," see 6.6.1.1 "Creating Cmdline Resources." This section describes the operations starting from "Select mount point."

■ **Selecting mount points**

Select the mount points.

Select mount point



Available mount point

Names of mount points where the file system can be mounted. The mount points that were configured for "/etc/vfstab" (described earlier) are displayed.

Selected mount point

Names of mount points to be used for file system mounting.

From *Available mount point*, select the mount point at which the file system is to be mounted, and then click *Add*. To add all listed mount points, click *Add all*. To delete a mount point on

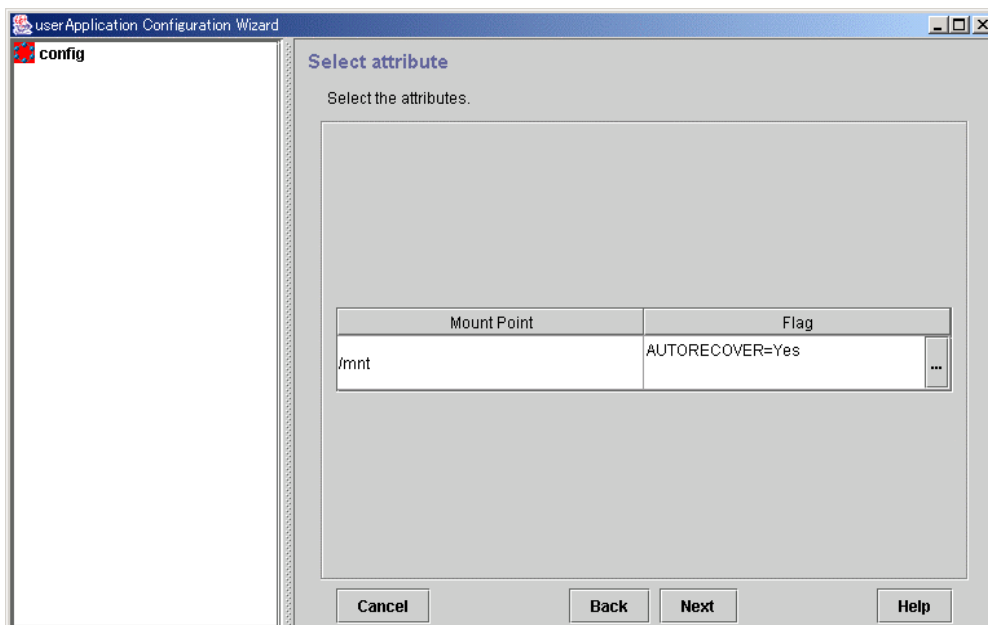
which the file system is not going to be mounted, select the mount point to be deleted from *Selected mount point*, and then click *Remove*. To delete all listed mount points, click *Remove all*.

After completing the setup, click *Next* to go to "Setting mount point attributes."

■ **Setting mount point attributes**

Set attributes for the mount points.

Select attribute



Mount point

The mount name is displayed.

Flag

The attributes that are set for the individual mount points are displayed.

[...] button

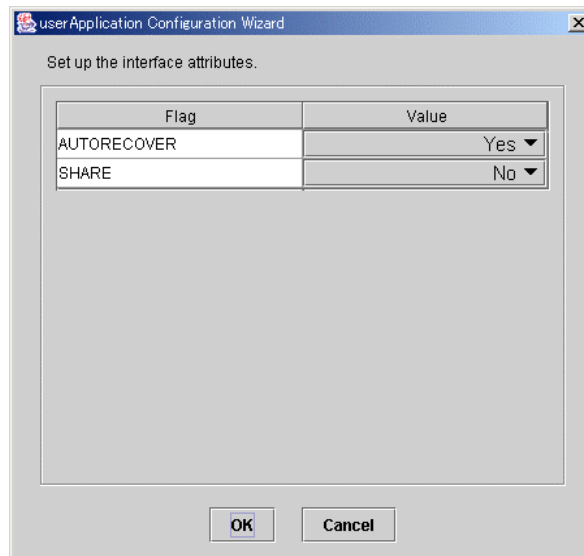
Press this button to set attributes for controlling mount point management. When this button is clicked, the Set Mount Button Attributes screen shown below is displayed.

After completing the setup, click *Next* to go to "Fsystem Registration Information Confirmation."

◆ **Attribute setup for mount points**

Configure the attributes for controlling the mount points.

Attribute setup for mount points



After completing the setup, click *OK* to go to the "Select Attribute" screen.

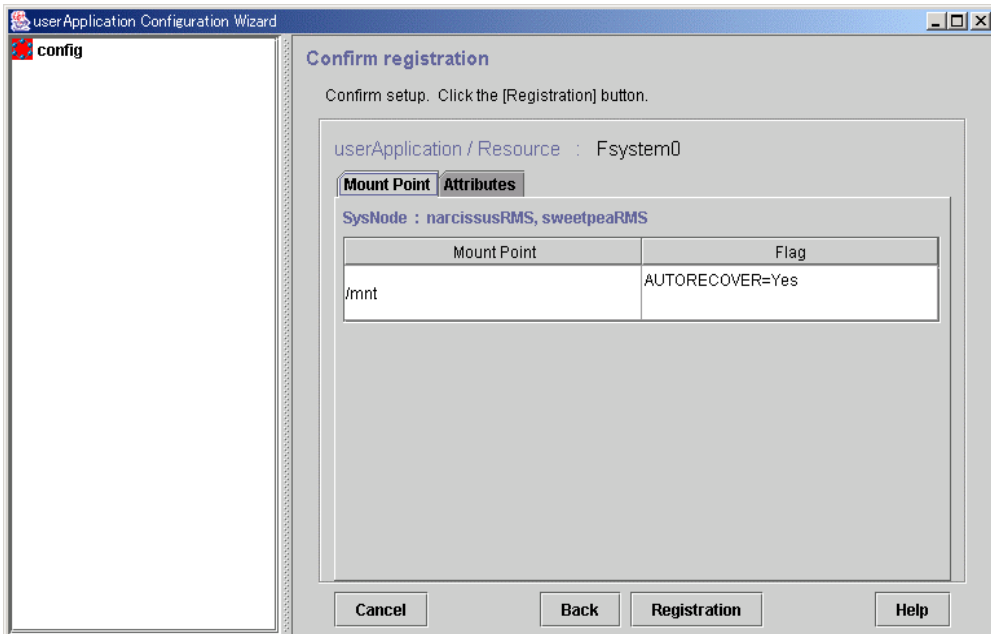
Flag	Outline
AUTORECOVER	If this flag is set to "Yes" and the specified file system is unmounted, RMS automatically attempts to remount the specified file system when it is unmounted. If this attempt fails, Fault processing is initiated. The default value is "Yes."
SHARE	If this flag is set to Yes, a mounted directory is shared (NFS). In such a case, make a specific entry to "/etc/dfs/dfstab". See "Preparations for Sharing a File System in the Network (NFS)" in "Prerequisites". For one userApplication, set only one Fsystem resource that has a mount point for which this attribute is set to "Yes." The default value is "No."
NFSLOCKFAILOVER	If this flag is set to "Yes," Lock information for NFS Lock Failover is stored for this mount point. To use NFS Lock Failover, you must set this flag to "Yes" for one of the mount points. If you set this attribute to "Yes," you must also set SHARE to "Yes" at the same time. The default value is "No." For each Fsystem resource, this flag can be set for only one mount point. Even if userApplication has multiple Fsystem resources and NFS Lock Failover is to be used, set this attribute to "Yes" for only one mount point in userApplication.

■ Checking Fsystem registration information

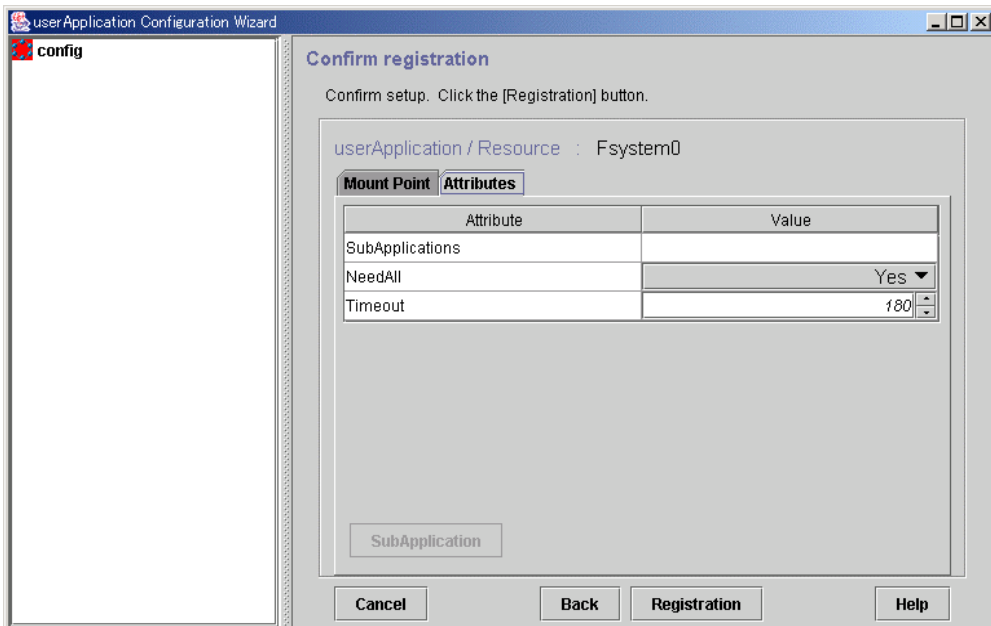
Check the Fsystem registration information. You can also select the *Attributes* tab, and set resource attributes by switching the screen.

For information on the resource attributes, see 6.6.5 "Attributes."

Confirmation of registration information



The attributes that are displayed in the "Flag" column are only those Resource attributes for which a value has been set. For example, if "No" is set for an attribute that takes a "Yes" or "No" setting, such as AUTORECOVER, that attribute is not displayed in the "Flag" column.



SubApplication button

This button is used for specifying other resources that the current resource depends on. For an Fsystem resource, this button is disabled.

For multiple directories in parent-child relationships, configure the directories in one resource.

Check the registration contents, and then click *Registration*.

6.6.1.3 Creating Gds Resources

Set up resources for the disk classes that are defined in Global Disk Services (GDS).

The disk classes must be created before this screen is used.

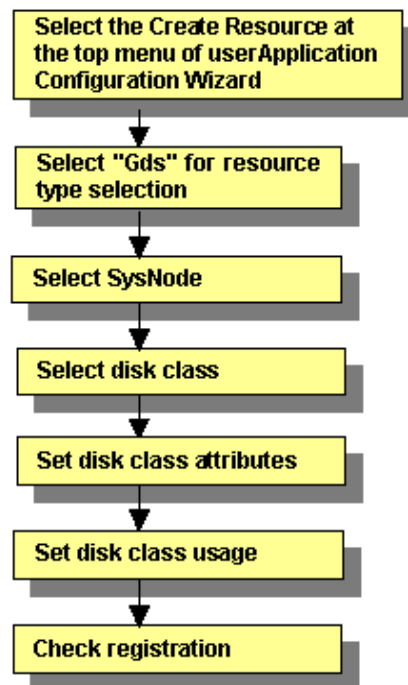


Note

If a disk class is registered to a Gds resource when equivalent volume copy is being executed, the equivalent copy operation is canceled. Therefore, the data becomes invalid in some of the slices. However, recovery is not necessary because equivalent copy is executed automatically when the volume is started. If you want to recover the slice state before the volume is started, complete Gds resource setup and then start equivalent copy. For instructions on starting equivalent copy, see "5.3.4 Copying Operation" or "D.10 sdxcopy - Synchronization copying operation" in the *"PRIMECLUSTER Global Disk Services Configuration and Administration Guide."*

For instructions on creating disk classes, see 6.2.2.2 "Setting Up Shared Disks."

Flow of Gds resource creation

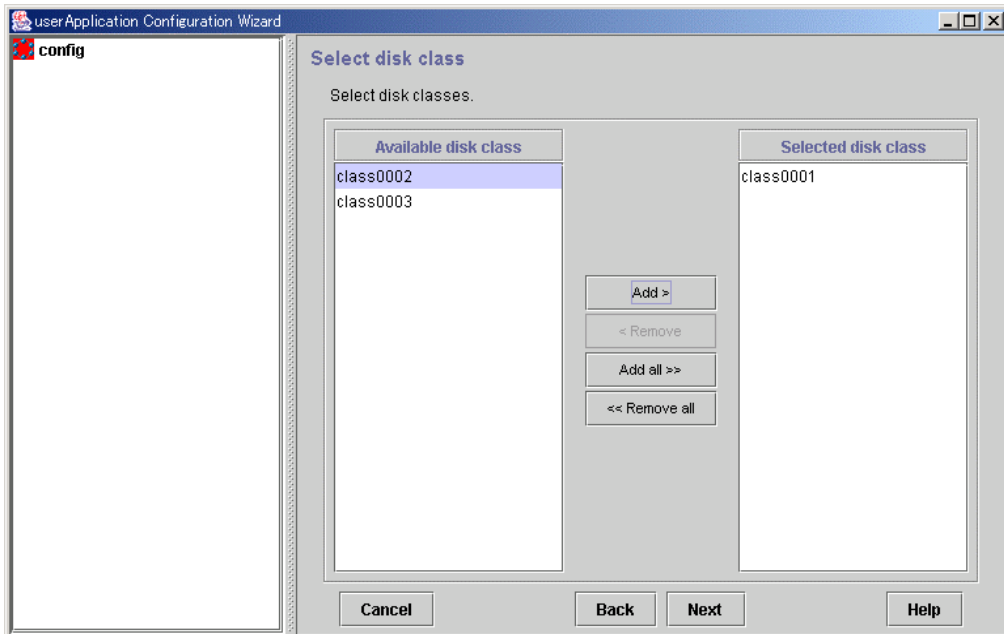


For information on the above operations up to "Select SysNode," see 6.6.1.1 "Creating Cmdline Resources." This section describes the operations starting from "Select disk class."

■ **Selecting the disk class**

Select the disk class.

Select disk class



Available Disk Class

Names of disk classes that can be set.

The disk classes (shared disks) that are defined in GDS are displayed.

Selected Disk Class

Names of disk classes to be set.

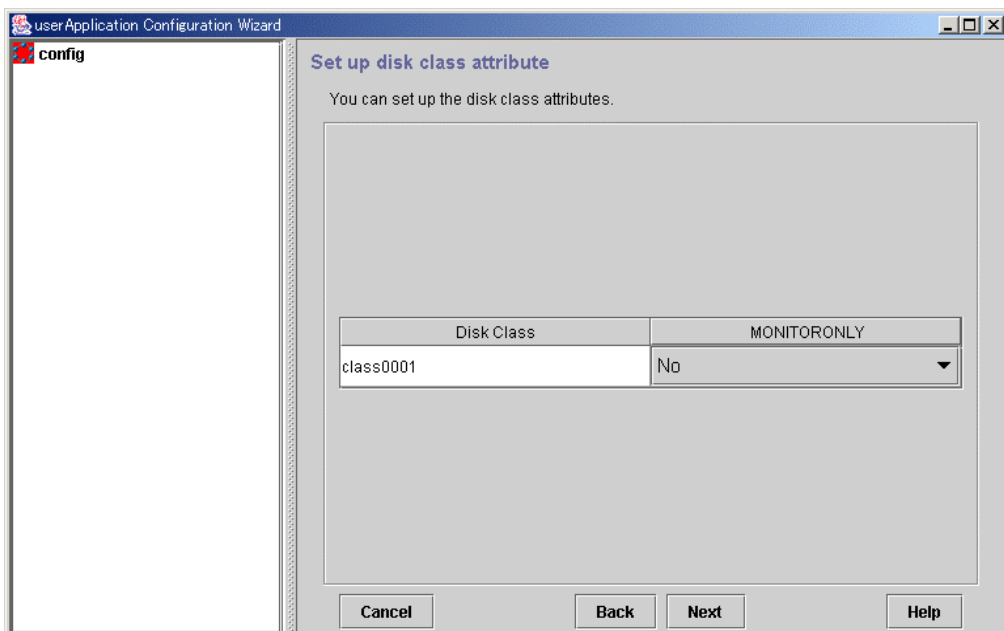
Select disk classes from *Available disk class*, and then click *Add*. To add all listed disk classes, click *Add all*. To delete a disk class to be set, select the disk class to be deleted from *Selected disk class*, and then click *Remove*. To delete all listed disk classes, click *Remove all*.

After completing the setup, click *Next* to go to the "Set Disk Class Attribute" screen.

■ Disk class attribute setup

Set the disk class attribute.

Disk class attribute setup



Disk Class

The disk classes (common disks) that were defined in GDS (described earlier) are displayed.

Flag	Outline
MONITORONLY	<p>This flag determines whether disk class failures are to be reported to the userApplication. If "Yes" is set and a disk class failure occurs, the disk class is switched to faulted state but the Gds resources remain online, and userApplication failover does not occur.</p> <p>Carry out the preliminary design, including the higher applications" before determining the disk classes for which this flag is to be set to "Yes."</p> <p>The default value is "No."</p>

The MONITORONLY attribute must be set to "No" for at least one disk class.

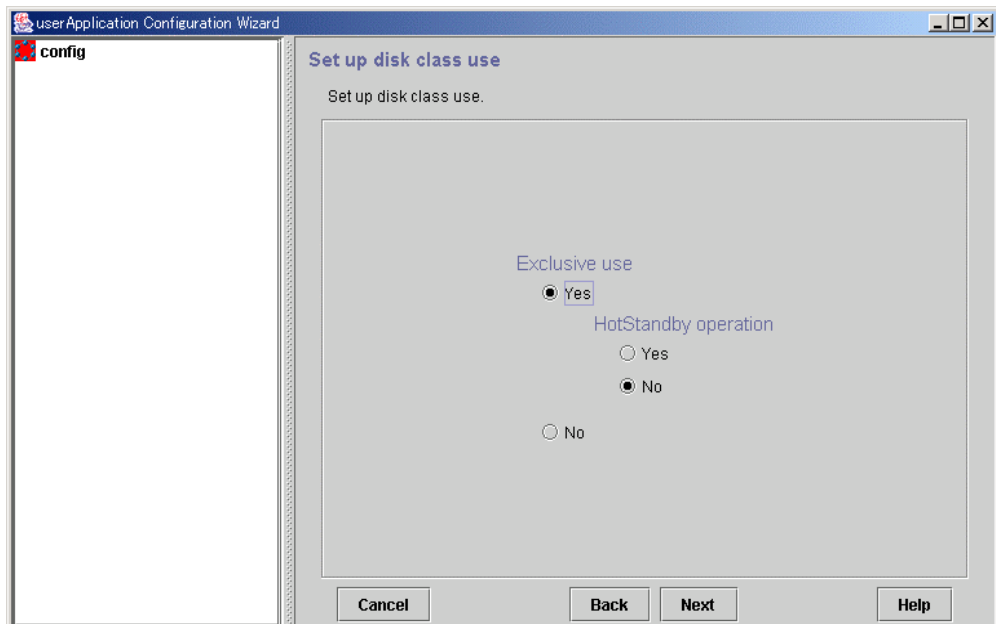
This will prevent userApplication failover in the event of all disk class failures and RMS' notifying the upper applications of the failures.

After completing the setup, click *Next* to go to the "Set up disk class use" screen.

■ Setting the disk class use

Configure the use of the disk class.

Set up disk class use



Exclusive use

Select "Yes" or "No" for *Exclusive use*. If you select "Yes", also select "Yes" or "No" for *HotStandby operation*.

Specify the options according to the use of the shared disk.

After completing the setup, click *Next* to go to the "Confirm Registration Information" screen.

● Shared disk uses

Shared disk uses and setting methods

Use	Exclusive use	HotStandby operation
Switched disk	Yes	No
Shared disk for simultaneous access	Yes	Yes
Simultaneous shared disk	No	

Shared disks have the following features for each use:

- **Switched disk**

Only the OPERATING node can use the shared disk.
The non-OPERATING nodes cannot access the volume.

- **Shared disk for simultaneous access**

All nodes can use the shared disk simultaneously.
Select this use if applications that require disk access from a node other than the OPERATING node are set inside the same userApplication.
The exclusive control for maintaining data integrity in the shared disk must be handled by the applications, and not by PRIMECLUSTER.

- **Simultaneous shared disk**

Select this use if multiple userApplications share the disk classes. An example is when Oracle real application clusters are used.
The exclusive control for maintaining data integrity in the shared disk must be handled by the applications, and not by PRIMECLUSTER.



Note

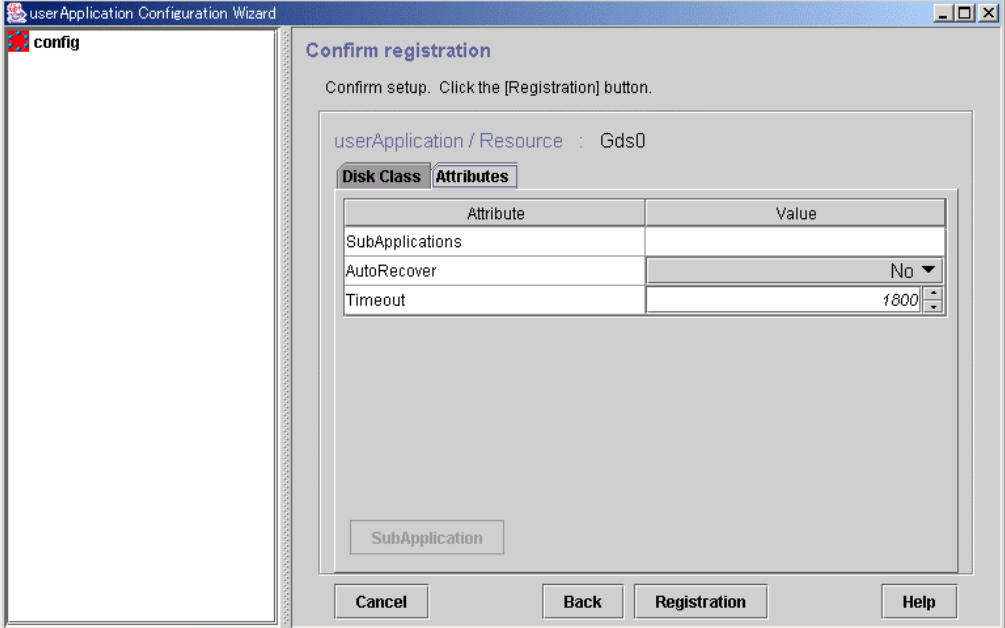
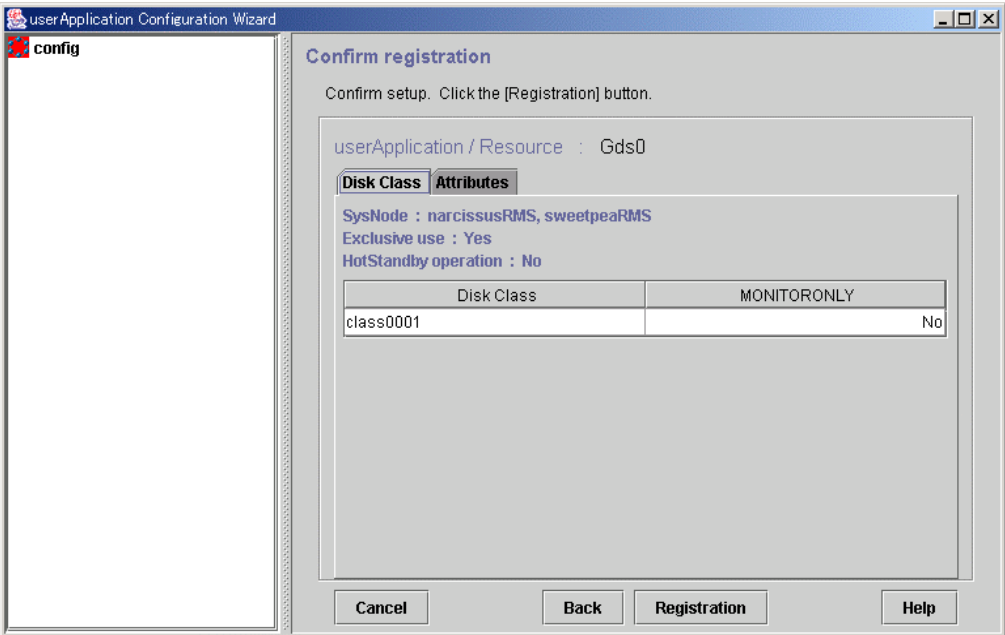
- During operation of a cluster application, try not to have applications or user processes that are not related to the cluster applications use the shared disks. If this occurs, the state transition might fail.
- Do not create a home directory for user accounts on a switchover disk. The reasons are as follows:
 - The file system on the switching disk is mounted only on the OPERATING node of the cluster application.
 - PRIMECLUSTER forcibly terminates process that uses the file system on the switching disk by executing the “kill(1M)” command to unmount the file system in the event of cluster application failover.
 - If the file system cannot be unmounted properly because of a failure of forced termination of process, PRIMECLUSTER might forcibly stop the node to prevent the file system data on the shared disk from being destroyed by double mounting.

- **Checking registration information for Gds resources**

Check the registration information for the Gds resources. You can also set resource attributes by selecting the *Attributes* tab and switching the screen.

For information on the resource attributes, see 6.6.5 "Attributes."

Confirmation of registration information



SubApplication button

Use this button to associate a previously created Gds resource under the current Gds resource. This button can be selected only if there are resources of the same type that can be associated. For setting instructions, see "Resource association" in 6.6.1.1 "Creating Cmdline Resources."

Check the registration information, and then click *Registration*.

6.6.1.4 Creating GIs Resources

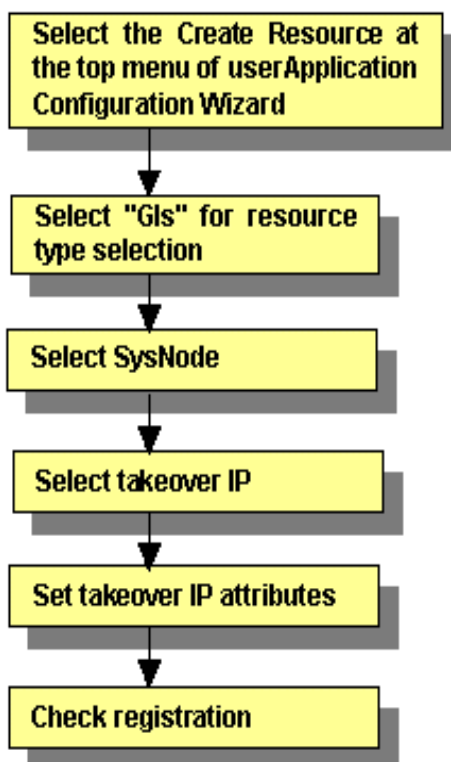
Configure the takeover IP addresses that are defined by the redundant line control function of Global Link Services (GLS).



Note

For details on using the multipath function of Global Link Services (GLS), see "Chapter 7 Administration on a Cluster System" in "*PRIMECLUSTER Global Link Services Configuration and Administration Guide: Multipath Function.*"

Flow of GIs (redundant line control function) resource creation

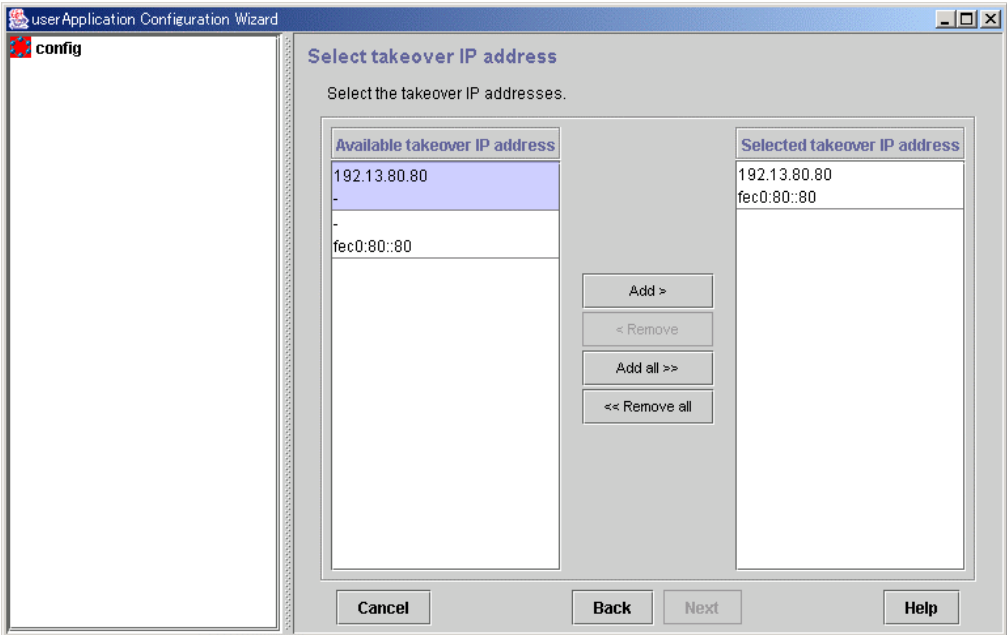


For information on the above operations up to "Select SysNode," see 6.6.1.1 "Creating Cmdline Resources." This section describes the operations from "Select takeover IP."

■ Selecting the takeover IP address

Select the takeover IP address.

Takeover IP address selection

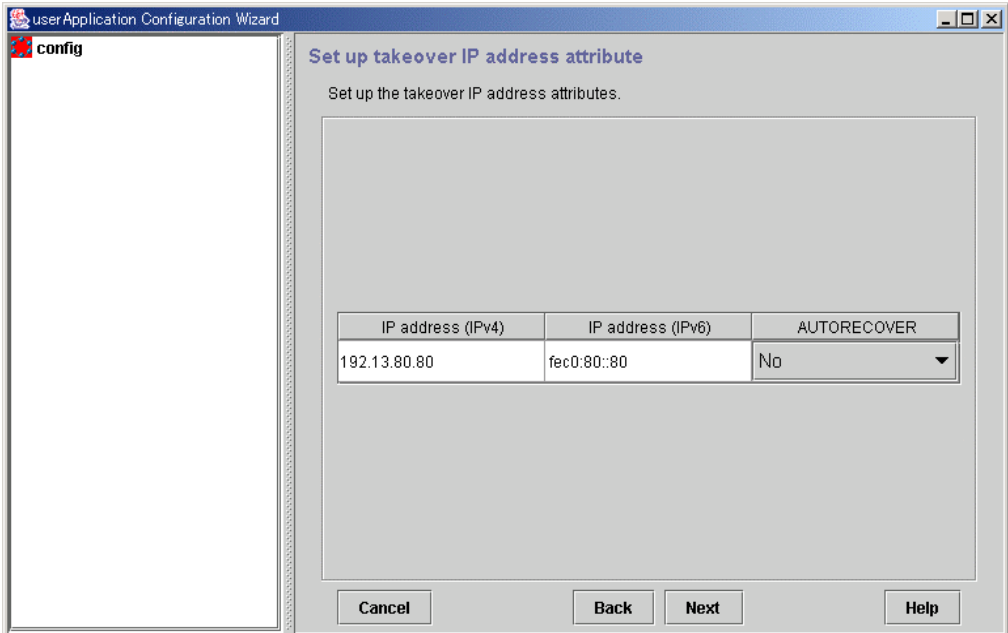


- Available takeover IP address**
IP addresses that can be taken over.
- Selected takeover IP address**
Takeover IP addresses.

From *Available takeover IP address*, select takeover IP addresses, and then click *Add*. To add all listed takeover IP addresses, click *Add all*. To delete a takeover IP address, select the takeover IP address to be deleted from *Selected takeover IP address*, and then click *Remove*. To delete all listed takeover IP address, click *Remove all*. After completing the setup, click *Next* to go to the "Set Takeover IP Address Attribute" screen.

- **Setting attributes of the takeover IP address**
Set the attributes of the takeover IP address.

Attribute setup for the takeover IP address



After completing the setup, click *Next* to go to "Checking GIs Resource Registration Information."

Flag	Outline
AUTORECOVER	If this flag is set to "Yes," RMS attempts to restore the faulted resource to prevent userApplication being switched to other host. The default value is "No." Be sure to set this flag to "No."

■ **Checking registration information for GIs resources**

Check the registration information for the GIs resources. You can also set resource attributes by selecting the *Attributes* tab and switching the screen.

For information on the resource attributes, see 6.6.5 "Attributes."

GIs resource names are displayed as GIsX (X is a number, such as 0 or 1).

To register a GIs resource to a cluster application, select this resource name from *Available Resources* on the Select Resource screen.

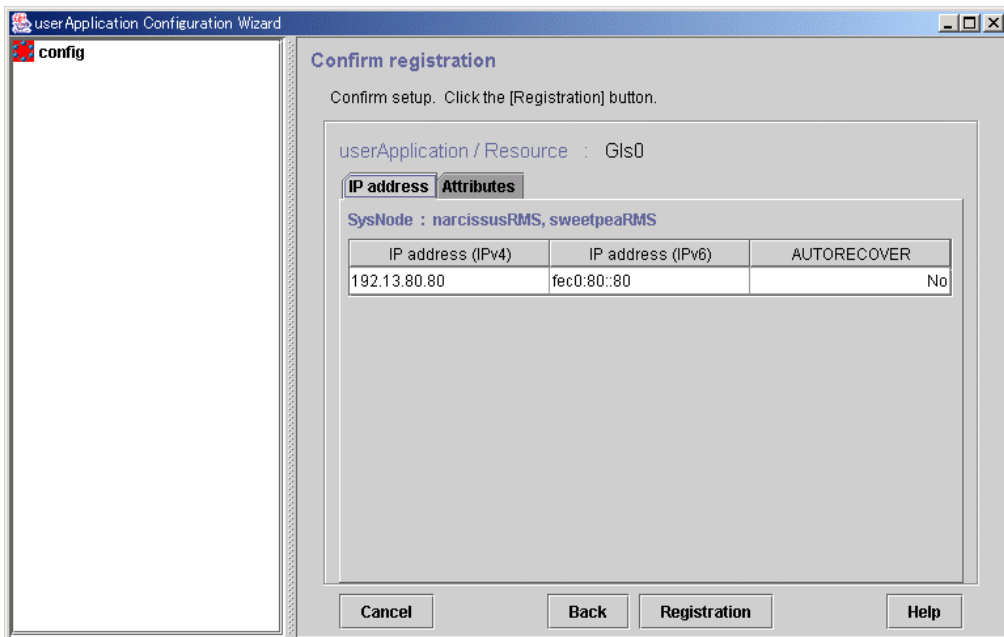
For details, see 6.6.2 "Creating Cluster Applications."

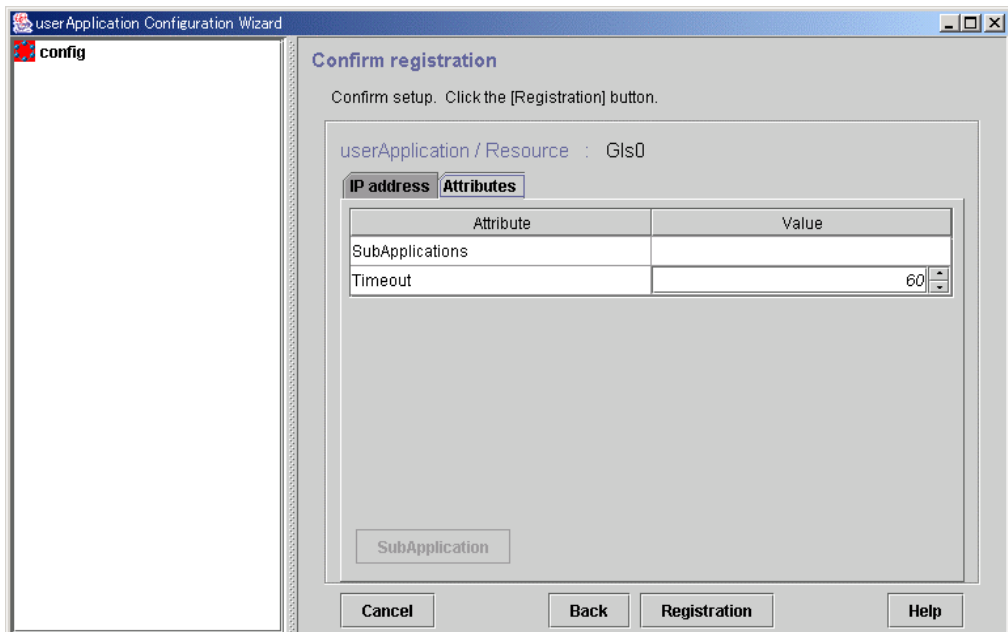
After registering the GIs resources to the cluster application, be sure to restart the system.

Then start RMS, look at the RMS tree, and check that the GIs resources are displayed correctly.

For details, see 7.1.3.1 "RMS Tree."

Confirmation of registration information





SubApplication button

Use this button to associate a previously created Gls resource under the current Gls resource. This button can be selected only if there are resources of the same type that can be associated. For setting instructions, see "Resource association" in 6.6.1.1 "Creating Cmdline Resources."

After check the registration information, click *Registration*.

6.6.1.5 Creating Takeover Network Resources

Normally to use a takeover network, use either "Gls" (Global Link Services) or "Ipaddress" as the resource type. If the availability of the takeover network is needed, use "Gls."

A takeover network must be set up if you are building a system like a client/server system that communicates with cluster services that operate in the cluster system.

Takeover networks allow communication to continue with the same network name from outside the cluster even if a cluster application that operates in the cluster system undergoes failover.

■ Takeover network types

The takeover network types are IP address takeover, MAC address takeover, and node name takeover.

- IP address takeover
When switchover takes place, the defined IP address is taken over to the OPERATING node.
This is the basic function of a takeover network.
- MAC address takeover
The MAC address is also taken over to the OPERATING node.
- Node name takeover
The node name* is also taken over to the OPERATING node.
Use this type if a program that operates as a cluster application in the cluster node recognizes node names.
* This is the same value as the host name that is obtained when `uname -n` is executed.

■ Files that are edited automatically by the GUI

If the GUI is used to execute the setup, certain files are edited as shown below.

The files differ according to the takeover network type.

```
# Start of lines added by FJSVwvucw - DO NOT DELETE OR CHANGE THIS LINE
# Mon Aug 05 21:01:43 JST 2002
<Specify information that is dependent on that particular file. For example, for
/etc/inet/hosts, the information becomes as follows:>
192.168.246.100 Ipaddress01
# End of lines added by FJSVwvucw - DO NOT DELETE OR CHANGE THIS LINE
```

- IP address takeover
/etc/inet/hosts
/usr/opt/reliant/etc/hvipalias
- Node name takeover
/etc/inet/hosts
/usr/opt/reliant/etc/hvipalias
/etc/nodename
- MAC address takeover
Lines are not created automatically. The lines must be specified beforehand.



Note

- In node name takeover, the same node name is set to both the OPERATING node and the STANDBY node.
- All cluster nodes must have at least one network interface card so the card can be used by IPv4.

- IPv6 is not supported. If you want to use IPv6, use GLs.
- Although a PRIMECLUSTER "takeover network" and the "IP address takeover" function of GLS can be set up in the same cluster system, do not use them on the same interface. If the two are used on the same interface, connection using takeover IP addresses will be disabled.
For example, if you select hme1 as the interface to be used when you set up the PRIMECLUSTER "takeover network," do not set hme1 in the GLS environment settings (do not specify hme1 in the -t option of the "hanetconfig create" command).

6.6.1.5.1 Prerequisites

This section describes the prerequisites for MAC address takeover.

MAC address takeover is enabled concurrently with takeover of an IP address. The MAC address takeover cannot be used by itself. To use MAC address takeover, you need to configure the following three files on each cluster node.

- /etc/opt/FSUNnet/mactool/macaddr.conf
- /usr/opt/reliant/etc/hvipalias
- /etc/inet/hosts

Although not mentioned in the procedure descriptions, the commands of a text editor such as vi(1) are generally used for file editing.

■ Using MAC address takeover

1. Edit the "/etc/opt/FSUNnet/mactool/macaddr.conf" file.
On all cluster nodes, add the takeover MAC address entry as shown below.
The format is "NIC MAC_address cluster."

```
hme0 02:11:22:33:44:55 cluster
```

For the MAC address, specify the value to be used in the Netcompo FNA-LAN.

2. Edit the "/usr/opt/reliant/etc/hvipalias" file.
On all cluster nodes, add entries for the target nodes of MAC address takeover as shown below.
The format is "CF_node_name takeover_network_name NIC Netmask MAC_address."

```
fuji2 Ipaddress01 hme0 0xffffffff00 02:11:22:33:44:55
fuji3 Ipaddress01 hme0 0xffffffff00 02:11:22:33:44:55
```

Add all cluster nodes that will be using MAC address takeover. The same information must be set in all cluster nodes.

To view more detailed information for the "/usr/opt/reliant/etc/hvipalias" file, see the comments in /usr/opt/reliant/etc/hvipalias.

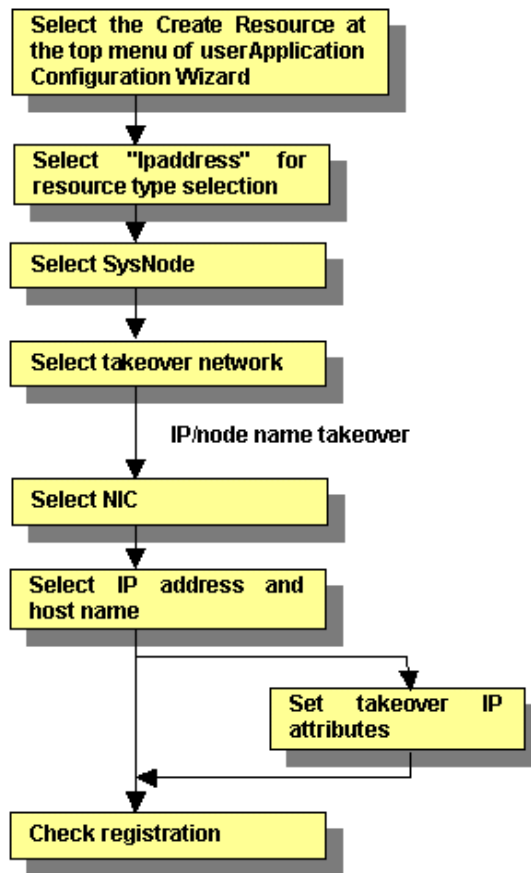
3. Edit the "/etc/inet/hosts" file.
On all cluster nodes, add the takeover network entry as shown below.

```
192.168.246.100 Ipaddress01
```

6.6.1.5.2 Setup Method

This section describes how to create takeover network resources.

Flow of takeover network resource creation

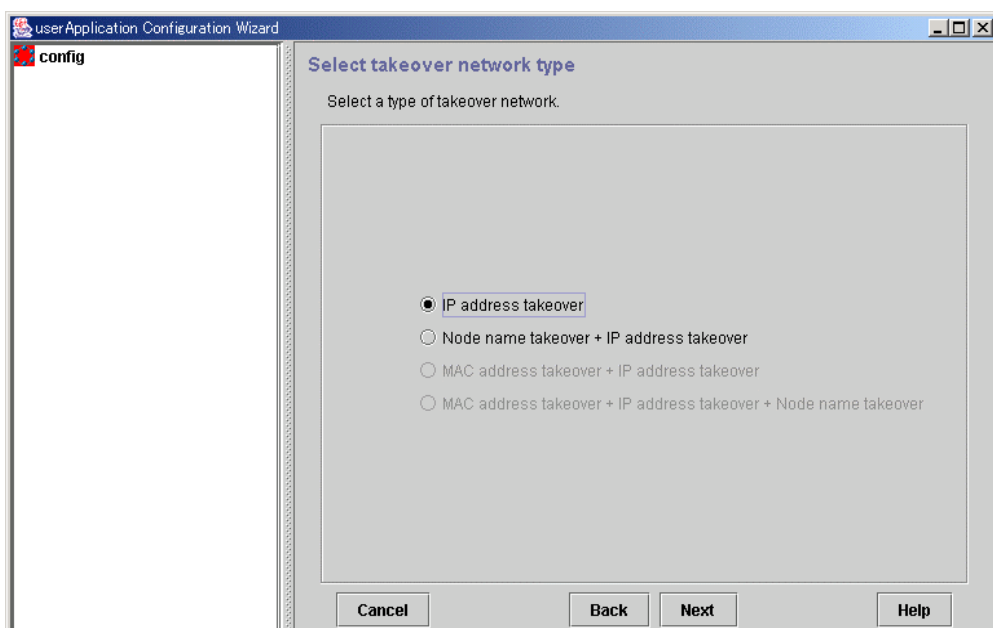


For information on the above operations up to "Select SysNode," see 6.6.1.1 "Creating Cmdline Resources." This section describes the operations starting from "Select takeover network."

■ Selecting a takeover network

Select the takeover network type.

Network type selection



IP address takeover

Select this item to enable IP address takeover.

Node name takeover + IP address takeover

Select this item to enable node name takeover and IP address takeover.

If node name takeover has already been set, you are not allowed to set twice.

In this version, "MAC address takeover + IP address takeover" and "MAC address takeover + node name takeover + IP address takeover" cannot be selected.

To set MAC address takeover, perform the operations described in 6.6.1.5.1 "Prerequisites," and then select "IP address takeover" or "node name takeover + IP address takeover" and create the takeover network resources.

You can configure a network interface for each SysNode. The takeover network settings are enabled for one network interface:

- Multiple IP address takeover settings are enabled for each network interface.
- Only one node name takeover setting is enabled in a cluster system.

After completing the setup, click *Next* to go to the "Select Interface" screen.

**Note**

- Do not configure MAC address takeover for a network interface that uses Web-Based Admin View.
- To activate a network interface card (NIC) when the system is started, you must create the `/etc/hostname.NIC-name` file. For instructions on creating and setting up the file, see "Solaris X Reference Manual Collection."
- Node name takeover changes the `uname` of the system. To set node name takeover for `userApplication`, you need to restart all nodes configuring `userApplication`.

If a node name takeover resource has been deleted, check whether `/etc/nodename` has been properly changed in all nodes, and then restart all nodes. If `/etc/nodename` has not been properly changed, change the node name by executing the `"setuname(1M)"` command, and then restart the nodes.

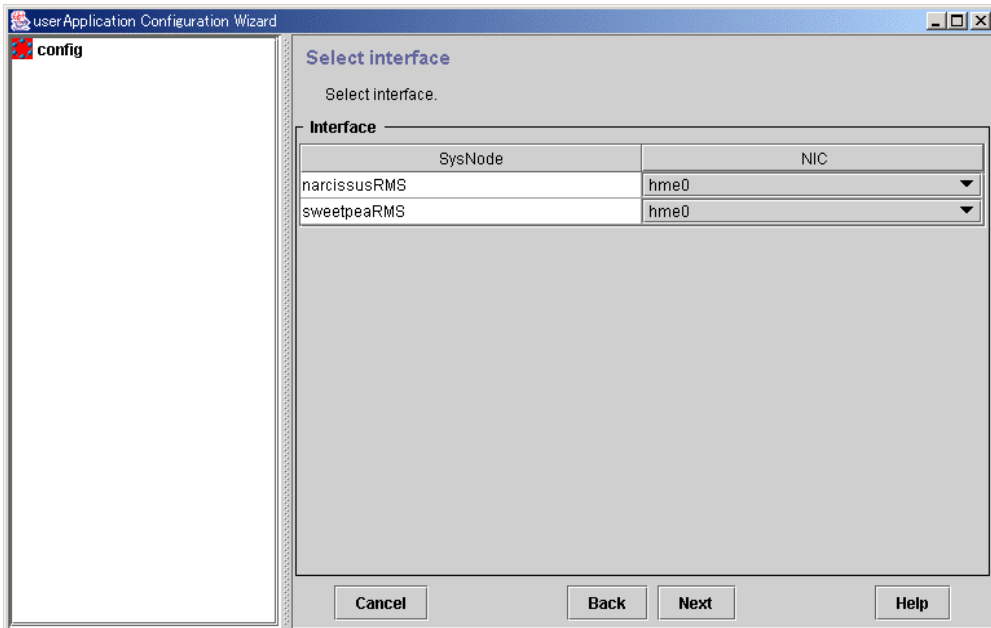
Also check whether `/etc/nodename` is set properly when system conversion or software upgrade is implemented. If `/etc/nodename` is not set properly, change the node name by executing the `"setuname(1M)"` command, and then restart the nodes.

■ Selecting an interface

Select a network interface card (NIC).

The NIC cards registered to Cluster Resource Manager are displayed.

Select interface



Interface

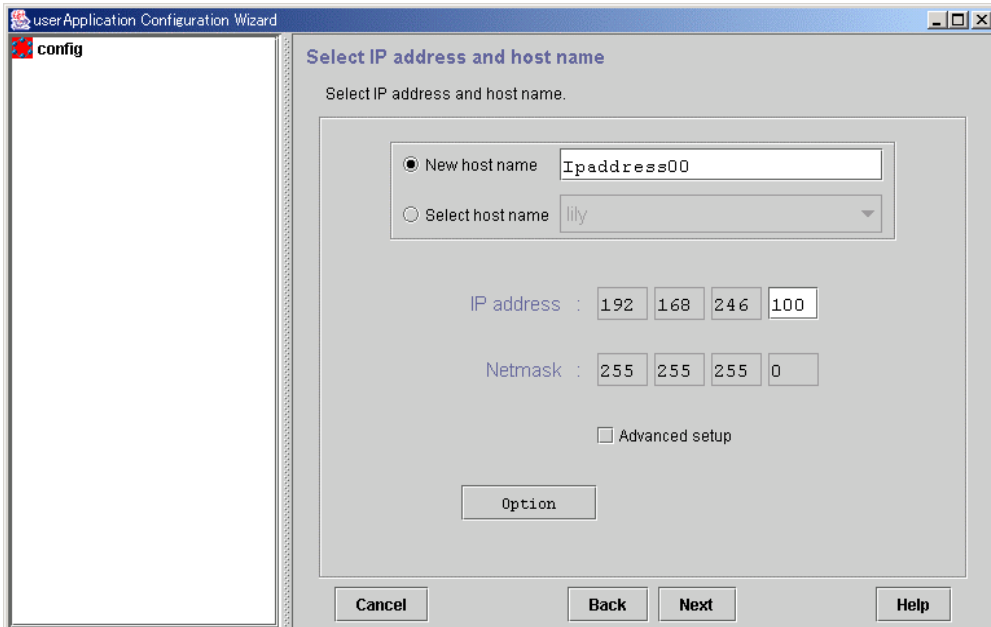
Select the network interface to be used in each SysNode.

After completing the setup, click *Next* to go to the "Select IP address and host name" screen.

■ Selecting or creating an IP address or host name

Select or create the takeover IP address or host name.

Select IP address and host name



New host name

You can set a new takeover IP address and a takeover node name. The setup information is added to the "/etc/inet/hosts" or "/usr/opt/reliant/etc/hvipalias" file on all nodes configuring the cluster system.

Specify a character string of up to 14 characters that begins with an alphabet letter and consists of only alphanumeric characters.

Select host name

You can select the IP address or node name from information that has been set. If IP addresses or node names were previously configured to `/etc/inet/hosts` and `/usr/opt/reliant/etc/hvipalias`, select the IP address or node name from those settings.

IP address

Enter the takeover IP address.

Enter 0 to 255 numbers in the address input area.

Netmask

Enter the net mask value.

Enter 0 to 255 numbers in the address input area.

Advanced settings

Set up a masked net mask or change an IP address.

Option button

Press this button to configure attributes for the takeover IP address. For more information, see "Setting up Takeover IP Address Attributes" below.

**Note**

If `/usr/opt/reliant/etc/hvipalias` and `/etc/inet/hosts` files have been modified to accommodate the entries for the takeover IP address and node name takeover in advance (as described in the Prerequisites section), message 0840 appears when the Next button is clicked. This message confirms whether the existing values are to be used without modification. To use the values, select Yes.

If you select *No*, the existing settings in the file are deleted and the GUI re-creates the information. In this case, takeover network information can be deleted automatically from `/usr/opt/reliant/etc/hvipalias` and `/etc/inet/hosts` when the `laddress` resource is deleted.

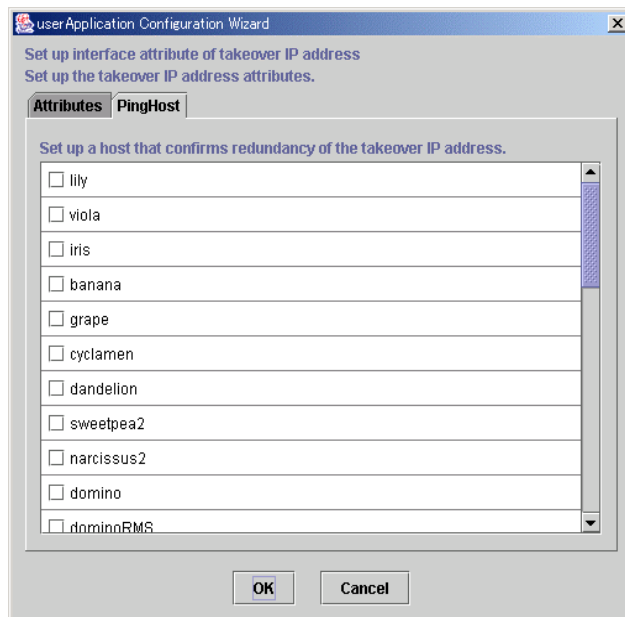
◆ **Attribute setup for the takeover IP address**

Configure the interface attributes for the takeover IP address.

Attribute setup for takeover IP address

Attribute	Value
BASE	virtual
AUTORECOVER	Yes

Flag	Outline
BASE	<p>If this flag is set to "base," the specified address is assigned to the physical interface.</p> <p>If this flag is set to "virtual," the specified address is assigned to the virtual interface.</p> <p>The default value is "virtual."</p> <p>[Note] To specify MAC address takeover in the interface attributes of the takeover IP address, change this setting from "virtual" to "base."</p>
AUTORECOVER	<p>If this flag is set to "Yes", RMS automatically attempts to create an interface if the specified address becomes disabled. A failure of this attempt might trigger Fault processing.</p> <p>The default value is "Yes."</p>

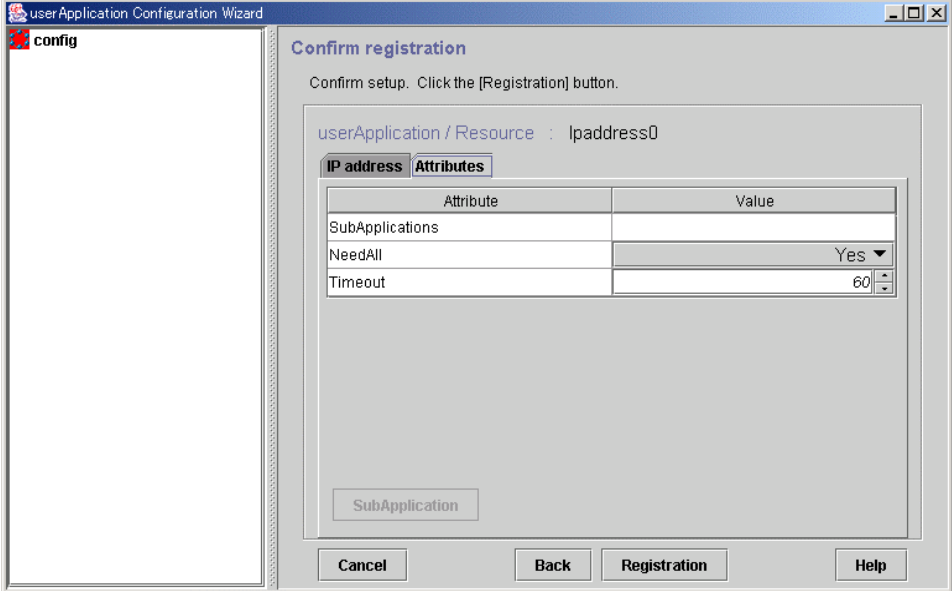
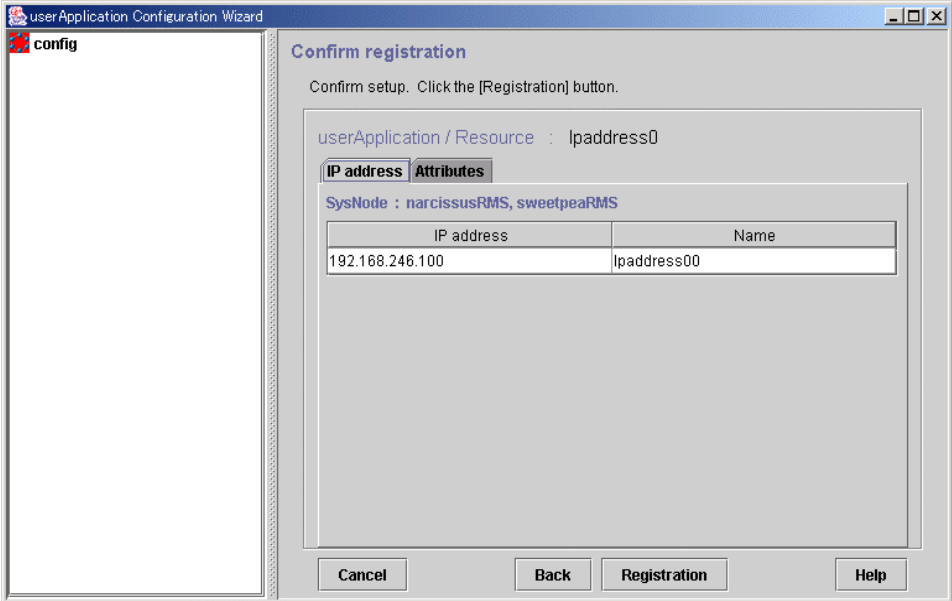


After the setup is completed, click *OK* to return to the "Select IP address and host name" screen. The availability of the takeover IP address is verified by executing the "ping" command. We recommend that you specify two or more hosts, which are not used for the cluster system, and are in the same network segment that does not use a hub or router. This prevents adverse effects from hub and router failures. The host information to be used by PingHost must be in `/etc/inet/hosts`.

■ **Checking registration information for the takeover network**

Check the registration information for the takeover network. You can also set resource attributes by selecting the *Attributes* tab and switching the screen. For information on the resource attributes, see 6.6.5 "Attributes."

Confirm registration



SubApplication button

Select this button to associate a previously created takeover network under the current takeover network. This button can be selected only if there are resources of the same type that can be associated. For setting instructions, see "Resource association" in 6.6.1.1 "Creating Cmdline Resources."

Check the registration information, and then click *Registration*.

6.6.1.6 Creating Procedure Resources

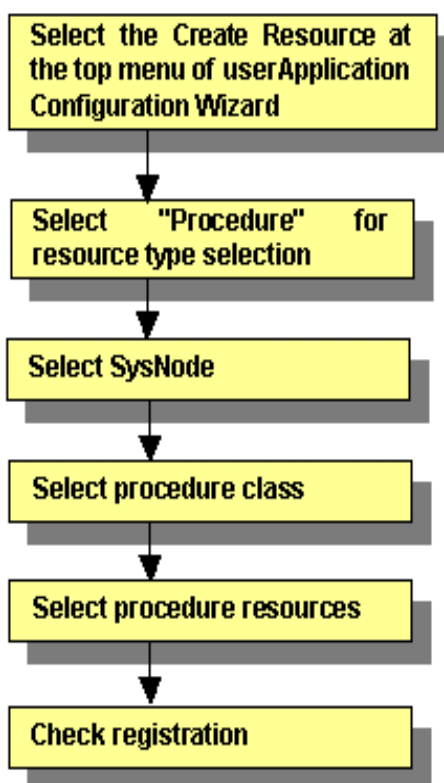
6.6.1.6.1 Prerequisites

To create a procedure resource, you must first create a state transition procedure and register the procedure to the resource database.

6.6.1.6.2 Setup Instructions

Register the procedure resources that were registered to the cluster resource manager to RMS.

Flow of procedure resource creation

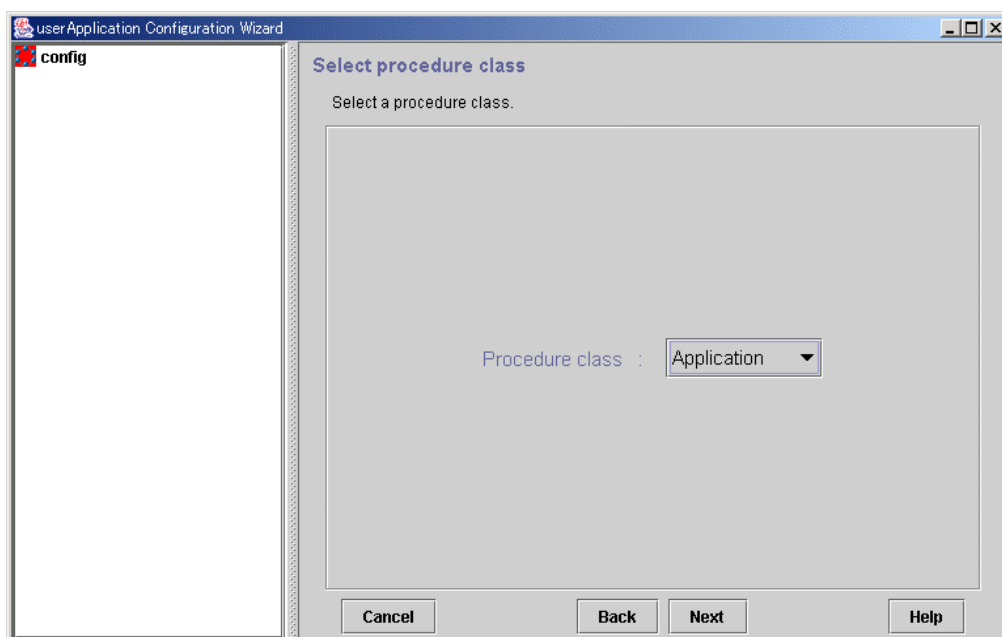


For information on the above operations up to "Select SysNode," see 6.6.1.1 "Creating Cmdline Resources." This section describes the operations from *Select procedure class*.

■ Selecting the procedure class

Select the procedure class to be created.

Select procedure class



Procedure class

Select the procedure class. Only the resource classes of resources that have been registered to the cluster resource manager are displayed. For example, if only procedure resources of the *Application* class have been registered, only *Application* is displayed.

The class resource manager provides four standard procedure classes:

- **Application**
This class is used to make general applications to be cluster-aware.
- **BasicApplication**
It is a class used for DBMS.
- **SystemState2**
It is used to make a part of OS functionality cluster-aware. This OS function should be started at "/etc/rc2.d" in a non-cluster single node. SystemState2 does not automatically start during OS startup. It is used to start a cluster application only on the OPERATING node.
- **SystemState3**
It is used to make a part of OS functionality cluster-aware. This OS function should be started at "/etc/rc3.d" in a non-cluster single node. SystemState3 does not automatically start during OS startup. It is used to start a cluster application only on the OPERATING node.



Note

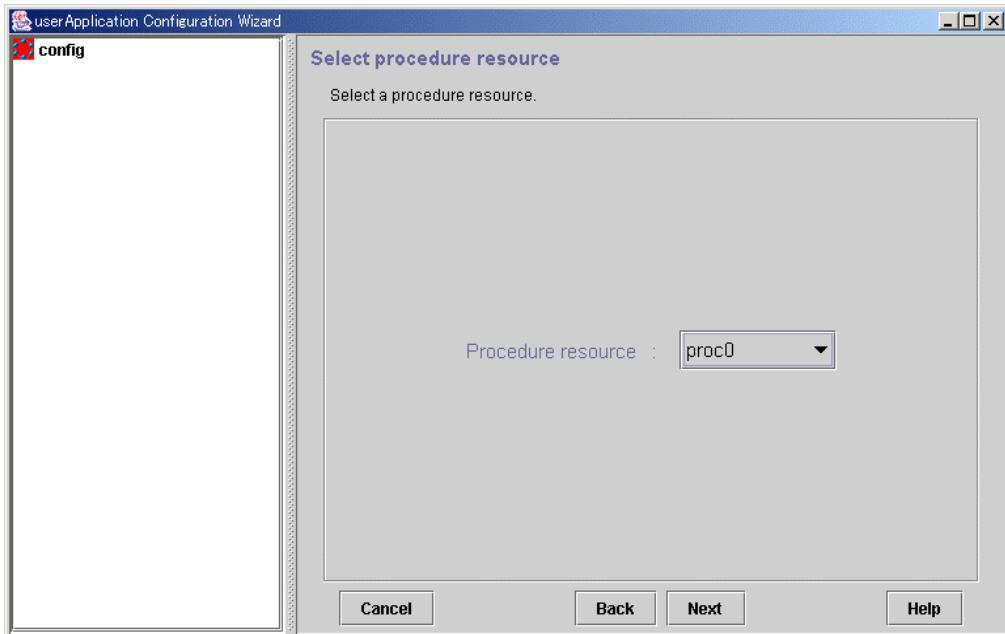
To create an application resource that is set in one cluster application on each node, the application resource name should be the same as the application type on each node.

After completing the setup, click *Next* to go to the "Select procedure resource" screen.

■ Selecting the procedure resource

Select the procedure resource to be created.

Select procedure resource



Procedure resource

Select the procedure resource to be created from the displayed list. The procedure resource name consists of up to 32 characters.

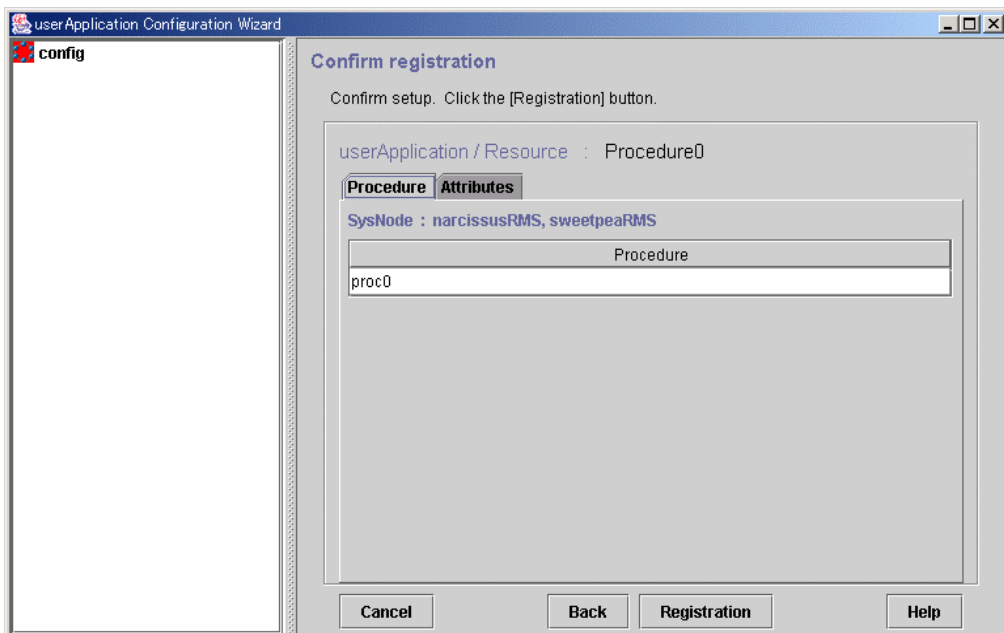
After completing the setup, click *Next* to go to the "Confirm registration" screen.

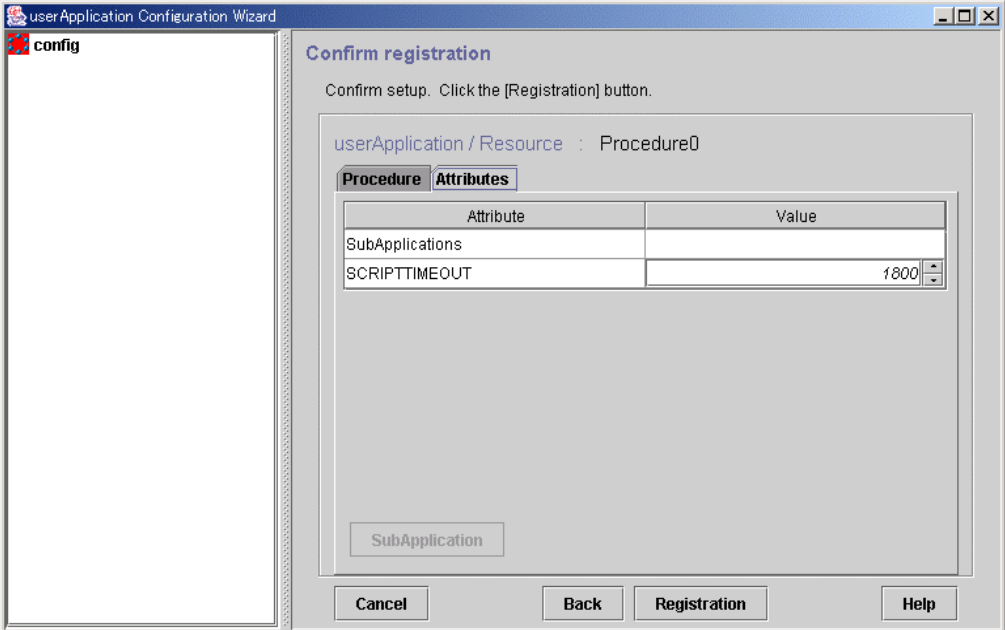
■ Checking the registration information for the procedure resource

Check the registration information for the procedure resource. You can also set resource attributes by selecting the *Attributes* tab and switching the screen.

For information on the resource attributes, see 6.6.5 "Attributes."

Confirm registration





SubApplication button

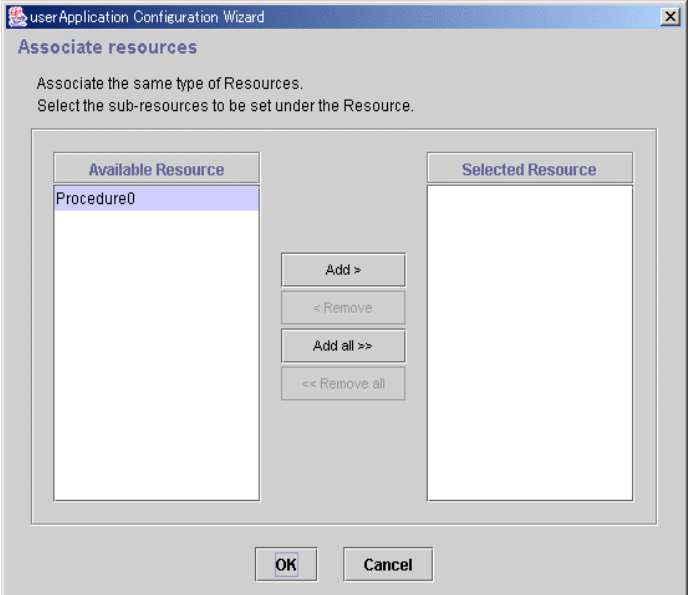
This button associates the other procedure resources to the procedure resource that has been created above. For more information, see "Associate resources," which is described later.

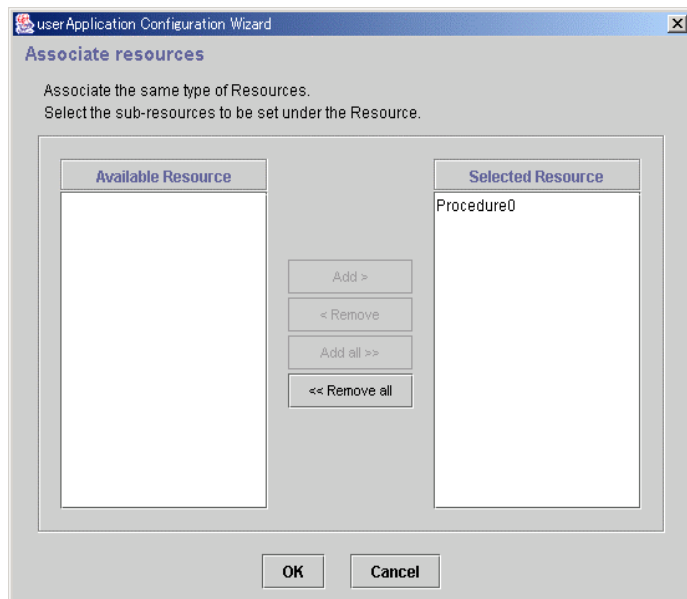
Check the registration information, and then click *Registration*.

■ **Resource Association**

Use resource association to assign a startup order to resources of the same type.

Associate resources





Available Resource

Available resource is referred to as the resource of the same type that can be associated, and satisfies the following conditions.

- The resource is of the same type as the resource that was called.
- The resource is not being used by another cluster application.

Selected Resource

Resources to be set under the current resource being created.

From *Available Resource*, select the resources to be configured under the current resource, and then click *Add*. To add all listed resources, click *Add all*. To remove a resource, select the resource to be removed from *Selected Resource*, and then click *Remove*. To delete all listed resources, click *Remove all*.

After completing the setup, select *OK* to return to the “*Confirm registration*” screen.

6.6.1.7 Creating Process Monitoring Resources

This section describes how to set up process monitoring resources.

Before describing the setup method, this section also outlines the process monitoring function and prerequisites for specific uses.

6.6.1.7.1 What Is the Process Monitoring Function?

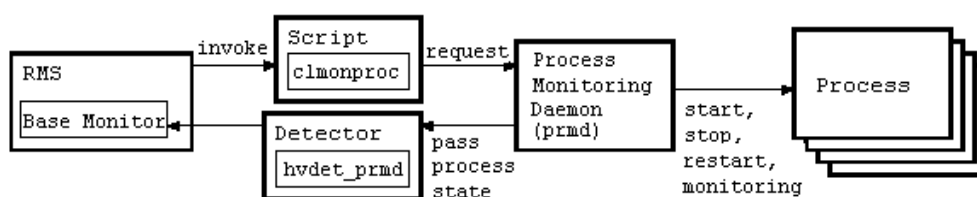
■ Overview of the process monitoring function

The process monitoring function monitors the live state of processes. The main features are as follows:

- Changes in the live status of a process can be monitored.
(This setup is quite easy, so the user does not need to prepare commands for monitoring the live status of a process.)
- Notifies RMS of the live state of any process immediately, and this provides high-speed switchover.
- If any process terminates abnormally because of an unexpected error, that process is automatically restarted.

A relationship diagram of the process monitoring function and RMS is shown below. The process monitoring function consists of three components: the “clmonproc” command, the Process Monitoring Daemon (prmd), and the Detector (hvdet_prmd).

- “clmonproc” command
The “clmonproc” command is executed from the Online or Offline script. The command requests prmd to start a specified process and to stop live monitoring.
- prmd daemon
prmd is a daemon process that starts a process and stops live monitoring according to requests received from the “clmonproc” command. If the live state of a process being monitored changes, prmd notifies hvdet_prmd immediately.
- hvdet_prmd daemon
After receiving change information on the live state of a process from prmd, the “hvdet_prmd” process notifies the RMS Base Monitor (BM) of the changes.



■ Benefits of using the process monitoring function

Described below are the benefits of using the process monitoring function.

- **Easy setup**
Since prmd monitors whether there are any processes to be monitored, the user does not need to create a check command for each process to be monitored. The check command is used to determine whether the process to be monitored exists. Therefore with little work, the user can easily monitor the existence of processes.
- **High-speed detection of abnormal process termination**
If the process monitoring function is not used, abnormal termination of a monitored process is detected by using a Cmdline resource to execute the “aforementioned check” command periodically. This delays detection of abnormal termination of a monitored process by execution

time interval of the check command. However, if the process monitoring function is used, `prmd` uses signal processing to detect abnormal termination in monitored processes. This process monitoring function allows abnormal process termination to be detected at high speed compared to when check commands are executed periodically.

- **Automatic restart of any process that terminates abnormally**

If any process terminates abnormally because of an unexpected error, the process monitoring function restarts that process automatically.

- **Reduction of CPU resource consumption**

To shorten the time required to detect abnormal termination of a monitored process without using the process monitoring function, you must shorten the execution time interval of the check command. However, since this leads to frequent generation and execution of the check command, many CPU resources may be used up. Generally a command like the “`ps`” command is used as the check command. However, when a command that uses relatively more CPU resources, like the “`ps`” command, is used, the CPU resource consumption may become even more pronounced.

When the process monitoring function is used, `prmd` uses a signal process to monitor abnormal termination of the monitored process. A process that uses many CPU resources, such as one that issues a check command periodically, is not executed.

With the method that uses `Cmdline` resources, the number of check commands increases in proportion to the number of RMS objects because a check command is executed for each RMS object that is defined by the process to be monitored. Therefore if many check commands are executed periodically, many CPU resources may be used.

When the process monitoring function is used, it is always just one `prmd` that monitors the live stage of the process. Therefore, `prmd` does not use many CPU resources in proportion to the increase in the number of processes to be monitored.

6.6.1.7.2 Prerequisites

Normally, you do not need to work on this prerequisite for using the process monitoring function. This is required only when you want to use the processing monitoring function for the specific purpose described below.

- **Monitoring an application consisting of multiple processes**

To use the process monitoring function to monitor an application composed of multiple processes, you must specify “`clmonproc`” command descriptions for starting those processes in one script. You must then specify that script to the “`start`” command that is described later.



Example

[Script creation example]

If an application composed from three processes (`/bin/proc0`, `/bin/proc1`, and `/bin/proc2`) is to be monitored, you need to create a script that describes the “`clmonproc`” command for starting the three processes.

```
#!/bin/sh
ExecProc () {
    /etc/opt/FJSVcluster/bin/clmonproc -s -R $HV_NODENAME -a "$1"
    if [ $? -gt 0 ]
    then
        exit 1
    fi
}
```

```
ExecProc "/bin/proc0"
ExecProc "/bin/proc1"
ExecProc "/bin/proc2"
exit 0
```

■ Changing the detector identification number

The identification number of the detector (the state notification module for notifying RMS) used by the process monitoring function is the same as the identification number to be used by other functions.



Note

- The GUI uses "0" (default value) as the detector identification number of the process monitoring function. If a detector identification number other than "0" is already used, use that value.
- This setup is required only for changing the detector identification number from the default value "0."
- In this setup, the setting of the detector identification number must not exceed the allowed value "127."
- Configure the same detector identification number on all cluster nodes.
- Stop RMS and all running cluster applications on all nodes before changing the identification number.



Example

In the example described below, the detector identification number of the process monitoring function is changed from the initial value "0" to "2."

If the process monitoring function is being used with the initial value "0," the setting "detector_name_of_process_monitoring_function.g"identification_number" will exist. Remove that setting.

```
# cd /usr/opt/reliant/bin
# ls -l hvdet_prmd.g0
lrwxrwxrwx 1 root other 31 Dec 20 12:21 hvdet_prmd.g0 ->
/usr/opt/reliant/bin/hvdet_prmd*
# rm hvdet_prmd.g0
```

Execute the "clmonsetdet" command as shown below. For the command argument, specify "2," which is the new detector identification number.

```
# /etc/opt/FJSVcluster/bin/clmonsetdet 2
```

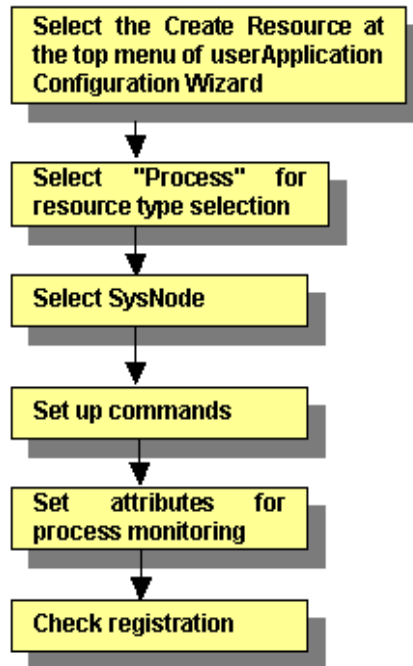
Check whether the settings were set correctly.

```
# ls -l hvdet_prmd.g2
lrwxrwxrwx 1 root other 31 Dec 27 12:21 hvdet_prmd.g2 ->
/usr/opt/reliant/bin/hvdet_prmd*
#
```

6.6.1.7.3 Setup Instructions

This section explains how to create process monitoring resources.

Flow of process monitoring resource creation

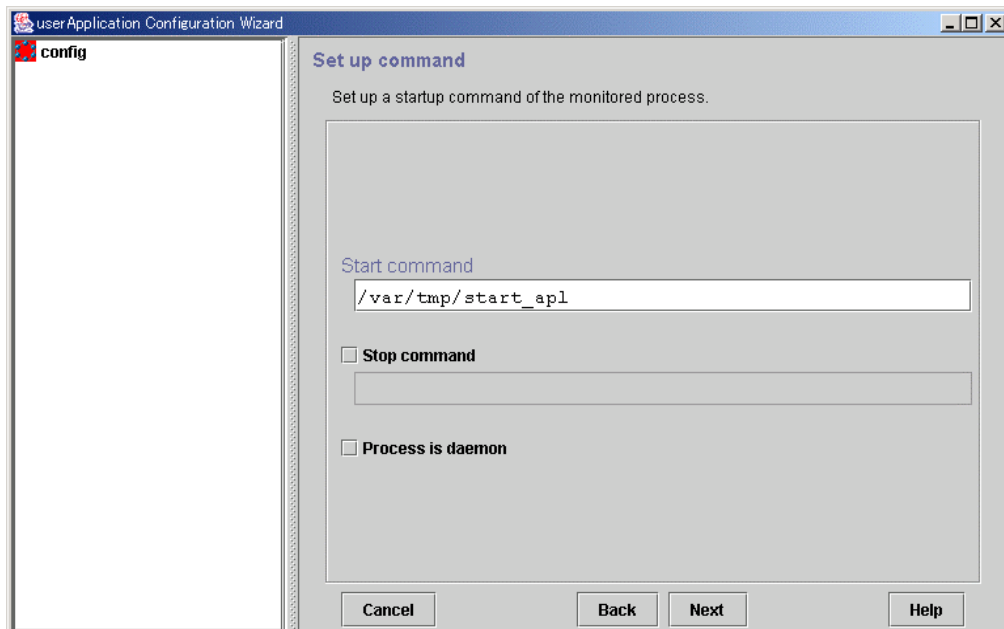


For information on the above operation up to "Select SysNode," see 6.6.1.1 "Creating Cmdline Resources." This section describes the operations from "Set startup path."

■ **Inputting the process startup command**

Enter the startup path of the process to be monitored.

Set up command



Start command

Enter the command line for starting the process to be monitored during online processing using a full path. If spaces are included in the command line, the startup path must be enclosed in double quotation marks ("").

For example, enter the command line as follows:

```
"/var/tmp 1/start_apl"
```

Stop command

Enter the method for stopping the monitored process during Offline processing. If there is a command for stopping the monitored process, set the checkbox to ON, and enter the command line using a full path. If spaces are included in the command line, the command line must be enclosed in double quotation marks (""). For example, enter the command line as follows:

```
"/var/tmp 1/stop_apl"
```

If the stop command is omitted, the software exit signal (hereafter referred as SIGTERM) is sent from the process monitoring facility to stop the monitored process. Some processes might not be stopped by SIGTERM. In that case, Offline processing will fail.

Process is daemon

Specify this item if the monitored process is to be operated as a daemon. A daemon refers to a process that executes the following types of processes at startup:

- Execution in the background
- Promotion to process group leader

The former refers to child process generation when the fork system call is issued and termination of the parent process when the exit system call is issued. The latter refers to promotion to process group leader when the setpgrp system call is issued.



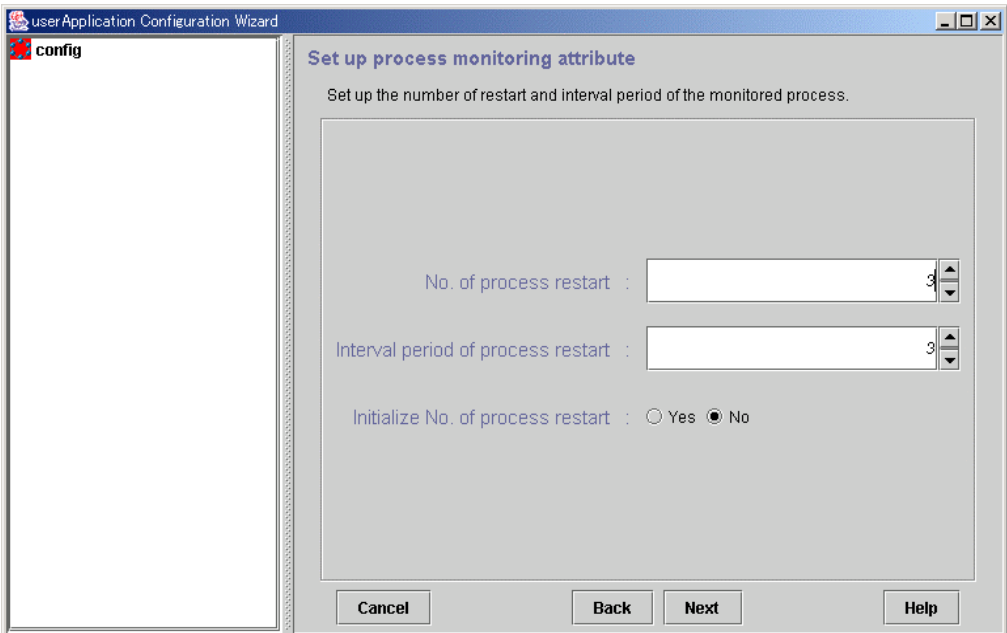
Note

- The following characters cannot be used in the file name or the arguments: back slash ("¥"), tilde ("~"), percent sign ("%"), ampersand ("&"), and at sign ("@").
- Single quotation marks ("'") and tabs cannot be entered.
- If a stop command is entered, a script for executing that command is created automatically. The script is stored in the following directory:
/opt/FJSVwvcw/scripts/process_stop

■ **Setting attributes for the process**

Enter attributes for the process to be monitored

Set up process monitoring attribute



No. of process restart

Specify the number of times the monitored process is to be restarted between 0 and 99 (default is 3). If 0 is specified and the monitored process stops, the process will become Faulted.

Interval period of process restart

This is the interval from when the process monitoring facility determines that the process has stopped until the facility executes restart. The specification range is 0 to 3600 seconds (default: 3 seconds).

Initialize No. of process restart

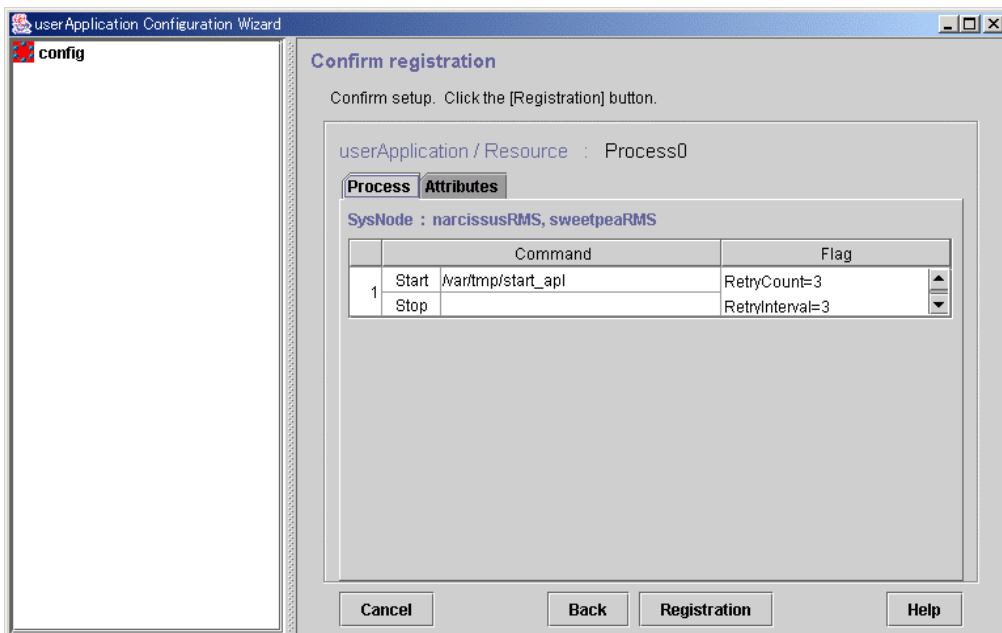
Specify whether or not the counter that has the specified *No. of process restart* value in the process monitoring facility as its maximum value is to be initialized periodically. If you select Yes, the counter is initialized every "*No. of process restart* value x 60 seconds." If you select No, the counter is not initialized periodically.

■ **Checking the registration information of the process monitoring resource**

Check the registration information for the process monitoring resource. You can also configure resource attributes by selecting the *Attributes* tab and switching the screen.

For information on the resource attributes, see 6.6.5 "Attributes."

Confirm registration



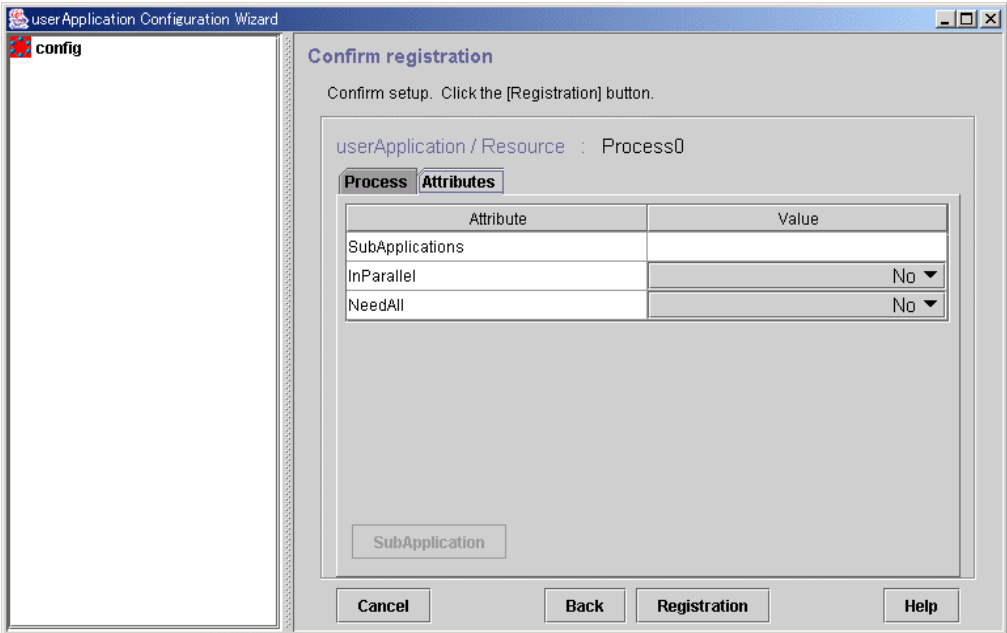
Flag

RetryCount indicates the number of times the process is to be restarted.

RetryInterval indicates the interval before starting the process.

Initialize=Yes indicates that the retry count of the process is to be initialized periodically. If No was specified for *Initialize No. of process restart* in the "Set up process monitoring attribute" screen, this attribute is not displayed.

Daemon=Yes indicates that the process is to be started as a daemon. If *Process is daemon* was not checked at the command setup screen, this attribute is not displayed.



SubApplication button

This button associates the other processing monitoring resources to the Cmdline or process monitoring resource that has been created above. This button can be selected only if there are resources that can be associated. For setting instructions, see "Resource association" in 6.6.1.1 "Creating Cmdline Resources."

After checking the registration information, click *Registration*.

6.6.1.8 Creating Line Switching Unit Resources

You should complete on the prerequisites before creating a line switching unit resource.

6.6.1.8.1 Prerequisites

You must always perform the setup described below before using a line switching unit resource.

■ Resource registration

To use a line switching unit, you must first register a switching line resource (SH_SWLine class) to the resource database.

This section describes the procedure for registering a switching line resource to the resource database.

◆ Registration procedure flow

1. Check the resource name of the line switching unit.
2. Register the switching line resource.
3. Check the registration information.

◆ Registration procedure

1. Confirmation of the resource name of the line switching unit resource
Check the resource names of the line switching units that are registered to the resource database by using the “clgettree(1)” command.

```
# clgettree
Cluster 1 cluster
  Domain 2 CLUSTER
    Shared 7 SHD_CLUSTER
      SHD_DISK 21 SHD_Disk21 UNKNOWN
        DISK 22 c5t0d0 ON node1
        DISK 27 c4t0d0 ON node2
      SH_SWU 18 SWU2002 UNKNOWN
    Node 3 node1 ON
      Ethernet 29 hme0 ON
      DISK 19 c0t0d0 UNKNOWN
      DISK 22 c5t0d0 ON
    Node 5 node2 ON
      Ethernet 30 hme0 ON
      DISK 25 c0t0d0 UNKNOWN
      DISK 27 c4t0d0 ON
```

In this example, the line indicating “SH_SWU” shows the resource name is “SWU2002”. If you cannot confirm the resource name, see 5.2.3.2 "Automatic Configuration" and register the line switching units to the resource database.



See

- For details on the information that is output by executing the “clgettree(1)” command, see "Explanation of resources related to line switching units."
- For details on the “clgettree(1)” command, see the manual page.

2. Registration of switching line resources

Execute the “claddswurc(1M)” command to add the switching line resources to the resource database.

```
# claddswurc -k sh_sw1_1 -s SWU2002 -0 node1 -1 node2 -m 0x3
```

In this example, the line switching unit called "SWU2002," which was checked in step 2, is used to register the switching line resource called "sh_sw1_1."

Port 0 of the switching unit is connected to "node1," and port 1 to "node2."

Since the two switching units LSU01 and LSU00 are to be used, the mask value is set to 0x3.



For details on the “claddswurc(1M)” command, see the manual page.

3. Confirmation of registration information

Execute the “clgettree(1)” command to check that the switching unit resources of the line switching unit have been registered to the resource database.

Example) Resources of the “SWLine” class are the switching unit resources of the line switching unit.

The resources of the “SH_SWLine” class show a sharing relationship of the switching units for the line switching unit.

```
# /etc/opt/FJSVcluster/bin/clgettree
Cluster 1 cluster
  Domain 2 CLUSTER
    Shared 7 SHD_CLUSTER
      SHD_DISK 21 SHD_Disk21 UNKNOWN
        DISK 22 c5t0d0 ON node1
        DISK 27 c4t0d0 ON node2
      SH_SWU 18 SWU2002 UNKNOWN
        SH_SWLine 19 sh_sw1_1 UNKNOWN
          SWLine 35 sh_sw1_1P0 UNKNOWN node1
          SWLine 36 sh_sw1_1P1 UNKNOWN node2
    Node 3 node1 ON
      Ethernet 29 hme0 ON
      DISK 19 c0t0d0 UNKNOWN
      DISK 22 c5t0d0 ON
      SWLine 35 sh_sw1_1P0 UNKNOWN
    Node 5 node2 ON
      Ethernet 30 hme0 ON
      DISK 25 c0t0d0 UNKNOWN
      DISK 27 c4t0d0 ON
      SWLine 36 sh_sw1_1P1 UNKNOWN
```

■ Explanation of resources related to line switching units

This section explains the information that is output by the “clgettree” command.

[Output example]

```
Cluster 1 cluster
  Domain 2 CLUSTER
```

```
Shared 7 SHD_CLUSTER
  SHD_DISK 21 SHD_Disk21 UNKNOWN
    DISK 22 c5t0d0 ON node1
    DISK 27 c4t0d0 ON node2
  SH_SWU 18 SWU2002 UNKNOWN ..... (a)
    SH_SWLine 19 sh_swl_1 UNKNOWN ..... (b)
      SWLine 35 sh_swl_1P0 UNKNOWN node1 ..... (c)
      SWLine 36 sh_swl_1P1 UNKNOWN node2 ..... (d)
Node 3 node1 ON
  Ethernet 29 hme0 ON
  DISK 19 c0t0d0 UNKNOWN
  DISK 22 c5t0d0 ON
  SWLine 35 sh_swl_1P0 UNKNOWN
Node 5 node2 ON
  Ethernet 30 hme0 ON
  DISK 25 c0t0d0 UNKNOWN
  DISK 27 c4t0d0 ON
  SWLine 36 sh_swl_1P1 UNKNOWN
```

[Explanation]

- (a) This line identifies a line switching unit resource.

In the example shown in the above figure, "SWU2002" is the resource name of the resource representing the line switching unit.

This resource is displayed when PRIMECLUSTER recognizes the line switching unit when automatic resource registration is executed.

- (b) This line identifies a switching line shared resource of the line switching unit.

In the example shown in the above figure, "sh_swl_1" is the resource name of the switching line shared resource (switching line name).

This resource is displayed when the switching line resources of the line switching unit are registered to the resource database with the "claddswursc" command.

As shown in the example of the above figure, this resource belongs to the "SH_SWLine" class.

- (c),(d)

These lines represent switching line resources of the line switching unit.

In the example shown in the above figure, "sh_swl_1P0" and "sh_swl_1P1" are resource names for switching line resources.

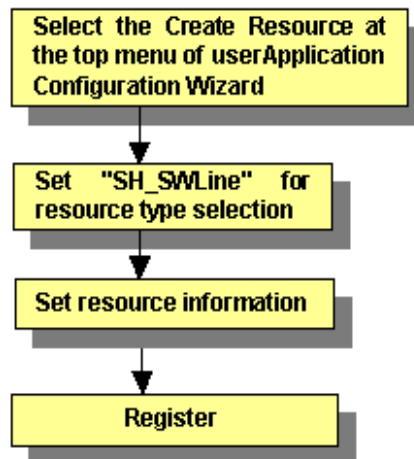
These resources are displayed when the switching line resources of the line switching unit are registered to the resource database with the "claddswursc" command.

As shown in the example of the above figure, these resources belong to the "SWLine" class.

6.6.1.8.2 Setup Procedure

This section describes the procedure for setting up a line switching unit resource.

Flow of creating a line switching unit resource



For information on the above operations up to "Selecting SH_SWLine for resource type selection," see 6.6.1.1 "Creating Cmdline Resources." This section describes the operations from "Set resource information."



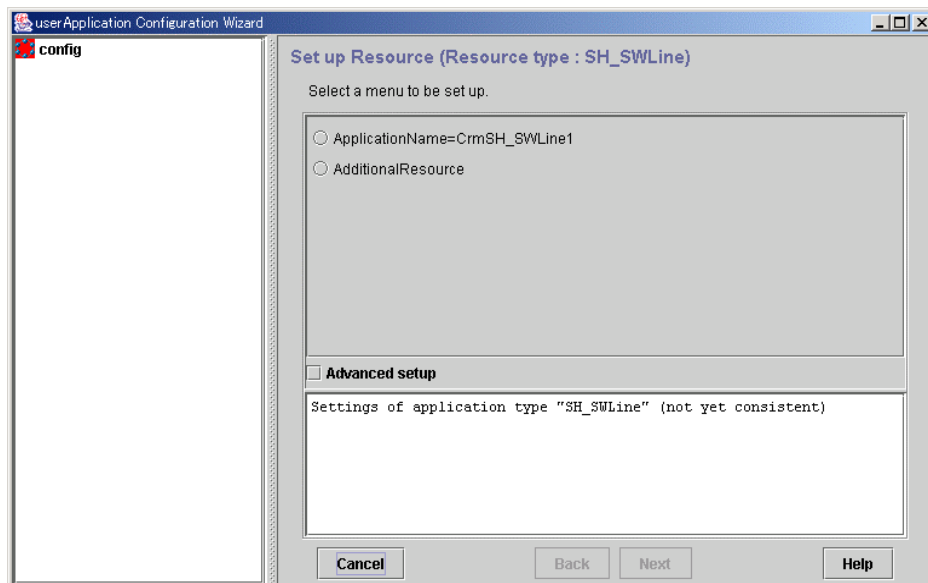
Note

The displayed Help information when you click the *Help* button includes the information for CUI only.

■ Setting resource information

1. Display the top screen.

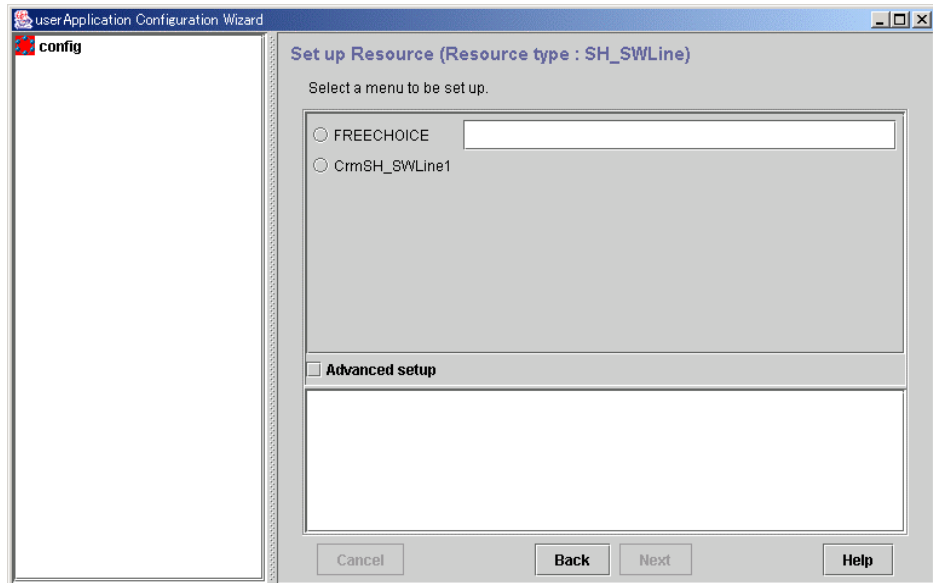
Select *SH_SWLine* for the resource type selection. The following screen is displayed:



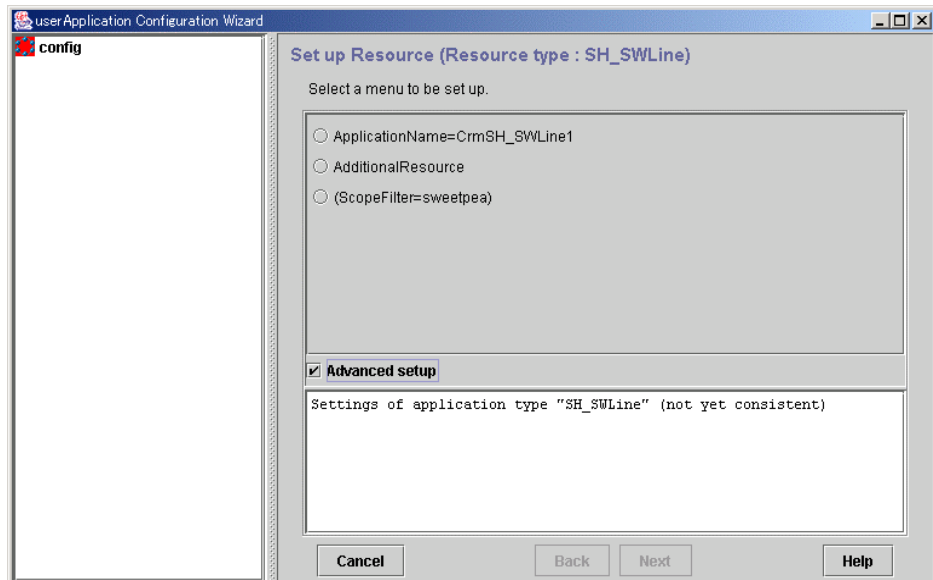
To terminate the selection process, click the *Cancel* button.

2. Check the name of the line switching unit resource.
 - name* in *ApplicationName=name* is the name of the line switching unit resource to be created.
 - If the name is correct, go to step 5.
 - To change the name, go to step 3.

3. Select *ApplicationName=name* and click the *Next* button.
The screen for changing the resource name is displayed.



4. Click *FREECHOICE* and enter the resource name. After entering the name, click the *Next* button.
An updated top screen containing the entered information is displayed. Go to step 2 to check the information.
5. Select the *Advanced setup* checkbox.
A new menu will be added to the screen.



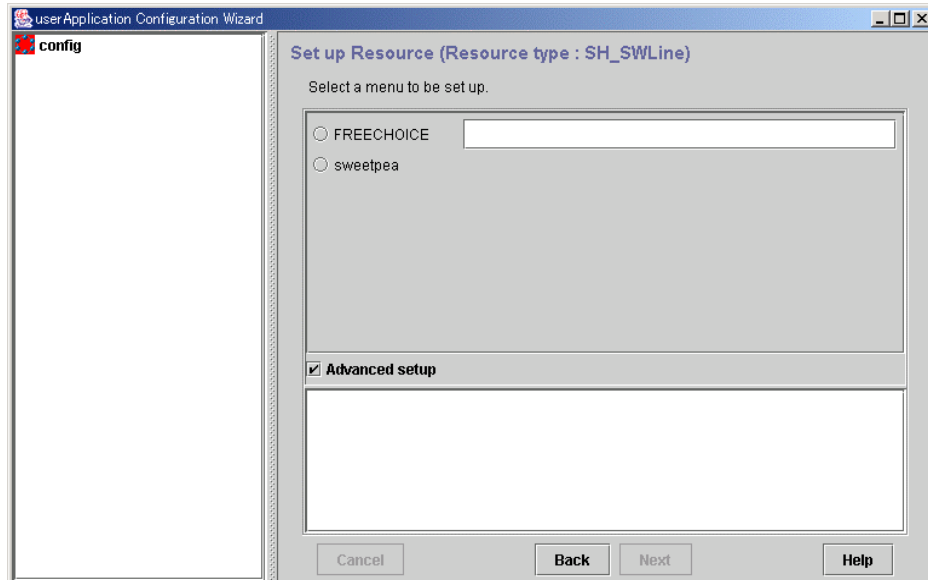
6. Check the nodes to which the line switching unit is connected.
node-names in *ScopeFilter=node-name* shows the CF node names, which are separated with colons (":").
 - If all nodes to which the line switching unit is connected are displayed, go to step 9.
 - If there is an error, go to step 7.



Of the switching line resources (SH_SWLine class) that are registered to the resource database, those resources that are common to these nodes can be added to the line switching unit resource according to the procedure described later.

7. Select *ScopeFilter=*node-names" and click *Next* button.

The screen for entering the nodes to which the line switching unit is connected are displayed.

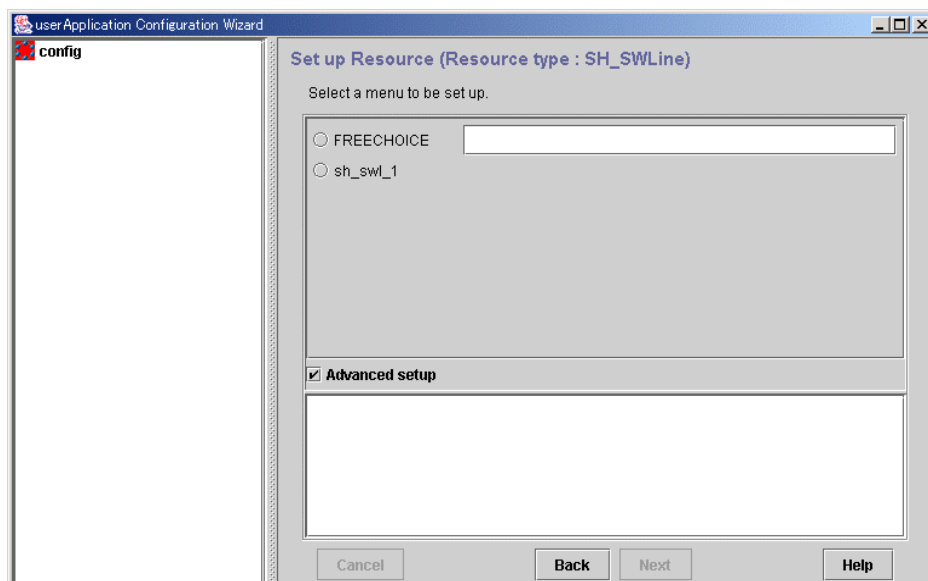


8. Click *FREECHOICE* and enter the names of the CF nodes to which the line switching unit is connected. Separate the names with colons (":"). After entering the CF node names, click the *Next* button.

An updated top screen containing the entered information is displayed. Go to step 5 and check the information.

9. Select *AdditionalResource* and then click the *Next* button.

The screen for selecting switching line resources that are registered to the resource database is displayed.



In the example shown in this screen, you can select the switching line resource called

sh_swl_1. If no other data is displayed besides *FREECHOICE*, the following causes can be considered:

- There is an error in the nodes that were checked in step 5.
- No switching line resource is registered to the resource database.

For the first case, return to step 5 and check the nodes. To return to step 5, click the *Back* button.

For the second case, see 6.6.1.8.1 "Prerequisites" and register a switching line resource to the resource database. To do this, click the *Back* button, and then click the *Cancel* button in the displayed screen. This stops the setup process, and you can start again from the beginning.

10. Select switching line resource from the candidate list, and click *Next*.

The top menu to which the switching line resource was added is displayed.

The information is displayed as follows:

```
cluster_resource[number]=rsc-name
      number      A number corresponding to the sequence in which the resource
was added is assigned.
      rsc-name    The resource name that was added is displayed.
```



Note

The attribute must not be changed. If you add a switching line resource, the Attribute menu is added. If you use this menu to change any attribute of the switching line resource, RMS will not operate correctly.

Go to step 1 of "Registering the information."

■ Registering the information

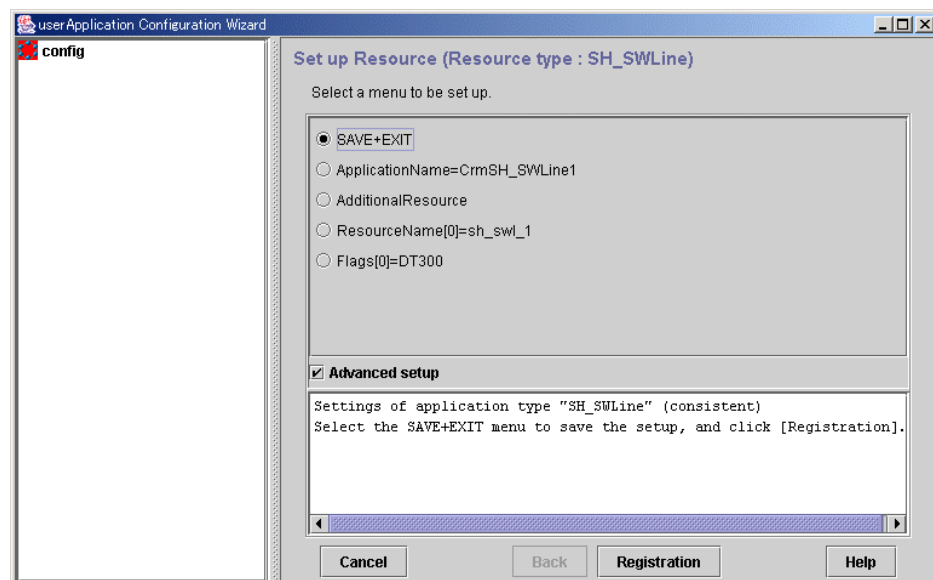
1. Select *SAVE+EXIT*.

When you select *SAVE+EXIT*, the *Next* button changes to the *Registration* button.



Note

If there is information that can be registered, the *SAVE+EXIT* menu will be added to the top screen.



2. Click the *Registration* button.

A line switching unit resource will be created according to the specified information, and the "userApplication Configuration Wizard Menu" screen will be displayed.
This ends the procedure.

6.6.1.9 Creating ISV Resources

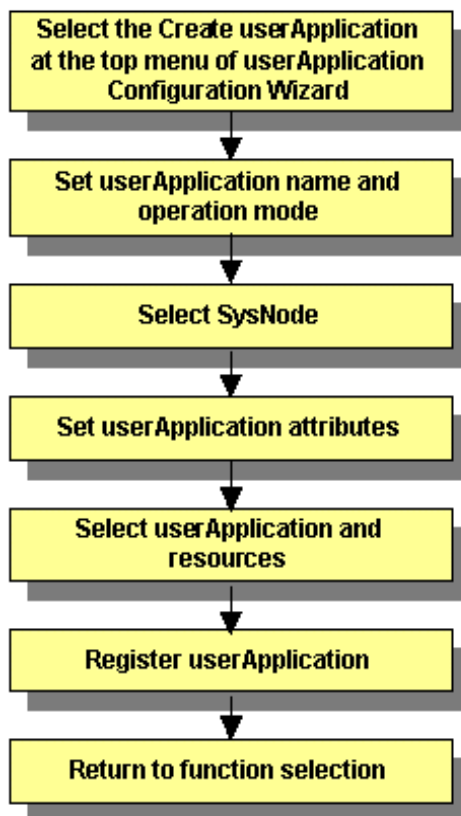
For information on ISV resource creation, refer to the manuals for the individual products.

6.6.2 Creating Cluster Applications

This section describes how to use the "userApplication Configuration Wizard" to register cluster applications (userApplication) to RMS.

The flow of cluster application (userApplication) registration is shown below.

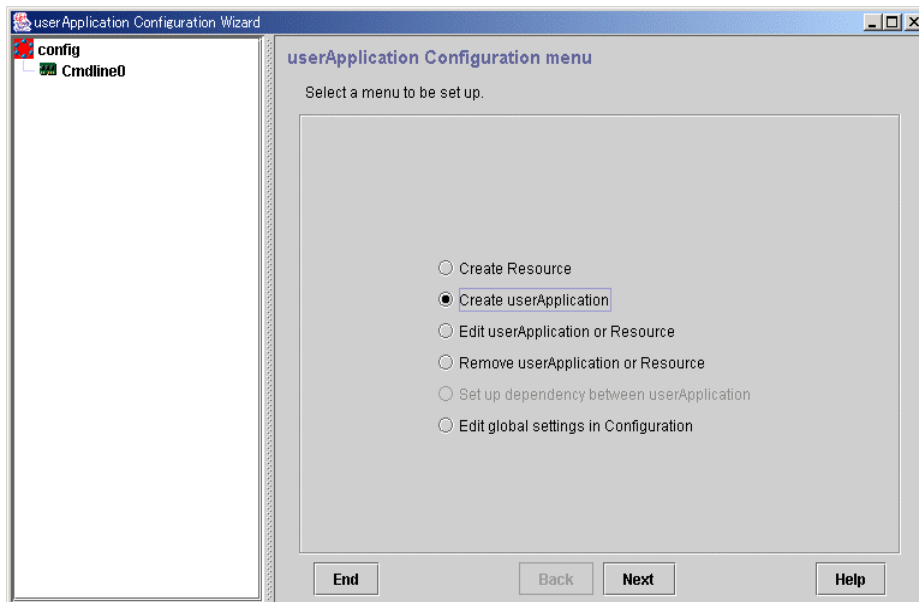
Flow of cluster application registration



■ Starting cluster application creation

At the top menu of the "userApplication Configuration Wizard," select *Create userApplication*.

Top menu of userApplication Configuration Wizard

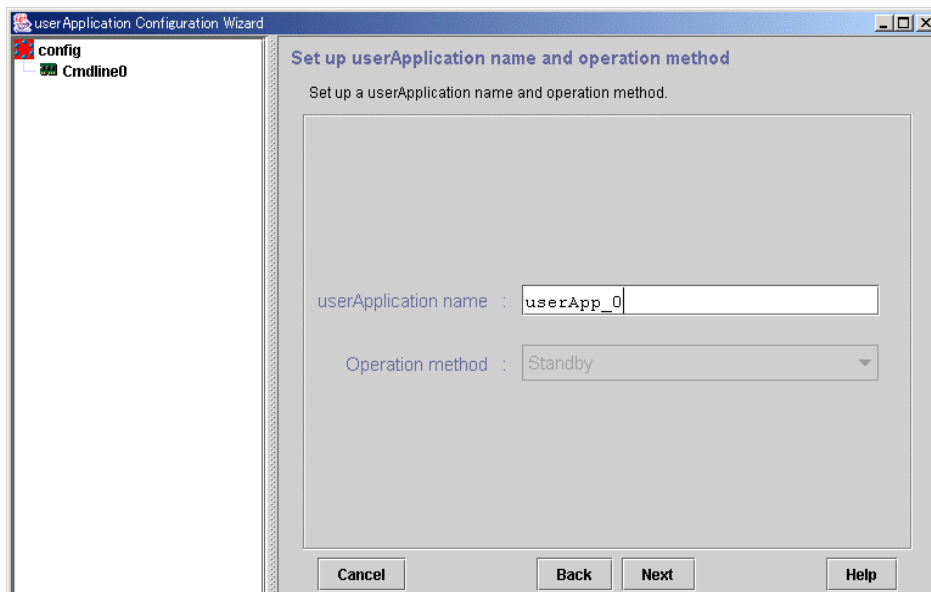


Click *Next* to go to the "Set up userApplication name and operation method" screen.

■ Setting the userApplication name and the operation method

Enter the userApplication name and the operation method.

Set up userApplication name and operation method



userApplication name

Specify the name of the cluster application.

Specify the input character string with **up to 18 characters**, starting with an alphabet letter and consisting of only alphanumeric characters and "_" (underscore). If a name that has 19 or more characters is specified for the cluster application name, RMS will not start.

Operation method

Specify Standby (standby operation) or Scalable (scalable operation) as the operation method of the cluster application. With this version, however, the operation method cannot be selected. Only Standby is supported.

— **Standby**

This is the default operation method. When multiple SysNode are selected, "priority" values must be set.

— **Scalable**

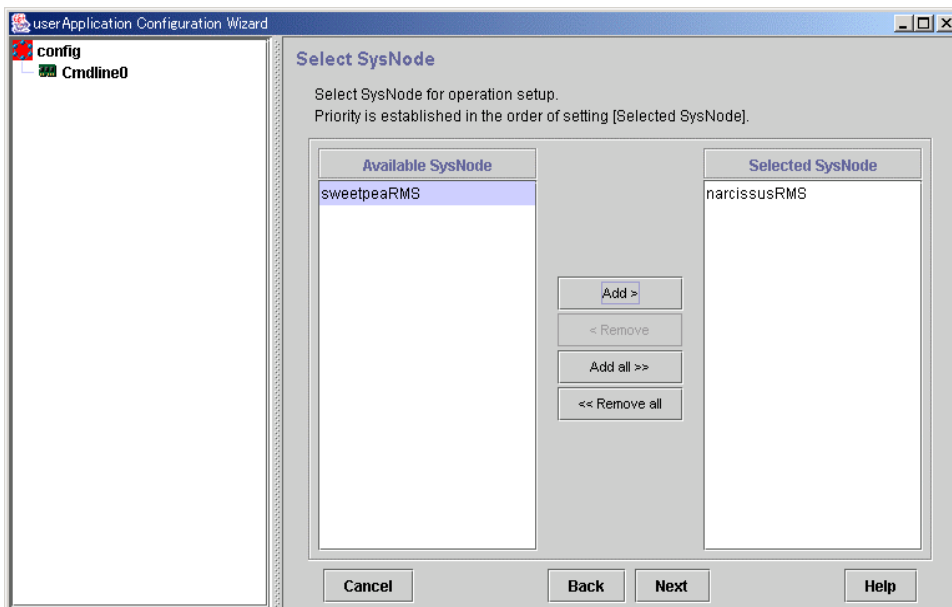
This is only for the cluster application resources displayed in *Resource Selection*. The priority does not need to be set even if multiple SysNode are selected. This operation method is not supported in this version.

After completing the setup, click *Next* to go to the "Select SysNode" screen.

■ **Selecting a SysNode**

Select the SysNode in which the cluster application is to be configured.

Select SysNode



Available SysNode

Contains names of available SysNodes that belong to the specified RMS configuration.

Selected SysNode

The name of the SysNode in which the cluster application is to be operated. The priority of SysNode is determined by the sequence in which SysNode are listed in this box. SysNode displayed at the top of the list becomes the Online SysNode when userApplication is started.

From *Available SysNode*, select the SysNodes in which the cluster application is to be built, and then click *Add*. To add all listed SysNodes, click *Add all*. To remove a SysNode, select the SysNode to be removed from *Selected SysNode*, and then click *Remove*. To remove all listed SysNodes, click *Remove all*.

After completing the setup, click *Next* to go to the "Set up attribute" screen.

■ **Setting cluster application attributes**

Refer to the items below when setting up the cluster application attributes:

- To start the cluster application automatically when the cluster is started
Set "AutoStartUp" to "Yes."
- Action to take if another error occurs during failover (double failure)
Set "HaltFlag" to "Yes."



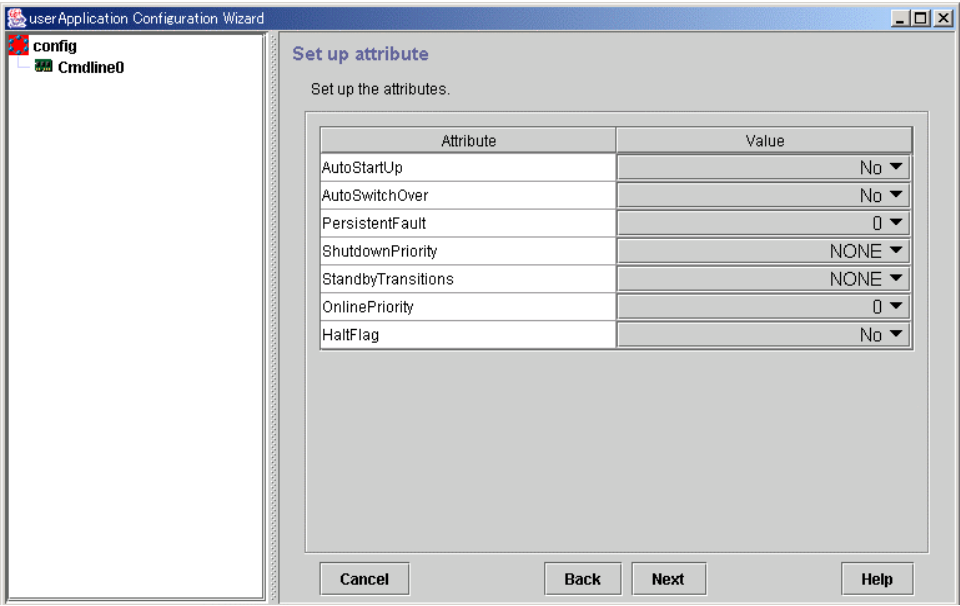
Note

To ensure safe operation, be sure to set this item to "Yes."

- For Standby operation
Set "StandbyTransitions" to "ClearFaultRequest|StartUp|SwitchRequest."

For details on attribute, see 6.6.5 "Attributes."

Set up attribute

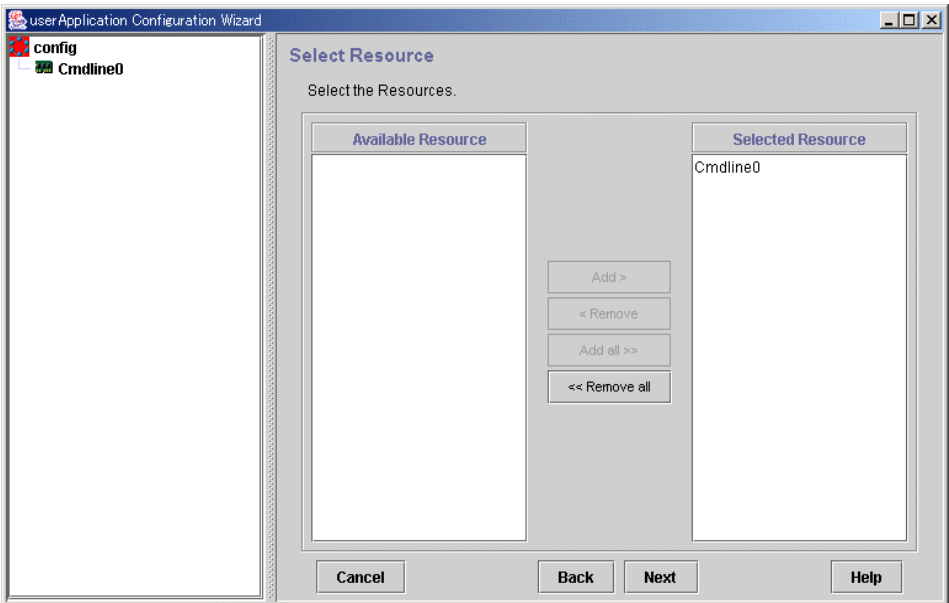


After completing the set up, click *Next* to go to the "Select Resource" screen.

■ **Selecting resources**

Enter the resources to be used by the cluster application.

Select Resource



Available Resource

The names of the resources that can be shared among the selected SysNodes are displayed. An available resource is one that was created with the same name in all the SysNodes that are specified by the cluster application.

Resources that are used by other userApplications are not displayed.

Selected Resource

The resources to be registered to the cluster application are displayed.

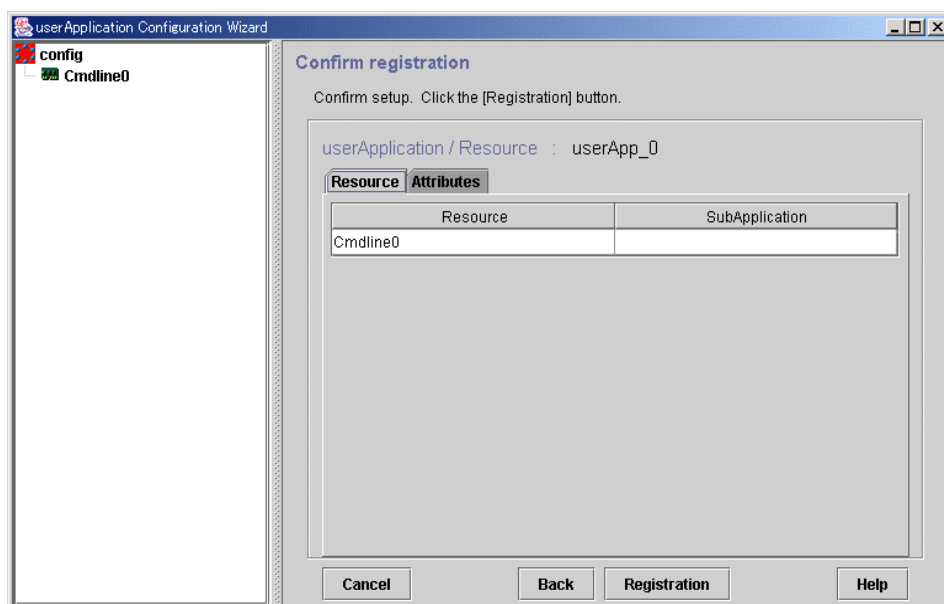
From *Available Resource*, select the resources to be used by the cluster application, and then click *Add*. To add all listed resources, click *Add all*. To remove a resource, select the resource to be removed from *Selected Resource*, and then click *Remove*. To remove all listed resources, click *Remove all*.

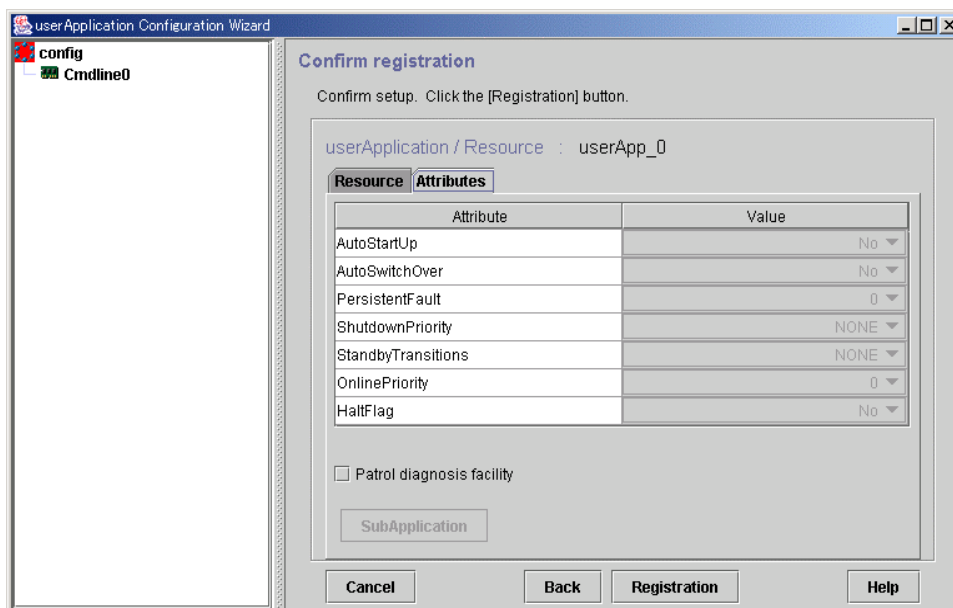
After completing the setup, click *Next* to go to the "Confirm registration" screen.

■ **Checking the registration information of a cluster application**

Check the registration information of the cluster application.

Confirm registration





Patrol diagnosis facility checkbox

Select this checkbox to enable the patrol diagnosis facility in the cluster application. See 6.7 "Setting Up Patrol Diagnosis."

SubApplication button

This button is always inactive.

The attributes displayed here cannot be changed. To change the attributes, you must return to "Setting Cluster Application Attributes."

Check the registration information, and then click *Registration*.



Note

The patrol diagnosis facility can be used in Standby operation. To enable the patrol diagnosis facility, set "ClearFaultRequest|Startup|SwitchRequest" to "StandbyTransitions" of the cluster application.

For details on attributes, see 6.6.5 "Attributes."

6.6.3 Setting Up Dependency Relationships Between Cluster Applications

You can set up exclusivity and startup priority as part of the RMS Configuration settings.

- **Setting up exclusive relationships between cluster applications**

Set exclusive control so that multiple cluster applications will not run concurrently in the same cluster node.

- **Setting the startup priority of a cluster application**

Determine the sequence in which the cluster applications are to be started.

If you omit this setup, the startup sequence of the cluster applications will be undefined.



Note

The startup priority setup function is not supported in this version.

6.6.3.1 Setting Exclusive Relationships Between Cluster Applications

If you set up exclusivity to a cluster application, that cluster application does not run with other applications at the same time.

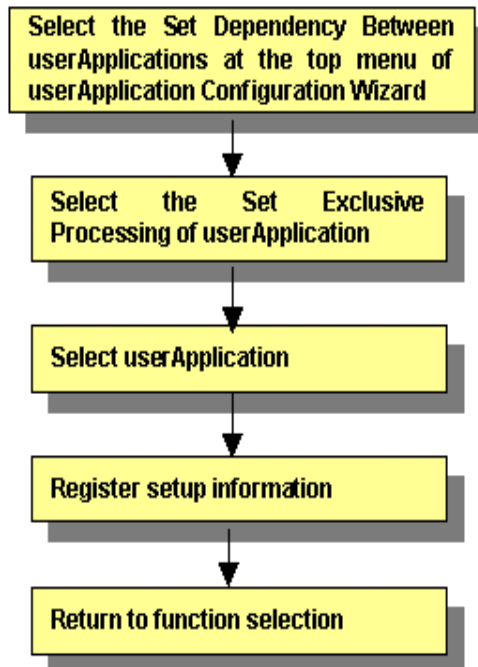
To set exclusivity, you need to create an exclusion group, and then add the cluster application to that group.

The features of an exclusion group are as follows:

- Exclusion group configuration
An exclusion group consists of one or more cluster applications.
- Business application priority
If a failover occurs, the cluster applications with high priority are run, and those with low priority are stopped.
 - A cluster application with exclusivity has a higher priority than cluster applications without exclusivity.
 - You can set an order of priority within the same exclusion group.
- Relationship with other exclusion groups
A cluster application that belongs to a different exclusion is not in a mutually exclusion relation with the current cluster application. Therefore that cluster operation can be operated at the same time in the same cluster node.

The procedure for setting up an exclusive relationship is described below.

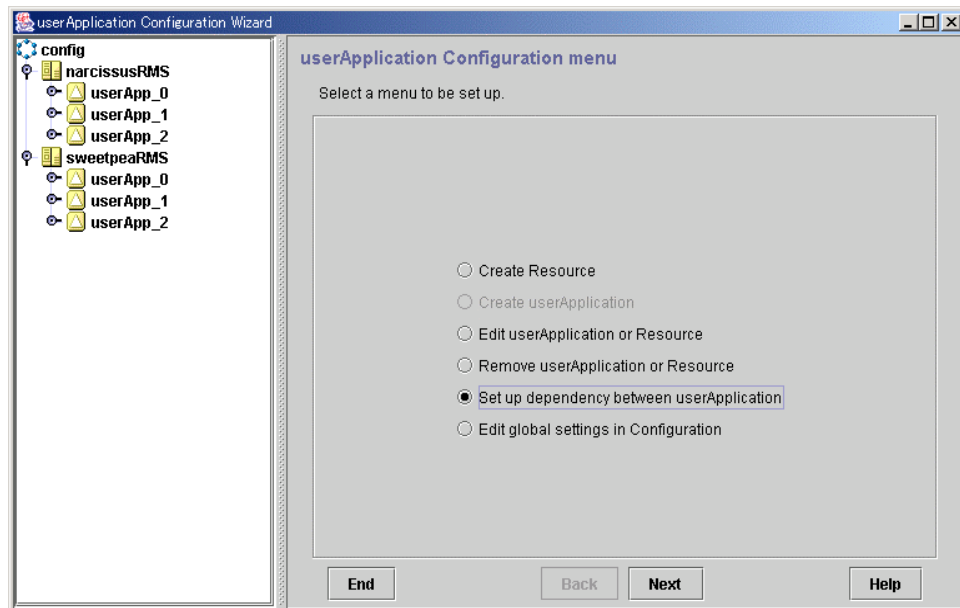
Flow of exclusive relationship setup



■ Starting the dependency relationship setup between cluster applications

At the top menu of the "userApplication Configuration Wizard," select *Set up dependency between userApplication*.

Top menu of the userApplication Configuration Wizard



Click *Next* to go to the "Set up startup priority and exclusivity of userApplication" screen.



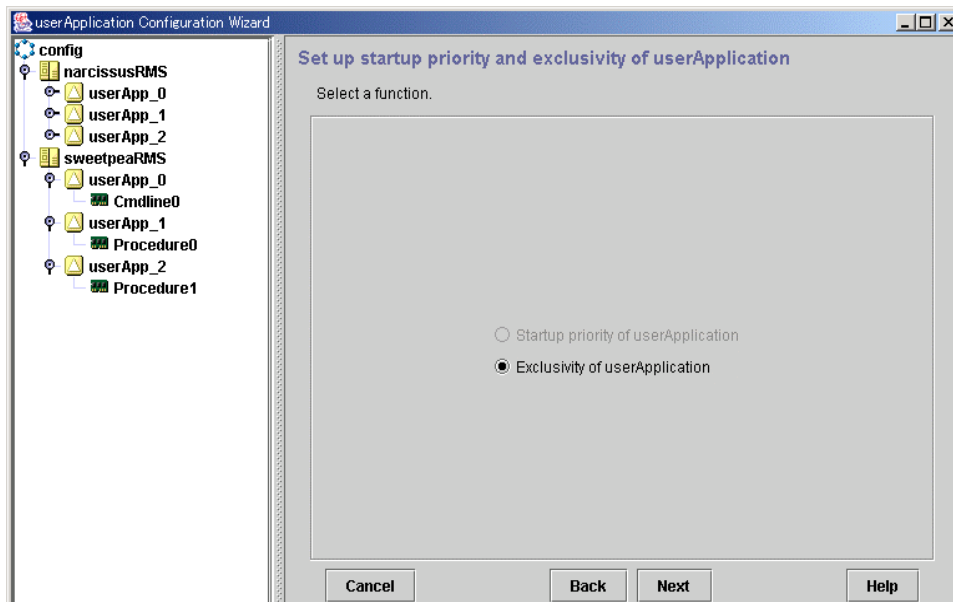
Note

The "Set up dependency between userApplication" menu item can be selected if there are two or more cluster applications in the cluster system.

■ Selecting a Dependency Relationship Between userApplications

Select *Exclusivity of userApplication*.

Set up startup priority and exclusivity userApplication

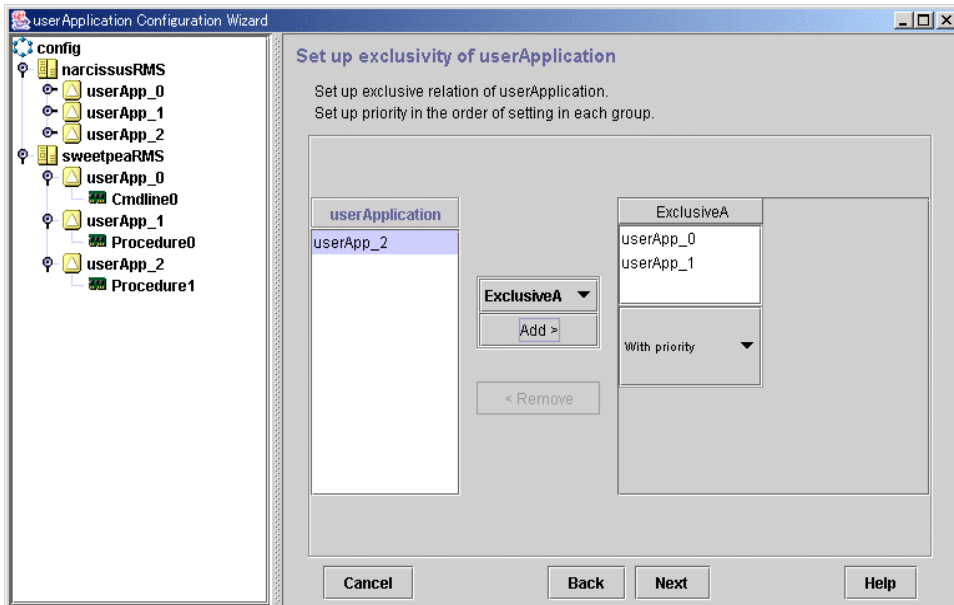
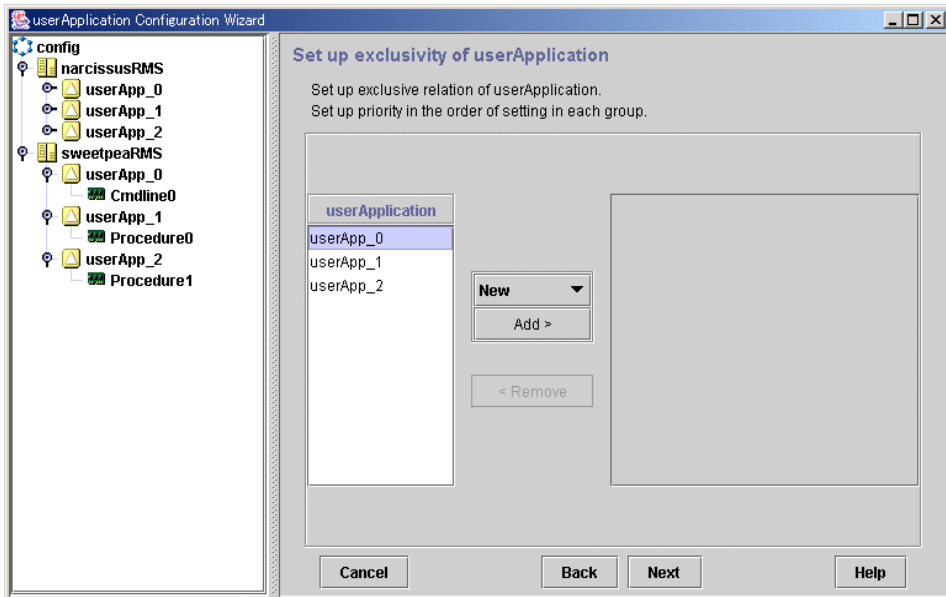


Click *Next* to go to the "Set up exclusivity of userApplication" screen.

■ Setting exclusion information between userApplication

Create an exclusion group and set up exclusivity in the cluster application.

Set up exclusivity of userApplication



userApplication

This section lists the cluster applications. Applications for which an exclusive relationship has been set are not displayed.

Exclusion group selection box

From the list box in the center of the setup screen, select the exclusion group to which the cluster application is to be added. If you select *New*, a new exclusion group will be selected.

If no exclusion group has been created, only *New* can be selected.

Add button

Click this button to add the cluster application that was selected from the cluster application list to the exclusion group.

You must select the exclusion group from the exclusion group selection box beforehand.

Delete button

This button deletes a cluster application from the exclusion group. Select a cluster application, and then click *Delete* to delete the setting.

ExclusiveA

The created exclusion group is displayed in the right frame.

With priority/Without priority

To set priorities for the cluster applications that have been added to the exclusion group, select *With priority*. The priorities are set in the sequence that the applications are displayed in the *ExclusiveA* box. The application that is in the top position has the highest priority.

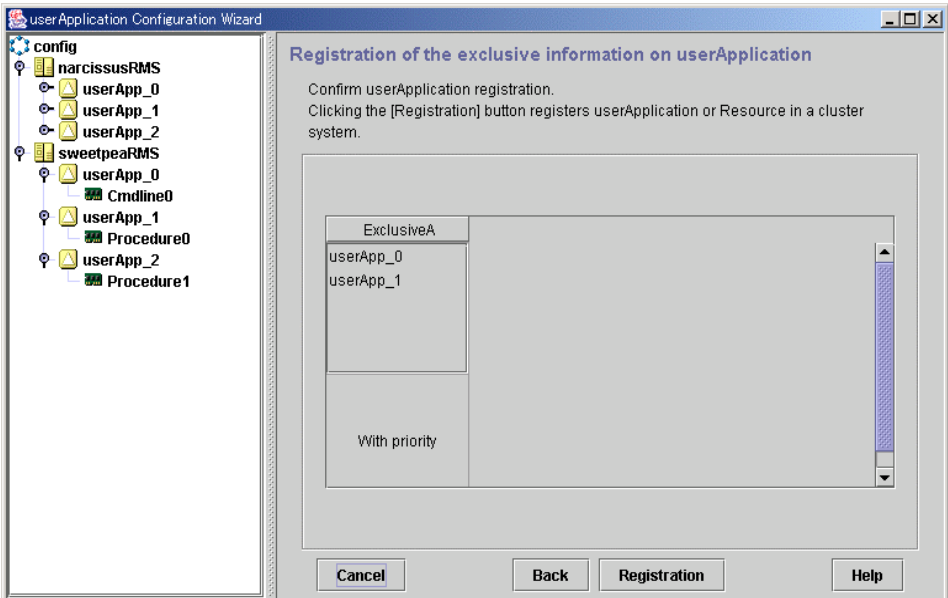
If you select *Without priority*, the cluster application that is already running has priority. If no cluster application is running, the priority sequence among the cluster applications is undefined.

After completing the setup, click *Next* to go to the "Registration of the exclusive information on userApplication" screen.

■ **Checking registration information for exclusion settings between cluster applications**

Check the setting information for the cluster application exclusive relationships.

Registration of the exclusive information on userApplication



The information is displayed.
Check the registration information, and then click *Registration*.

6.6.4 Editing global settings in Configuration

Set global settings in the configuration for the RMS configuration.

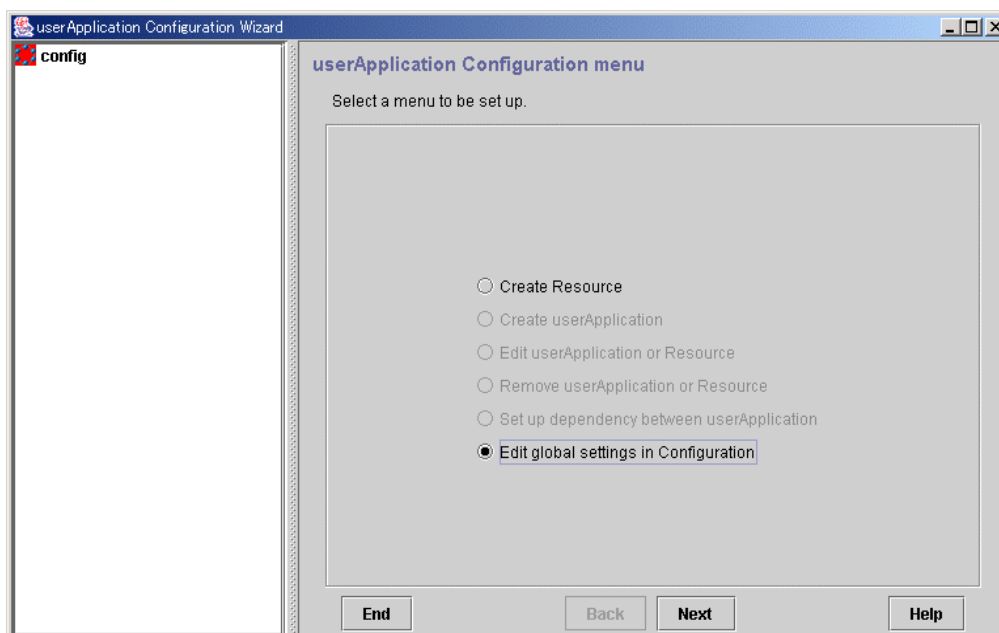
This function is not used except to change the timeout value of PreCheck or to use NFS Lock Failover.

The procedure for changing NFS Lock Failover is described below.

■ Starting setup of global settings in the configuration

At the top menu of the "userApplication Configuration Wizard," select *Edit global settings in Configuration*.

Top menu of userApplication Configuration Wizard

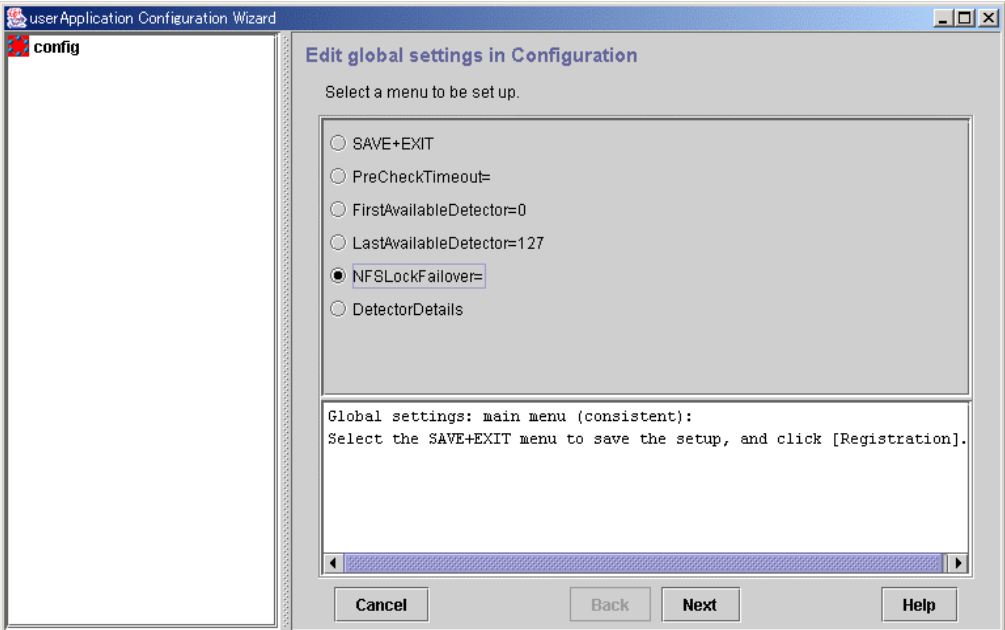


Click *Next* to go to the "Edit global settings in Configuration" screen.

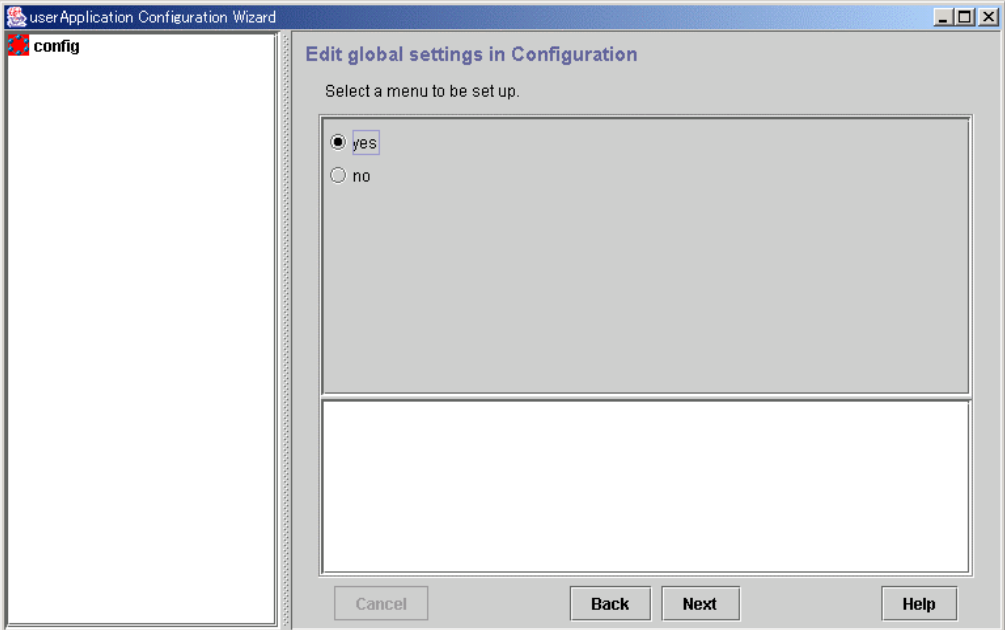
■ Setting up global settings in the configuration

Set NFS Lock Failover to "yes."

Edit global settings in Configuration



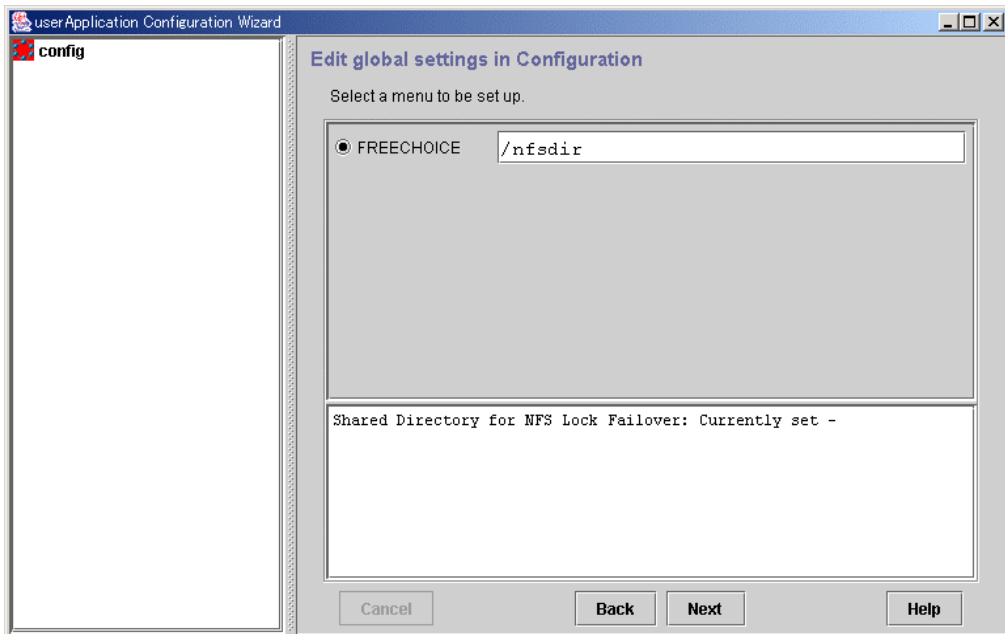
Select *NFS Lock Failover* and click *Next*.



Select *yes* and click *Next* to go to the "Edit global settings in Configuration" screen.

- **Setting a common directory**
Set a common directory.

Common directory setup



In *FREECHOICE*, enter the directory for storing NFS file lock information. During Fsystem resource creation, the specified directory is created automatically in the file system in which the NFSLockFailover attribute was set (under the mount point).

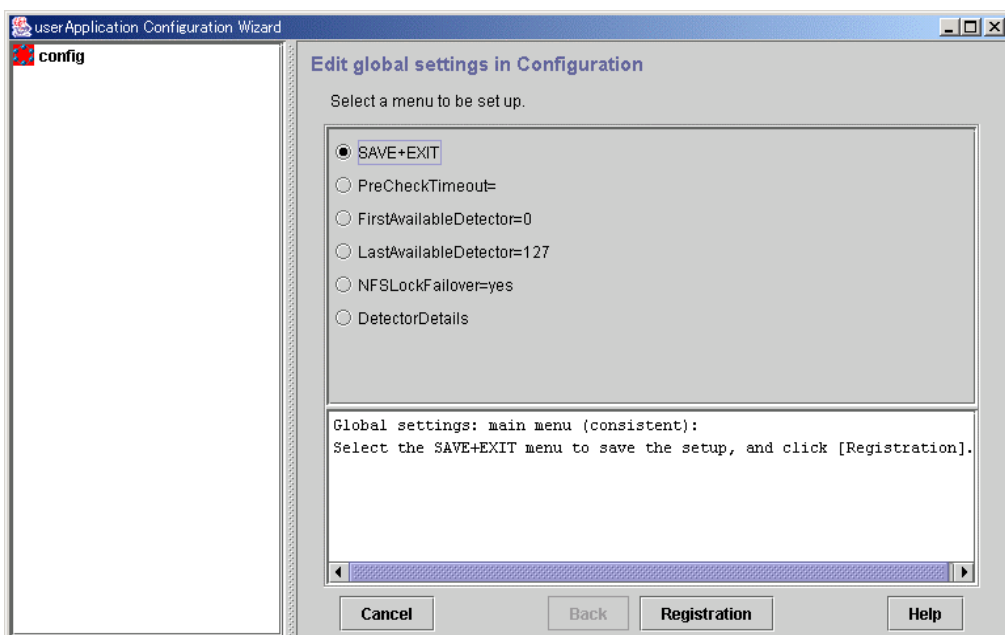


NFS file lock information is stored in this directory. This directory or any directory or file found in this directory should not be removed. After completing the setup, click *Next* to go to the Top of "Edit global settings in Configuration" screen.

■ **Checking the setup information**

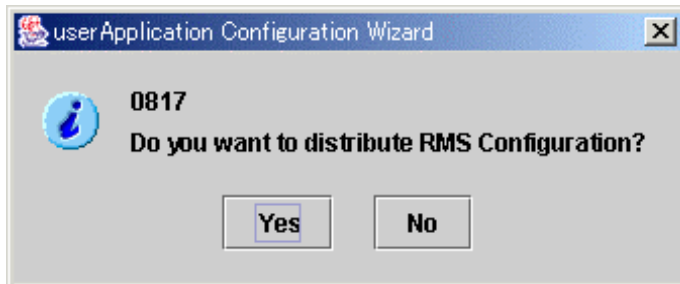
Check that NFS Lock Failover is set to *yes*.

Top of global settings in Configuration



After completing the setup, select *SAVE+EXIT*, and then click the *Registration* button.

If there is one or more cluster applications and there is no inconsistency in RMS Configuration, the following message is displayed:



To distribute the Configuration information immediately, click *Yes* to this message.

If you still need to create or change a cluster application or resource, select *No*.



Note

Make sure that you thoroughly verify and understand the operation of the Detector before changing *DetectorDetails*. If you are changing the settings for the first time, you need to follow the procedure described below because no default values have been set.

1. Select *DetectorDetails* and click the *Next* button.
2. Select "*Return to Default Values*" and click the *Next* button.
3. Click the *Back* button.

6.6.5 Attributes

■ Resource attributes

Attribute	Outline
InParallel	Normally, in Online or Offline processing, the programs for starting or stopping all the monitored programs run sequentially. If this attribute is set to yes, the programs run simultaneously. The default value is No (the programs are processed sequentially).
NeedAll	If this attribute is set to No, Online processing succeeds if there's at least one monitored Online program. If this attribute is set to Yes, all defined monitored programs are required to bring userApplication Online. The default value differs according to the resource. <ul style="list-style-type: none"> ● Cmdline: No ● Fsystem: Yes ● Takeover network: Yes Process monitoring: No
Timeout SCRIPTTIMEOUT	Sets the timeout duration (seconds) for resource start and stop processing. The default value differs according to the resource. <ul style="list-style-type: none"> ● Fsystem: 180 ● Gds: 1800 ● Gls: 60 ● Takeover network: 60 Procedure: 1800

Attribute	Outline
AutoRecover	<p>If this attribute is set to Yes, RMS attempts to recover the faulted resources to prevent userApplication from switching to other host.</p> <p>This attempt is executed only once.</p> <p>If this attribute is set to No, userApplication switches to other host in the event of a failure according to the AutoSwitchOver setting.</p> <p>The default value for Gds resources is "No."</p>

■ userApplication attributes

Attribute	Outline
AutoStartUp	<p>If this attribute is set to "Yes," the userApplication starts automatically when RMS is started.</p> <p>The default value is "No," and automatic userApplication startup is disabled.</p>
AutoSwitchOver	<p>If a failure occurs in a userApplication, this attribute allows userApplication to be switched over automatically.</p> <p>The switchover condition can be selected from the following:</p> <ul style="list-style-type: none"> ● No Automatic switchover by RMS is not executed. The cluster application must be switched over manually by the administrator. ● HostFailure If a failure occurs in the host (SysNode). ● ResourceFailure If a failure occurs in a resource. ● ShutDown If RMS shuts down. <p>Combinations of the above values can be selected. Example) HostFailure ResourceFailure HostFailure ShutDown ResourceFailure ShutDown HostFailure ResourceFailure ShutDown</p> <p>The default value is "No."</p>
PersistentFault	<p>If this attribute is set to 1, the Faulted state of userApplication remains the same even after RMS restart.</p>
OnlinePriority	<p>If this attribute is set to 1, when all clusters are stopped and restarted, RMS starts userApplication in the host that was Online last.</p> <p>The default value is "0," and after RMS is restarted, userApplication goes Online in the node with the highest priority. The priority is determined by the node setup sequence that was specified in "SysNode Setup" when userApplication was created.</p>

Attribute	Outline
ShutdownPriority	<p>This attribute is a weight coefficient that is assigned to userApplication. If a failure occurs in a cluster interconnect, this attribute also becomes one of the factors in determining which node has the highest priority to survive. The higher value, the higher is the priority of that userApplication.</p> <p>Select a value from the range of 1 to 20. The default value is "NONE," which means no weight coefficient is assigned. The node in which this userApplication is Online may be stopped because it does not contain elements that have a high priority to survive. For details on ShutdownPriority, see "<i>PRIMECLUSTER RMS Configuration and Administration</i>."</p>
StandbyTransitions	<p>This attribute determines the time when Standby state transition is executed. The following values can be selected.</p> <ul style="list-style-type: none"> ● NONE An execution time for Standby state transition is not set. ● ClearFaultRequest ● The Faulted state of userApplication is cleared and switched to the Offline state. ● StartUp Standby state transition is executed when RMS is started. If AutoStartUp is set to No, userApplication remains Offline regardless RMS startup. ● SwitchRequest ● UserApplication is switched to other node. <p>Combinations of the above values can be selected. Example) ClearFaultRequest StartUp ClearFaultRequest SwitchRequest StartUp SwitchRequest ClearFaultRequest StartUp SwitchRequest</p> <p>The default is "NONE."</p>
HaltFlag	<p>If this attribute is set to "Yes," the node is forcibly shut down when another failure occurs (double failure) during fault processing. In this case, RMS forcibly stops the node and completes failover of userApplication even if a resource failure occurs during failover processing. The default value is "No," and node elimination is not executed. Accordingly, userApplication does not execute failover. For details on HaltFlag (Halt attribute), see "<i>PRIMECLUSTER RMS Configuration and Administration</i>."</p>

6.6.6 Changing the RMS Configuration Name

userApplication Configuration Wizard provides a command for changing the Configuration name ("config") to be used as the default.

You can change the RMS Configuration name to be used by userApplication Configuration Wizard by executing this command in the management server of Web-Based Admin View. For detailed usage instructions, see below.

■ wgcnfclient—RMS Configuration name setup/reference command

◆ Function explanation

This command allows you to change the RMS Configuration name to be displayed and operated by userApplication Configuration Wizard. As much as possible, the modified information is distributed to all clusters. Normally, the RMS Configuration name does not need to be changed.

◆ Prerequisites:

To enable this command, the following conditions must be satisfied:

- The cluster resource manager package must be installed.
If this package is not installed, the 3-tier configuration of Web-Based Admin View is assumed, and only the information in the local node is changed. If the 3-tier configuration of Web-Based Admin View is being used, this command must also be executed in the secondary management server of Web-Based Admin View.
- Initial installation of the resource database must be completed.
Check the resource database by executing the "clchkconf(1)" command.

◆ Usage examples

1. Changing the RMS Configuration name

As shown below, specify the new RMS Configuration name in the "-o" option and execute the command.

```
# /etc/opt/FJSVwvucw/bin/wgcnfclient -s config-name -o config2
#
```

2. Inquiring the RMS Configuration name

```
# /etc/opt/FJSVwvucw/bin/wgcnfclient -g config-name
config2
#
```

Since no value is set as the initial value of config-name, no data is displayed.

◆ Supplement

If this command terminates abnormally, a system command error message may be displayed. If an error message is displayed, respond according to that message.



Note

The RMS Configuration name must be **80 character or less**. If the RMS Configuration name has 81 or more characters, RMS Configuration generation and RMS activation will fail.

6.7 Setting Up Patrol Diagnosis

The patrol diagnosis facility periodically diagnoses the following hardware units that are connected to the STANDBY node.

- **Shared disk units**
The function diagnoses whether a shared disk unit has become unusable because the power is switched off, a cable is disconnected (adapter side or device side) or because of some other reason.
If the diagnosis results indicate that an error was detected in a shared disk unit, a message is output to "syslogd(1M)" and the CRM main window.
- **Network interface cards**
The function diagnoses whether any network interface card cannot communicate because a cable is disconnected or because of some other reason.
If the patrol diagnosis results indicate that an error was detected in a network interface card, a message is output to "syslogd(1M)" and the CRM main window, and brings userApplication Faulted.
If a cluster application uses a Global Link Services (GLS) resource, patrol diagnosis is disabled for the network interface card that is managed by the GLS resource. If a cluster application uses a GLS resource, use the GLS monitoring function. For details on the GLS monitoring function, see "Failure Monitoring Function" and "Standby Patrol Function" in the "*PRIMECLUSTER Global Link Services Configuration and Administration Guide: Redundant Line Control Function.*"

Set up patrol diagnosis according to the following flow:

1. Register the patrol diagnosis resource to userApplication.
2. Set up the patrol diagnosis configuration.



Note

- Set up patrol diagnosis after initial setup of the cluster resource manager is completed. If the patrol diagnosis setup command (clspconfig) is executed before initial setup of the cluster resource manager, the following message is displayed:
6615: The cluster configuration management facility is not running.
- If you do not configure the patrol diagnosis configuration, the patrol diagnosis facility will not diagnose the hardware.
- To view the manual pages of the individual commands, add "/etc/opt/FJSVcluster/man" to the MANPATH variable.

■ Registering a patrol diagnosis resource to a userApplication

To register a patrol diagnosis resource to userApplication, use the userApplication Configuration Wizard (GUI) or the RMS Wizard (CUI).

For instructions on resource registration with the userApplication Configuration Wizard (GUI), see 6.6.2 "Creating Cluster Applications."

For instructions on resource registration with the RMS Wizard (CUI), see "[/usr/opt/reliant/htdocs.solaris/wizards.en/wizards/CRM.htm](#)."

■ Setting the patrol diagnosis configuration

Before starting RMS, set up the following configuration for patrol diagnosis by executing the "clspconfig(1M)" command on an arbitrary node.

For details on the “clspconfig(1M)” command, see the manual page for “clspconfig(1M).”

◆ **Specifying the target hardware for patrol diagnosis execution**

Specify the hardware product that runs patrol diagnosis if either of the following conditions applies. This hardware is used by the specified userApplication.

- If the cluster application uses a Gds (Global Disk Services) resource
- If the cluster application uses an laddress (takeover network) resource

● **Operation Procedure: (When the cluster application uses Gds resources)**

If the cluster application is using Gds resources, specify the physical disks that were defined to the Gds resources as hardware for patrol diagnosis execution. The physical disks can be obtained by the procedure below.

1. Confirmation of the disk class

Check the disk class to be used by the cluster application. The disk class is the class that was specified in 6.6.1.3 "Creating Gds Resources."

Example) **class0001**

2. Confirmation of the physical disks

Check the physical disks that were defined in the disk class. The physical disks are those that were defined in 6.2.2.2 "Setting Up Shared Disks." Use the class configuration setup screen or the “sdxinfo(1M)” command to check the physical disks. For information on the class configuration setup screen, see 6.2.2.2 "Setting Up Shared Disks." For details on the “sdxinfo(1M)” command, see the *"PRIMECLUSTER Global Disk Services Configuration and Administration Guide."*

Example) **c1t4d0, mplb2048**

3. Setup of the target hardware for patrol diagnosis execution

Set the physical disks that were defined in the disk class as hardware for patrol diagnosis execution.

Example 1) For c1t4d0

```
# /etc/opt/FJSVcluster/bin/clspconfig -u app1 TARGET_DISK=c1t4d0  
TARGET_DISK=c1t4d1
```

Example 2) For mplb2048

```
# /etc/opt/FJSVcluster/bin/clspconfig -u app1 TARGET_DISK=mplb2048
```

● **Operation Procedure: (When the cluster application uses laddress resources)**

If the cluster application is using laddress resources, specify the network interface card to be used in the takeover network as hardware for patrol diagnosis execution. Follow the procedure below to determine the network interface card.

1. Confirmation of the network interface card

Check the network interface card to be used by the takeover network. The network interface card is the interface card that was selected in “Selecting an Interface” of 6.6.1.5 "Creating Takeover Network Resources."

Example) hme0

2. Setup of target hardware for patrol diagnosis execution

Configure the network interface card to be used by the takeover network as hardware for patrol diagnosis execution.

Example)

```
# /etc/opt/FJSVcluster/bin/clspconfig -u app1 TARGET_LAN=hme0
```

◆ **Time interval for patrol diagnosis**

Specify the time interval for patrol diagnosis. If this setting is not specified, patrol diagnosis

runs at 360-minute intervals.

Example) To run patrol diagnosis at 60-minute intervals

```
# /etc/opt/FJSVcluster/bin/clspsconfig -u app1 INTERVAL=60
```

You can also check the current setting.

Example) Checking the current setting (INTERVAL=360)

```
# /etc/opt/FJSVcluster/bin/clspsconfig -u app1
ACTIVE=true
INTERVAL=360
TARGET_LAN=hme1
TARGET_DISK=c1t4d0
TARGET_DISK=c1t4d1
TARGET_DISK=c1t4d2
TARGET_DISK=c1t4d3
```

■ Stopping and restarting patrol diagnosis

Stop and restart patrol diagnosis by executing the “clspsconfig(1M)” command. For details on the “clspsconfig(1M)” command, see the manual page for “clspsconfig(1M).”

To stop patrol diagnosis, specify "ACTIVE=false" as an operand in the “clspsconfig(1M)” command.

Example)

```
# /etc/opt/FJSVcluster/bin/clspsconfig -u app1 ACTIVE=false
```

To restart patrol diagnosis, specify "ACTIVE=true" as an operand in the “clspsconfig(1M)” command.

Patrol diagnosis is restarted from the next time with the same configuration as when patrol diagnosis was stopped, including hardware for executing patrol diagnosis and the time interval for patrol diagnosis.

Example)

```
# /etc/opt/FJSVcluster/bin/clspsconfig -u app1 ACTIVE=true
```


Part 3 Operations

Chapter 7 Operations

This chapter describes the functions that manage PRIMECLUSTER system operations.

The following user groups are allowed to do each specific operation:

- Viewing the PRIMECLUSTER system operation management screens (All user groups)
- Operating the PRIMECLUSTER system (wvroot, clroot, cladmin)
- Monitoring the PRIMECLUSTER system (All user groups)
- Actions to take if the state of a resource changes (wvroot, clroot, cladmin)

7.1 Viewing the PRIMECLUSTER System Operation Management Screens

PRIMECLUSTER provides GUIs for viewing and performing cluster system operations.

- CF main window
Use this screen to set up the configuration of the nodes that make up the cluster, manage the nodes, and display the node state.
- CRM main window
Use this screen to identify faulted hardware and to execute hardware diagnosis.
- RMS main window
Use this screen to monitor the state of the cluster system and to manage cluster applications and resources.
- MSG main window
This screen displays messages for cluster control.

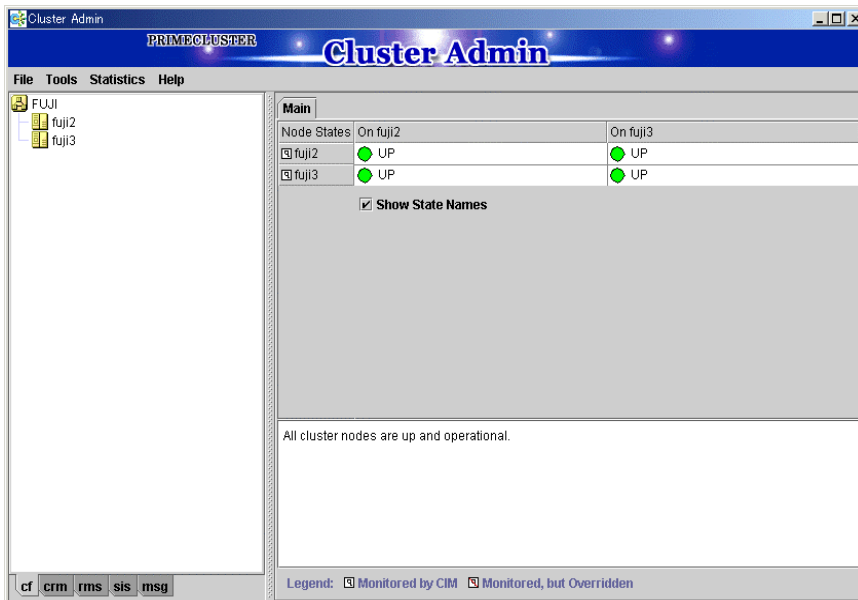


See

For instructions on displaying each screen, see 4.3.3 "Cluster Admin Functions."

7.1.1 CF Main Window

The CF main window allows you to set up the configuration of the cluster nodes in the cluster, manage the nodes, and display the node state.



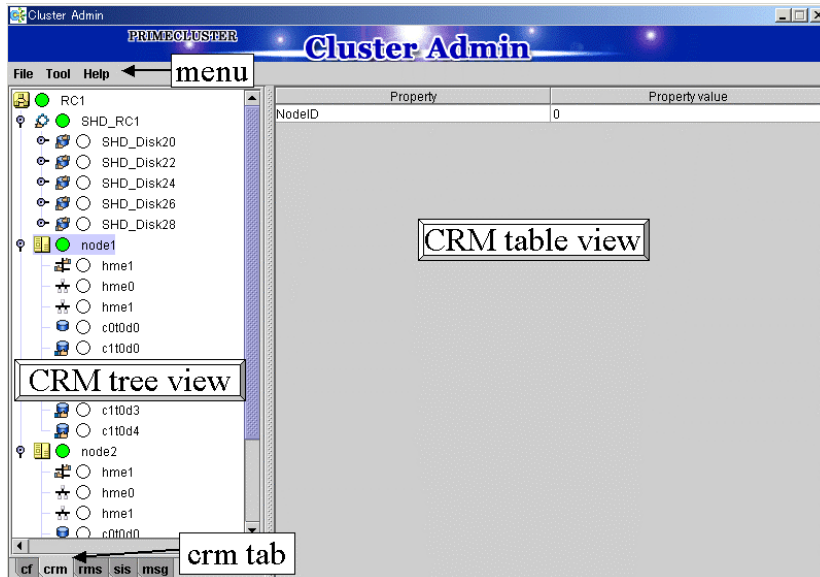
See

For details, see "5 GUI administration" in *"PRIMECLUSTER Cluster Foundation Configuration and Administration."*

7.1.2 CRM Main Window

When you monitor the state of the PRIMECLUSTER system, the CRM main window allows you to view the states of the resources managed by the cluster resource management facility and identify failed hardware.

This section describes resource states and operation methods related to hardware resources.



See

The CRM main window is a screen of the cluster resource monitoring facility. See "crm" in 4.3.3 "Cluster Admin Functions."


7.1.2.1 Displayed Resource Types











This section shows the resources associated with the hardware resources that are displayed in the CRM main window.






The detailed resource information lists the icons that are used in the CRM main window.

7.1.2.1.1 Resource Icons

This section describes the icons that are displayed in the CRM tree view.

Items that are related to resources under shared resources are displayed with overlapping .

Icon	Resource
	Shared resource
	DISK class managed by Global Disk Services
	Local disk
	Multipath disk
	Shared disk device
	Multipath disk
	IP address
	MAC address
	Network interface
	Takeover node name




Icon	Resource
	Node resource of a switching line used in a line switching unit Shared resource of a line switching unit Shared resource of a switching line used in a line switching unit
	Takeover network
	Resource that is not a multi-tiered resource under a shared resource Resource that is not related to a shared resource under a node and is not a multi-tiered resource
	Cluster
	Node

7.1.2.1.2 Resource States

In the CRM main window, the displayed icon types and states differ for each resource class. For each resource, an icon that indicates a failure (OFF-FAIL or ON-FAILOVER) is displayed if there is a fault in a subordinate resource. In the CRM tree view, expand the icons sequentially from cluster icon to node icons to subordinate resource icons, and identify the faulted resource. If the resource state is OFF-FAIL or ON-FAILOVER, see 7.4 "Corrective Actions for Resource Failures," and take corrective actions. If the resource state is ON, OFF-STOP, or UNKNOWN, you don't need to take any corrective actions.







Cluster states

The following cluster states are displayed.



Icon	Icon color	Outline	Details
	 Green	ON	All nodes and shared resources are operating normally.
	 Red	OFF-FAIL	One of the nodes in the state other than the ON state, or a shared resource is in the OFF-FAIL state.

Node states

The following node states are displayed.

Icon	Icon color	Outline	Details
	 Green	ON	The node has been started normally.
	 Green with vertical red lines	ON-FAILOVER	One of the resources under the node is in the Faulted state.
	 Blue	OFF-STOP	The cluster resource management facility is stopped.
	 Red	OFF-FAIL	A failure has occurred in the node.
	 White	UNKNOWN	The node has not been monitored or controlled.

If a failure occurs in the node, the following icons are displayed:

Icons	Outline	Details
	Error	Immediate replacement is necessary.
	Warning	Life replacement or preventive replacement is necessary.

If either icon is displayed, see the "Machine Administration Guide," and take corrective actions.

**Note**

- If a node is LEFTCLUSTER in CF, it becomes ON in the CRM tree view.
- After you execute the “clinitreset(1M)” command to initialize the resource database, the resource states displayed in the CRM main window differ according to the actual resource states. Execute “clinitreset(1M)”, reboot the nodes, and then close the browser and redisplay the screen.

■ Shared resource states

The following states are displayed for shared resources.

Icon	Icon color	Outline	Details
	Green	ON	The sub-resource under the shared resource is ON, OFF-STOP, or UNKNOWN.
	Red	OFF-FAIL	One of the sub-resources under the shared resource is OFF-FAIL.

■ Other resource states

The following states are displayed for other resources.

Icon color	Outline	Details
Green	ON	The resource is operating normally.
Green with vertical red lines	ON-FAILOVER	The resource is operating normally, but some devices or resources that are multiplexed and managed internally are in the Faulted state.
Blue	OFF-STOP	The resource has been stopped normally.
Red	OFF-FAIL	The resource is in the Faulted state.
White	UNKNOWN	The resource has not been monitored or controlled.

7.1.2.1.3 Operations

You can perform the operations described below from the CRM main window.

In the table below, "Selection resource" is the resource class name of the selectable resource.

For details on resource class names, see 7.1.2.2 "Detailed Resource Information."

Operations of the CRM main window

Feature	Operation method		Target group
	Menu	Selection resource	
Build CRM resource database	<i>Tool - Initial setup</i>	None (*1)	wvroot clroot
Configure automatically	<i>Tool - Automatic configure</i>	Cluster	wvroot clroot
Run patrol diagnosis immediately	<i>Tool - Diagnosis</i> (*2)	DISK (*3) Ethernet (*3) MPDisk(*3)	wvroot clroot cladmin
Request Resource activation	<i>Tool - Start</i>	SDX_DC (*4)	wvroot clroot cladmin
Request Resource deactivation	<i>Tool - Stop</i>	SDX_DC (*5)	wvroot clroot cladmin
Display machine information	<i>Tool - Machine Information</i>	Node (*5)	wvroot cladmin clmon
Exit Cluster Admin	<i>File - Exit</i>	All	All

Feature	Operation method		Target group
	Menu	Selection resource	
screen		No selection	
View Help	<i>Help – Content (*6)</i>	All No selection	All
View version	<i>Help - About</i>	All No selection	All

- *1 Set Initial Configuration menu can be selected only if the resource database has not been set up. This menu item is not displayed in the pop-up menu.
- *2 This feature is enabled only for the resources for which the patrol diagnosis has been set.
- *3 Only the resources of the DISK, Ethernet, and MPDisk classes, which have been registered in hardware where the patrol diagnosis facility runs, are enabled. For the hardware settings, see 6.7 "Setting Up Patrol Diagnosis."
- *4 Only the disk resources that are registered to Global Disk Services are enabled.
- *5 This feature is enabled only if the Enhanced Support Facility is installed.
- *6 Help for the CRM main window is displayed with a separate browser from the browser that displays Help for CF, RMS, and SIS.



Note

- Only available menus are displayed in the pop-up menu.
- If there are no available menu items for the resource selected from the CRM tree view, "None" is displayed in the pop-up menu. Selecting this item will not initiate any operation.
- For information about user groups, see 4.1.1 "Assigning Users to Manage the Cluster."

Initial setup

Select this item to set up the resource database to be managed by the cluster resource management facility. Select *Tool -> Initial setup* to display the Initial Configuration Setup screen. The initial configuration setup cannot be operated simultaneously from multiple clients. See 5.2.3.1 "Initial Configuration Setup."

Automatic configure

Select this item to register the devices connected to the system to the resource database. Automatic configuration cannot be operated simultaneously from multiple clients. See 5.2.3.1 "Initial Configuration Setup."

Diagnosis

Select this item to diagnose the selected resource. Execute this diagnosis operation to check whether faulted hardware has been properly recovered after hardware recovery is performed. See 7.4.2 "Corrective Action when Patrol Diagnosis Detects a Fault."

Yes button

Executes resource diagnosis.

No button

Does not execute resource diagnosis.

Start

This menu item activates the selected resource. The start operation is executed during maintenance work. If the selected resource is registered to a cluster application, the start operation can be executed only when that cluster application is in the Deact state. Use the RMS main window to check the cluster application state.



Note

- After completing the maintenance work, be sure to return the resource that you worked on to its state prior to the maintenance.
- If the resource that was maintained is registered to a cluster application, be sure to stop the resource before clearing the Deact state of the application.

Yes button

Executes resource start processing.

No button

Does not execute resource start processing.

Stop

This menu item deactivates the selected resource. The stop operation is executed during maintenance work. If the selected resource is registered to a cluster application, the startup operation can be executed only when that cluster application is in the Deact state. Use the RMS main window to check the cluster application state.



Note

- After completing the maintenance work, be sure to return the resource that you worked on to its state prior to the maintenance.
- If the resource that was maintained is registered to a cluster application, be sure to stop the resource before clearing the Deact state of the application.

Yes button

Executes resource stop processing.

No button

Does not execute resource stop processing.

Machine Information

This menu item displays the machine management screen of the selected node. This menu item can be used only if Enhanced Support Facility (ESF) is installed. For details on the machine management screen, see the "*Machine Administration Guide*."



Note








If a message is displayed during operating at the CRM main window and the frame title of the message dialog box is "Cluster resource management facility," then see the following references for information:





- H.5 "Cluster Resource Management Facility Messages"
- D.5 "Failed Resource and Operator Intervention Messages (GUI)"
- D.7 "Shared Disk Connection Confirmation Messages"
- D.8 "Patrol Diagnosis Messages"

7.1.2.2 Detailed Resource Information

This section describes the resource attributes that are defined in the CRM main window.

Detailed resource information

Icon/ resource class name	Attributes	Meaning/attribute value (Top: Meaning, Bottom: Attribute value)
 Node	NodeID	Node identifier number.
		Node identifier number (0 to 127).
 SH_SWLine	lsu_mask	Mask information for the LSU used by the line switching unit
		Logical sum of the mask information for the LSU used by the line switching unit LSU machine information LSU00 0x0001 LSU01 0x0002 LSU02 0x0004 ... LSU14 0x4000 LSU15 0x8000
 SH_SWU	lsu_num	Number of switchover units installed in the line switching unit 4, 16
	addr	RCI device address of the line switching unit RCI device address
 SWLine	Port	Port number of the LSU (group) used by the line switching unit
		0, 1
 DISK	Disk_Attr	This item indicates the physical connection mode and usage mode of a disk that can be used from the cluster system.
		LOCAL Local disk that can be accessed only from one node SHD_DISK The disk is physically shared, but the usage mode (shared disk or switchover disk) is not specified. SHD_SHARE Shared disk that can be accessed from multiple nodes SHD_SWITCH Switching disk that is used exclusively between two nodes Blank The disk connection or usage mode is not set up.
 MPDisk	Disk_Attr	This item indicates the physical connection mode and usage mode of a disk that can be used from the cluster system LOCAL Local disk that can be accessed only from one node SHD_DISK The disk is physically shared, but the usage mode (shared disk or switchover disk) is not specified. SHD_SHARE Shared disk that can be accessed from multiple nodes SHD_SWITCH Switching disk that is used exclusively between two nodes Blank The disk connection or usage mode is not set up.
	path_stat	This item indicates the stage of each path of a multipath disk. The state value of each path in the multipath disk is indicated in sequence for up to eight paths starting from path 0. The values are shown with the format below. (The values in parenthesis are used when there are five or more paths.) active (A) Active standby (B) Standby discon (D) Low-order driver is disconnected. fail (F) Failed stop (S) Stopped because a path from another node to the same controller is faulted or is undergoing maintenance
 SHD_DISK	Disk_Attr	This item indicates the physical connection mode and usage mode of a disk that can be used from the cluster system.

Icon/ resource class name	Attributes	Meaning/attribute value (Top: Meaning, Bottom: Attribute value)
 SHD_MPD isk		<p>SHD_DISK The disk is physically shared, but the usage mode (shared disk or switchover disk) is not specified.</p> <p>SHD_SHARE Shared disk that can be accessed from multiple nodes</p> <p>SHD_SWITCH Switching disk that is used exclusively between two nodes</p>
 SDX_DC, SDX_SHD DC	Disk_Attr	<p>This class indicates the physical connection mode and usage mode of a GDS-managed disk class that can be used from the cluster system.</p> <p>SHD_DISK The disk is physically shared, but the usage mode (shared disk or switchover disk) is not specified.</p> <p>SHD_SHARE Shared disk class that allows access from multiple nodes</p> <p>SHD_SWITCH Switching disk class for exclusive use between two nodes</p>
 Ethernet	node_name	<p>This item indicates the name of the node in which this LAN board is set.</p> <p>The node name is set.</p>
	org_mac	<p>This item indicates the MAC address that the operating system has assigned to this LAN board.</p> <p>The MAC address is in the format 00:11:22:33:44:55.</p>
	WebView	<p>This item indicates the network interface to be used by Web-Based Admin View.</p> <p>If Web-Based Admin View is being used, USE is set. If not, UNUSE is set.</p>
 SHD_Host	Ip_addr	<p>This item indicates the takeover IP address.</p> <p>The takeover IP address information is set in the format XXX.XXX.XXX.XXX. If IP address takeover has not been set, this item is blank.</p>
	mac_addr	<p>This item indicates the takeover MAC address.</p> <p>The takeover MAC address information is set in the format 00:11:22:33:44:55. If MAC address takeover has not been set, this item is blank.</p>
	node_name	<p>This item indicates the takeover node name.</p> <p>The takeover node name is set. If node name takeover has not been set, this item is blank.</p>
	LanDev_Rid	<p>If a takeover MAC address is used, this item indicates the resource ID of LanDev (maintenance information for customer support representative).</p> <p>If a takeover MAC address is used, the resource ID of LanDev is set.</p>

7.1.3 RMS Main Window

The RMS main window consists of the following elements:

- RMS tree
- Configuration information or object attributes
- Switchlogs and application logs

7.1.3.1 RMS Tree

The RMS tree displays the configuration information of the cluster in a hierarchical format. The tree has the following levels:

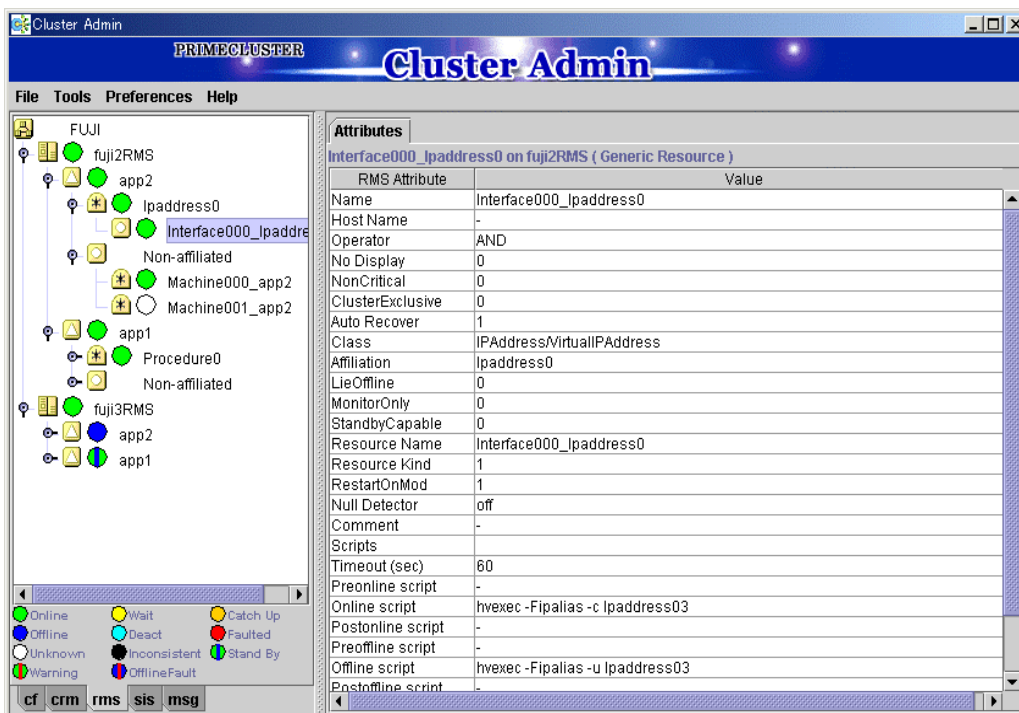
- Root of the tree — Represents the cluster.

- First level — Represents the system nodes in the cluster.
- Second level — Represents the userApplication objects running on each of the system nodes.
- Third level — Represents the sub-applications (an aggregation of objects if any exist).
- Fourth level — Represents the resources required for each of the sub-applications.

If an application has sub-applications, the fourth level represents resources used by that sub-application. If an application does not have sub-applications, then the third level represents all the resources used by userApplication.

Dependency relationships between cluster applications are indicated by controller objects in the RMS tree.

RMS main window



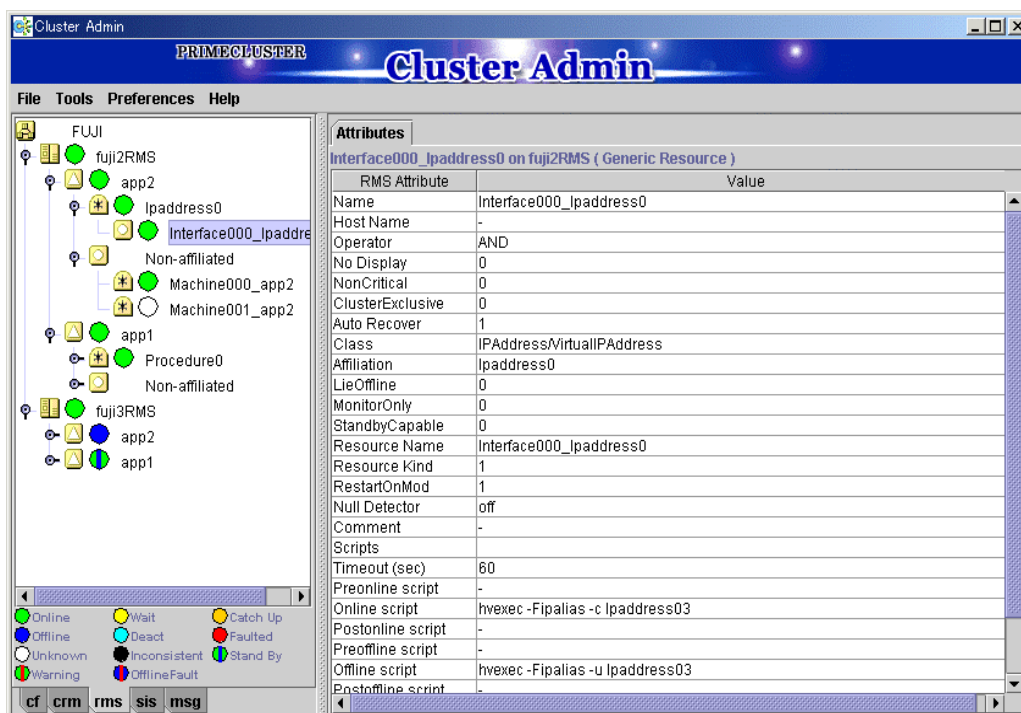
■ Meanings of object icons

Icon	Meaning
	Represents the cluster.
	Represents a node.
	Represents a parent object (cluster application) that has a child object.
	Represents a child object (cluster application or resource).
	Represents a leaf object (cluster application or resource). A leaf object is an object that cannot have a child object.
	Represents a controller object (cluster application). This object controls an object of another cluster application.

■ Meanings of state display icons

On the right side of the object icons shown above is displayed a color-coded circle that indicates the state of each object. This section describes the meaning of the colored circles (state

display icons).



State display icons are not displayed in cluster icons. Instead, the RMS cluster table can be displayed. For details, see 7.3.3 "Concurrent Viewing of Node and Cluster Application States."

◆ **Node state display**

The state icons that are displayed in nodes are shown below.

Icon	Icon color	Outline	Details
		Online	Node is enabled and ready for use.
		Offline	Node is disabled and should not be used.
		Faulted	Node encountered an error condition.
		Wait	Node is undergoing a state transition.

◆ **State display of other objects**

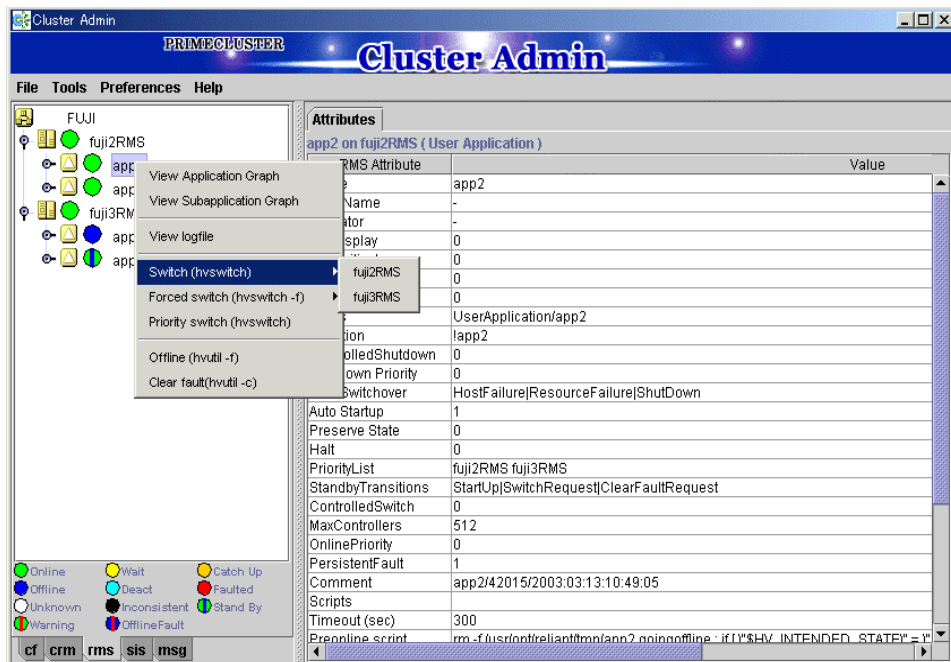
The following state icons are displayed with object icons that fall under parent objects.

Icon	Icon color	Outline	Details
		Online	Object is enabled and ready for use.
		Warning	Object has exceeded some warning threshold.
		Offline	Object is disabled and should not be used.
		Faulted	Object encountered an error condition.
		Unknown	Monitoring and control are not being executed for the object.
		Wait	Node is undergoing a state transition.
		Deact	Node is deactive because of maintenance, etc.
		Inconsistent	Node state is inconsistent.
		Stand By	Object is in such a state that it can be quickly brought Online when needed

Icon	Icon color	Outline	Details
	Blue with vertical read lines	OfflineFault	Object is Offline Fault, but a fault occurred in the past and has not yet been cleared

■ **Pop-up menu**

If you right-click an object in the RMS tree, a pop-up menu lists the operations for that object. You can also use this menu for monitoring the state.



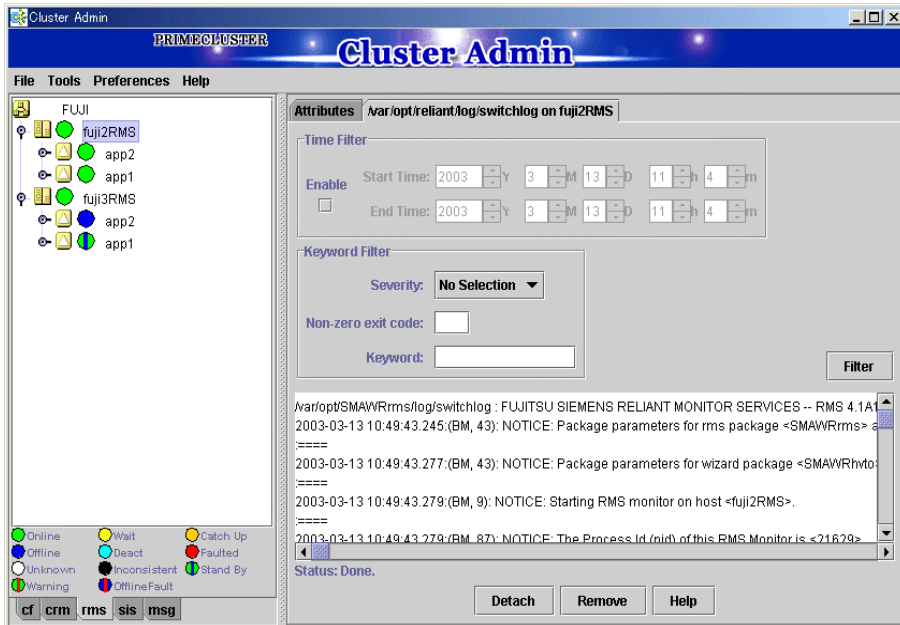
7.1.3.2 Configuration information or object attributes

View the configuration information for the individual objects by left-clicking the object in the RMS tree. The properties are displayed in a tabular format on the right-hand side panel of the RMS main window.

7.1.3.3 Switchlogs and application logs

Each node has a log file referred to as the switchlog. In this file, switchover requests and node failures are recorded. The switchlog is displayed in a tab on the right-side panel. Display the application log by right-clicking on an application on the RMS tree and choosing *View Application Log*.

7.1 Viewing the PRIMECLUSTER System Operation Management Screens



7.2 Operating the PRIMECLUSTER System

7.2.1 RMS Operation

To monitor RMS, RMS needs to be activated.

To stop multiple nodes at the same time, you must stop the user applications and RMS.



Note

To stop two or more nodes at the same time, it is necessary to first stop RMS.

Note that the user application is also stopped when you stop RMS. For instructions on stopping RMS, see 7.2.1.2 "Stopping RMS."

The sections below explain how to start and stop RMS.

7.2.1.1 Starting RMS

This section explains how to start RMS.

◆ **Operation Procedure:**

From the top screen of Web-Based Admin View, open Cluster Admin according to the following procedure:

1. Select Global Cluster Services.
2. Click *Cluster Admin* to switch to the cluster menu.
3. Select the *rms* tab.
4. Start RMS.
 - 1) Use the *Tools* pull-down menu of the RMS main window, and click *Start RMS -> all available nodes*. When the confirmation screen is displayed, click *Ok*.
 - 2) To specify an option for the RMS start command, click the *Option* box.

You can also start RMS on one or all nodes using the command pop-up as follows:

- 3) Choose either one node or all the nodes from the pop-up window.
- 4) To specify an option for the RMS start command, click the *Option* box.



See

See "4.3.1 Starting RMS" in "*PRIMECLUSTER RMS Configuration and Administration*."

7.2.1.2 Stopping RMS

This section explains how to stop RMS.

◆ **Operation Procedure:**

1. Use the *Tools* pull-down menu, or right-click on a system node, and select the mode of shutdown in the subsequent option screen.
 - 1) Choose either a specific node or all the nodes.
 - 2) Choose to stop all user applications, leave the applications running, or forcibly shut down the node(s).



See

See "4.3.2 Stopping RMS" in "*PRIMECLUSTER RMS Configuration and Administration*."

7.2.2 Cluster Application Operations

This section explains how to change the operation state of the PRIMECLUSTER system. The operations include starting and stopping a cluster application.

7.2.2.1 Starting a Cluster Application

The procedure for starting a cluster application is described below.

◆ Operation Procedure:

1. On the RMS tree in the RMS main window, right-click the cluster application to be started, and select *Online* from the pop-up menu that is displayed.

The cluster application will start.



Information

You can also display the pop-up menu by right-clicking the target icon in an RMS graph or the RMS cluster table. For details on RMS graphs and the RMS cluster table, see 7.3.5 "Viewing Detailed Resource Information" and 7.3.3 "Concurrent Viewing of Node and Cluster Application States."

7.2.2.2 Stopping a Cluster Application

The procedure for stopping a cluster application is described below.

◆ Operation Procedure:

1. On the RMS tree in the RMS main window, right-click the cluster application to be stopped, and select *Offline* from the displayed pop-up menu.

The cluster application will stop.



Information

You can also display the pop-up menu by right-clicking the target icon in an RMS graph or the RMS cluster table. For details on RMS graphs and the RMS cluster table, see 7.3.5 "Viewing Detailed Resource Information" and 7.3.3 "Concurrent Viewing of Node and Cluster Application States."

7.2.2.3 Switching a Cluster Application

The procedure for switching a cluster application is described below.

◆ Operation Procedure:

1. Right-click on the application object and select the *Switch* menu option.
A pull-down menu appears listing the available nodes for switchover.
2. Select the target node from the pull-down menu to switch the application to that node.



Information

You can also display the pop-up menu by right-clicking the target icon in an RMS graph or the RMS cluster table. For details on RMS graphs and the RMS cluster table, see 7.3.5 "Viewing Detailed Resource Information" and 7.3.3 "Concurrent Viewing of Node and Cluster Application States".

7.2.2.4 Bringing Faulted Cluster Application to Online State

The procedure for bringing a Faulted cluster application to Online is described below.

◆ **Operation Procedure:**

1. Right-click on the cluster application object in the RMS tree, and select *Clear Fault*.
If you clear Fault while the cluster application is Online, RMS brings the faulted resource Online.
If you clear Fault while the cluster application is Offline, RMS brings the faulted resource Offline.



Information

You can also display the pop-up menu by right-clicking the target icon in an RMS graph or the RMS cluster table. For details on RMS graphs and the RMS cluster table, see 7.3.5 "Viewing Detailed Resource Information" and 7.3.3 "Concurrent Viewing of Node and Cluster Application States."

7.2.2.5 Clearing the Wait State of a Node

The procedure for clearing the Wait state of a node is described below.

◆ **Operation Procedure:**

1. Right-click on the system node and select the "Online" or "Offline" option from the pop-up menu.



Note

If you clear the Wait state of a system node manually with the GUI, `hvutil -u SysNode`, or `cftool -k`, then RMS, SF, and CF assumes that you have already checked that the target node is stopped.

If you clear the Wait state when the node has not been stopped, this may lead to the data corruption.



Information

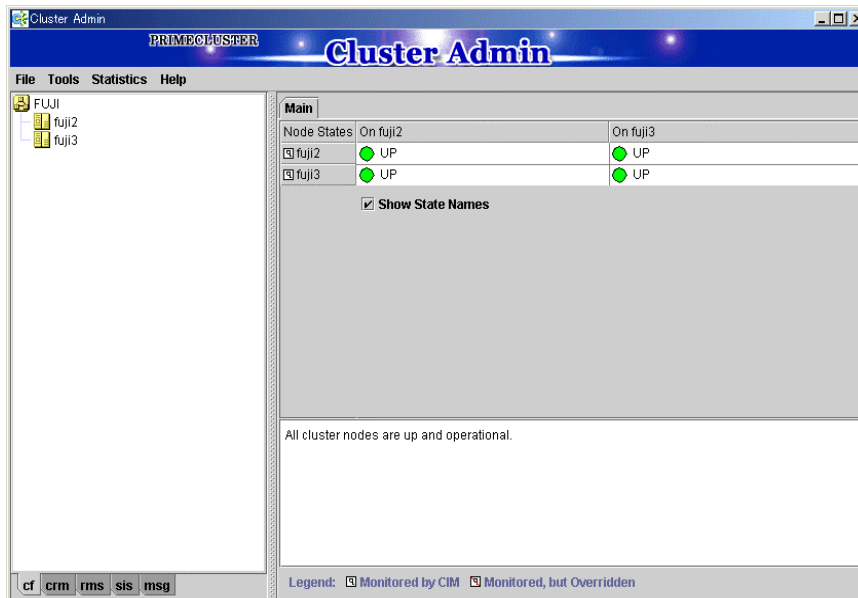
You can also display the pop-up menu by right-clicking the target icon in an RMS graph or the RMS cluster table. For details on RMS graphs and the RMS cluster table, see 7.3.5 "Viewing Detailed Resource Information" and 7.3.3 "Concurrent Viewing of Node and Cluster Application States."

7.3 Monitoring the PRIMECLUSTER System

This section describes how to monitor the state of a cluster application or node from the Cluster Admin screen.

7.3.1 Monitoring the State of a Node

Click a node on the CF tree. The node state will appear in the right panel.

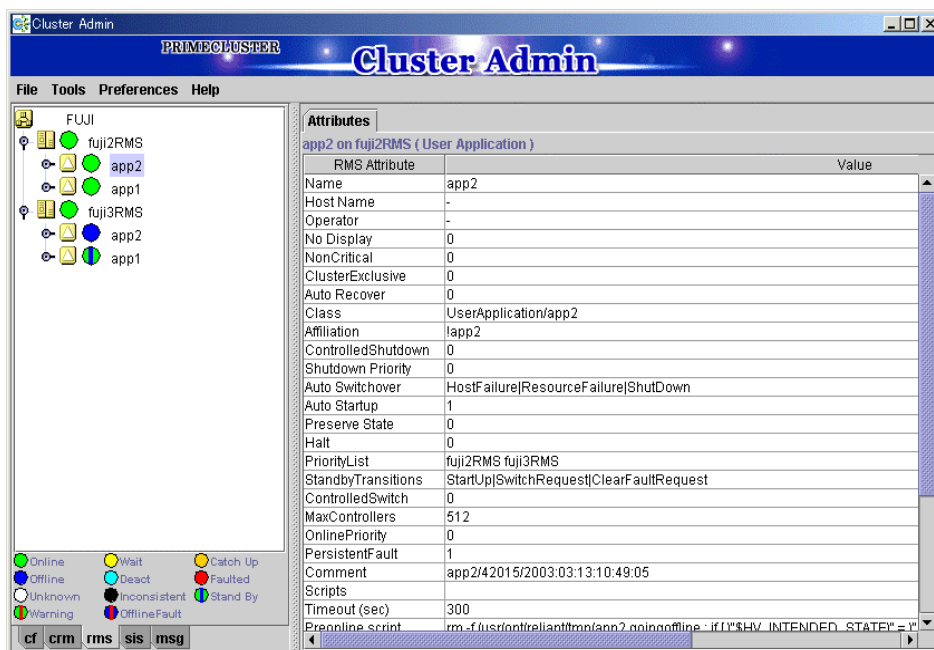


The node indicates one of the following states;

- States
 - UP: The node is running as part of the cluster system.
 - DOWN: The node is down and not in the cluster.
 - UNKNOWN: The node state is unknown.
 - LEFTCLUSTER: The node state is unknown since nodes are not connected each other.

7.3.2 Monitoring the State of a Cluster Application

When you display a cluster application in an RMS tree, the cluster application state appears to the right of the icon. The right panel displays the properties of the cluster application.



The cluster application shows one of the following states:

- Online
- Offline
- Unknown
- Wait
- Deact
- Inconsistent
- Faulted
- Stand By
- OfflineFault



See

See "State display of other objects" in 7.1.3.1 "RMS Tree."

7.3.3 Concurrent Viewing of Node and Cluster Application States

To view the states of the nodes and cluster applications concurrently, display the RMS cluster table.

Right-click the cluster icon on the RMS tree, and select *View Cluster Wide Table* from the displayed pop-up menu. The RMS cluster table is displayed as shown below.

- **RMS clusterwide table**

Applications	fuji2	fuji3
app1		
app2		

Show State Names

The first line shows the names of the nodes that RMS is managing (fuji2 and fuji3 in the example above). To the left of each node name is a state display icon that shows the state of that node. The second and subsequent lines show the names of all cluster applications that RMS is managing and the states of those applications. The RMS cluster table enables you to display the states of nodes and cluster applications in one table.

- **Viewing the RMS Cluster Table**

If the background color of the cluster application name is the same as that of the background of the window

It indicates that the cluster application is online.

If the background of the cluster application name is pink

This condition indicates that the cluster application is in the Faulted state and a failure has occurred in one or more SysNode.

If the background of the cluster application name is sky blue

This condition indicates that the cluster application is in the Offline state.

If the state display icon of a cluster application is enclosed in a rectangle

This condition indicates that the node has the highest priority among those nodes that configure the cluster application. If the cluster application is started after creating the cluster application, the node in a rectangle will be in the online state.

Displaying/hiding state names

Select the *Show State Names* checkbox to display state names to the right of the state display icons.



See

For details on the RMS cluster table, see "4.2.6 RMS clusterwide table" in *"PRIMECLUSTER RMS Configuration and Administration."*

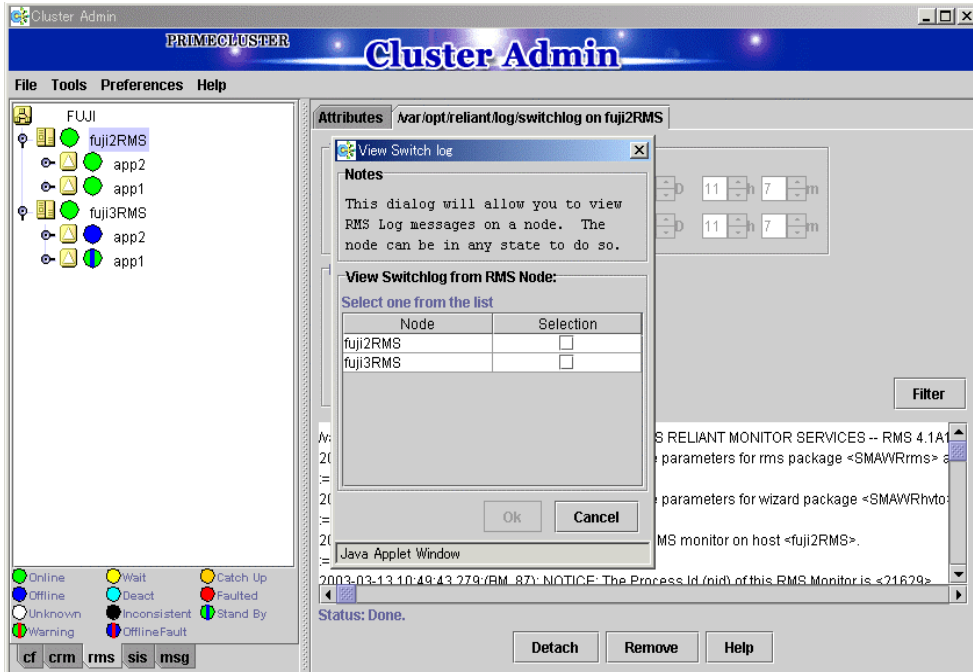
7.3.4 Viewing Logs Created by the PRIMECLUSTER System

There are two types of logs that can be viewed in the PRIMECLUSTER system:

- **Switchlog**
The switchover requests or failures that occur in nodes are displayed.
- **Application log**
The operation log of the cluster application is displayed.

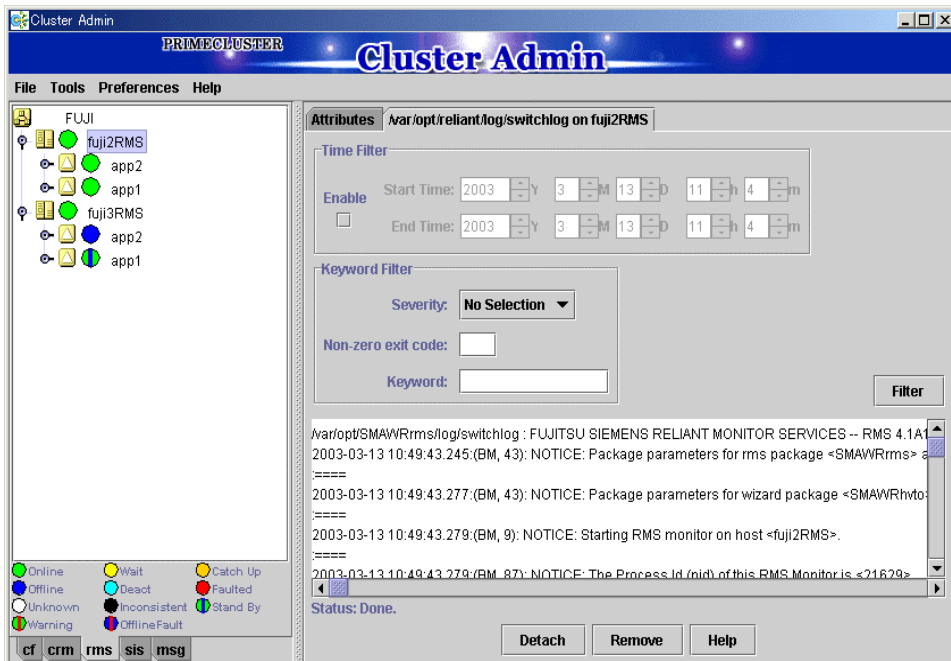
7.3.4.1 Viewing switchlogs

Right-click the system node and select the *View Switchlog* option from the pop-up menu. The switchlog is displayed on the right side of the screen.



7.3.4.2 Viewing application logs

Right-click an application on the RMS tree and choose *View Log File*. The application log for that application will be displayed on the right side of the screen.





Information

The following display formats are enabled for the log. For details, see "4 Administration" in *"PRIMECLUSTER RMS Configuration and Administration."*

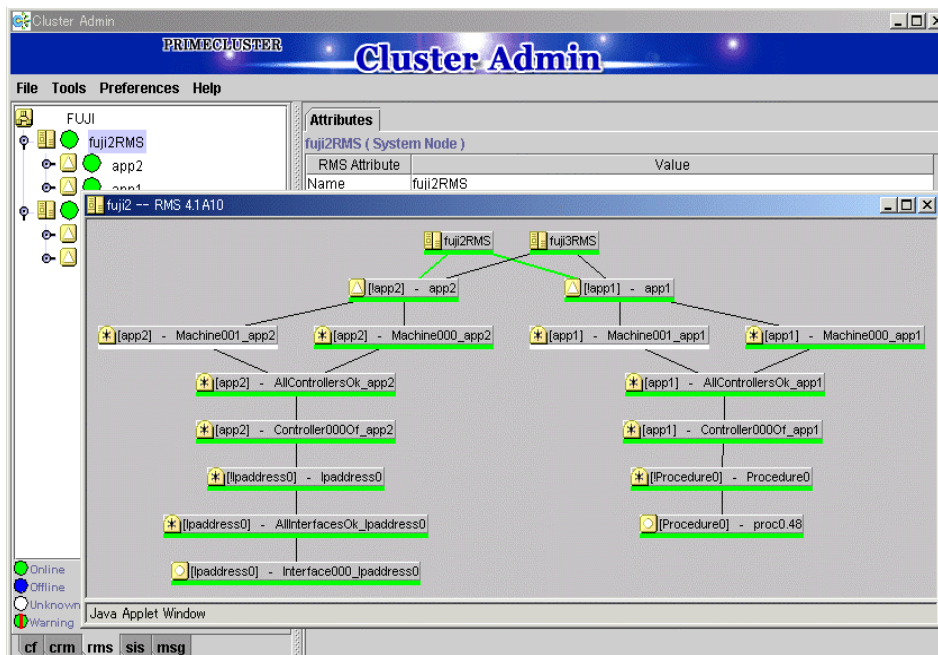
- Narrow the log by date or keyword.
- Scroll or jump to any entry.
- Search by keyword, date range, error message significance, or exit code other than 0 to exclude unrelated entries.

7.3.5 Viewing Detailed Resource Information

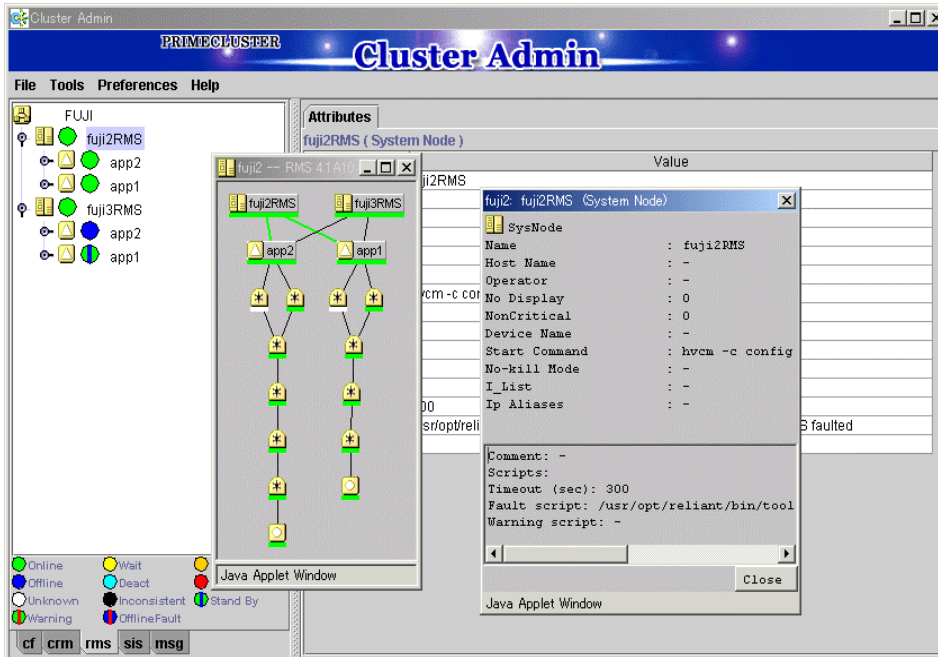
Use RMS graphs to display detailed resource information for each cluster application. There are four types of RMS graphs. Each type can be displayed from the menu when you right-click an object on the RMS tree.

- Full graph
Displays the configuration of the entire cluster system in which RMS is running.
- Application graph
Shows all objects used by the specified application. You can check the details of the specific object using this graph.
- Sub-application graph
Lists all sub-applications used by a given application and shows the connections between the sub-applications.
- Composite sub-applications graph
Shows all sub-applications that the application depends on directly or indirectly.

■ RMS graphs



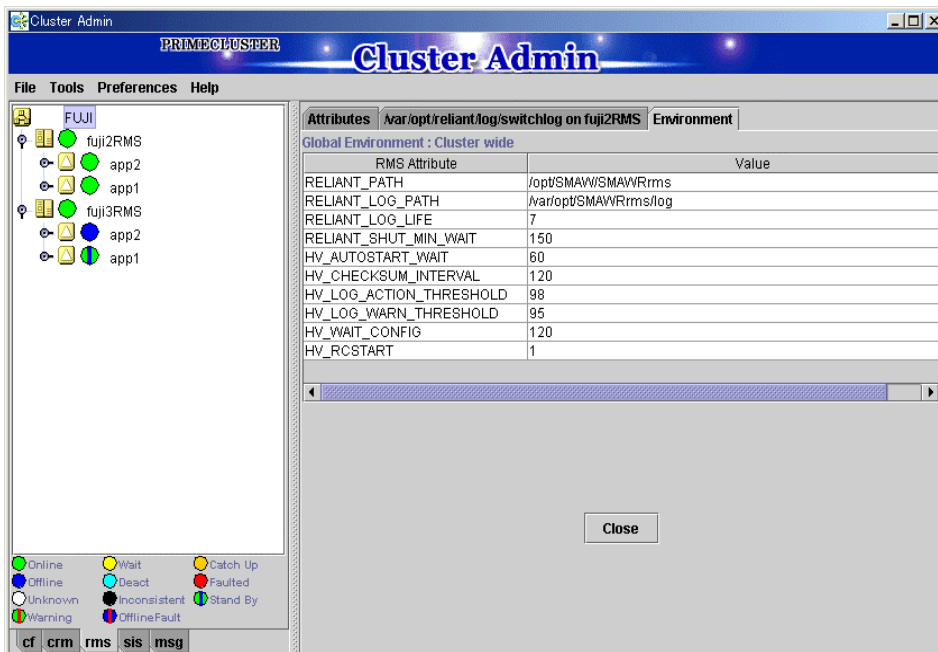
If you left-click the target object, the attributes of the object will be displayed on a pop-up screen.



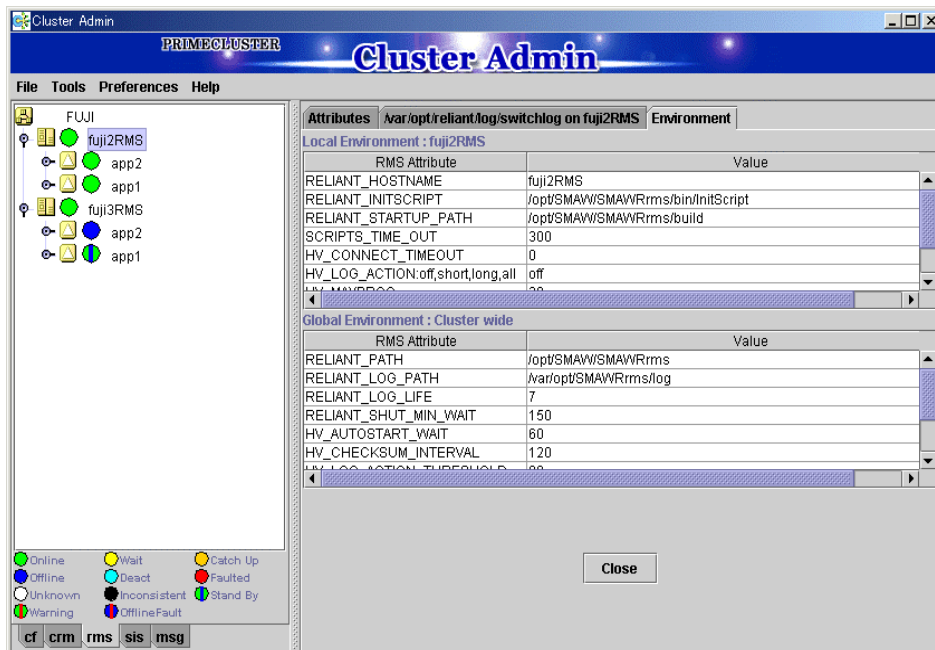
See "4.2.5 RMS graphs" in "PRIMECLUSTER RMS Configuration and Administration."

7.3.6 Displaying environment variables

Right-click a cluster in the RMS tree window and select *View Environment*. The local and global variables are displayed.



Right-click a node in the RMS tree, and select *View Environment*. The local variables are displayed.



7.3.7 Monitoring Cluster Control Messages

Select the *msg* tab, which is found at the bottom of the tree panel. If a new message was added to the text area since the last time the area was displayed, this tab is displayed in red. You can clear the message text area or isolate it from the main panel.

7.4 Corrective Actions for Resource Failures

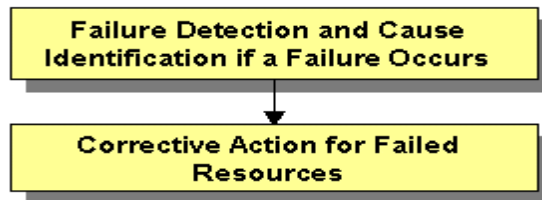
A hardware or software failure might occur while the cluster system is running. If a failure occurs in a resource, a message indicating that a failure occurred is displayed in the Cluster admin pop-up screen. Based on this message, you need to identify the faulted resource using the CF, CRM, and RMS main window and take corrective actions to maintain high availability in the cluster system.

This section describes the actions to be taken for the following cases:

- If the resource state became Faulted.
- If the Patrol Diagnosis Facility detects a failure.

7.4.1 Corrective Action when the resource state is Faulted

This section describes the corrective actions to take when the resource state became Faulted.



7.4.1.1 Failure Detection and Cause Identification if a Failure Occurs

If a failure occurs in a resource, you can use the functions of PRIMECLUSTER and the operating system to detect the failure and identify the faulted resource that caused the failure.

◆ Failure detection

Normally, the RMS main window (b) is used to monitor the cluster applications.

- If a failure occurs in a resource or the system
Failover of the userApplication or node panic will occur.
In such a case, you can detect the failure by observing the following conditions:
 - A pop-up message screen (a) is displayed.
 - The color of the icons in the RMS main window (b) changes.
 - A message is output to the msg main window (g), Syslog(i), and the console (j).
- If a warning-level failure occurs in the system
If a warning-level failure (for example, insufficient disk space or insufficient swap area) occurs in the system, you can detect the failure by observing the following conditions:
 - The node icon in the CRM main window (d) changes.
 - A message is output to Syslog(i) and the console (j).

In addition, you can use the features described in "Failure confirmation features" to detect the failure.

◆ Cause identification

You can also use the function that detected the failure and the features listed in "Failure confirmation features" below to identify the faulted resource that caused the failure.

- **Failure confirmation features**
 - a. Message screen
For details, see C.3.1 "Failed Resource Message."
 - b. RMS main window
The RMS tree and the RMS cluster table can be used from this screen.

- For instructions on viewing the RMS main window, see 7.1.3 "RMS Main Window."
- c. CF main window
 - The CF tree can be used from this screen.
 - For instructions on viewing the CF main window, see 7.1.1 "CF Main Window."
- d. CRM main window
 - The CRM tree can be used from this screen.
 - This screen is useful in detecting hardware resource faults.
 - For instructions on viewing the CRM main window, see 7.1.2 "CRM Main Window."
- e. "Resource Fault History" screen
 - This screen is useful in detecting hardware resource faults.
 - For details, see C.3.2 "Resource Fault History screen."
- f. Current list of resources in which a failure has occurred
 - For details, see C.3.3 "Fault resource list."
- g. MSG main window
 - The cluster control messages can be viewed in this screen.
 - To display this screen, select the *msg* tab in the Cluster Admin screen.
- h. Application log
 - For instructions on displaying the application log, see 7.3.4.2 "Viewing application logs."
- i. Syslog
- j. Console
 - Messages that are displayed on the console can be checked.
 - For message details, see Appendix D "Messages."
 - Viewing the "console problem" information on the console can help you identify the fault cause.
- k. Machine management GUI
 - For details, see the "*Machine Administration Guide*."
- l. MultiPathDisk view
 - For details, see the "*Multipath Disk Control Load Balance option x.x Guide*."
- m. GDS GUI
 - For details, see the "*PRIMECLUSTER Global Disk Services Configuration and Administration Guide*."

7.4.1.2 Corrective Action for Failed Resources

Take the following steps for failed resources;

1. Correct the faulted resource
 - Correct the problem in the failed resource. For details, see "5 Troubleshooting" in "*PRIMECLUSTER RMS Configuration and Administration*."
 - If an error message of patrol diagnosis is displayed, see 7.4.2 "Corrective Action when Patrol Diagnosis Detects a Fault,"

"hvdet_sptl" is displayed in the name of the program that outputs the patrol diagnosis message.



Note

If you are using an operation management product other than a PRIMECLUSTER product, you may need to take corrective actions prescribed for that product. For details, see the manual provided with each operation management product.

[Examples] Machine Administration, MultiPathDisk view, GDS

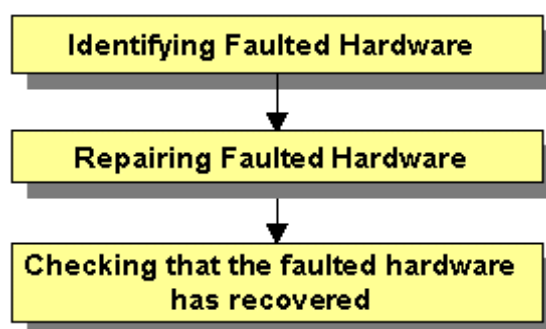
2. Recover the cluster application

At the RMS main window, check the state of the cluster application to which the corrected resource is registered. If the cluster application is in the Faulted state, execute the Faulted clear operation.

For details on the Fault clear operation, see 7.2.2.4 "Bringing Faulted Cluster Application to Online State."

7.4.2 Corrective Action when Patrol Diagnosis Detects a Fault

This section explains the actions to take when the patrol diagnosis facility detects a failure



7.4.2.1 Identifying Faulted Hardware

Use one of the following methods to identify the faulted hardware:

- Message text output to the CRM main window or syslogd(1M)
See D.8 "Patrol Diagnosis Messages."
- CRM main window
The CRM main window displays the OFF-FAIL state for the faulted hardware. See 7.1.2 "CRM Main Window."
- clgettree(1) command
The clgettree(1) command displays the OFF-FAIL state for the faulted hardware. See the manual page for clgettree(1M).

7.4.2.2 Corrective Action for Faulted Hardware

Correct the faulted hardware according to the operation procedure below.

- **Operation Procedure:**
 1. Stop the node to which the faulted hardware is connected.
 2. Repair the faulted hardware.
 3. Start the node.



Note

When a disk unit that is registered with GDS is to be exchanged, follow the steps described in the GDS disk replacement procedure. For information on GDS disk replacement, see "In Case of Disk Abnormality" in the *PRIMECLUSTER Global Disk Services Guide*.

4. Check that the faulted hardware has recovered using one of the following methods:
 - 1) Use the CRM main window.
 - 2) Execute the `clgettree(1)` command.

If the above procedure shows that the fault was not corrected, you need to continue the following procedure:

- 1) Execute the diagnosis operation for the faulted hardware from the CRM main window

Then, use the CRM main window to check whether the fault was corrected. If the fault was corrected, the ON state is displayed.

- 2) Execute the `clsptl(1M)` command to initiate the diagnosis operation.

The `clsptl(1M)` command has two functions. One function allows you to specify a faulted hardware unit and diagnoses only the specified device. The other function runs batch diagnosis of all shared disk units or all network interface cards. If faults occur in multiple hardware units, it is convenient to use the batch diagnosis function.

- Example in which a faulted shared disk unit is specified and diagnosis is executed:

```
# /etc/opt/FJSVcluster/bin/clsptl -u generic -n c1t4d4
```

- Example in which batch diagnosis is executed for all shared disk units:

```
# /etc/opt/FJSVcluster/bin/clsptl -a DISK
```

Execute the `clgettree(1)` command to check whether the fault was corrected. If the fault was corrected, the ON state will be displayed for the hardware.

5. Bring the Faulted cluster application Online.

Confirm that the state of the cluster application to which the recovered hardware is registered, either in the RMS main window or with the `hvdsp(1M)` command.

If the cluster application is Faulted, switch the cluster application from the failed to the active state, either in the RMS main window or with the `hvutil(1M)` command. For information on the procedures related to the CRM main window, see 7.2.2.4 “Bringing Faulted Cluster Application to Online State”.

If operator intervention request is enabled, a message will be displayed with the `syslogd(1M)` command and Cluster Admin when RMS is started. By entering a response to this message, you can switch the state of the cluster application from the failed state to active. For information on the setup procedure for operator intervention requests, see 5.5 “Setting Up Fault Resource Identification and Operator Intervention Requests”.

An example of an operator intervention request is shown below. For details on the messages requesting operator intervention, see D.5 “Failed Resource and Operator Intervention Messages (GUI)” and D.6 “Failed Resources and Operator Intervention Messages (CLI).”

```
1422 userApplication "app0 of SysNod "node1RMS" is in the Failed state due to a
failure in the resource "apl1." Do you want to clear the Failed state? (yes/no)
Message number: 1001
```



Note

If “Yes” is set for the “AutoStartUp” attribute, an operator intervention request message will be displayed at node startup. You need to respond to the to the operator intervention message after executing step 4. of the procedure.

Part 4 System Configuration

Modification

Chapter 8 Changing the Operation Configuration

This chapter explains how to add nodes and cluster applications to the PRIMECLUSTER system and change the configuration contents.

8.1 Changing the Cluster Configuration

This section explains how to modify a cluster configuration related to the followings:

1. Change a cluster application configuration.
2. Change an operation attribute of a cluster application.
3. Change a resource.



Note

Be sure to stop RMS before changing the cluster configuration. If you start the "userApplication Configuration Wizard" screen while RMS is running, the message 0833 will be displayed. If this happens, stop RMS, and then restart the "userApplication Configuration Wizard" screen. For instructions on stopping RMS, see 7.2.1.2 "Stopping RMS."



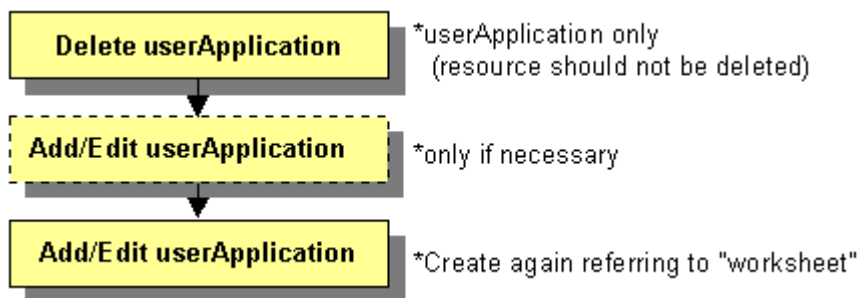
Information

After you finish changing the cluster application, execute "RMS startup" from the Cluster Admin screen. If necessary, also start the cluster application. For instructions on starting RMS, see 7.2.1.1 "Starting RMS." For instructions on starting the cluster application, see 7.2.2.1 "Starting a Cluster Application."

8.1.1 Changing the Cluster Application Configuration

To change the configuration of a cluster application, you must first delete the cluster application. The procedure is shown below.

◆ Operation flow



◆ Operation Procedure:

1. Stop RMS.
If RMS is running, see 7.2.1.2 "Stopping RMS" and stop RMS.
2. Delete the cluster application.
Delete only the target cluster application.
For details on how to make this deletion, see 8.9.1 "Deleting a userApplication."



Note

Deleting a userApplication

Do not delete a resource that is necessary to configure the cluster application.

3. Add, delete, or change the resource.
Add a new resource and delete any unnecessary resources.



See

For details on how to perform the above operations, see the following:

When a resource is to be added: 6.6.1 "Setting Up Resources"

When a resource is to be deleted: 8.9.2 "Deleting a Resource"

When a resource is to be changed: 8.1.3 "Changing Resources"

4. Create a cluster application.
Create the same cluster application as that deleted in step 2.
For details on how to create the cluster application, see 6.6.2 "Creating a Cluster Application."
If cluster application dependency relationships have been set up, they must be set up again.
For details on how to make these settings, see 6.6.3 "Setting Up Dependency Relationships Between Cluster Applications."



Note

If it is not necessary to change the operation attributes of the cluster application, leave the attribute unchanged as explained in the A.10 "Cluster Application Worksheet."

8.1.2 Changing the Operation Attributes of a Cluster Application

The procedure for changing the operation attributes of a cluster application is described below.

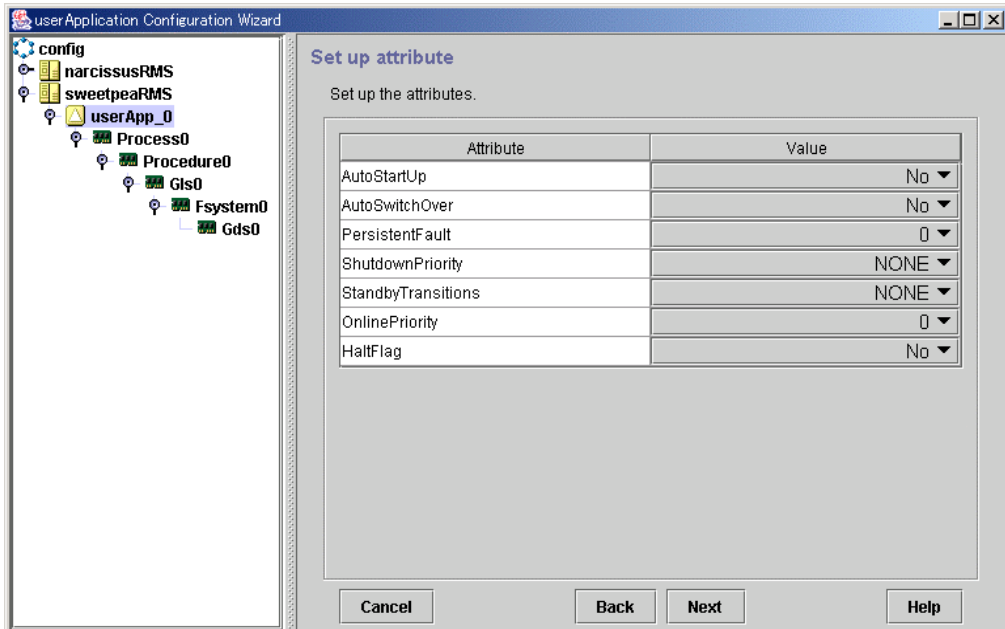
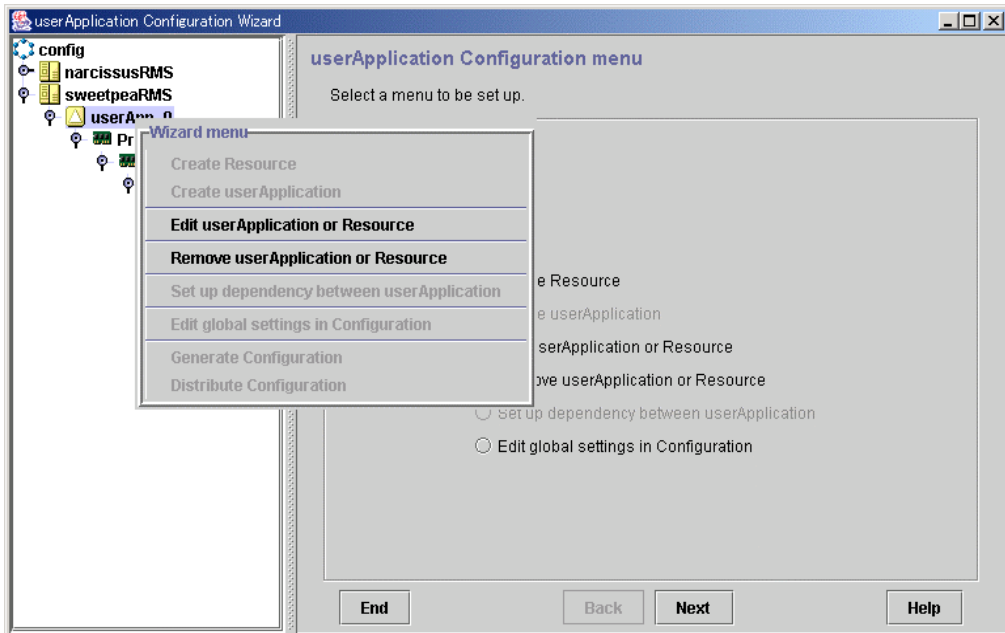
◆ Operation Procedure:

1. Stop RMS.
If RMS is running, see 7.2.1.2 "Stopping RMS" and stop RMS.
2. Change the operation attributes of the target userApplication.
At the "Global Cluster Services" screen, select *userApplication Configuration Wizard*.
From the tree on the left of the "userApplication Configuration Wizard" screen, select the userApplication to be changed, right-click the mouse to display the pop-up menu, and select *Edit userApplication or Resource*.

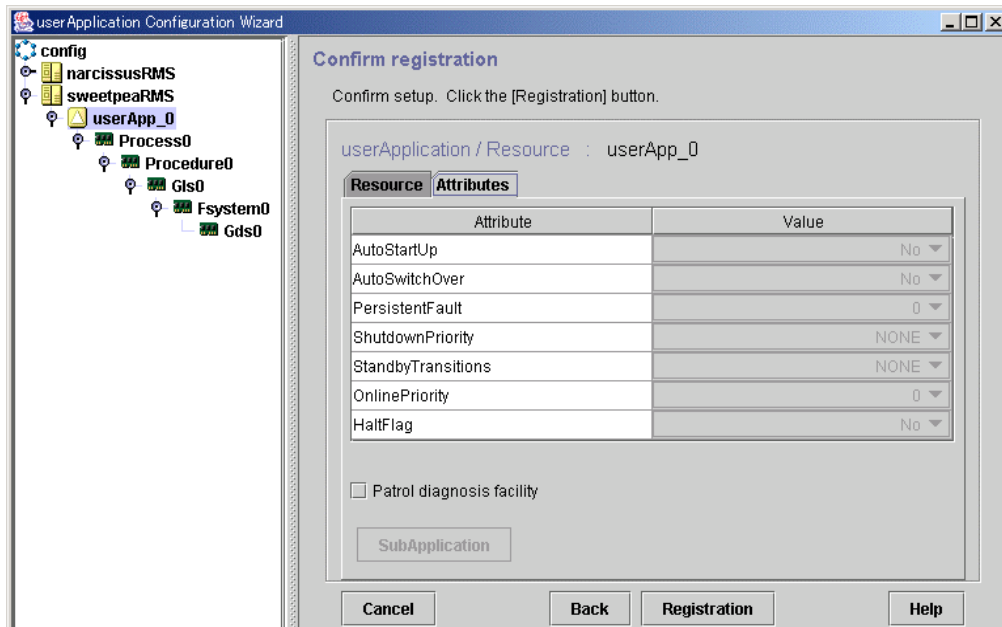
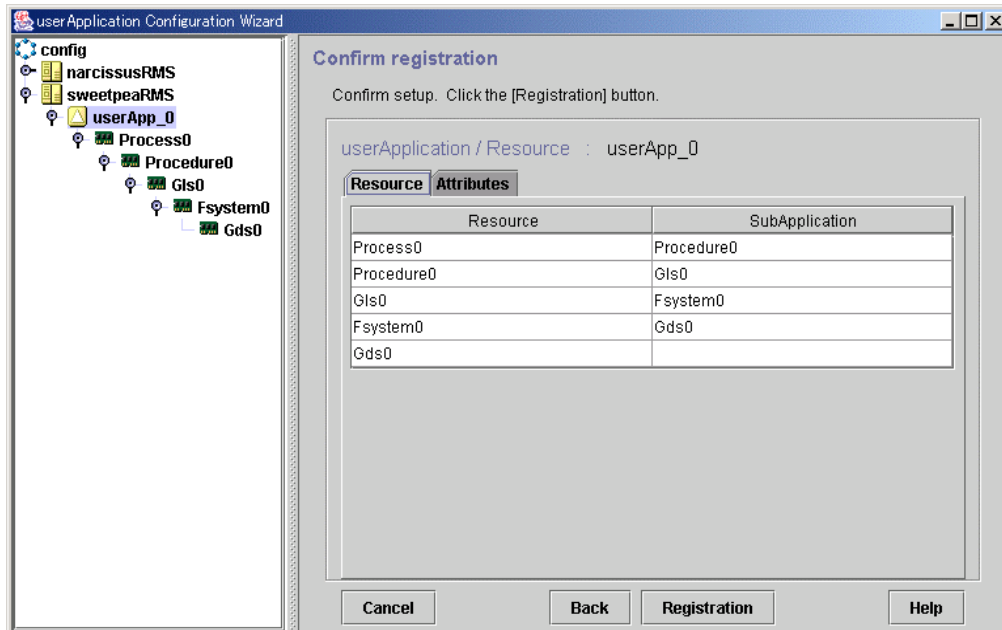


Point

To change the cluster application, you can also select *Edit userApplication or Resource* at the top menu of the userApplication Configuration Wizard, and click *Next*.

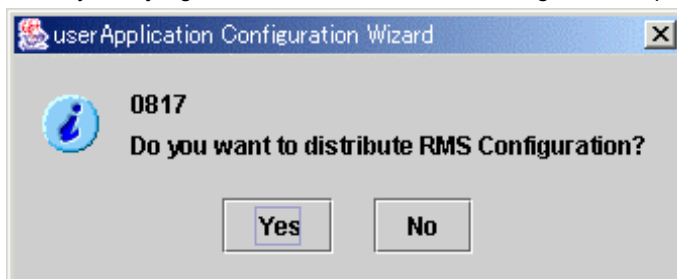


Change the operation attributes. For information on the individual operation attributes, see 6.6.5 "Attributes."



After you finish changing the operation attributes, register the attributes. Click the *Registration* button to register the attributes to RMS Configuration.

After registration to RMS Configuration is completed, the following message screen is displayed if the system judges that distribution of RMS Configuration is possible.



If you are not changing the operation attributes or resource attributes of another cluster application, click Yes.

8.1.3 Changing Resources

The resource modification includes the followings:

1. Change the interface used by a resource.
2. Change the attributes to the resources and resource interfaces.



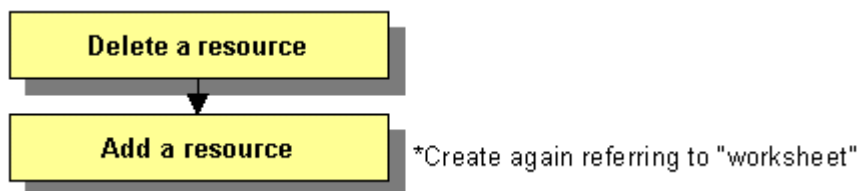
Point

Resources can be changed only when RMS is stopped.

8.1.3.1 Changing the Interface Used by a Resource

To change the interface used by a resource, you must delete first resource and then add it back again. Interface examples include a takeover network for an Ipaddress and a disk class for a Gds resource.

◆ Operation flow



◆ Operation Procedure:

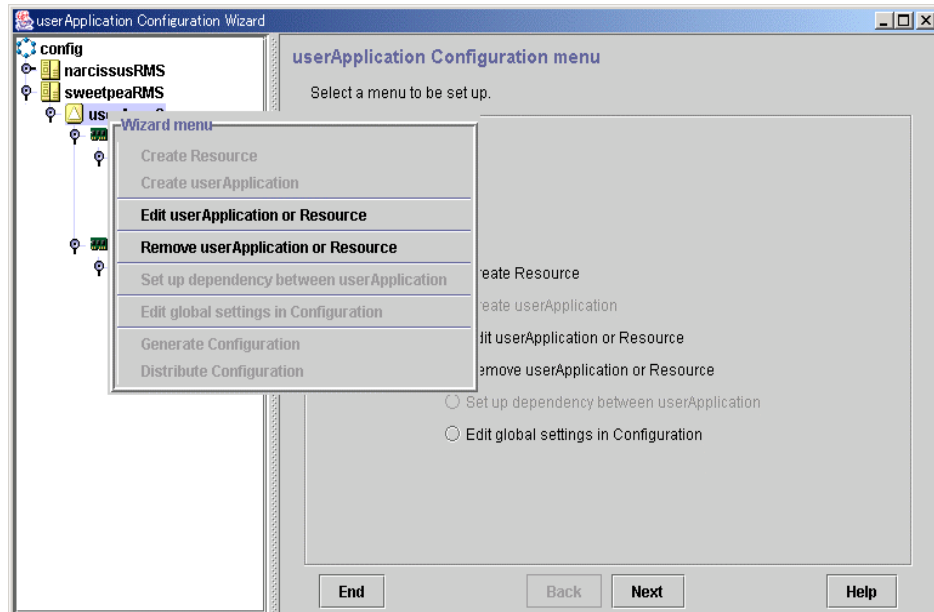
Use the "userApplication Configuration Wizard" screen change a resource used by a cluster application.

1. Stop RMS
If RMS is running, see 7.2.1.2 "Stopping RMS" and stop RMS.
2. Delete the resource.
Return to the "Global Cluster Services" screen, and select *userApplication Configuration Wizard*.
From the tree on the left of the "userApplication Configuration Wizard" screen, select the userApplication to be changed, right-click the mouse to display the pop-up menu, and select *Remove userApplication or Resource*.



Note

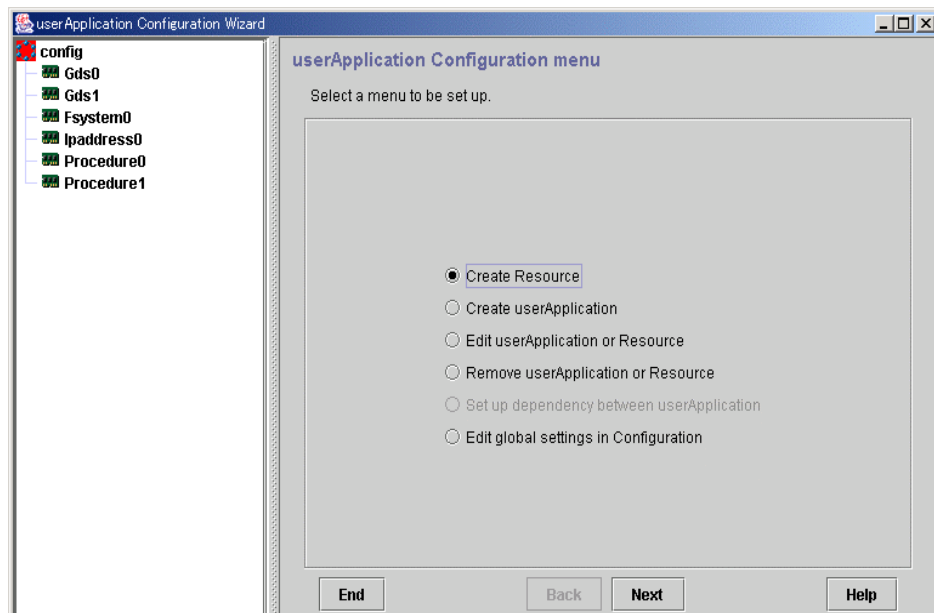
If you delete a resource included in the cluster application, the other resources found under the target resource are also deleted. In other words, the entire hierarchy of objects found under the resource on the tree in the left panel will be deleted regardless of those objects being related to other resources.



3. Re-create the resource.

If new resources are required, create resources.

Select *Create Resource* from the *userApplication Configuration Wizard* menu.



Note

If changes are not required, refer to the A.10 "Cluster Application Worksheet" and set up the resource so that the setup information is the same as before.



See

For setup instructions, see 6.6.1 "Setting Up Resources."

8.1.3.2 Changing the Attributes Used by a Resource or a Resource Interface

Change the attributes used by a resource or a resource interface according to the following procedure.

◆ **Operation Procedure:**

Use the "userApplication Configuration Wizard" screen to change a resource used by the cluster application.

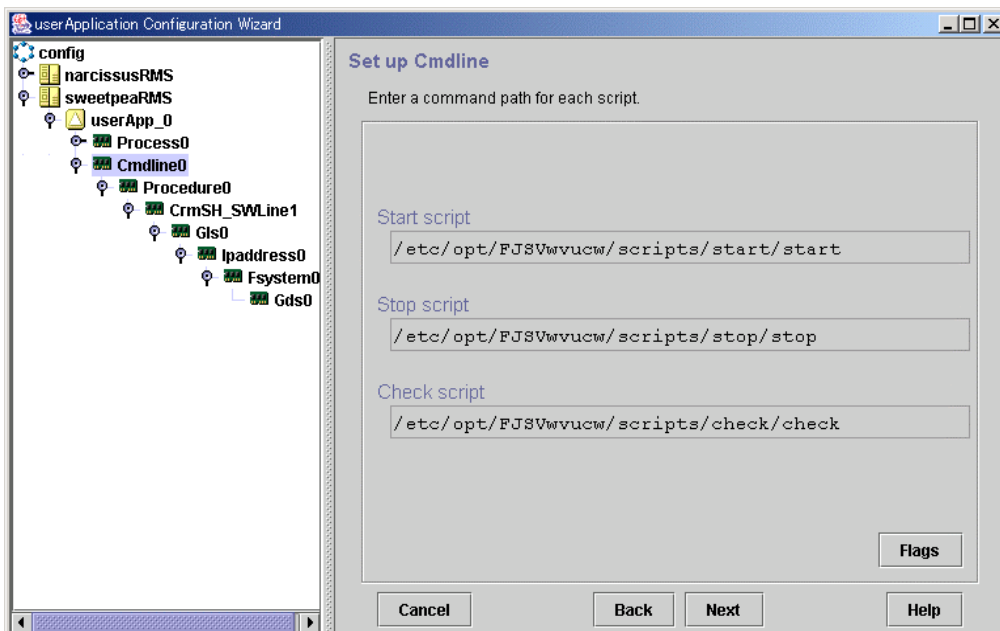
1. Stop RMS.
If RMS is running, see 7.2.1.2 "Stopping RMS" and stop RMS.
2. Select the resource.
Return to the "Global Cluster Services" screen, and select *userApplication Configuration Wizard*.
From the tree on the left of the "userApplication Configuration Wizard" screen, select the resource to be changed, right-click the mouse to display the pop-up menu, and select *Edit userApplication or Resource*.



Point

To change the attributes used by the resource or an interface of the resource, you can also select *Edit userApplication or Resource* from the top menu of the userApplication Configuration Wizard, and then select *Next*.

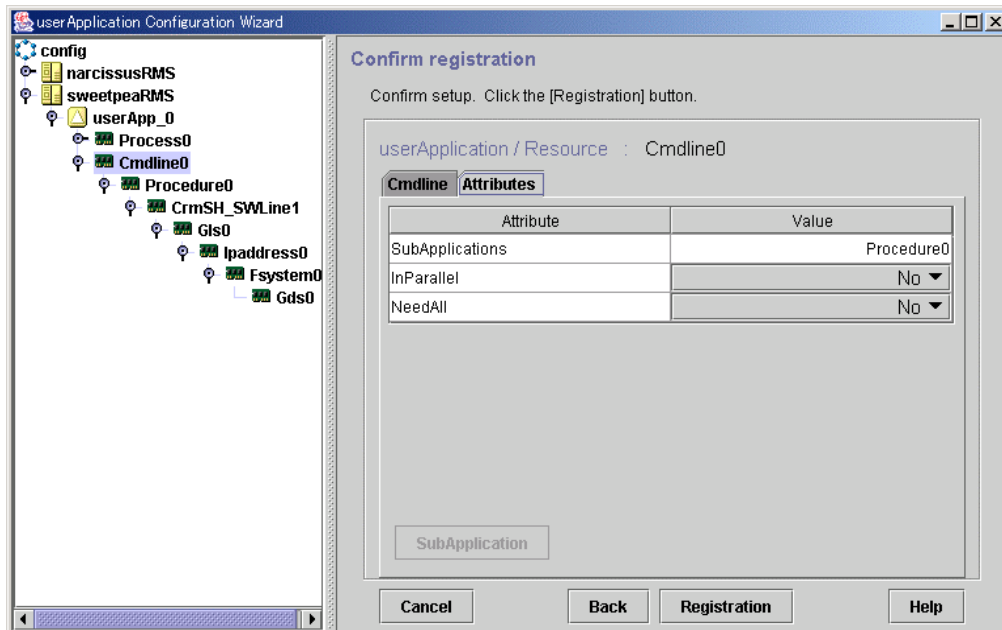
● **Cmdline**



Flag button

Click this button to change the script attributes, if necessary.

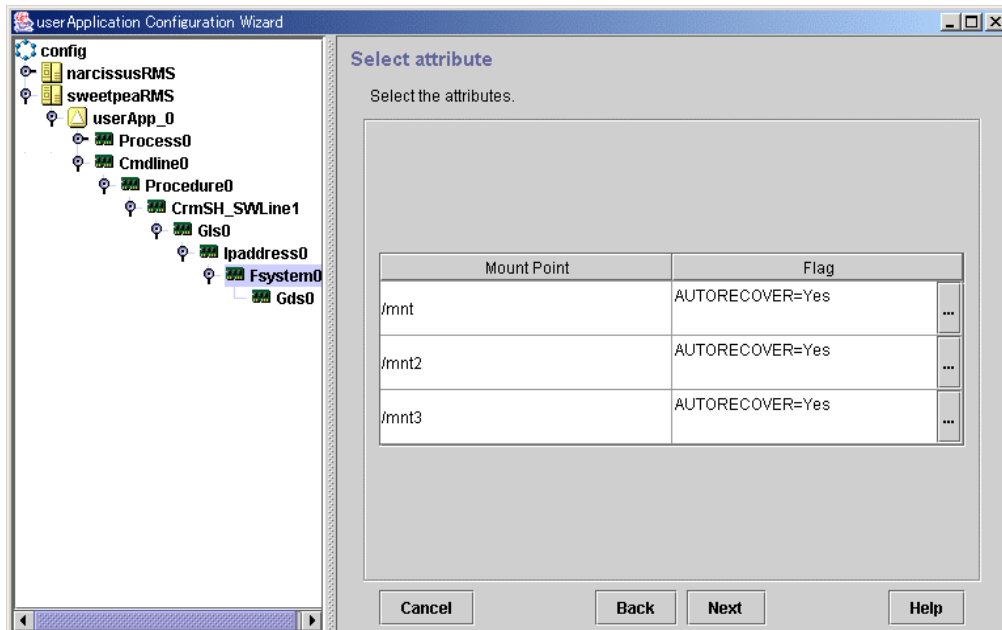
A dialog box for setting the attributes of the created script will be displayed. For details, see "Setting Cmdline Flags" in 6.6.1.1 "Creating Cmdline Resources."



SubApplication button

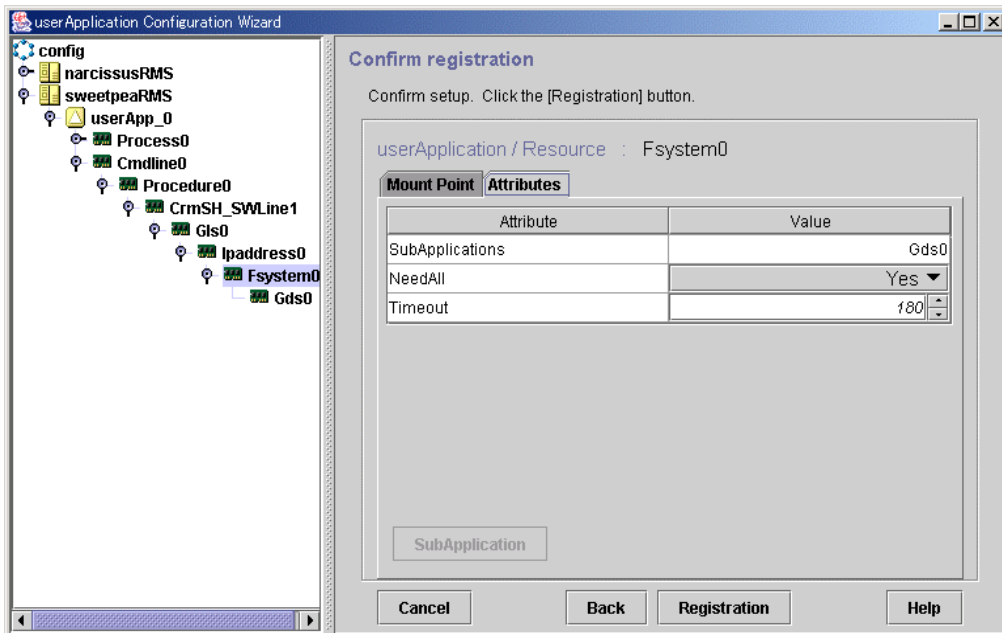
Click this button to associate a previously created Cmdline resource or processing monitoring resource found under the current Cmdline resource. This button cannot be selected if the resource belongs to a userApplication.

- **Fsystem**



"..." button

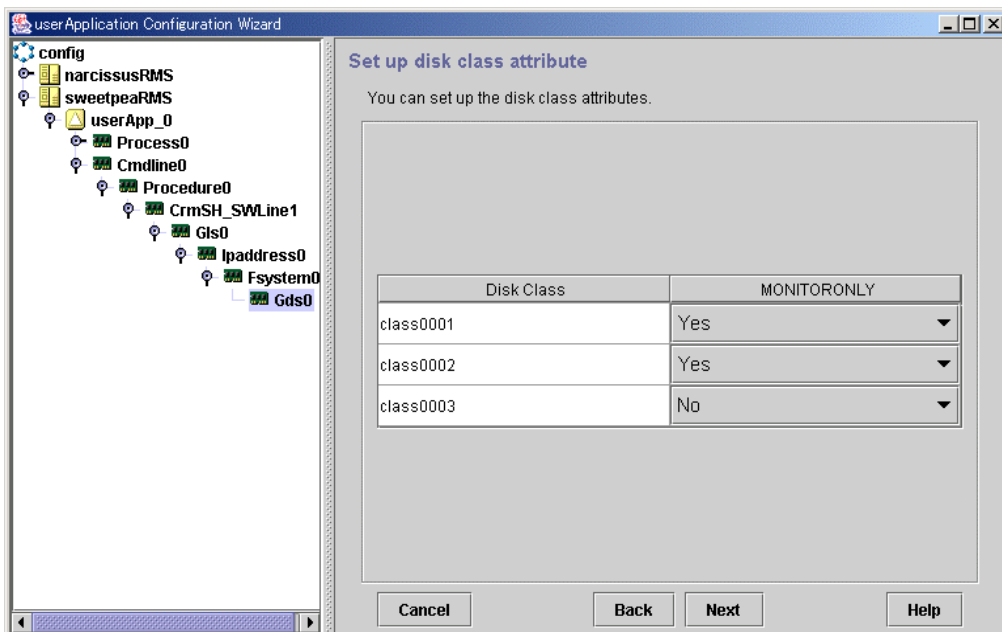
Select this button to change an attribute that controls management of mount points. If you click this button, the "Change Mount Point Attributes" screen is displayed.



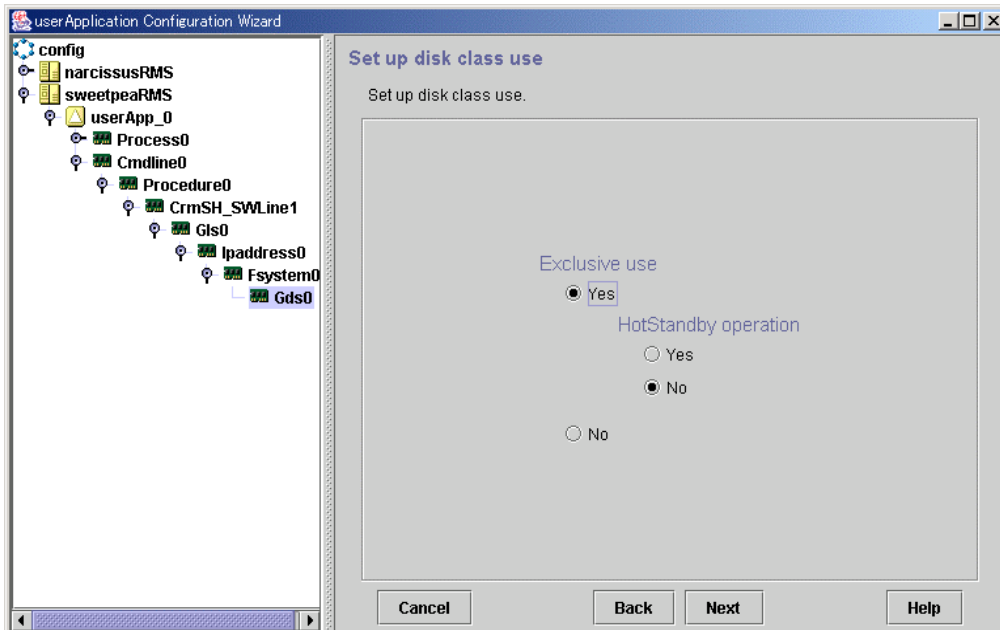
SubApplication button

This button is for specifying another resource that depends on the current resource. However, in Fsystem, this button is disabled.

- **Gds**



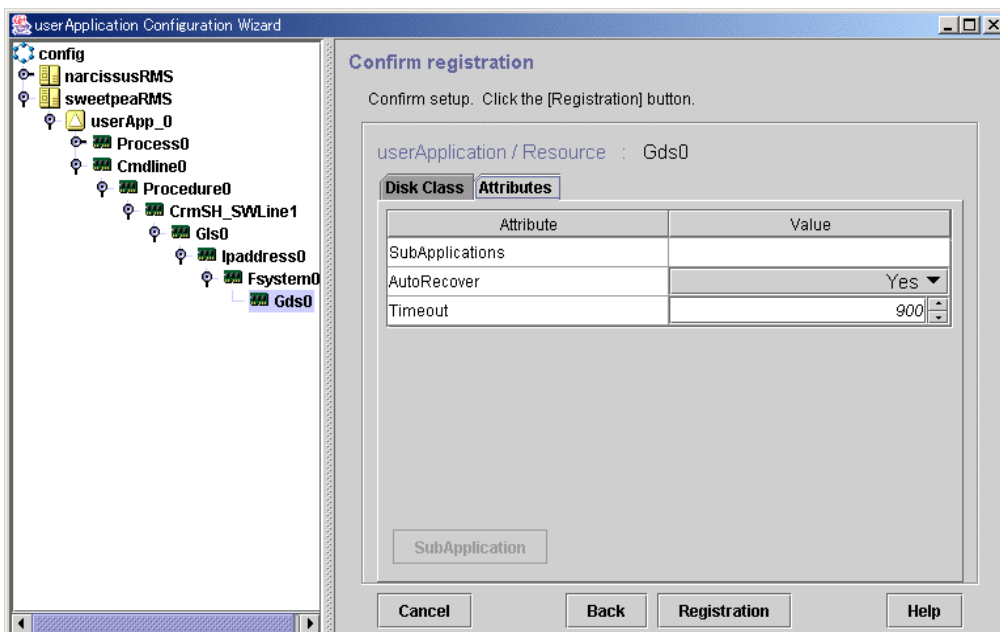
Flag	Outline
MONITORONLY	This flag sets whether the Faulted state of a disk class is to be reported to userApplication if the disk class fails. If this flag is set to "Yes" and a failure of the disk class occurs, the disk class is set to Faulted but the Gds resource remains Online and failover of userApplication does not occur.



Exclusive use

Click "Yes" or "No" for *Exclusive use*. If you select "Yes", select "Yes" or "No" for *Hot-Standby operation*.

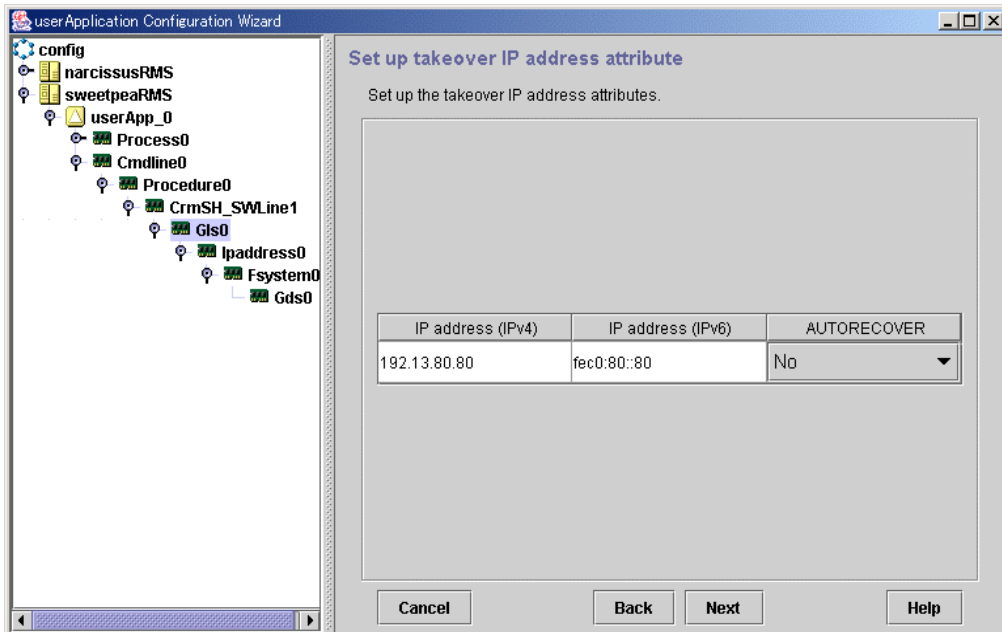
For information on the shared disk, see "Shared disk uses" in 6.6.1.3 "Creating Gds Resources." Note that if you change *Exclusive use* from "No" to "Yes," there is the risk of disk damage if another Gds resource is using the same disk class.



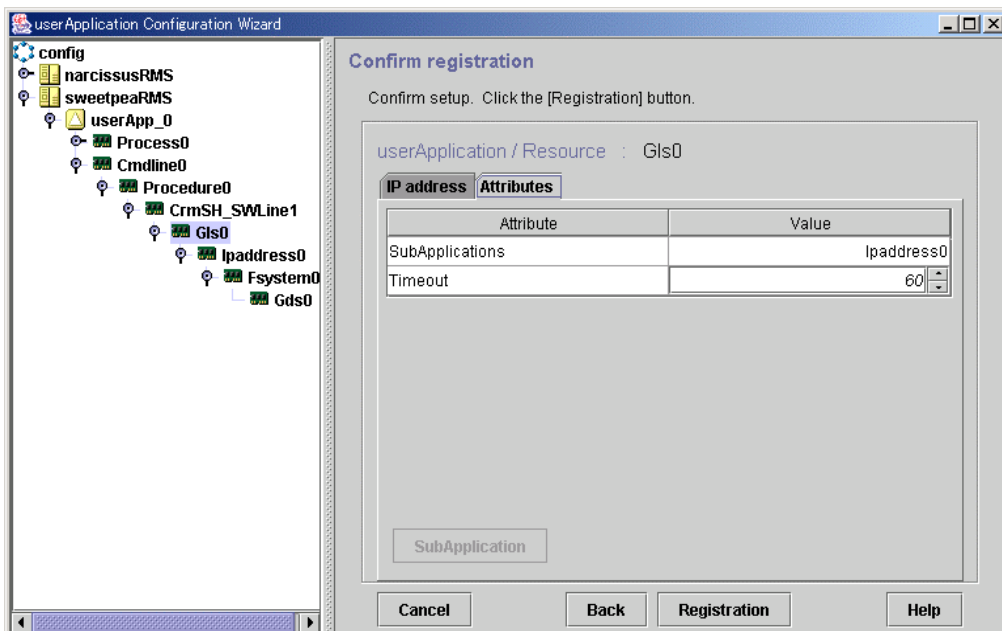
SubApplication button

Click this button to associate the other Gds resources with the Gds resource that has been created above. This button cannot be selected if the resource belongs to userApplication.

- **Gls**



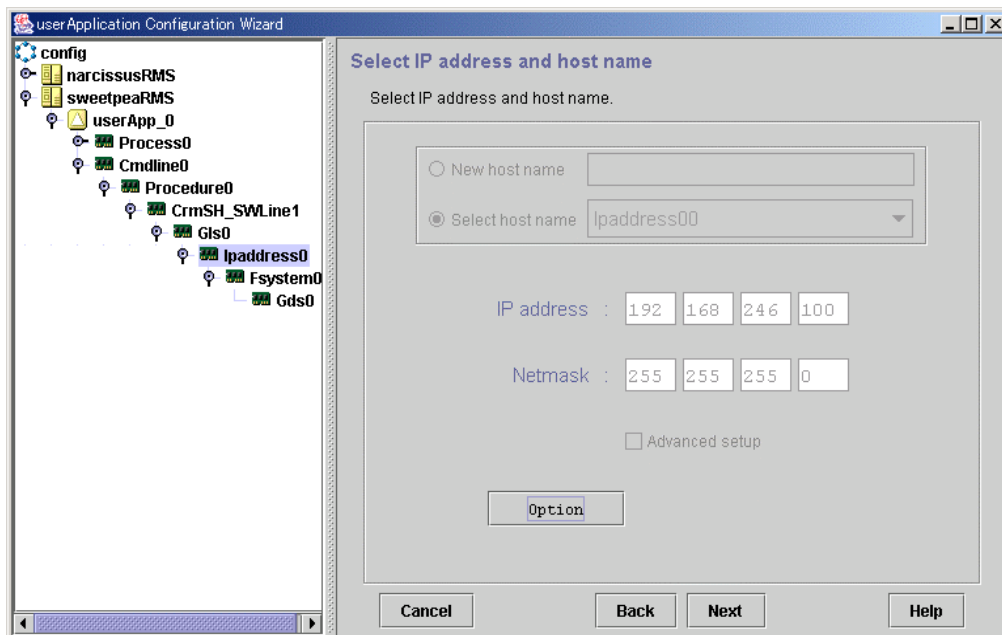
Flag	Outline
AUTORECOVER	Set to "Yes," RMS attempts to restore the faulted resource to prevent userApplication from being switched to other host. For GLS, this flag must be set to "No."



SubApplication button

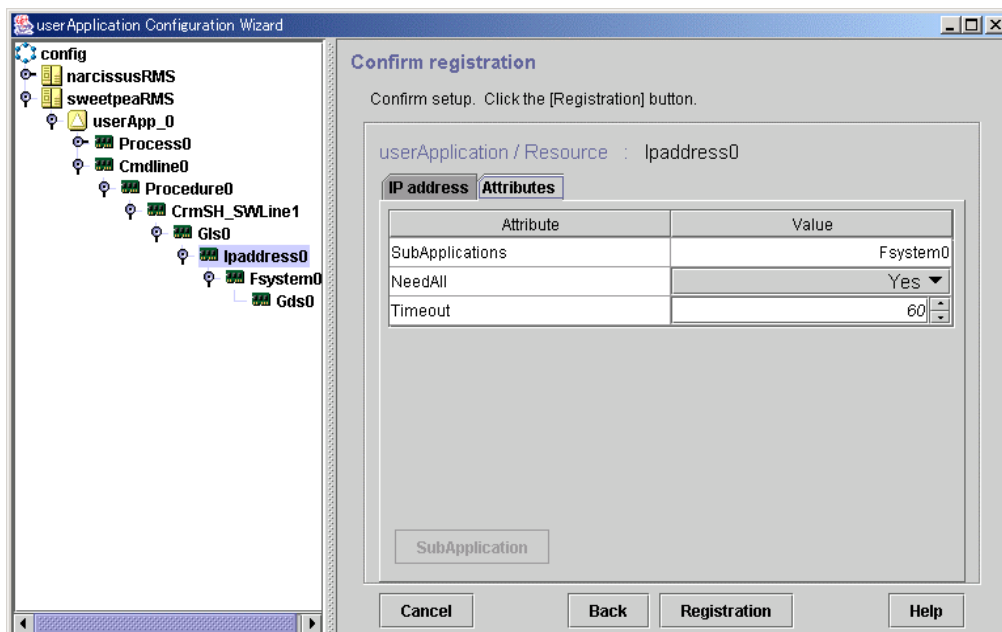
Click this button to associate the other Gls resources with the Gls resource that has been created above. This button cannot be selected if the resource belongs to userApplication.

- **Ippaddress**



Options button

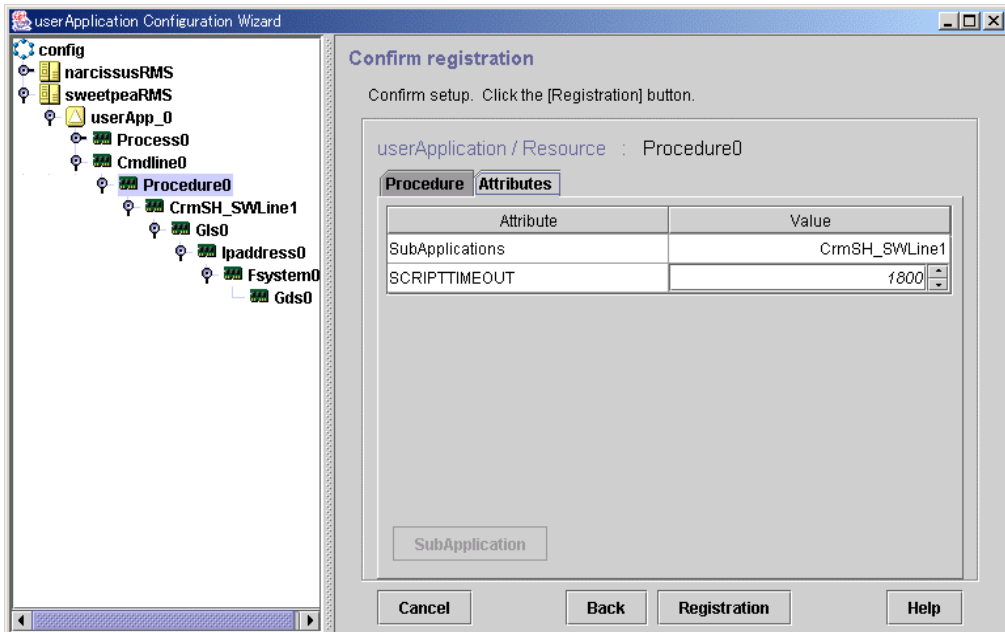
Use this button to change attributes of a takeover IP address. For operation instructions, see "Setting Attributes for a Takeover IP Address."



SubApplication button

Click this button to associate the other Ippaddress resources with the Ippaddress resource that has been created above. This button cannot be selected if the resource belongs to userApplication.

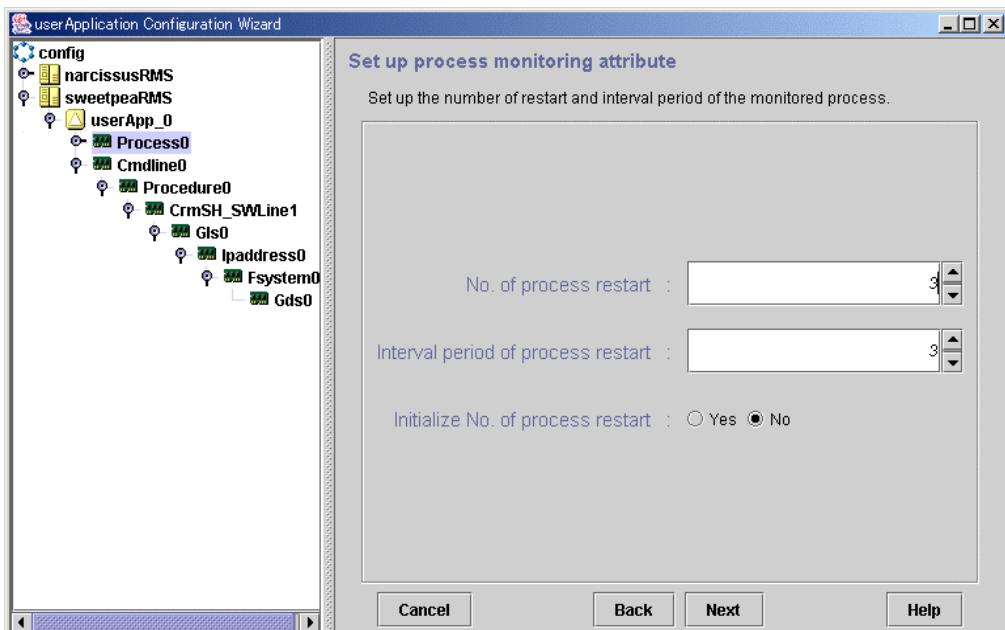
● Procedure



SubApplication button

Click this button to associate the other Procedure resources with the Procedure resource that has been created above. This button cannot be selected if the resource belongs to userApplication.

● Process



No. of process restart

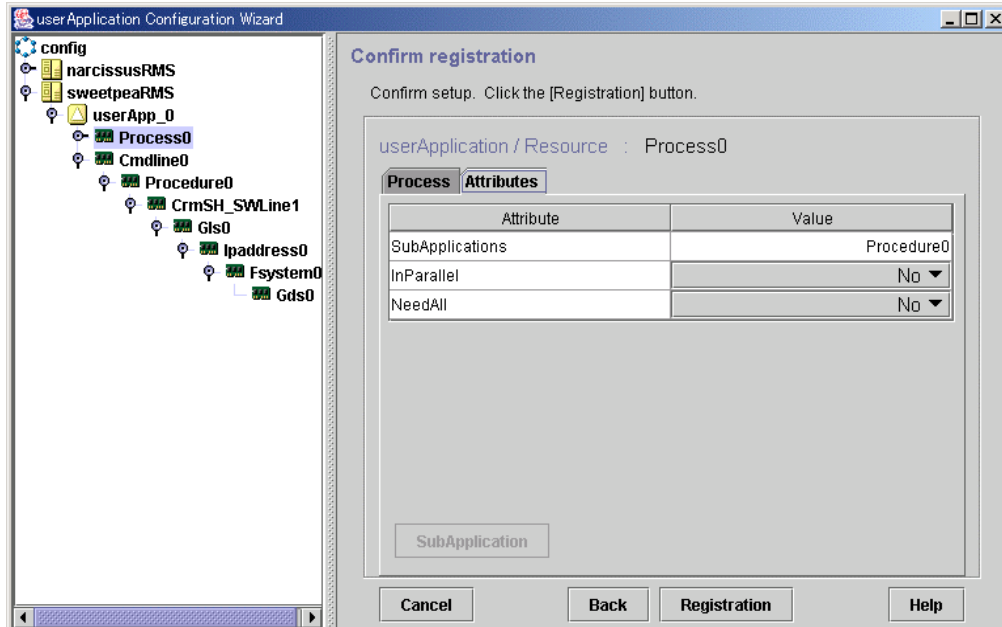
Specify the number of times the monitored process is to be restarted between 0 and 99 (default is 3). If 0 is specified and the monitored process stops, the process is not restarted and becomes Faulted.

Interval period of process restart

Specify the interval period when the process monitoring facility determines that the process has stopped until the facility executes restart. The specification range is between 0 and 3600 seconds (default is 3).

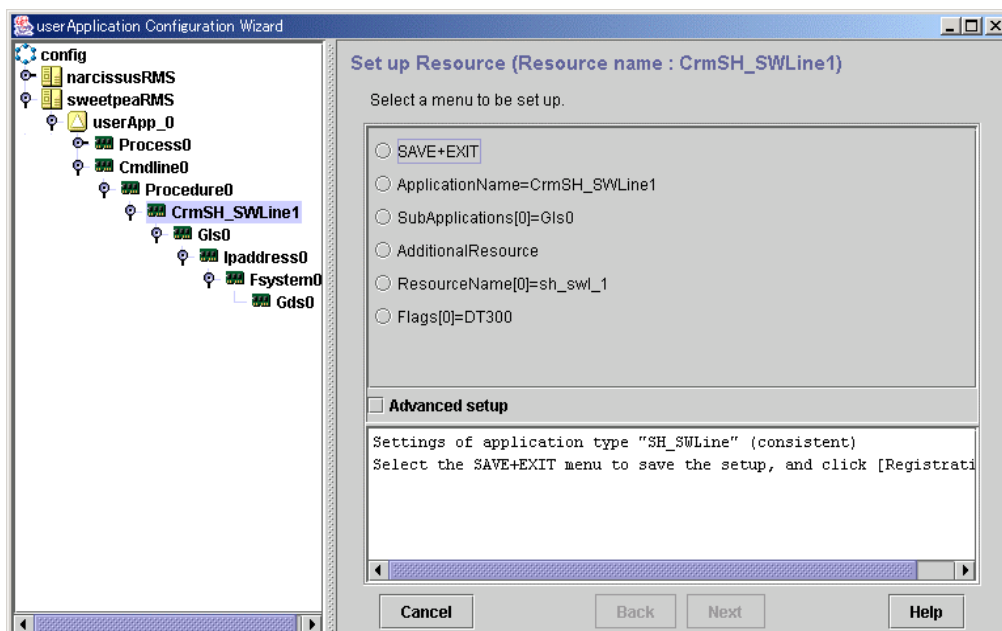
Initialize No. of process restart

Specify whether or not the counter that has the specified *No. of process restart* value in the process monitoring facility as its maximum value is to be initialized periodically. If you select "Yes," the counter is initialized every "*No. of process restart* value × 60 seconds." If you select "No," the counter is not initialized periodically.

**SubApplication button**

Click this button to associate the Process resources or Cmdline resources with the Process resource that has been created above. This button cannot be selected if the resource belongs to userApplication.

- **SH_SWLine**

**Advanced setup**

Check this box to display attributes that do not need to be changed, during resource creation. Use this checkbox to display items such as the setup menu for the resource

timeout value.



Note

Specify "Application name" of the resource only if the resource is not associated with userApplication. If this resource is associated with userApplication, you must delete and then re-create the resource.

- **ISV**

For information on changing an ISV resource, see the manuals for the product.



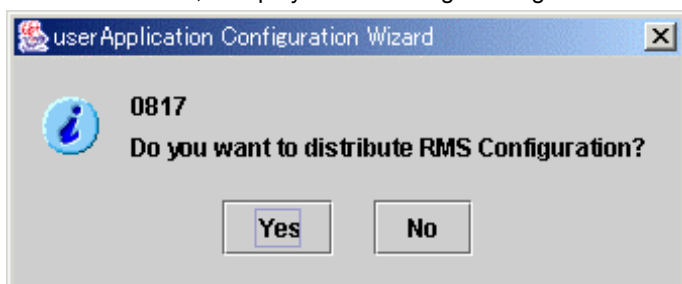
Note

Specify "Application name" of the resource only if the resource is not associated with userApplication. If this resource is associated with userApplication, you must delete and then re-create the resource.

- **RMS Configuration distribution messages**

After you finish changing the operation attributes, click the *Registration* button on the screen to register the new information to RMS Configuration.

If the system judges that registration to RMS Configuration is completed and RMS Configuration can be distributed, it displays the following message screen:



If you have completed making changes, click Yes.

8.2 Changing an IP Address on the Public LAN

This section explains how to change the IP address setting if the IP address of a public LAN or management LAN changes after the PRIMECLUSTER system is installed. Note that when you change an IP address, do not change the host name.



Note

This operation requires shutting down all nodes.

◆ Operation Procedure:

1. Execute the following command on one of the cluster nodes to stop RMS operation:

```
# hvshut -a
```
2. Execute the following commands on all nodes to start the system in single-user mode.

```
# /usr/sbin/shutdown -y -g0 -i0
```

```
:
```

```
ok> boot -s
```
3. Execute the following command on all nodes to mount the file system.

```
# /usr/sbin/mountall -l
```
4. Edit the "/etc/inet/hosts" file, and change the IP address on each node.
5. If the IP address of a remote console unit was changed along with the public/management LAN change, correct the "/etc/inet/hosts" file on each node.
6. If the IP address used by the shutdown facility must be changed along with the public/management LAN change, correct the "/etc/opt/SMAW/SMAWsf/etc/rcsd.cfg" file on each node.
 If the IP address of a remote console unit was changed, correct the "/etc/opt/SMAW/SMAWsf/SA_rccu.cfg" file in each node.



See

For details, see 5.2.2 "Setting Up the Shutdown Facility."

7. In each node, change the IP address of the public LAN used by Web-Based Admin View.



See

For details, see "7.1 Network address," "7.3 Management server," and "7.5 Multi-network between server and client by classified use" in the "*PRIMECLUSTER Web-Based Admin View Operation Guide*."

8. If a takeover IP address must be changed, correct the IP address being used as the takeover IP address in the "/etc/inet/hosts" file of each node.
9. If you used the userApplication Configuration Wizard to create an Ipaddress or GIs resource, edit the "/opt/SMAW/SMAWRrms/bin/hvsnv.local" file on each cluster node as shown below to disable RMS automatic startup during system restart.

```
# vi /opt/SMAW/SMAWRrms/bin/hvsnv.local <Return>
```

```
export HV_RCSTART=0
```

10. Restart the system on all nodes.

```
# /usr/sbin/shutdown -y -g0 -i6
```
11. If you used the userApplication Configuration Wizard to set up an Ipaddress or GIs

resource, take the following steps to change the takeover IP address in the resource database.

- 1) Identify the takeover IP address resource to be changed in the resource database. Execute the “clgettree(1)” command on one of the cluster nodes. The takeover IP address resource has the resource class name for IP addresses.

Example) In the following example, the resources with resource IDs 56 and 57 are the takeover IP address resources.

```
# /etc/opt/FJSVcluster/bin/clgettree
Cluster 1 cluster
  Domain 2 RC2
    Shared 7 SHD_RC2
      SHD_Host 58 config_Ipaddress0_ip1 UNKNOWN
        IP_Address 56 hme0:1 UNKNOWN narcissus
        IP_Address 57 hme0:1 UNKNOWN sweetpea
    Node 3 narcissus ON
      Ethernet 21 hme0 UNKNOWN
        IP_Address 56 hme0:1 UNKNOWN
      Application 31 procl UNKNOWN
      DISK 19 c0t0d0 UNKNOWN
    Node 5 sweetpea ON
      Ethernet 22 hme0 UNKNOWN
        IP_Address 57 hme0:1 UNKNOWN
      Application 32 procl UNKNOWN
      DISK 20 c0t0d0 UNKNOWN
```

- 2) Identify the shared resources of the takeover IP address. To identify the shared resources, execute the “clgettree(1)” command on one cluster node. The shared resources of the takeover IP address are resources that have the SHD_Host resource class name.

Example) For the example shown in Step 1), the resource that has resource ID 58 is the shared resource of the takeover IP address.

- 3) Change the takeover IP address. To change the address, execute the “clsetrsc(1M)” command. The takeover IP address is defined in the attributes of the shared resource for the takeover IP address that was identified in Step 2. On each cluster node, execute the “clsetrsc(1M)” command with the following format.

```
# /etc/opt/FJSVcluster/sys/clsetrsc -A ip_addr=new-IP-address
resource-ID-of-shared-resource-having-IP-address
```

Example) To change the takeover IP address of a shared resource (resource with resource ID=58) to 10.10.10.10

```
# /etc/opt/FJSVcluster/sys/clsetrsc -A ip_addr=10.10.10.10 58
```

- 4) Execute the “clgetrsc(1)” command to check that the takeover IP address was changed.

Using the command format below, execute the “clgetrsc(1)” command on one of the cluster nodes and check that the takeover IP address was changed.

```
# /etc/opt/FJSVcluster/sys/clgetrsc -a ip_addr
```

resource-ID-of-shared-resource-having-IP-address

Example) If the takeover IP address of a shared resource (resource with resource ID=58) was changed to 10.10.10.10

```
# /etc/opt/FJSVcluster/sys/clgetrsc -a ip_addr 58
ip_addr 10.10.10.10
```

12. If you edited the /opt/SMAW/SMAWRrms/bin/hvenc.local file in Step 9, return the file to its previous setting.



Note

- An interface or IP address to which MAC address takeover has already been configured cannot be used in Web-Based Admin View.
- If a takeover IP address has been defined by GLS and if the takeover IP address is specified directly with an IP address value, not a host name, in the GLS environment settings and the Gls resource settings, first delete the Gls resource. Then change /etc/inet/hosts and the GLS environment settings, and register the Gls resource. For details, see 8.9.3 "Supplement on Cluster Application and Resource Deletion," 6.1.1 "GLS Setup," and 6.6.1.4 "Creating Gls Resources."

8.3 Changing a CIP Address

This section describes how to change the IP address if the IP address of interconnect is changed after installation of the PRIMECLUSTER system.

◆ **Operation Procedure:**

1. Start all nodes in the cluster system.
If the nodes are already operating, you do not need to restart them.
2. Stop CF in all nodes.
For instructions on stopping CF, see "5.4.1 Starting and Stopping CF" in "*PRIMECLUSTER Cluster Foundation Configuration and Administration*."
3. View `/etc/cip.cf` and check the CIP name in all nodes.
For details on `/etc/cip.cf`, see "2.2 CIP Configuration File" in "*PRIMECLUSTER Cluster Foundation Configuration and Administration*."
4. Change the IP address of the CIP name that is defined in `/etc/hosts`."
5. Start CF in all nodes.
For instructions on starting CF, see "5.4.1 Starting and Stopping CF" in "*PRIMECLUSTER Cluster Foundation Configuration and Administration*."
6. Check that the IP address was changed by executing the `ciptool(1M)` command. For details on the `ciptool(1M)` command, see the manual page of `ciptool(1M)`.

8.4 Changing Settings for the Shared Device Connection Confirmation Feature

For instructions on changing the operation environment for shared disk connection confirmation, see 5.4 "Setting Up Shared Disk Connection Confirmation."

8.5 Changing the Operation Environment for Patrol Diagnosis

To change the operation environment for patrol diagnosis, execute the `clspconfig(1M)` command. For details on the `clspconfig(1M)` command, see the manual page for `clspconfig(1M)`.

8.6 Changing a Node Name



Note

Changing a node name is a very risky operation. You should change a node name only if it is required.

To change a node name, execute the “sys-unconfig(1M)” command. The “sys-unconfig(1M)” command configures the system again. In addition to the node name, the name service, the time zone, the IP address, the IP subnet mask, the root password and other settings are first all deleted, and then are set up again when the node is restarted.



See

For details on the “sys-unconfig(1M)” command, see the manual page for “sys-unconfig(1M).“

◆ Operation Procedure:

1. Stop CF.
From the CF window of Cluster Admin, stop CF.
2. Change the RMS settings so that RMS is not started automatically when the node is started.
Define HV_RCSTART=0 to the “hvenv.local(4)” file of all nodes for which the node name is to be changed.
3. Change the node name.
 - 1) Execute the “sys-unconfig(1M)” command.
sys-unconfig
 - 2) When the “sys-unconfig(1M)” command is executed, the system is shut down, and the ok prompt is displayed. At the prompt, execute boot, and enter the node name and other information items according to the displayed screen.
ok **boot**



Note

Do not use the “sys-unconfig(1M)” command to change any information other than the node name.

4. Recover the “hosts(4)” file.
Refer to the /etc/inet/hosts.saved file, which contains the previous system configuration that was backed up by the “sys-unconfig(1M)” command, and recover the “hosts(4)” file.
5. Restart the system.
shutdown -y -i6 -g0
6. If you modified the “HV_RESTART” environment variable of the “hvenv.local(4)” file in Step 2, return the “HV_RCSTART” definition to its previous value.

8.7 Changing the Operation Attributes of a userApplication

PRIMECLUSTER allows operation attributes to be set by CUI operation, according to the needs of the user. Change the operation attributes to match the desired operation.

- Operation attribute types
A list of the userApplication operation attributes is shown. For details, see 8.7.1 "Operation Attribute Types."
- Change methods
The methods for changing the RMS environment variables are described. For details, see 8.7.2 "Changing Environment Variables."



Note

Be sure to stop RMS before you change the operation attributes of userApplication. For instructions on stopping RMS, see 7.2.1.2 "Stopping RMS."

8.7.1 Operation Attribute Types

The table below shows the operation attributes and environment variables of userApplication objects and the values that can be set for those attributes and variables.

Operation attributes of userApplication objects

Operation	userApplication attribute/environment variable	Setting value (Bold: Default)	Description
Failover operation	AutoSwitchOver	No	Automatic failover is disabled.
		HostFailure	Failover occurs if a node fails.
		ResourceFailure	Failover occurs if a resource fails.
		Shutdown	Failover occurs if RMS stops.
Operation if resource inactivation fails	Halt	0	The node is not forcibly stopped.
		1	The node is forcibly stopped.
Operation for cluster application startup	OnlinePriority	0	The highest node of the PriorityList attribute becomes the active system.
		1	The node that was the active system last becomes the active system.
Operation of failover function for node startup	HV_RCSTART environment variable in hvenv.local file	0	The failover function is not started automatically.
		1	The failover function is started automatically.
Handling of failed nodes	PersistentFault	0	The failed node is not eliminated after the node is restarted.
		1	The failed node is eliminated even after the node is restarted.

Operation	userApplication attribute/environment variable	Setting value (Bold: Default)	Description
Hot-standby operation	StandbyTransitions	No	Hot-standby is not adopted.
		StartUp	Hot-standby is adopted when the failover function is started.
		SwitchRequest	Hot-standby is adopted after the switchover operation.
		ClearFaultRequest	Hot-standby is adopted after the fault clear operation.

8.7.2 Changing Environment Variables

This section explains how to change RMS environment variables.

The environment variables are configured in the following RMS environment files (`/opt/SMAW/SMAWRrms/bin`). You can change the environment variables by editing the files directly and setting or changing the values.

File Names	Contents
hvenv	Environment variable file that is defined in the entire cluster
hvenv.local	Environment variable file that is defined only in that node



See

- For details on the RMS environment variable files (hvenv and hvenv.local), see "2.8 Environment Variables" in "*PRIMECLUSTER RMS Configuration and Administration*."
- For details on the RMS environment variables, see "8 Appendix – Environment Variables" in "*PRIMECLUSTER RMS Configuration and Administration*."

8.8 Changing PRIMECLUSTER Operation Attributes

The PRIMECLUSTER operation attributes are set with RMS environment variables. To change the PRIMECLUSTER operation attributes, change the environment variables in the `hvenv.local` file, and restart RMS.

Note that the change procedure differs depending on whether the environment variable is global or local.



[See](#)

- For information on the RMS environment variables and how to change the variable settings, see "2.8 Environment Variables" in "*PRIMECLUSTER RMS Configuration and Administration*."
- For details on the RMS environment variables, see "8 Appendix – Environment Variables" in "*PRIMECLUSTER RMS Configuration and Administration*."

8.9 Deleting a Cluster Application

This section explains how to delete a cluster application and its resources.



Note

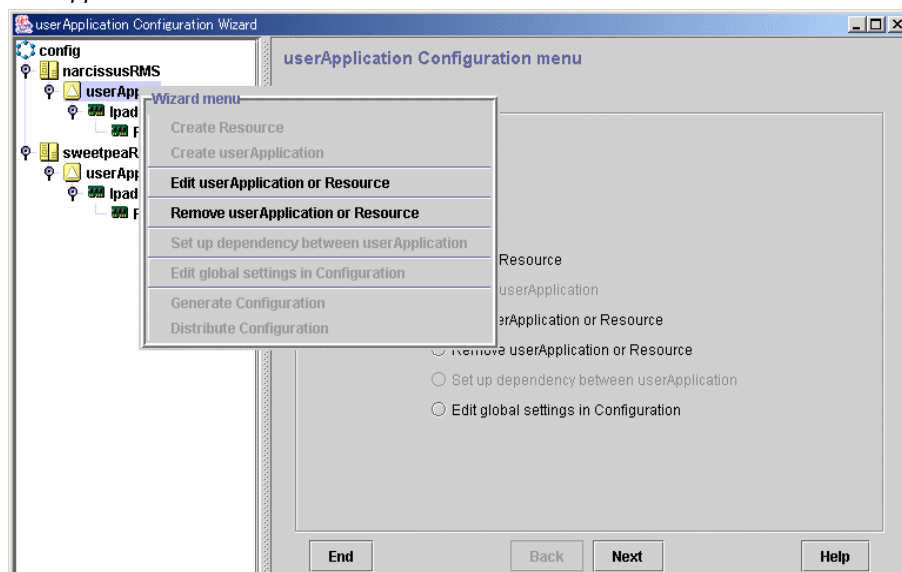
Be sure to stop RMS before deleting a cluster application and its resources. If the "userApplication Configuration Wizard" screen is started while RMS is operating, message 0833 will be displayed. If this happens, stop RMS, and then start the "userApplication Configuration Wizard" screen again. For instructions on stopping RMS, see 7.2.1.2 "Stopping RMS."

8.9.1 Deleting a userApplication

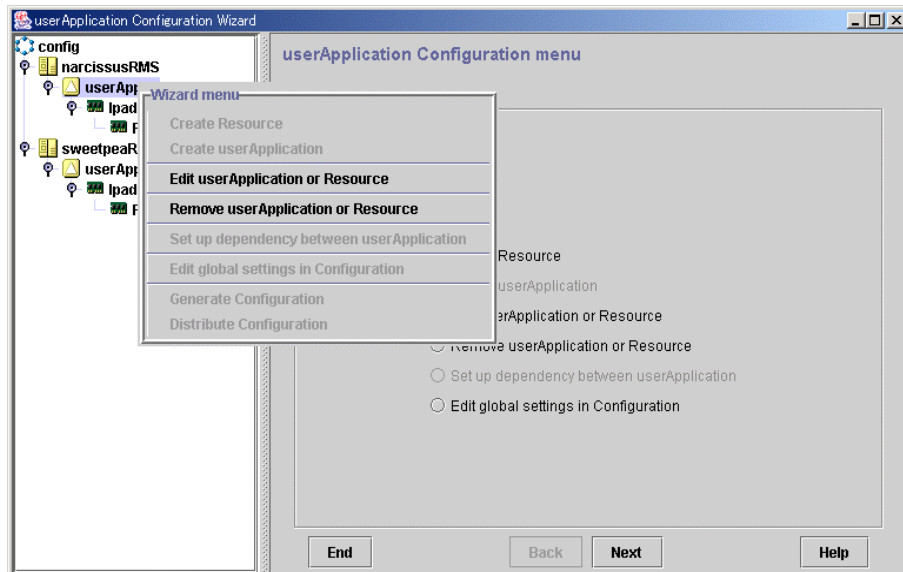
This section explains how to delete the userApplication.

◆ Operation Procedure:

1. At the top menu of the *userApplication Configuration Wizard*, select *userApplication* to be deleted from the tree shown on the left of the screen.
2. Click the right mouse button to display the pop-up menu, and select *Remove userApplication or Resource*.



3. At the displayed dialog box, select *userApplication*. Only the *userApplication* will be deleted.



userApplication

Select this button to delete the specified userApplication.



Note

The resources that are specified to userApplication will not be deleted. The hierarchical relationships of the resources will be initialized. However, levels that were set with "Resource association" will not be initialized.

All

Select this button to delete the specified userApplication and all related resources. If resources are to be deleted, delete as described in the 8.9.3 "Supplement on Cluster Application and Resource Deletion."

Cancel

Select this button to cancel the deletion.

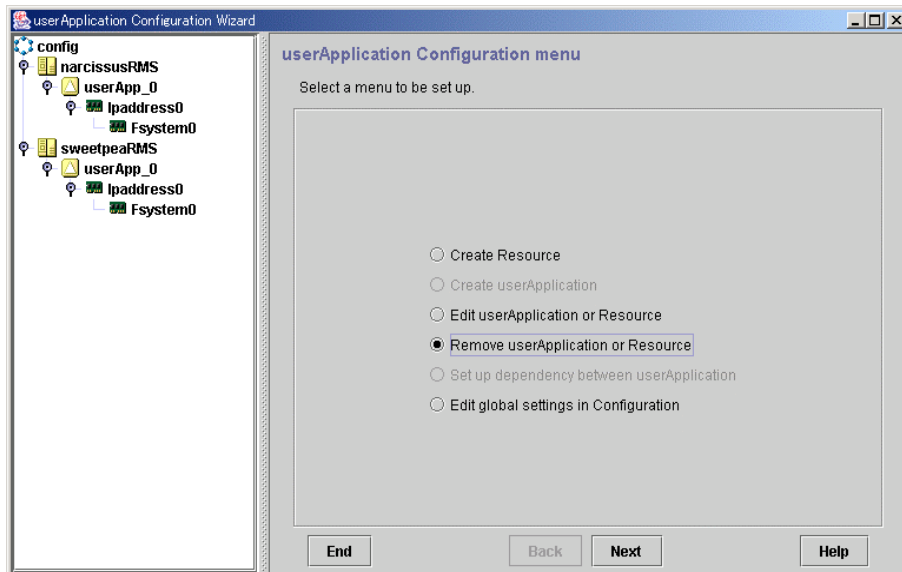
You can confirm that userApplication has been deleted by observing that the userApplication no longer appears in the tree on the "userApplication Configuration Wizard" screen.

8.9.2 Deleting a Resource

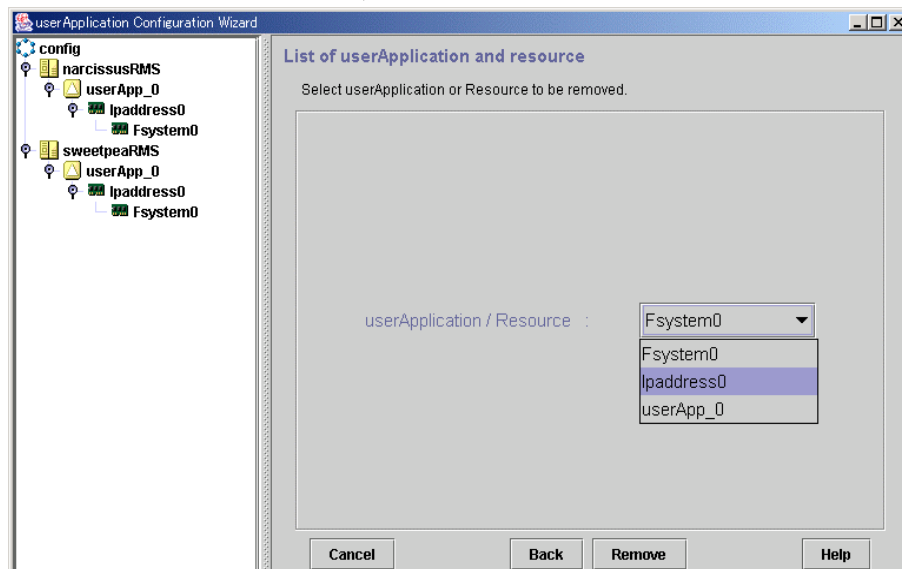
This section explains how to delete a resource.

◆ **Operation Procedure:**

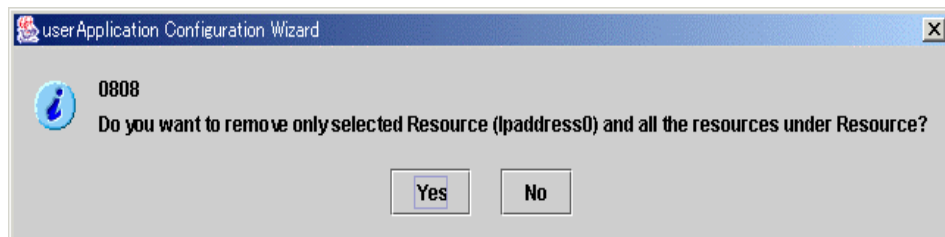
1. At the top menu of the *userApplication Configuration Wizard*, select *Remove userApplication or Resource*.



2. Select the resource to be deleted, and then select *Remove*.



3. Respond to the displayed dialog box.



Yes

Select this button to delete the specified resource and all subordinate resources.

If deleting the selected resources deletes all the resources that construct userApplication, message 0835 will confirm with you whether you want to delete all the resources. To continue the deletion, select "Yes".

No

Select this button to cancel the deletion.

You can confirm the deletion by checking that the resource disappears in the tree on the "userApplication Configuration Wizard" screen.



Note

When deleting resources, refer to the 8.9.3 "Supplement on Cluster Application and Resource Deletion."

◆ **Deleting the hardware resource that was registered with the automatic configuration facility**

When deleting a hardware resource that was registered with the automatic configuration facility, use the following command:

Resource	Command
Shared disk device	cldeldevice(1M) command
Network interface card	cldelrsc(1M) command
Line switching unit	cldelwursc(1M) command

See the relevant manual pages for details on each command.

Delete the hardware resource that was registered with the automatic configuration facility using the following procedure.

◆ **Procedure**

1. Stop RMS.
If RMS is activated, stop RMS as explained in 7.2.1.2 "Stopping RMS_."
2. Delete the hardware resource.
Delete the hardware resources that were registered with the automatic configuration facility by using the appropriate commands.



Note

- If you have deleted an available network interface card by mistake, reregister the resources for the accidentally deleted network interface card by executing the "clautoconfig(1M)" command.
- If you have deleted other than the correct network takeover resource, reregister the deleted network takeover resource. See G.2 "Associating Resources to a Cluster Service Instances_."

8.9.3 Supplement on Cluster Application and Resource Deletion

This section explains the operations to be done after 8.9.1 "Deleting userApplication" and 8.9.2 "Deleting Resources."

8.9.3.1 Supplement on Cmdline resource deletion

Delete each script used in the Cmdline resources.



Note

Do not execute deletion if a Cmdline resource must remain for safety.

Each script is stored in the following directories:

- /etc/opt/FJSVwwucw/scripts/start
- /etc/opt/FJSVwwucw/scripts/stop
- /etc/opt/FJSVwwucw/scripts/check

Execute the deletion command as follows:

```
# cd /etc/opt/FJSVwwucw/scripts/start
# rm <script name to be deleted>
# cd /etc/opt/FJSVwwucw/scripts/stop
# rm <script name to be deleted>
# cd /etc/opt/FJSVwwucw/scripts/check
# rm <script name to be deleted>
```

8.9.3.2 Supplement on Fsystem resource deletion

Restore the environment files related to the mount point to the original state.



Note

Do not execute restoration if an Fsystem resource remains for safety.

■ Deleting mount point entries that were added at prerequisites

Delete the relevant entry from the following environment files that were edited as part of the 6.6.1.2.1 "Prerequisites."

- /etc/vfstab
- /etc/dfs/dfstab

If a dummy entry is deleted from /etc/dfs/dfstab, delete the actual directory.

■ When an NFS Lock Failover was used

If the NFS Lock Failover functions are no longer used due to deletion of the Fsystem resources, take the following steps:

◆ Procedure:

1. Change the settings for shared information with the configuration.
Change the value of NFSLockFailover to "no."



See

See 6.6.4 "Editing global settings in Configuration."

8.9.3.3 Supplement on Gds resource deletion

Delete the disk class if it is no longer necessary.

See the "PRIMECLUSTER Global Disk Services Guide."

8.9.3.4 Supplement related to GIs resource deletion

Delete the takeover network definition if it is no longer necessary.

See the *"PRIMECLUSTER Global Link Services Configuration and Administration Guide: Redundant Line Control Function."*

8.9.3.5 Supplement on takeover network resource deletion

Restore the environment files related to the takeover network to the original state.

■ When MAC address takeover was used

Delete the entries that were added to the following environment files during the prerequisite procedure of the MAC address takeover.

- /etc/opt/FSUNnet/mactool/macaddr.conf
- /usr/opt/reliant/etc/hvipalias
- /etc/inet/hosts

For details on the added entries, see 6.6.1.5.1 "Prerequisites."

■ When node name takeover was used

Change the node name in the cluster system used for node name takeover. To bring the system state back to the state before the change, take the following steps on all the nodes where node name takeover resources were created.

◆ Operation

1. Execute the command on all the nodes, as follows:

```
# setuname -n fuji2
```

fuji2 is used as the node name in this example.

2. Reboot the system.

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

8.9.3.6 Supplement on procedure resource deletion

Delete the procedure resource from the cluster resource management facility when it is no longer necessary.

See the relevant manual pages describing `cldelprocrsc(1M)`.

8.9.3.7 Supplement on process monitoring resource deletion

Delete scripts that were created automatically if the stop command of the process monitoring resource was used.



Note

Do not delete a process monitoring resource that remains for safety.

Each script is stored in the `/etc/opt/FJSVwvucw/scripts/process_stop` directory.

Execute the deletion command as shown below.

```
# cd /etc/opt/FJSVwvucw/scripts/process_stop
```

```
# rm ./*
```

8.9.3.8 Supplement on line switching unit resource deletion

Delete the line switching unit resource from the cluster resource management facility if it is not necessary.

See the manual pages of the “cldelwursc(1M)” command.

8.9.3.9 ISV resource deletion procedure (supplement)

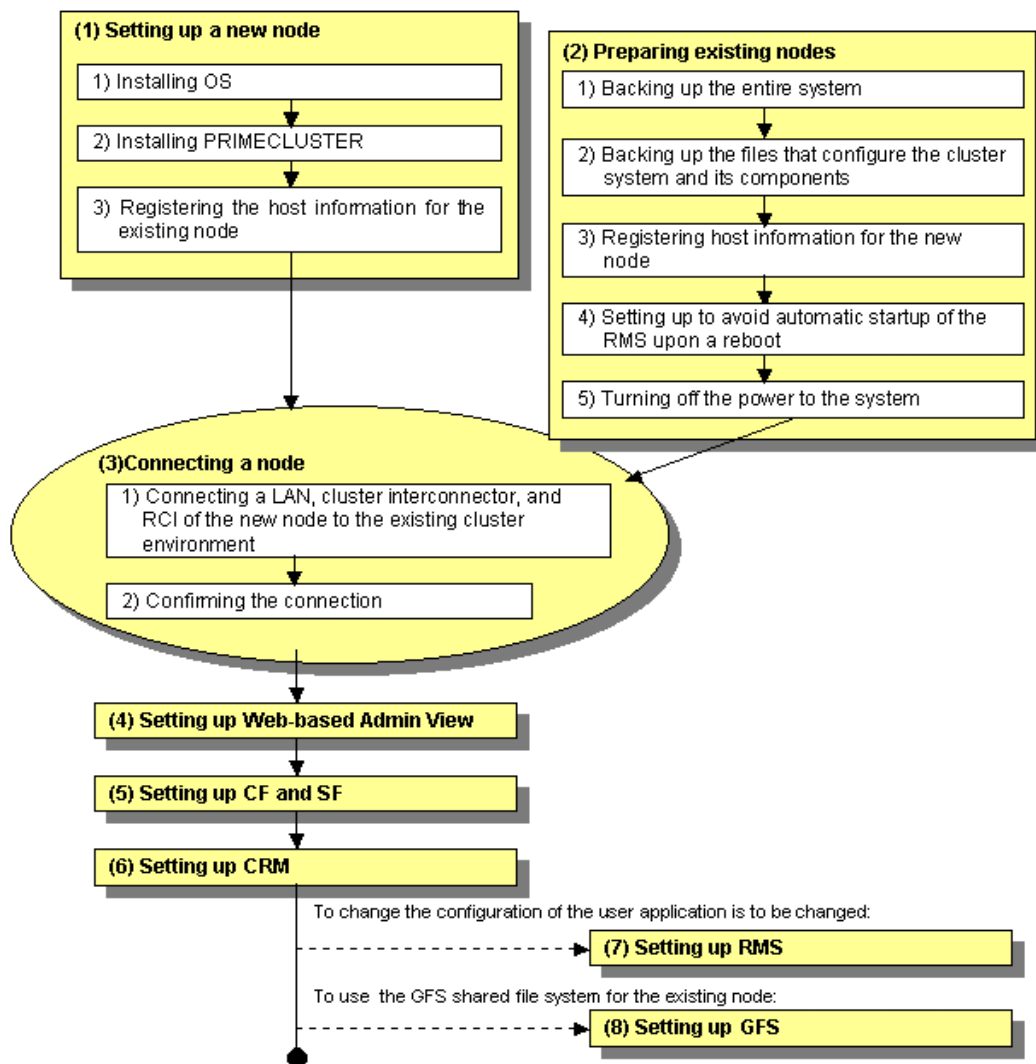
For information on the deletion procedure, see the manuals provided with each product.

Chapter 9 Expanding the Operation Configuration

This chapter explains how to add to the configuration of a PRIMECLUSTER system.

9.1 Adding a Node

Node expansion means adding on an extra node to an operating cluster system. The purpose of node expansion is to provide high availability and extend available business operations. The node expansion procedure is explained below:



Note

- Use the same OS version, collective updates, and patches as that of the existing cluster nodes.
- Stop operation when nodes are to be added.
- Two or more nodes cannot be added at the same time. When multiple nodes are to be added, add them one by one.
- The nodes to be added must be of the same model as the existing cluster nodes.

In the following explanation, node1 and node2 are used as the node names of the existing cluster nodes while node3 is used as the node name of the new node.

9.1.1 Setting Up a New Node

Take the following steps to set up the new node.

The new node should be prepared such that the operating system, PTFs, FibreChannel, and packages such as the multipath software have already been installed.

◆ Procedure

1. Install PRIMECLUSTER on the new node.
This must be done in a single user mode.
For details, see the “*PRIMECLUSTER Installation Guide*.”
2. Configure NTP.
Configure NTP for the new node according to the existing nodes and the network environment.
3. Define the following information in the “/etc/inet/hosts” file of the new node.
 - IP address of the existing cluster nodes and the host name which is used by that IP address
 - IP address of the remote console that is connected to the existing cluster nodes and the host name that is used by that IP address
 - The IP address of the CIP interface of the existing cluster nodes and the CIP name which uses that IP address
4. Turn off the power to the new node.

9.1.2 Preparing the Existing Nodes

Take the following steps to prepare the existing nodes.

◆ Procedure

1. Preparing for unexpected failures, you need to back up the entire system of all existing cluster nodes, the PRIMECLUSTER system and the configuration files of each component.

1) Back up the entire system.

- 1- Execute the following command on any one of the existing cluster nodes to stop RMS.

Stop RMS by executing the following command on any one of the existing cluster nodes.

```
node1# hvshut -a
```

- 2- Reboot all the existing cluster nodes from a single user mode.

```
node1# /usr/sbin/shutdown -g0 -i0 -y
```

```
....
```

```
ok boot -s
```

```
....
```

```
Type control-d to proceed with normal startup,  
(or give root password for system maintenance):
```

```
....
```

- 3- Mount the file system on all the existing cluster nodes.

```
node1# mountall -l
/dev/rdisk/c0t0d0s1: is clean.
node1#
```

- 4- Back up the entire system or property in the shared disk by executing the “ufsdump(1M)” or “dd(1M)” command.
- 2) Back up the PRIMECLUSTER system and the configuration files of each component.
 - 5- Back up the configuration files of the PRIMECLUSTER system on all existing cluster nodes. See Chapter 10 “Backing Up and Restoring a PRIMECLUSTER System”.
 - 6- Back up the configuration files that are used for GLS on all existing cluster nodes.

Back up the configuration files for redundant line control by using the following command. For details on the “hanetbackup” command, see the “PRIMECLUSTER Global Link Services Configuration and Administration Guide.”

```
node1# /opt/FJSVhanet/usr/sbin/hanetbackup -d
/var/tmp/backup
```

Back up the configuration files for the GLS multipath function:

```
node1# cd /etc/opt/FJSVmpnet
node1# tar cvf - conf | compress >
/var/tmp/backup/mpnetfile.tar.Z
```

2. Define the following information in the /etc/inet/hosts file of all the existing cluster nodes.
 - The IP address of the node to be added and the name of the host that is used by that IP address
 - The IP address of the remote console that is connected to the node to be added and the host name that is used by that IP address
3. Edit the "/opt/SMAW/SMAWRrms/bin/hvenv.local" file as shown below so that RMS does not start automatically on any of the existing cluster nodes, even when a cluster node is rebooted.

```
node1# vi /opt/SMAW/SMAWRrms/bin/hvenv.local
```

```
export HV_RCSTART=0
```

4. To add a new node, all the existing cluster nodes must be turned off.

9.1.3 Connecting a Node

Connect the new node the existing cluster nodes.

◆ Procedure

1. Connect the LAN, Cluster Interconnect, and the RCI of the new node to the existing cluster environment.
At this time, configure the RCI address for the new node.
(This operation is done by your Fujitsu CE.)
2. After setting the RCI address, boot up the existing cluster nodes and check that no error message is output to the console or syslog.
3. Boot the new node and confirm that the new node and its remote console are correctly configured in the network by executing the “ping(1M)” command.

4. Confirm that the RMS is stopped on any one of the existing cluster nodes, and then stop the SF by executing the following command on each existing cluster node.

Confirm that RMS is stopped.

```
node1# hvdisp -a
hvdisp: RMS is not running
```

Stop SF. Execute the following command on all the existing cluster nodes.

```
node1# sdtool -e
node1# sdtool -s
(SMAWsf, 30, 13) : The RCSD is not running
```

9.1.4 Setting Up Web-Based Admin View

This section explains how to set up Web-Based Admin View.

The node to be configured is determined by the node on which the management server is to be set.

Determine the node referring to the following instructions;

- When the existing management server is used
The management server must also be defined on the new node.
Set up Web-Based Admin View on the new node.
- When the added node is to be used as the management server
The definition of the new management server must be set up for all nodes.
Set up Web-Based Admin View on all nodes.

◆ Procedure

1. Set up Web-Based Admin View on the node.
See 4.1.3.1 "Initial setup of the operation management server."
2. Confirm that Web-Based Admin View is running correctly.
For confirmation, use any one of the cluster nodes as explained in 4.1.3.2 "Confirming Web-Based Admin View Startup"

9.1.5 Setting Up CF and SF

Make the CF and SF configuration by using Cluster Admin. This section explains how to configure CF and SF. See "2.1.4 An example of creating a cluster" in the "*PRIMECLUSTER Cluster Foundation Configuration and Administration*."

◆ Procedure

1. Start the Web browser on the management client and connect to the primary management server to display Web-Based Admin View.
2. Log on to Web-Based Admin View and then select the "Global Cluster Services" menu (see Figure 3).
3. Select a node name to be added on the node selection screen (see Figure 6).
4. Click the "Load driver" button in the left-hand side panel on the screen, and then select the "Configure" button to start the CF wizard (see Figures 7 and 8).
5. Select an existing cluster system name from the "Create/Join Cluster" screen and then click the "Add local node to an existing CF Cluster" option button. Then, choose the "Next" button (see Figure 10).
6. When the Cluster Interconnect confirmation screen appears, confirm that the combination of network interface cards is correct on all nodes. Then, click the "Next" button (see

Figure 14).

7. Check the "For RMS" checkbox for the CIP subnet settings (note that the RMS cannot use the CIP if this is not set.)
8. When the *Configuration complete "Complete Configuration"* dialog box appears, close that screen and click the OK "Exit" button. This completes the CF settings.
9. Configure SF.
For details, see "8. Shutdown Facility (SF)" in the *"PRIMECLUSTER Cluster Foundation Configuration and Administration."*
10. Confirm that the CF and SF have been configured correctly by executing the following command on the GUI screen or on any one of cluster nodes.

```
node1# cftool -n
Node   Number State   Os      Cpu
node1  1      UP      Solaris Sparc
node2  2      UP      Solaris Sparc
node3  3      UP      Solaris Sparc
```

```
node1# sdtool -s
Cluster Host Agent          SA State   Shut State Test State Init State
-----
node1      SA_pprcip.so Idle       Unknown   TestWorked InitWorked
node1      SA_rccu.so  Idle       Unknown   TestWorked InitWorked
node1      SA_pprcir.so Idle       Unknown   TestWorked InitWorked
node2      SA_pprcip.so Idle       Unknown   TestWorked InitWorked
node2      SA_rccu.so  Idle       Unknown   TestWorked InitWorked
node2      SA_pprcir.so Idle       Unknown   TestWorked InitWorked
node3      SA_pprcip.so Idle       Unknown   TestWorked InitWorked
node3      SA_rccu.so  Idle       Unknown   TestWorked InitWorked
node3      SA_pprcir.so Idle       Unknown   TestWorked InitWorked
```

9.1.6 Setting Up CRM (Resource Database)

This section explains how to set up the Customer Resource Management (CRM) resource database.

◆ Procedure

1. Reconfigure the resource database on the existing nodes.

Confirm the following:

- All of the existing nodes must have been started.
- CIP of the new node must be in `/etc/cip.cf` of the existing nodes.
The resource database uses `/etc/cip.cf` to associate CF node names with CIP names.

Reconfigure the resource database.

The procedure is shown below:

- 1) Log into any one of existing nodes using a system administrator access privilege.
- 2) Specify the `-a` and the `-g` options in the `clsetup(1M)` command.

```
# /etc/opt/FJSVcluster/bin/clsetup -a node -g file
```

As a result of this operation, a new node will be added to the resource database of the existing nodes.

The configuration information on the resource database, created after the execution of the `clsetup(1M)` command, is used when the resource database of the new node is configured. Therefore, do not specify a directory (example: `/tmp`) that will

be automatically deleted when rebooting the node with the “-g” option.

Specify the CF node name in *node*, and a full path name of the file name of the resource database configuration information. *tar.Z* will be appended to the resource database configuration information.

Do not specify the “-g” option to suffix *tar.Z*.

For example, to add a new node which has a CF node name of *fuji4*, and a configuration information file name of */mydir/rdb*, the command to be executed will be as shown below:

```
# /etc/opt/FJSVcluster/bin/clsetup -a fuji4 -g /mydir/rdb
```

The configuration information file of the resource database will be created as */mydir/rdb.tar.Z*.

- 3) Confirm that the new node has been added to the resource database.

Execute the “*clgettree(1)*” command, and then confirm that the new node is displayed on the output result. At this time, the state of the new node is displayed as UNKNOWN.

2. Set up the resource database of the new node.

Confirm the following:

- The content of */etc/cip.cf* of the new node must be the same as that of the existing nodes.

Confirm that the CIP of the new node is in */etc/cip.cf* of the new node and that the content of */etc/cip.cf* is the same as that of the existing nodes.

- The new node is connected to all of the existing nodes by CIP

Execute the “*ping(1M)*” command.

If two or more CIPs are configured in the new nodes, use the first CIP for the resource database. Then, connection will be enabled. An example using “*fuji4RMS*” as the new node is shown below:

```
# ping fuji4RMS
```

After confirming the above, set up the resource database of the new node.

The procedure is as follows:

- 1) Log into the new node using a system administrator access privilege.
- 2) Copy the “resource database configuration information” file created in Step 2) in “Recreate the settings for the resource database of the existing nodes” to the new node.
- 3) Specify the *-s* option in the *clsetup(1M)* command, and execute it.

```
# /etc/opt/FJSVcluster/bin/clsetup -s file
```

Specify *file* with a full path name of the resource database configuration file.

When the resource database configuration information file “*rdb.tar.Z*” is copied to */mydir*, the command to be executed will be as shown below:

```
# /etc/opt/FJSVcluster/bin/clsetup -s /mydir/rdb.tar.Z
```

- 4) Confirm that the resource database of the new node is configured.

Execute the *clgettree(1)* command for the new node and confirm the following:

- The new node is displayed.
- The state of the new node is displayed as ON.
- The output result is the same as that of the existing nodes.

3. Register the hardware, which is connected to the new node, to the resource database.

Log into any one of nodes using a system administrator access privilege, and execute the command shown below:

```
# /etc/opt/FJSVcluster/bin/clautoconfig -r
```

◆ **Setting up synchronization with the resource database**

If the individual nodes are restarted at different times after node expansion, the tuning parameter must be set up to be synchronized with the resource database. For details, see “4.4.1 Start up synchronization and the new node” in the “*PRIMECLUSTER Cluster Foundation Configuration and Administration Guide.*”

9.1.7 Setting Up RMS

This section explains how to register a new node (SysNode) in a userApplication that has been running on an existing node.

◆ **Procedure**

1. Configuration for each resource

Take the following steps depending upon the resources in the existing userApplication:

— Cmdline

Create the Start, Stop, and Check scripts in the new node or copy them from the existing node. If “*Path enter*” is selected from “*Creation method*” when creating the existing Cmdline resource, allocate the scripts to that path. If “*New*” is selected, the scripts under `/opt/FJSVwvucw/scripts/start`, `/opt/FJSVwvucw/scripts/stop`, and `/opt/FJSVwvucw/scripts/check` must be allocated to the same path of the new node. You also need to add the access privilege by executing the “`chmod(1)`” command.

— Fsystem

If the file system is UFS, add the mount point entry to `/etc/vfstab` on the new node. If the file system is GFS, take the following steps and then create a GFS local file system on the GDS volume of the new node. Confirm that a GDS volume is available, and that the volume is ACTIVE. If the volume is STOP, start the volume. For information on how to start a volume, see “4.2.3 Operation” in the “*PRIMECLUSTER Global Disk Services Configuration and Administration Guide.*”

1- Acquire hostid for the new node.

```
node3 # hostid
80b1a621
```

2- Add the information on the new node to the GFS local file system by executing the following command on any one of the existing cluster nodes.

```
node1 # sfxnode -a -n node3 -i 80b1a621
/dev/sfdsk/class/rdsk/volume
```

7- Register the GFS local file system on the new node by executing the following command:

```
node3 # sfxadm -A /dev/sfdsk/class/rdsk/volume
```

8- Using the vi text editor, add the entry of the GFS local file system to `/etc/vfstab` in the new node.

Each line must begin with #RMS#.”

```
node3# vi /etc/vfstab
#RMS#/dev/sfdsk/class/dsk/volume
/dev/sfdsk/class/rdsk/volume /disk1 sfxfs - no -
```

9- Create a mount point in the new node.

```
node3 # mkdir /disk1
```

— Gds

Take the following steps to expand the cluster scope:

- 1- Reboot all the cluster nodes.

```
# shutdown -g0 -i6 -y
```

- 2- Expand the cluster scope.

See "5.4 Changes" in the *"PRIMECLUSTER Global Disk Services Configuration and Administration Guide."*

- 3- Execute the following command on any one of the cluster nodes:

```
# /usr/opt/reliant/bin/hvgdsetup -a class
hvgdsetup with -a option performs the following processes.
  1) Automatically deactivates the GDS disk class in the
resource database when the node boots.
  2) Stops the disk volumes of the specified disk class
immediately.
      These processes are executed on those nodes to which disk
class has belonged.
Do you want to continue with these processes? [yes/no] yes
hvgdsetup completed.
```

The following message might appear after executing the "hvgdsetup" command. This does not disrupt ongoing operation.

```
FJSVcluster: error: clrmd: 7516: An error occurred in the
resource deactivation processing. (resource:resource
rid:rid detail:detail)
WARNING !!
Failed to control 'dc_class' in the following node(s).
node(s) node_name:
Check the state of the nodes. If any nodes have failed, you
may ignore this message.
```

— GlS

Take the following steps for GLS:

- 1- Set up the virtual interface for the takeover IP address on the new node and register it as a cluster resource. For details, see the *"PRIMECLUSTER Global Link Services Configuration and Administration Guide: Redundant Line Control Function."*

Restart redundant line control by executing the following command:

```
node3# /opt/FJSVhanet/usr/sbin/resethanet -s
```

— Takeover network

Nothing need be done at this time. In Procedure 3, however, it is necessary to recreate the resources.

— Procedure

Create a state transition procedure on the new node and register the procedure resource with the cluster resource manager. For more details, see F.1 "Registering a Procedure Resource".

- Process monitoring
Add the startup command to the new node. Also, you need to add the access privilege by using the “chmod(1)” command. Then, recreate the resources in Procedure 3.

2. Deleting userApplication

Delete the existing userApplication by using the userApplication Configuration Wizard. At this time, select “Delete only userApplication.”

For more details, see 8.1.1 “Changing the Cluster Application Configuration.”

3. Recreating the takeover network and process monitoring resources

If the takeover network resource and the process monitoring resource are contained, first delete and then recreate those resources.

See 8.9.2 “Deleting the resources,” 6.6.1.5 “Creating the takeover network resource,” and 6.6.1.7 “Creating the process monitoring resource.”

4. Recreating userApplication

Recreate the userApplication that was deleted in Procedure 1, using the same procedure as that used to create it. Note that the new node must be registered when SysNode is to be selected. For details, see 6.6.2 “Building Cluster Applications.”

5. Copy /opt/SMAW/SMAWRrms/bin/hv env.local of the existing node to /opt/SMAW/SMAWRrms/bin/hv env.local of the new node.

6. Edit /opt/SMAW/SMAWRrms/bin/hv env.local in each node with the “vi” editor, and delete the following setting:

```
export HV_RCSTART=0
```

9.1.8 GFS Shared Settings

If the GFS shared file system is used in an existing node, set up the GFS shared file system on the new node by using the following procedure:

◆ Procedure

1. Execute `sfcumntgl` for the entire GFS shared file system on any one of cluster nodes, and then unmount the file system.
2. Execute `sfcfrmstop`, and then stop the GFS daemon on all cluster nodes.
3. Execute `sfcsetup` on the new node, and then register the node information in the management partition.
4. Execute `sfcfrmstart` and then start up the GFS daemon on all cluster nodes.
5. Execute `sfcnode` on any one of cluster nodes, and then add the node configuration information of the new node.
6. Create a mount point and set up `/etc/vfstab` on the new node.
7. Execute `sfcmntgl` on any one of cluster nodes and then mount the GFS shared file system.



See

For information on how to use each command, see the “PRIMECLUSTER Global File Services Configuration and Administration Guide.”

9.2 Recovering the Original Cluster Configuration at Node Expansion

When the original cluster configuration must be restored due to a fault or interruption during node expansion, take the following steps for recovery:

◆ Procedure

1. Cancel the configuration changes in GFS.

If a new node was added to the GFS configuration at node expansion, it is necessary to cancel the GFS configuration in multi-user mode before deleting the new node.

- When the GFS local system is used:

Execute `sfxnode`, and then delete the node configuration information on the node to be deleted.

- When the GFS shared file system is used:

Execute `sfcnnode` on any one of cluster nodes and delete the node configuration information. Then, execute `sfcfrmstop` and stop GFS on all the nodes. In this state, execute `sfcsetup` on the node to be deleted, and then delete the node information from the management partition.



See

For information on how to use each command, see the “*PRIMECLUSTER Global File Servers Configuration and Administration Guide*.”

2. Change the class scope.

If a new node was added to the GDS configuration, it is necessary to change the class scope by executing the `sdxattr` command. For information on the change procedure, see the “*Global Disk Services Configuration and Administration Guide*.”

3. Recover the PRIMECLUSTER system configuration files in single user mode.

See Chapter 10 “Backing Up and Restoring a PRIMECLUSTER System.”

4. Recover the GLS configuration files.

Restore the environment definition files that are used by the GLS redundant line control by executing the following command.

```
node1# /opt/FJSVhanet/usr/sbin/hanetrestore -f
/var/tmp/backup/<save file name>
```

Use “hanetYYYYMMDD.bk” as the *save file name*.

For details on the `hanetrestore` command, see the “*PRIMECLUSTER Global Link Services Configuration and Administration Guide*.”

Restore the environment definition files used by the GLS multipath function by using the following procedure:

```
node1# cd /etc/opt/FJSVmpnet
node1# uncompress /var/tmp/backup/mpnetfile.tar.Z
node1# tar xvf /var/tmp/backup/mpnetfile.tar
```

5. Restore the original cluster configuration.

Restore the cluster interconnect, LAN cable, and RCI cable to the original cluster configuration. At this time, restore the original RCI settings. This should be done by your Fujitsu customer engineer (CE).

Part 5 Maintenance

This section explains how to maintain a PRIMECLUSTER system.

Chapter 10 Backing Up and Restoring a PRIMECLUSTER System

The PRIMECLUSTER system supports the collective backup and restoration of a variety of environmental files that constitute PRIMECLUSTER, for the purpose of recovering from problems caused by operating errors during upgrading of, or configuration changes to, the system.

The following properties of the PRIMECLUSTER system can be backed up and restored with this function.

- CF configuration
- SF (Shutdown Facility) configuration
- RMS configuration
- GUI (including Web-Based Admin View) configuration



Note

- The hardware configuration must not change between back up and the restoring .
- Among the RMS configuration files, special commands and utilities that can be invoked by the user from the configuration are backed up.
- GLS, GFS, and GDS are not supported at present. For details on how to back up and restore these, refer to the corresponding manual.
- For details on the backup and restoration of PRIMECLUSTER-related products, refer to the corresponding manual.

■ Prerequisites for backup and restoration

The following conditions must be satisfied to use the backup and restoration functions of PRIMECLUSTER:

- PRIMECLUSTER 4.1A10 or later.
- The version to be used for restoration must be of the same PRIMECLUSTER version as that which was used for backup, or later.
- When backup and restoration are to be implemented, use the commands provided by the PRIMECLUSTER version that is installed on the machine.
- Execute the backup procedure on all the nodes in the PRIMECLUSTER operation environment. It is preferable to execute this procedure simultaneously. You can back up in either multi-user or single user mode.



Note

If backup is not executed for all nodes simultaneously, the machines may contain backup data with a different configuration. If the configuration of the backup data

differs between machines, the consistency of the cluster configuration cannot be maintained at restoration.

- e. Execute the restoration procedure in single user mode.



Note

- If the OS is newly installed, and the PRIMECLUSTER environment is restored, the normal operations of a cluster system cannot be guaranteed.
- If restoration is not done on all nodes but only on some nodes, the consistency of the cluster configuration might not be maintained between nodes, and failures might occur.

- f. When restoration is to be performed, the hardware configuration must be the same as that used for backup.
- g. With the restoration function, Solaris OE standard system files cannot be restored. The backup function also cannot be used to back up all the system files in a PRIMECLUSTER system. You need to manually back up or restore the system files, if necessary. For details on the method of restoring system files that have been backed up with the backup function, refer to Procedure 3) in the explanation of the restoration procedure.



Information

You should back up a cluster configuration each time it is modified.

10.1 Backing Up the PRIMECLUSTER Operation Environment

Execute the following command to back up the PRIMECLUSTER operation environment:

```
/opt/SMAW/bin/cfbackup [ -f ] [ n ]
```



See

For details on the command parameters, refer to the description of the “cfbackup(1M)” command.



Example

Back up the PRIMECLUSTER environment.

```
# cfbackup
08/07/02 11:17:55 cfbackup 1 started
...
08/07/02 11:21:23 cfbackup 1 ended
#
```



Example

Confirm the backup files.

```
# ls -l /var/spool/pcl4.1/ccbr
-rw-rw-rw- 1 root other 2860 Aug 7 11:21 fuji2_ccbr1.tar.Z
```


10.2 Restoring the PRIMECLUSTER Operation Environment

Take the following steps to restore the PRIMECLUSTER operation environment::

◆ Procedure

1. Boot the machine to be restored in single-user mode.



Note

After booting the machine in single-user mode, mount the file system by executing the “mountall -l” command.

Example: Reboot in single-user mode.

```
# shutdown -g0 -i0 -y
...
ok boot -s
...
INIT: SINGLE USER MODE
```

Enter control-d to proceed with normal startup,
(or enter the root password for system maintenance):

```
...
# mountall -l
/dev/rdisk/c0t0d0s4: is clean.
/dev/rdisk/c0t0d0s3: is clean.
#
```

2. To restore the PRIMECLUSTER operation environment, execute the following command.
`/opt/SMAW/bin/cfrestore [-f] [-p] [-y] [-M] [n]`



See

For details on the command parameters, refer to the explanation of the `cfrestore(1M)` command.

Example: Restore the PRIMECLUSTER operation environment.

```
# cfrestore
08/07/02 11:17:55 cfbackup 1 started
...
08/07/02 11:21:23 cfbackup 1 ended
#
```

3. Restore a single configuration file.



Note

The restoration function does not restore backed-up files. The system files mentioned here in are provided by the operation system (environment). You need to restore according to the necessity of each system file.

Example: Pick up the “/etc/vfstab” file from the backup data “fuji2_ccbr1.tar.Z”.

- 1) Confirm the backup data “fuji2_ccbr1.tar.Z” and then check for the backed-up

```

system file.
# ls /var/spool/pcl4.1/ccbr/*.tar.Z
fuji2_ccbr1.tar.Z
# zcat /var/spool/pcl4.1/ccbr/fuji2_ccbr1.tar.Z | tar tvf - ./OS
drwxrwxrwx  0/1          0 Nov 20 13:58 2002 ./OS/
drwxrwxrwx  0/1          0 Nov 20 13:57 2002 ./OS/etc/
...
-rw-r--r--  0/1          909 Nov 20 13:57 2002 ./OS/etc/vfstab
...
#

```

- 2) Put the "/etc/vfstab" file in the "/tmp" directory.

```

# cd /tmp
# zcat /var/spool/pcl4.1/ccbr/fuji2_ccbr1.tar.Z | tar xvf - ./OS
x ./OS, 0 bytes, 0 tape blocks
x ./OS/etc, 0 bytes, 0 tape blocks
x ./OS/etc/hosts, 401 bytes, 1 tape blocks
...
x ./OS/etc/vfstab, 909 bytes, 2 tape blocks
...
#

```

- 3) Restore part or all of the file contents by executing the "cp(1)" or "vi(1)" command.



Note

If an invalid correction is made to the system file, login may be disabled and the system may fail to boot.

4. If the AutoStartUp function of the RMS has been validated, invalidate it.
For details, see the "*PRIMECLUSTER RMS Installation/Administration Guide.*"
5. Reboot the machine.
Example: The machine is rebooted.
shutdown -g0 -i6 -y
6. Activate the RMS configuration.
For details, see the "*PRIMECLUSTER RMS Installation/Administration Guide.*"
7. Enable the AutoStartup function if it is disabled.
For details, see the "*PRIMECLUSTER RMS Installation/Administration Guide.*"
8. Start up the RMS.
For details, see the "*PRIMECLUSTER RMS Installation/Administration Guide.*"

10.3 Environment Setup File

The two environment configuration files for backup and restoration are “ccbr.conf” and “ccbr.gen”. The storage destination of the data to be backed up or restored can be changed by editing these files using the text editor “vi(1)”.

Environmental variables and environment configuration files used for backup and restoration are shown below:

- /opt/SMAW/ccbr/ccbr.conf

This file defines variables for PRIMECLUSTER backup and restoration. The variables include the following:

CCBRHOME :

This variable indicates a directory. The backup data is stored into this directory.

The following is a default value:

```
/var/spool/pc14.1/ccbr
```

- /opt/SMAW/ccbr/ccbr.gen

This file defines the number of generations to be used for PRIMECLUSTER backup and restoration. The file name appends the number of the generations. This number uses the defined value and increases one by one every time the backup process is normally done.



Information

The number of generations can be also changed with the arguments of cfbackup (1M) / cfrestore(1M). For details, refer to the explanation of each command.



Example

The backup configuration is as follows:

<Setup contents>

- Host name : fuji2
- CCBRHOME variable : /var/spool/pc14.1/ccbr
- The value of the “ccbr.gen” file : 1

In the case of above, the following file will be created as the backup data:

```
/var/spool/pc14.1/ccbr/fuji2_ccbr1.tar.Z
```

◆ Configuration procedure example

Configure the backup data storage destination to “/var/spool/pc14.1/ccbr” and the number of generations to “1”.

1. Edit the “/opt/SMAW/ccbr/ccbr.conf” file using the “vi(1)” text editor, and then change the value of the CCBRHOME file to “/var/spool/pc14.1/ccbr”.
If the value has already been entered, go to Procedure 2.

Confirm the contents.

```
# cat /opt/SMAW/ccbr/ccbr.conf
...
CCBRHOME=/var/spool/pc14.1/ccbr
```

```
export CCBRHOME
```

```
...
```

```
#
```

2. Edit the `"/opt/SMAW/ccbr/ccbr.gen"` file using the "vi(1)" text editor, and then change the value to "1". If the value has already been configured, go to Procedure 3.

Confirm the contents.

```
# cat /opt/SMAW/ccbr/ccbr.gen
```

```
1
```

```
#
```

3. Back up the PRIMECLUSTER configuration.

```
# cfbbackup
```

```
08/07/02 11:17:55 cfbbackup 1 started
```

```
...
```

```
08/07/02 11:21:23 cfbbackup 1 ended
```

```
#
```

Confirm the contents of the backup file.

```
# ls /var/spool/pcl4.1/ccbr
```

```
fuji2_ccbr1
```



Example

The restoration configuration is as follows:

<Setup contents>

- Host name : fuji2
- CCBRHOME variable : /var/spool/pcl4.1/ccbr
- Value of the "ccbr.gen" file : 2

In the above case, the following file will be used as the data to be restored:

```
/var/spool/pcl4.1/ccbr/fuji2_ccbr1
```

◆ Configuration procedure example

Configure the destination of the restoration data to `"/var/spool/pcl4.1/ccbr"` and the number of generations to "1".

1. Edit the `"/opt/SMAW/ccbr/ccbr.conf"` file using the "vi(1)" text editor, and then make the value of the CCBRHOME variable `"/var/spool/pcl4.1/ccbr"`.

If the value has already been configured, proceed to Procedure 2.

Confirm the contents.

```
# cat /opt/SMAW/ccbr/ccbr.conf
```

```
...
```

```
CCBRHOME=/var/spool/pcl4.1/ccbr
```

```
export CCBRHOME
```

```
...
```

```
#
```

2. Edit the `"/opt/SMAW/ccbr/ccbr.gen"` file using the "vi(1)" text editor, and then change the value to "2" (specify a value that is 1 greater than the target number of generations).

If the value has already been configured, proceed to Procedure 3.

Confirm the contents.

```
# cat /opt/SMAW/ccbr/ccbr.gen
```

```
2
```

```
#  
3. Restore the PRIMECLUSTER environment.  
# cfrestore  
08/07/02 11:17:55 cfrestore 1 started  
...  
08/07/02 11:21:23 cfrestore 1 ended  
#
```

Part 6 PRIMECLUSTER Products

This section explains the PRIMECLUSTER products.

- PRIMECLUSTER Product List
- PRIMECLUSTER Wizard for NetWorker
- PRIMECLUSTER Wizard for Oracle
- Interstage Application Server Enterprise Edition
- Softek AdvancedCopy Manager
- Symfoware Server Hot-standby Option
- Symfoware (Standby)
- Systemwalker CentricMGR
- Systemwalker OperationMGR
- Systemwalker WebMGR

Chapter 11 PRIMECLUSTER Product List

The following lists the version levels of PRIMECLUSTER products and the range of support:

Table 11-1 PRIMECLUSTER product list

Product name	Operation mode	Standby operation					Scalable operation	Notes
	System Configuration	Standby		Mutual Standby	Cascade			
	IP address takeover	1:1	N:1	Yes	Yes			
	Node name takeover	Yes	No	No	No			
Interstage Application Server Enterprise Edition 5.0	×	○	×	○	×	×		
Symfoware Server5.0	○	○	×	×	×	×		
Symfoware Server Hot Standby Option 5.0	○	○	×	×	×	×		
Softek AdvancedCopy Manager 10.1	○	○	×	○	×	×		
Systemwalker CentricMGR EE/GEE 10.1	×	○	×	×	×	×		
Systemwalker OperationMGR EE/GEE 10.1	○	○	○	○	×	×		
Systemwalker WebMGR-M EE 10.1	×	○	×	×	×	×		
PRIMECLUSTER Wizard for Oracle 4.1	○	○	○	○	○	○	For scalable operation, the Oracle Real Application Clusters for PRIMECLUSTER required	
PRIMECLUSTER Wizard for NetWorker 4.1	○	○	○	○	○	×		
Oracle Real Application Clusters for PRIMECLUSTER 9.2.0	×	×	×	×	×	○	PRIMECLUSTER Wizard for Oracle required	

11.1 What Are the PRIMECLUSTER Operation Modes?

This section explains the cluster operation mode of PRIMECLUSTER, based on SynfinityCluster. Note that the “cluster service” of SynfinityCluster is relevant to the “cluster application” of PRIMECLUSTER.

Also, “network takeover” of SynfinityCluster relates to the “public LAN takeover” of PRIMECLUSTER.

For the terminologies, see Appendix E.1 “Terminology”.

◆ Cluster operation mode

Cluster operation mode	Description
Standby operation mode	General name for the four operation modes are 1:1 standby, N:1 standby, mutual standby, and cascade.
1:1 standby	A single standby cluster application runs on a system that consists of two nodes. One is an operating node, and the other is a standby node.
N:1 standby	<p>“N” standby cluster applications run on a system consisting of “N+1” nodes. One application runs on each operating node. Two or more applications stand by on one node.</p> <p>—N:1 standby - with exclusive relation:</p> <p>An exclusive relation is set up for the cluster application that constitutes N:1 standby. The purpose of the exclusive relation is to run only one cluster application on each node. When a failure occurs in one cluster application, the standby applications enter Offline on the node to which the disabled application is switched. This operation mode is not supported for PRIMECLUSTER 4.1A10.</p>
Mutual standby	One cluster application runs, and the other cluster application stands by on each node. Generally, a cluster system consists of 2 nodes. This is referred to as two-node mutual standby.
Cascade	One operating node has two or more standby nodes. Even when one node stops, the cluster application assures its redundancy by using other node. This operation mode is effective for maintaining the availability of a cluster application during maintenance.
Scalable operation mode	One scalable cluster application consists of two or more operating nodes. If one node stops in the event of a failure, ongoing operations are continued on other operating nodes. Each operating node can be configured to be in the standby operation mode. This Scalable operation mode is not supported for PRIMECLUSTER 4.1A10.

◆ Public LAN takeover function

Public LAN takeover function	Description
IP address takeover	If a failover occurs during standby operation, one or more IP addresses are taken over to other node. In such a case, two or more network interface cards can be used.
MAC takeover	If a failover occurs during standby operation, the MAC address of the network interface card is taken over to other node. This

Public LAN takeover function	Description
	function enables ongoing operations on a client that uses MAC addresses.
Node name takeover	If a failover occurs during standby operation, the node name is taken over to other node. This function enables access to the logical IP address corresponding to the node name.

◆ **Combination of the takeover network**

Status of support		Type of takeover		
SynfinityCluster	PRIMECLUSTER	IP	MAC	Node name
○	○	○	×	×
○	○	○	×	○
○	○	○	○	○
○	×	×	○	×
○	○	○	○	×

* MAC takeover **must be used at the same time** as IP address takeover with PRIMECLUSTER.



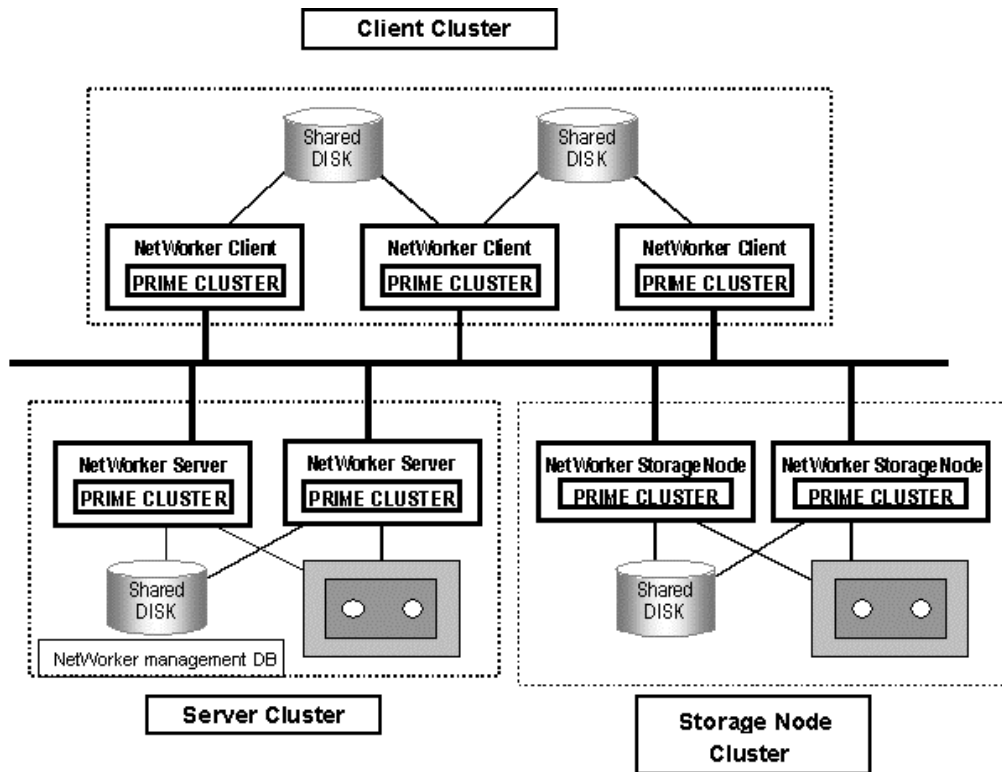
Note

Physical IP address takeover and MAC address takeover deactivate a physical IP address at failover. To avoid disrupting ongoing operations of Web-Based Admin View or Shutdown Facility, set up physical IP address takeover or MAC address takeover for a network interface that is not being used by that Web-Based Admin View or Shutdown Facility.

Chapter 12 PRIMECLUSTER Wizard for NetWorker

12.1 Functional Overview

You can back and restore the data on the shared disk managed by PRIMECLUSTER using NetWorker regardless of the operation mode. The standby configuration is enabled for NetWorker operating on a PRIMECLUSTER system.



The configuration in which a NetWorker client operates on a cluster system is called a client cluster.

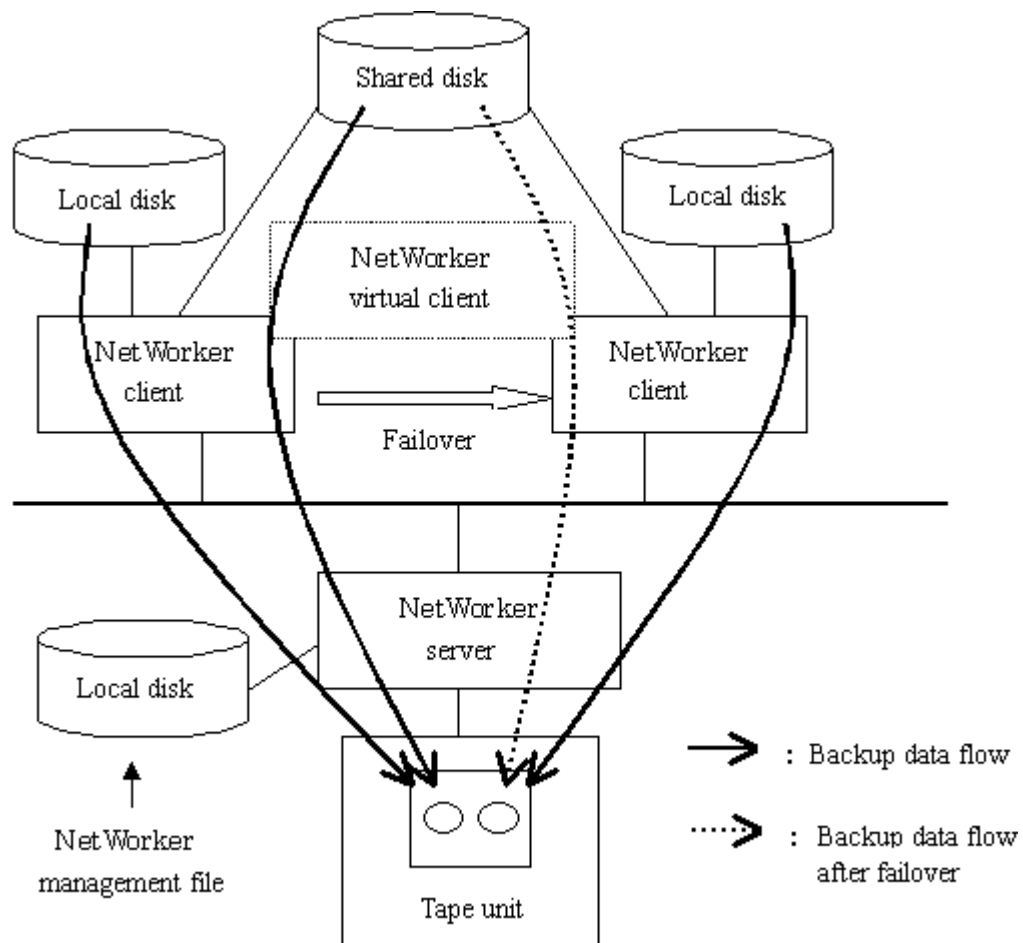
The configuration in which a NetWorker storage node operates on a cluster system is called a storage node cluster.

The configuration in which a NetWorker server operates on a cluster system is called a server cluster.

12.1.1 Client Cluster

Takeover of consistent settings for backup operation in the cluster environment (that does not require the NetWork definition changes in the event of a failover) is enabled for the data on a shared disk or local disk of a PRIMECLUSTER system.

Also, standby operation of the NetWorker client is supported.



■ Virtual client backup

Data on the shared disk, which is managed by PRIMECLUSTER, can be backed up with a logical node name (virtual server name).

The logical node name is a virtual name associated with a virtual IP address that is defined by the PRIMECLUSTER takeover IP address. This name is controlled by the PRIMECLUSTER Wizard for NetWork control to support virtual NetWorker client/server/storage nodes.

By using the logical node name, NetWorker can handle the cluster system easily in the same way as a single system. Thus, data on the shared disk can be backed up from the standby node (new active node) without changing the definition of NetWorker and the backup data can be recovered from either of the nodes.

The logical node names can be specified for each user application in the cluster. Even in a cluster system with multiple user applications that are shown in an operation mode such as N:1 standby or mutual standby, each user application is handled as a single system. This enables the data on each shared disk to be backed up and recovered with the logical node name.

■ Local backup of the cluster configuration node

The data on the local disk of each cluster node can be backed up with the physical node name of the cluster node. Since the NetWorker client operates on all nodes that configure the cluster, the data on the local disk of the standby node can also be backed up. The settings for backup operation are taken over to the standby node without the NetWorker definition changes in the event of a failover.

■ Standby operation of NetWorker client

Standby operation of the NetWorker client can be provided on PRIMECLUSTER by:

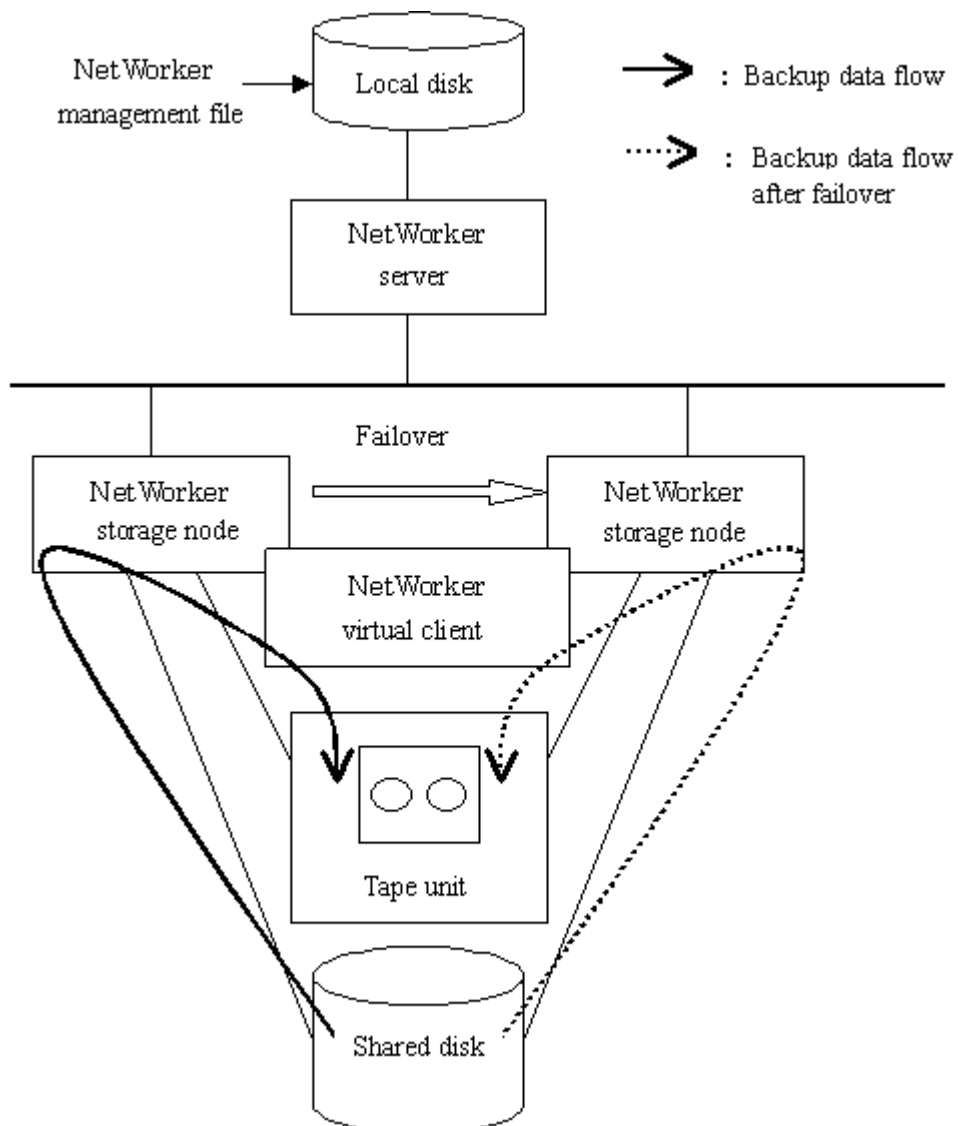
- Starting up the NetWorker client for data backup on the local and shared disks on an

operating node.

- Starting up the NetWorker client for data backup on the local disk on a standby node. Also, the process monitoring facility (detector) that is exclusive to the NetWorker client monitors the NetWorker client process, and if a failure occurs, detects and notifies PRIMECLUSTER of the failure. This feature enhances the availability of the backup system.

12.1.2 Storage Node Cluster

By using NetWorker storage nodes and SAN storage nodes in a cluster system, a tape unit can be shared, and the process monitoring facility (detector) that is exclusive to NetWorker can monitor the process of NetWorker storage nodes and SAN storage nodes. This enhances the availability of the backup system.



With the standby operation of the storage node and SAN storage node, the availability of LAN-free backup that is compatible with the SAN environment is enhanced.

By operating the NetWorker storage node on PRIMECLUSTER, the PRIMECLUSTER failover function enables the standby node to take over the functions provided by the NetWorker storage node without the NetWorker definition changes.

The client cluster configuration also allows backup operation using a logical node. The process monitoring facility (detector) that is exclusive to NetWorker can monitor the NetWorker client. This enhances the availability of the backup system.

Also, a tape unit can be shared between cluster nodes. Note that a tape unit can be shared between the NetWorker server and the NetWorker storage using of an optional NetWorker product.

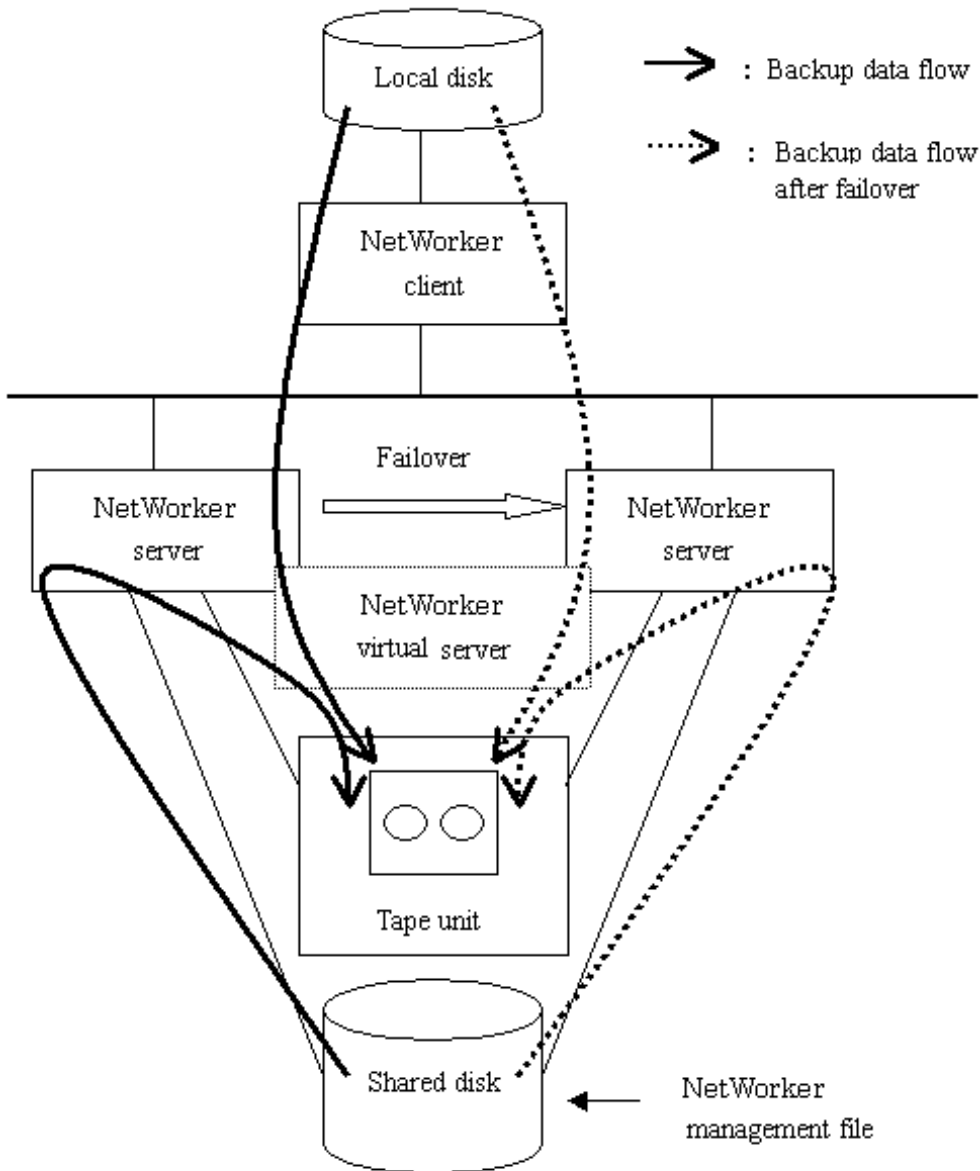


Note

The NetWorker storage node serves as a NetWorker client.

12.1.3 Server Cluster

Standby operation of the NetWorker server is provided on PRIMECLUSTER. The process monitoring facility (detector), which is exclusive to NetWorker provided by PRIMECLUSTER Wizard for NetWorker, automatically detects and recovers from a failure. This enhances the availability of the backup system.



By running the NetWorker server on a cluster system, the tape unit and the NetWorker management database (index and NetWorker settings) can be shared. The backup operation is taken over to the standby node in the event of a failover. Backup using the logical node is also enabled.



Note

The NetWorker storage node serves as a NetWorker client.

12.1.3.1 Backup takeover

The backup takeover is enabled by running RMS (Reliant Monitor Services) configuration script that is exclusive to NetWorker provided by PRIMECLUSTER Wizard for NetWorker and using the process monitoring facility that monitors the NetWorker server on PRIMECLUSTER.

When a failover occurs during backup operation, backup is automatically switched to the standby node. The NetWorker server automatically starts on the standby node (Next Online node), and backup is restarted without the NetWorker backup definitions.

Also, the backup data is recovered on the next online node using the data that is backed up with the previously online node.

12.1.3.2 Automatic detection and NetWorker failure recovery

NetWorker errors are automatically detected and corrected by running the RMS (Reliant Monitor Services) configuration script that is exclusive to NetWorker provided by PRIMECLUSTER Wizard for NetWorker and the process monitoring facility that monitors the NetWorker server on PRIMECLUSTER.

This automatic detection and recovery function reduces downtime of backup application.

■ RMS configuration script

RMS starts the RMS (Reliant Monitor Services) configuration script to start or stop NetWorker. Also, when an error occurs during NetWorker operation, the RMS configuration script is restarted with the AutoRecover function to recover the NetWorker operation. The RMS configuration script checks the NetWorker management database index during NetWorker startup. If an error occurs in the index, then it is automatically corrected.

■ NetWorker process monitoring facility

The PRIMECLUSTER NetWorker process monitoring facility monitors the process of NetWorker. When the process monitoring facility detects a NetWorker error, it notifies RMS of the error. First, RMS attempts to restart NetWorker once, but if it doesn't work, it brings the Online node Faulted. The process monitoring facility continues monitoring NetWorker even after notifying RMS of the error. When NetWorker is restarted with the RMS configuration script, the process monitoring facility starts monitoring NetWorker again.

Details on each error and its recovery are given below:

◆ Failure recovery

The process monitoring facility monitors NetWorker, if an error is detected, it notifies RMS of the error. If the AutoRecover attribute is enabled, the RMS starts up NetWorker startup script after receiving the error notification.



See

To determine whether the AutoRecover function should be enabled, refer to the PRIMECLUSTER manuals.

◆ Correcting the index of the NetWorker management database

The RMS configuration script checks the index by executing the NetWorker commands. If it determines that it is necessary to correct the index of the NetWorker management database, it corrects the index of the target client by executing the NetWorker commands. The RMS configuration script also determines if it is necessary to correct the index when the NetWorker command is executed, and if an index error is detected, and this error is notified RMS.

The index error might be caused by the following cases:

- A failure occurs in NetWorker during backup
- A running node is powered off during backup, and a failover occurs

You can select Yes or No in the recovery mode parameter provided by PRIMECLUSTER Wizard for NetWorker for index correction.



For details on how to set the recovery mode, see the *“PRIMECLUSTER Wizard for NetWorker Configuration and Administration Guide.”*

For details on how to correct index errors manually, see the *“PRIMECLUSTER Wizard for NetWorker Configuration and Administration Guide.”*

12.1.4 Suspending NetWorker Monitoring

You can stop NetWorker monitoring by executing the “hvnwdisable” command of PRIMECLUSTER Wizard for NetWorker. By doing this, you can shut down NetWorker without disturbing the ongoing operations of other user applications and do maintenance work of NetWorker regardless of cluster operation. At this time, the state of user applications of NetWorker is Online. When restarting the NetWorker monitoring feature, you need to execute the “hvnwenable” command of PRIMECLUSTER Wizard for NetWorker. For details, see *“PRIMECLUSTER Wizard for NetWorker Installation/Administration.”*

12.1.5 Standby Operation

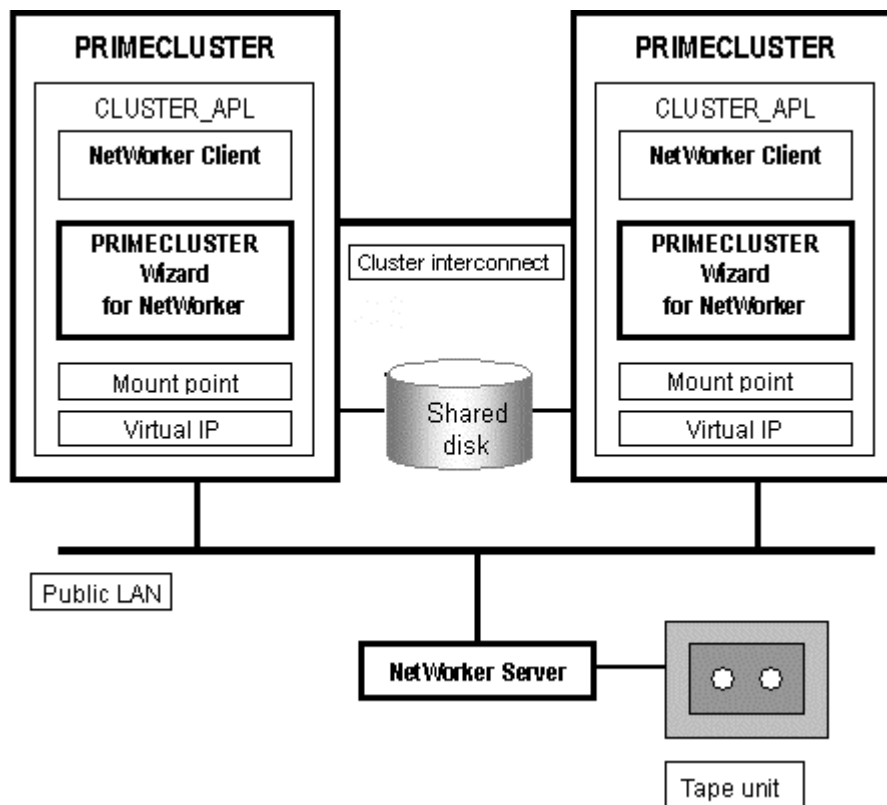
In the server cluster topology, the online node runs as the NetWorker server, and the standby node runs as a NetWorker client. The NetWorker process is monitored on the standby node. If NetWorker on the standby node is abnormally terminated, RMS attempts to restart NetWorker once. If it does not start normally, the NetWorker user application resource enters the faulted state. When a failure occurs, and the monitoring process is killed, the standby node enters Faulted. The Faulted node can restart the standby operation by clearing the faulted state if the database on the standby node is not damaged.

Also, if the NetWorker server is mistakenly booted on the standby node, the NetWorker process monitoring facility considers it as an error and notifies RMS of the error. Then, RMS brings that node Faulted.

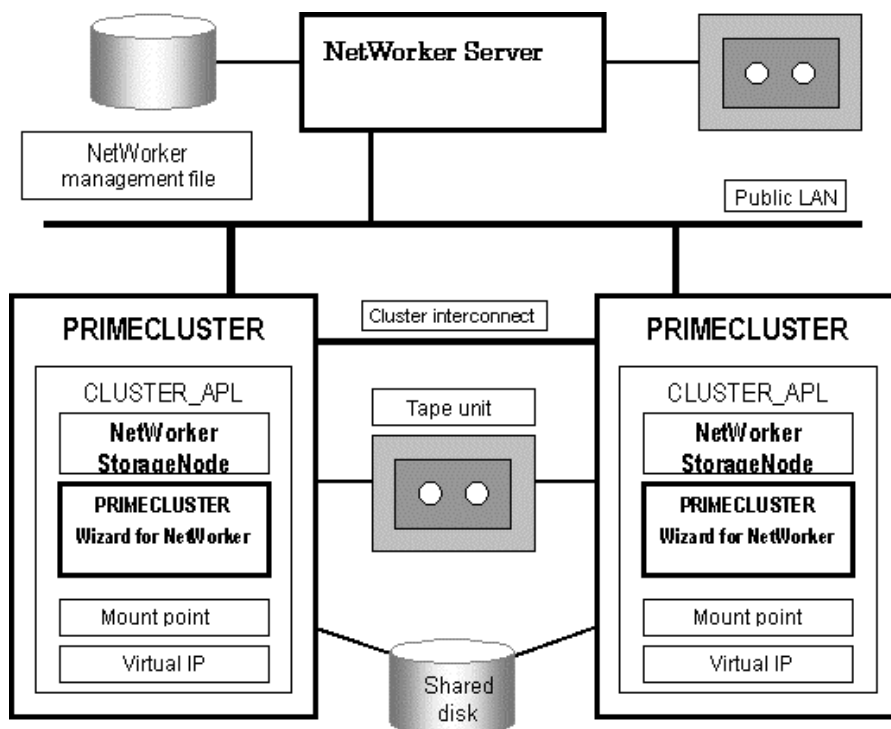
12.2 Operation Environment

12.2.1 System Configuration

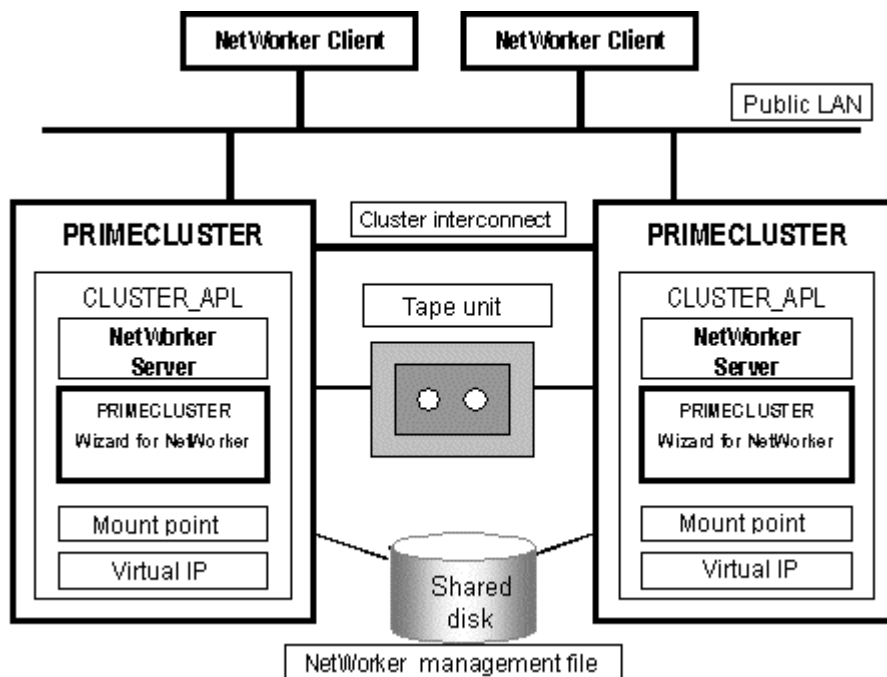
12.2.1.1 Client cluster



12.2.1.2 Storage node cluster



12.2.1.3 Server cluster



12.2.2 Supported Modes

For details, see the Table 11-1 "PRIMECLUSTER Product List".

12.2.3 Overview of Cluster System Support

The PRIMECLUSTER Wizard for NetWorker provides the environment setup wizard that is used to build a backup system on the cluster system by using NetWorker, startup/stop scripts, and state monitoring detectors, and supports standby operation using NetWorker.

12.3 Notes

For details on the environment setup with the PRIMECLUSTER Wizard for NetWorker, see *PRIMECLUSTER Wizard for NetWorker Configuration and Administration Guide*,” which is provided with the PRIMECLUSTER Wizard for NetWorker.

Chapter 13 PRIMECLUSTER Wizard for Oracle

13.1 Functional Overview

PRIMECLUSTER Wizard for Oracle is a software product that facilitates cluster operation management for Oracle operating on a PRIMECLUSTER system.

This is required for scalable operation and standby operation for a cold standby Oracle instance. The scalable operation requires Oracle9i Real Application Clusters (Oracle9i RAC). The standby operation does not require Oracle9i RAC, but requires Oracle cold standby instead.

Startup and stop control

In line with the state transition of the cluster system, scripts automatically start or stop an Oracle instance or an Oracle listener. These scripts first check and then start up the Oracle instance. If damage has occurred, the scripts automatically recover the Oracle instance. For example, if the Oracle instance fails during online backup, the scripts automatically execute “end backup” to start up the Oracle instance. (When the AutoRecover is set to “Yes”.) When stopping the Oracle instance, the scripts stop it in the immediate mode (default). If this does not occur properly, the scripts stop the instance in the abort mode. This means operational node switchover can be performed at high-speed.

Monitoring

A detector monitors an Oracle instance and an Oracle listener. The detector connects itself to Oracle using system user. Then, this enables the detector periodically to create, update and delete a dummy table, which should be generated in the system user’s default tablespace, by executing an SQL command. Consequently, a logical failure can be detected as well as the process of the Oracle instance being active or inactive. When the Oracle instance hangs, and if the SQL command is not returned within a specified time, the detector times out and notifies a user of the failure. The two types of monitoring of the Oracle listener are process detection and the “tnsping” command.

Environment setup

The environment setup tool provides an “ORACLE” Wizard that generates userApplications in the RMS configuration by executing the “hvw” command of PRIMECLUSTER RMS Wizard.

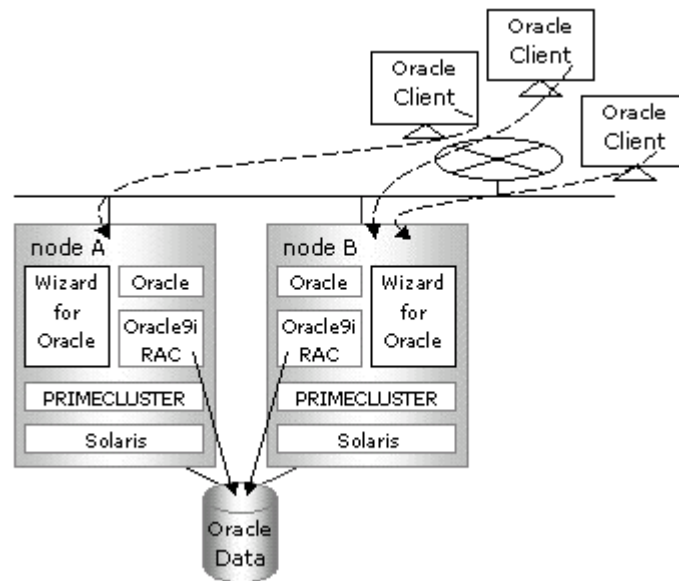
13.2 Operation Environment

13.2.1 System Configuration

System configuration figures are shown below:

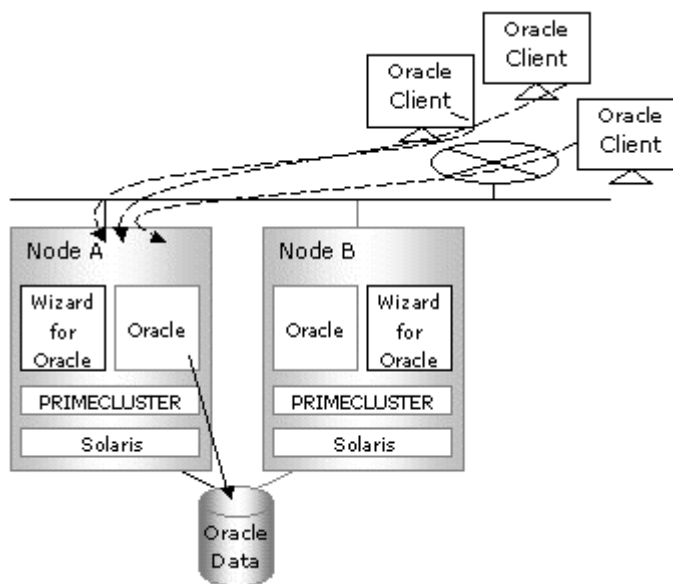
Scalable operation (Oracle9i RAC)

In scalable operation with Oracle9i RAC, Oracle is operated on all nodes. A client can use a database that is connected to either node.



Standby operation (cold standby)

In standby operation, a cluster system consists of an operational node and standby nodes. On the operational node, Oracle applications, a logical IP address and shared disks are active. On the standby nodes, these resources are inactive. In the event of a failure, production operation is switched to one of the standby nodes, and the resources in this standby node are activated. The client can connect to the running node using the logical IP address without configuration changes.



13.2.2 Supported Modes

For details, see the Table 11-1 "PRIMECLUSTER Product List."

13.2.3 Overview of Cluster System Support

The PRIMECLUSTER Wizard for Oracle provides the environment setup wizard that is used to build Oracle on the cluster system, the start/stop script, and the state-monitoring detector. It also supports scalable operation using Oracle9i RAC and Oracle cold standby operation.

13.3 Notes

For details on the environment setup, etc., see “*PRIMECLUSTER Wizard for Oracle Configuration and Administration Guide*,” which is attached to the PRIMECLUSTER Wizard for Oracle.

Chapter 14 Interstage Application Server Enterprise Edition

14.1 Functional Overview

The Interstage Application Server is an infrastructural support software product in which the latest international standard technologies including J2EE, SOAP, UDDI, ebXML, and COBRA are integrated with well-proven high-reliability and high-performance trunk system construction technologies.

The Interstage Application Server Enterprise Edition is the highest-ranking of the editions provided by the Interstage Application Server. Assuming the need to provide round-the-clock service, the Interstage Application Server Enterprise Edition guarantees a stable response even in under high load.

14.1.1 Overview of Cluster System Support

The Interstage Application Server Enterprise Edition supports two modes: Namely, 1:1 standby, which is a so-called hot standby system in which the operation is automatically taken over by the standby node if a failure occurs in the OPERATING node; and mutual standby, in which two nodes perform each operation and, if a failure occurs on one node, the other node takes over the operation.

With the Interstage Application Server Enterprise Edition, operating on the cluster system allows high-speed switching to another server to take over the operation even in the event of a failure. The client can continue the transaction through reconnect processing and can minimize downtime.

14.1.2 Supported Modes

For details, see the Table 11-1 "PRIMECLUSTER Product List_"

14.2 Registering a SynfinityCluster-compatible State Transition Procedure

This section explains how to register a SynfinityCluster-compatible state transition procedure of Interstage Application Server 5.0.

- Descriptions of other than how to register a state transition procedure
Refer to the description of how to use SynfinityCluster, which is included in the Interstage Application Server 5.0 manual.
- How to register a state transition procedure
The registration process is explained below:

14.2.1 Setting Resource Information

Set “No. of process restart” to “0”; “Interval period of process restart” to “0”; and “Initialize No. of process restart” to “No” for the resource information of the state transition procedure.

14.2.2 Setting State Transition Instruction Timings

Set up the state transition procedures provided by Interstage so that they can be invoked at the timings shown below:

- [START-RUN]
 - AFTER
 - CUTOFF/BUILDIN
- [START-WAIT]
 - AFTER
- [STOP-RUN]
 - BEFORE
- [STOP-WAIT]
 - BEFORE
- [FAIL-RUN]
 - BEFORE
- [FAIL-WAIT]
 - BEFORE

14.2.3 Registering a State Transition Procedure to a userApplication

Register the state transition procedures to userApplication. The “Resource startup procedure” must be set up so that resources can be invoked with the following priority:

- ◆ **Resource startup priority**
 - Startup priority to be registered to BasicApplication in the procedure
(Set up to be invoked in the descending order.)
service name.IS_INTERSTAGE
service name.OTS_RMP_INTERSTAGE
service name.ES_INTERSTAGE
service name.SOAP_INTERSTAGE

- Startup priority of the resources to be registered to Application of the procedure class (optional)

```
service name.TDWU_INTERSTAGE
service name.EJBWU_INTERSTAGE
service name.UTYWU_INTERSTAGE
service name.ODWU_INTERSTAGE
service name.EB_INTERSTAGE
```

◆ Operation Procedure

Parameters to be specified for options:

*: Must be omitted if it is to be specified for TDWU_INTERSTAGE/ EJBWU_INTERSTAGE/ UTYWU_INTERSTAGE.

**: Must be changed according to the name of the resource to be registered.

Execute the following operation in each procedure on all nodes in which the state transition procedure is to be executed:

1. Register the state transition procedure.

```
clsetproc -c BasicApplication *
-m IS_INTERSTAGE **
-o /etc/opt/FJSVisas/HA/SynfinityCLUSTER/IS_INTERSTAGE **
```

2. Register the application resource that uses the state transition procedure.

```
claddprocrsc -k IS_INTERSTAGE **
-m IS_INTERSTAGE **
-c BasicApplication *
-K AFTER -w -L AFTER -S BEFORE -T BEFORE -V BEFORE -W BEFORE -u 0 -t 0 -p 100
```

3. Register a resource used for the state transition procedure as a resource for PRIMECLUSTER.

Register the resource created in "Procedure 2" as a resource for PRIMECLUSTER.

Operation must be implemented from "Create Resource" of "userApplication Configuration Wizard."

Use the format described in "Resource startup priority," above, for the resource name.



See

For details on the "userApplication Configuration Wizard", see 6.6.1.6 "Creating Procedure Resources."



Note

If two or more resources of the same kind are registered, the *SubApplication* button on the lower left will be enabled when the *Attributes* tab is selected on the "Confirm registration" screen.

When the final resource is to be registered, click *SubApplication* and then **specify the resource startup priority** on the "Associate resources" screen.

The startup priority can be set up by setting the resources so that resources are listed in the order described in "Resource startup priority," above, in the *Selected Resource* list of the "Associate resources" screen.

4. Registering state transition procedure resources to userApplication.
Register all the resources created in Procedure 3. to userApplication.

The operation must be implemented from “*Create userApplication*” of “*userApplication Configuration Wizard*.”

With this operation, set “*ClearFaultRequest|Startup|SwitchRequest*” to “*StandbyTransitions*” of “*userApplication* attributes.”



[See](#)

For more details on “*userApplication Configuration Wizard*,” see 6.6.2 “*Creating Cluster Applications*”.

Chapter 15 Softek AdvancedCopy Manager

15.1 Functional Overview

This product realizes storage management for open systems and consists of the following three solutions:

◆ High-speed backup (round-the-clock support)

Data can be backed up at high speed by using the hardware [advanced copy function (OPC, EC)] of the Fujitsu disk array unit (ETERNUS3000, GR720, GR730, GR740). Since the advanced copy function is a high-speed data copy function that is not dependent on the volume of data, a constant, high-speed backup time can be always maintained even when the amount of data to be backed up increases. Thus, the backup time does not increase even when the data quantity increases.

By linking this solution with the following DBMS, high-speed backup can be done without stopping the job:

- ORACLE
- SymfoWARE

For those jobs that are constructed using a database other than the above or a general file system, the job non-stop time required for the backup is significantly reduced compared with that in the past.

◆ Database backup without stopping the job

Oracle and SymfoWARE database backup can both be done without stopping the job by using Softek AdvancedCopy Manager.

When combined with SynfinityDisk, Softek AdvancedCopy Manager can be used to perform backup without stopping SynfinityDisk, even in the mirror volume (SDX object) environment.

◆ High-speed replication

By using the hardware [advanced copy function (OPC, EC)] of the Fujitsu disk array unit (ETERNUS3000, GR720, GR730, GR740), the data can be used for various purposes and a data replication (copy) can be collected to guard against accidental data destruction.

A remote disk array unit in the SAN environment is also available for storing the replication (copy) for the purpose of restoring the data after a catastrophic failure.

15.1.1 Overview of Cluster System Support

With Softek AdvancedCopy Manager, units constituting a cluster system that has been constructed by using cluster software is controlled as a single business server. By monitoring failover and the like, recovery from errors can be done quickly.

15.1.2 Supported Modes

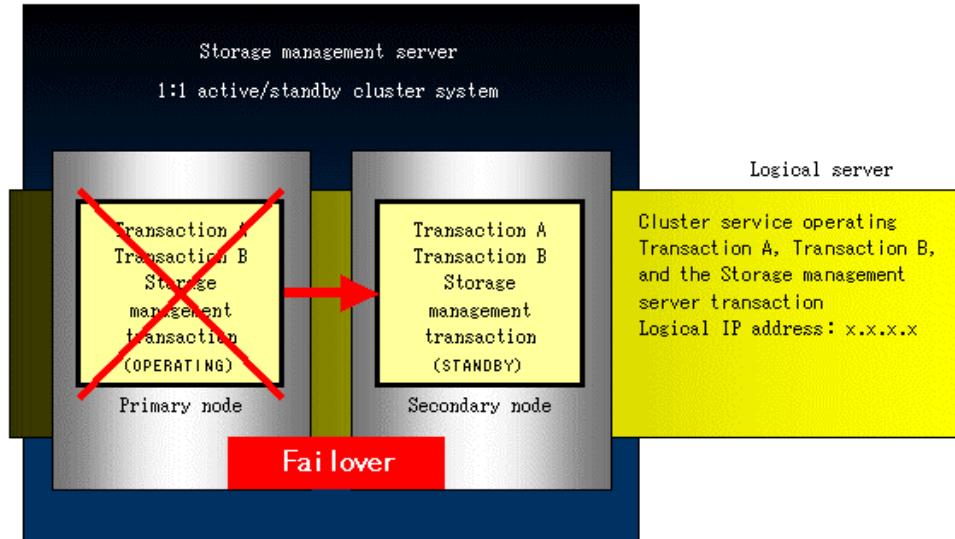
Softek AdvancedCopy Manager supports 1:1 standby and mutual standby by means of IP address takeover. For details, see Table 11-1 "PRIMECLUSTER Product List."

15.2 Standby Classes

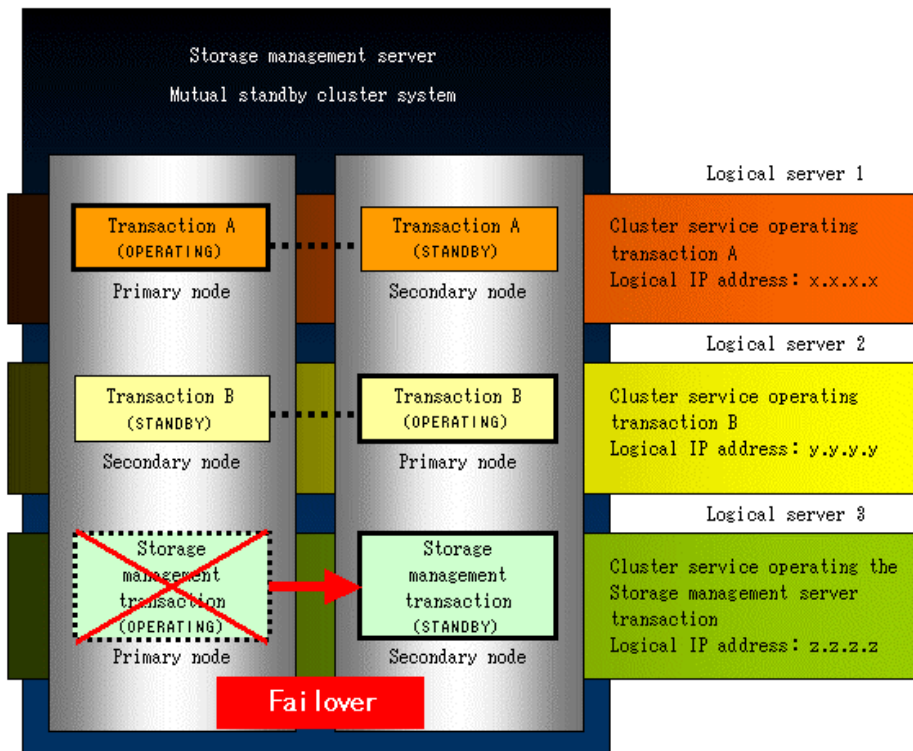
15.2.1 System Configuration

The supported system configurations are shown below:

◆ Standby type cluster system configuration



◆ Mutual standby type cluster system configuration



15.2.2 Setting Up the Environment

For details, see the “Softek AdvancedCopy Manager Cluster Application Guide (SynfinityCluster/PRIMECLUSTER).”

Chapter 16 Symfoware Server Hot-Standby Option

16.1 Functional Overview

Symfoware is a database system that can be applied to mission-critical transaction fields with its high-performance inquiry/loader, more efficient maintenance of large amounts of data, and highly reliable operation. High performance and high throughput equal to that of mainframe computers can be provided by making use of open system materials. Also, information interconnection with multiple servers and the support of network computing technologies allowing the use of any type of client enables the future expansion of operations.

16.1.1 Overview of Cluster System Support

The Symfoware Server hot-standby option provides the relational database of the Symfoware Server with the hot-standby function. A quick restart of the operation is enabled in the event of failures in hardware and software products. By using the Symfoware Server hot standby option, userApplication switches to other server at high speed, so continuous availability of userApplication is provided even if an error occurs on the server. The client reconnects itself to the server, and this ensures operational continuity and minimizes downtime. Symfoware supports a standby operation system.

16.1.2 Supported Modes

For details, see the Table 11-1 "PRIMECLUSTER Product List."

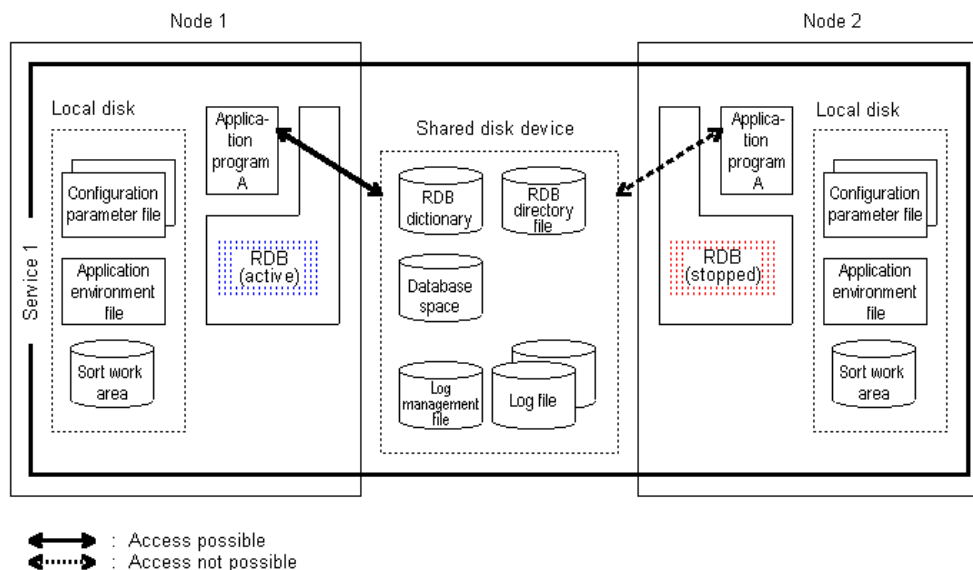
16.2 Standby Classes

Standby classes include 1:1 standby and N:1 standby.

16.2.1 System Configuration

■ Standby system configuration

A standby system configuration is shown below:



16.2.2 Design and Development

To ensure high reliability and high availability in a hot-standby system, you need to consider the following for the system design.

■ File duplication

To prevent an application program from stopping due to a hardware failure or dual system failure, files assigned to the shared disk device must be duplicated with a disk array unit or mirrored with PRIMECLUSTER Global Disk Services or SynfinityDisk.

■ Consider failover

Preopen the routine work that does not require the resource modification or deletion and if the environment of the operating database is fixed. This does not cause open processing for the database after switchover, so you can shorten the switchover time.

However, you cannot preopen the no-routine database environment in which you need to modify definitions such as changing or deleting DSI, deleting the DSI-allocated database space, or deleting the database space that is specified as the allocation destination of the DSI automatic expansion area. Open the database after switching from standby to operating mode.

16.2.3 Setting Up the Environment

You need to register the RDB system in the cluster system as a resource and set up the resource in userApplication that is to be operated.

For details, see the "SymfoWARE (R) Server Cluster Installation/Administration Guide."

16.2.4 Operation

During cluster operation, the registered state transition procedure is executed, and then the processing to activate or deactivate the Symfoware database is done according to the state transition caused by a resource failure or operator intervention.

16.2.5 Operation at Startup

On the operating node, Symfoware/RDB and Symfoware/RDA-SV are activated to start the operation. On the standby node, Symfoware/RDB is activated in standby mode in case of a failure on the operating node.

16.2.6 Operation at Shutdown

On the operating node, Symfoware/RDB and Symfoware/RDA-SV are deactivated to stop the operation. On the standby node, Symfoware/RDB is deactivated.

16.2.7 Operation at Switchover

If a failure occurs on the operating node, the attribute is switched from the standby mode to the operating mode of Symfoware/RDB, and RDA-SV is activated. This processing allows an operation that was executed on the operating node to be taken over.

16.2.8 Performance

On the standby server, the Symfoware relational database can remain active, so the servers can be switched every several minutes.

Chapter 17 Symfoware (Standby)

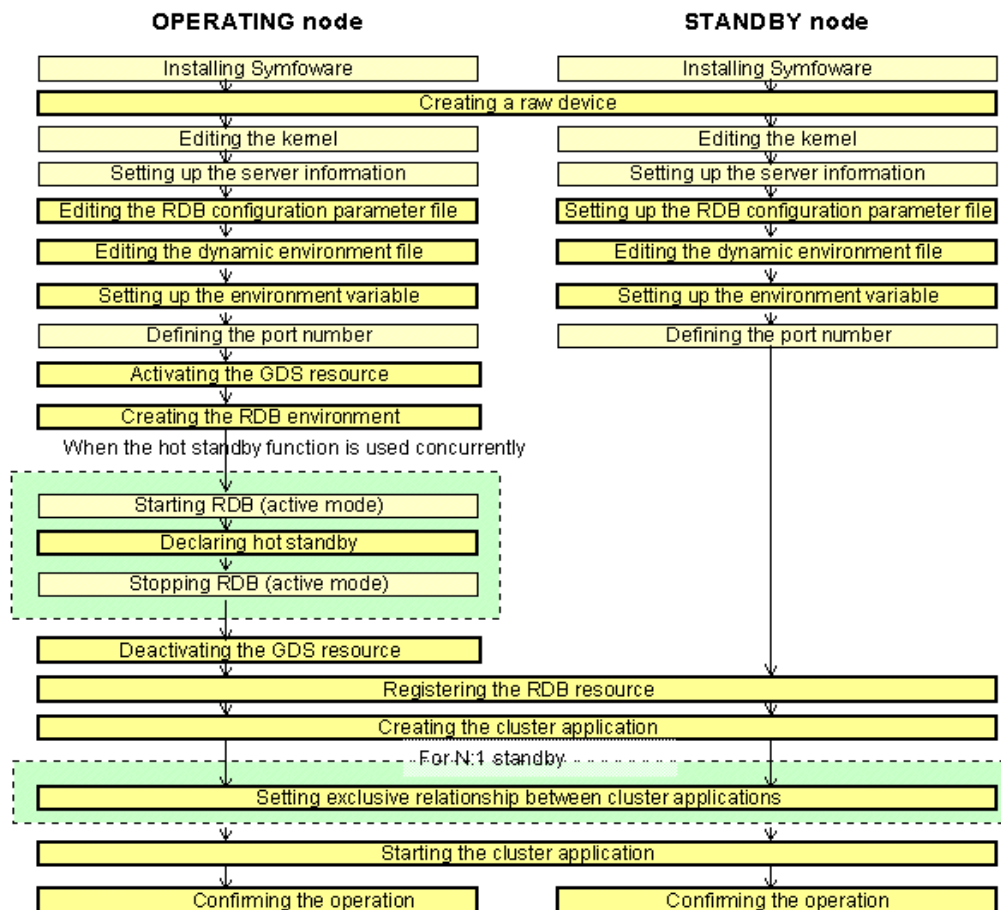
Taking Symfoware as an example, this chapter explains how to configure the environment required for hot standby, prerequisites for operation, and maintenance and management in the event of a failover.

- Environment setup procedures for hot standby operation
- Preparation prior to environment setup
- Environment setup for Symfoware and cluster system
- Maintenance and management in the event of a failover

17.1 Hot Standby Operation and Environment Setup Procedure

Environment setting procedures for hot standby operation is shown below.

Operations such as startup of RDB during hot standby operation are done automatically with the online/offline scripts.



The tasks enclosed in the heavy lines are explained in this chapter. All other tasks are the same as those performed when hot standby operation is not performed.



See

For details on the server information, see the “SymfoWARE(R) Server RDA-SV Operations Guide.”

For details on all other tasks, see the “SymfoWARE(R) Server RDB Operation Guide.”

17.2 Preparation Prior to Environment Setup

Before configuring the Symfoware environment, you need to complete all the operations from PRIMECLUSTER installation to cluster building.



[See](#)

For details, see the sections from Chapter 3 "Software Installation" to Chapter 5 "Building a Cluster."

17.3 Setting Up Symfoware and the Cluster System Environment

This section explains how to configure Symfoware and the cluster system environment.

17.3.1 Creating Raw Devices

Set up the raw device that is used for RDB on the shared disk.



See

- For details how to estimate the raw device in the RDB directory file and the resources to be registered in the raw device, see the “*SymfoWARE (R) Server Cluster Installation/Administration Guide.*”
For details on how to set up disk partitions when the shared disk is to be used as the raw device, see 6.2 "Initial GDS Setup."
- If two or more shared disks are to be grouped into a single disk group, the necessary settings must have already been made as part of the GDS setup. you need to set this up when setting GDS.

17.3.2 Editing RDB Configuration Parameter Files

Modify the RDB configuration parameter files in the operating and standby nodes as follows:

- Add "RDBDIRSPACE"
- Add or change "RDBLOGMANAGE"
- Add or change "RDBLOGGROUPMANAGE"

Add or modify the RDB configuration parameter files that was copied "RDBSYS.cfg" within "/opt/FSUNrdb2b/etc." When creating text files, specify "RDBSYS.cfg" for the copy source and "RDB_system_name.cfg" for the copy destination.

If operating without an RDB system name, you need to define the RDB system configuration parameter in the text file "rdbsysconfig" in the "/opt/FSUNrdb2b/etc" directory.



See

For details on the other parameters, see the “*SymfoWARE(R) Server RDB Operation Guide.*”

◆ RDBDIRSPACE

Define the information for the RDB directory files.

The description format is as follows:

```
RDBDIRSPACE=raw device name of the shared disk device
```

● Raw device name of the shared disk device

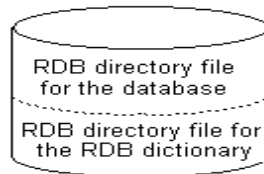
Specify the absolute path name for the raw device to which RDB directory files are allocated.

Delete RDBDIRSPACE1 and RDBDIRSPACE2 within the RDB configuration parameter files.

Set the same value on the OPERATING and the STANDBY node.

Both RDB directory files for database and RDB directory files for RDB dictionary are created for the raw device of the shared disk unit specified herein.

Raw device specified by RDBDIRSPACE



◆ RDBLOGMANAGE

Define the information for the log management files.

The description format is as follows:

```
RDBLOGMANAGE=raw device name of the shared disk
device
```

● Raw device name of the shared disk device

Specify an absolute path name for the raw device to which log management files are allocated.

Set the same value on both the OPERATING and STANDBY nodes.

◆ RDBLOGGROUPMANAGE

When a scalable log operation is to be performed, specify the path for the log group management file information. The description format is shown below:

```
RDBLOGGROUPMANAGE = raw device name of the shared disk device
[,operation flag]
```

● Raw device name of the shared disk device

Specify an absolute path name for the raw device that is at the allocation destination of the log group management file.

Describe the same raw device name on both the OPERATING and STANDBY nodes.

● Operation flag

Specify whether to adopt scalable directory operation. The default value is SCLDIR_NOUSE.

SCLDIR_USE:

Specify when adopting the scalable directory operation.

SCLDIR_NOUSE:

Specify when not adopting the scalable directory operation.



Note

Specify a system file on the local disk as the absolute path name for RDBCORE.

17.3.3 Editing Operation Environment Files

Specify the following setup to operational environment files with OPERATING and STANDBY nodes:

◆ WORK_PATH

Specify the allocation destination directory of the sort work area and work table area to be used by the server. The sort work area is allocated in the local disk. So, this sort work area remains in the UNIX file in the event of a failover. Before the RDB system is changed to the standby state, you need to delete the sort work area (SYMFORDB*) by executing the "rm(1)" command. Users are recommended to prepare the volume exclusively for working, to set up work_path parameter, and to clarify the location of the sort work area so that the sort work area can be deleted easily. Use the sort work area by preparing a different directory for each RDB

operation environment.

The sort work area can be easily deleted by registering the subprocedures.



See

For information about specifying this parameter, refer to the "SymfoWARE(R) Server RDB Operation Guide" and the "FUJITSU SymfoWARE(R) Server RDB User's Guide: Application Program Development."

For information on how to register a subprocedure, see the "SymfoWARE (R) Server Cluster Installation/Administration Guide."

17.3.4 Setting Up Environment Variables

Set up the environment variables on the OPERATING and STANDBY nodes, as follows:

- Set ja, japanese (when the EUC character code system is being used), ja_JP.PCK (when the shift JIS character code system is being used), or C for the environment variable LANG.
- Set /opt/FSUNrdb2b/bin for the environment variable PATH.
- Set /opt/FSUNrdb2b/lib:/etc/opt/FJSVcluster/lib:/etc/opt/FSUNiconv/lib/ for the environment variable LD_LIBRARY_PATH.
Note that when Symfoware Enterprise Extended Edition is to be used, also set /opt/FSUNrdb2b/lib:\$ LD_LIBRARY_PATH_64 for the environment variable LD_LIBRARY_PATH_64.
- Specify the RDB system name in the environment variable RDBNAME. For standby operation without an RDB system name, this setting is not required.
- Set /opt/FSUNrdb2b/man for the environment variable MANPATH.
- When Symfoware Server Enterprise Edition and Symfoware Server Standard Edition are to be used, set the environment variable /etc/opt/FSUNiconv/lib/libicv.so to LD_PRELOAD.



Note

Specify the same character code for the environment variable LANG on the OPERATING and STANDBY nodes. If you use EUC code and shift JIS code together, this will cause an error.

17.3.5 Activating Gds Resources

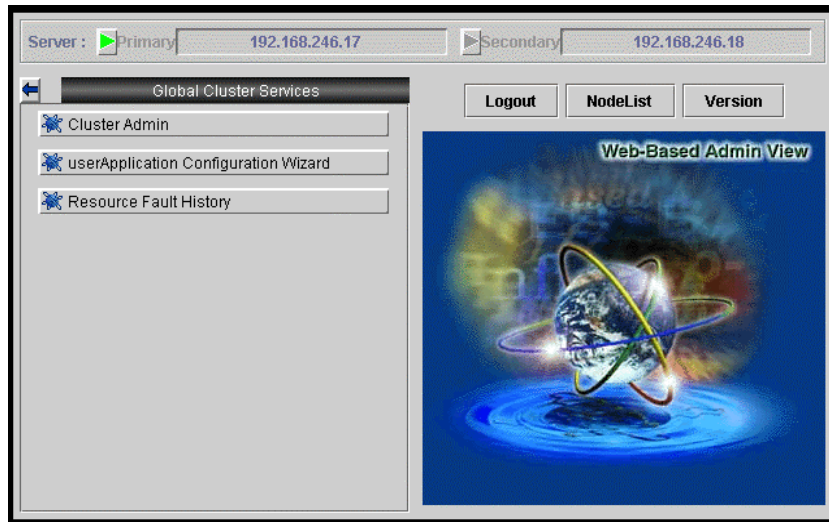
There are two methods of activating Gds (Global Disk Services) resources. These involve the use of GUI and CLI, as follows:

- GUI (Cluster Admin is used.)
- CLI (clstartsc(1M) command is used.)

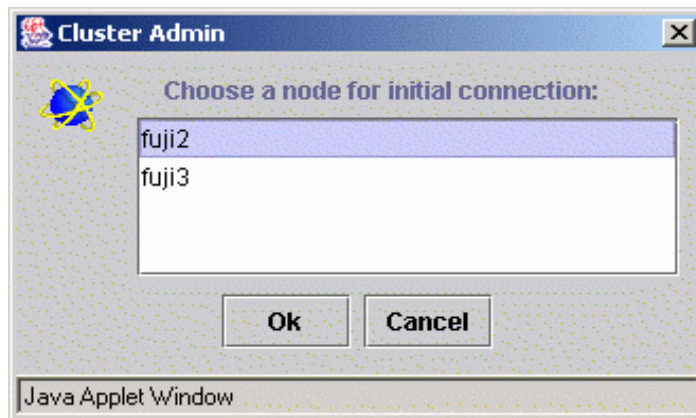
This section explains the use of Cluster Admin. For information on how to use the "clstartsc(1M)" command, see the relevant page in this manual.

◆ Procedure

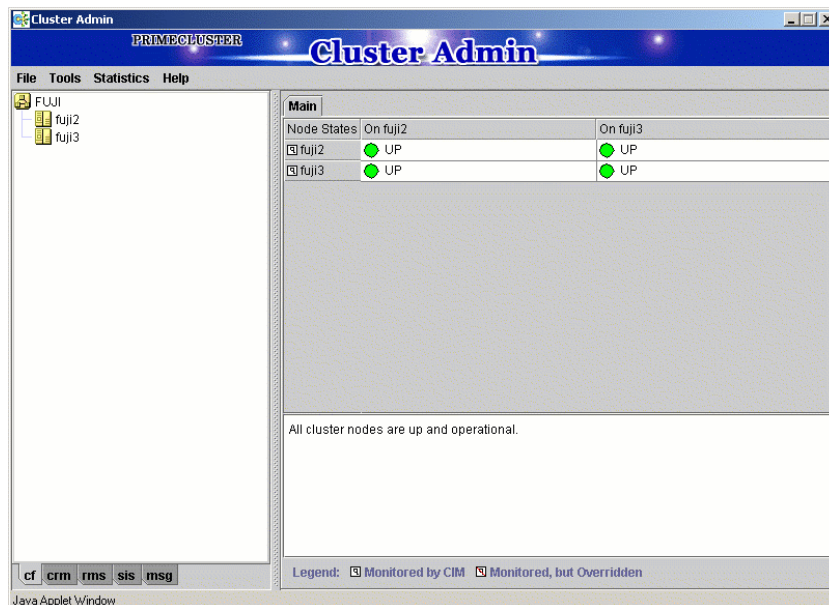
1. After logging on to the Web-Based Admin View screen, select *Global Cluster Services*. The "Global Cluster Services" screen appears.



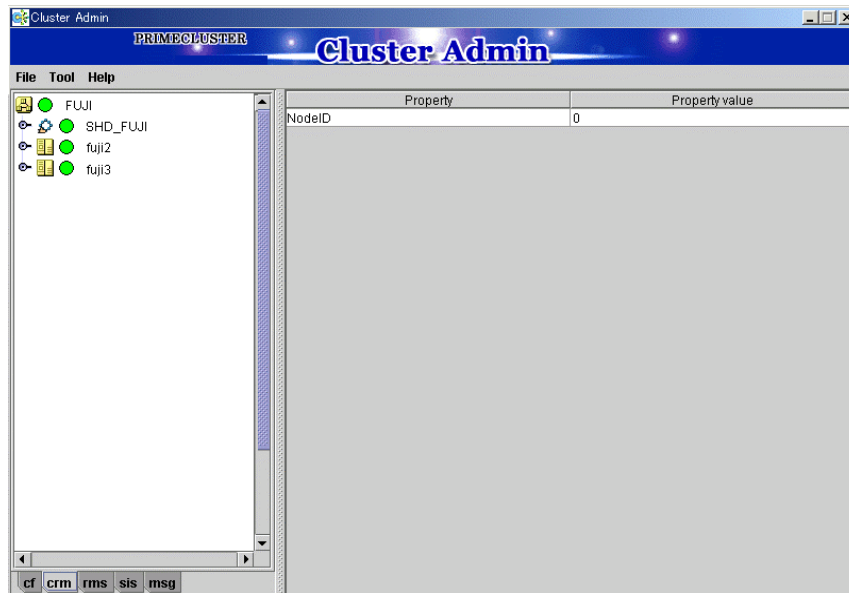
2. Click the *Cluster Admin* button.
The node selection screen appears.



3. Select *node name* and then click the *OK* button. Then, the main menu appears.



4. Select the "*crm*" tab to display the CRM main window.



5. Select a Gds resource on the "crm" tree view and then right-click. Choose *Start* from the pop-up menu that appears.
The Gds resource is activated.

17.3.6 Creating the RDB Environment

Use the following procedure to create the RDB environment. Create the files on the raw device.

Specify a shared disk device for the raw device.

- Log management file
- Temporary log file
- Archive log file
- RDB dictionary
- RDB directory file

When adopting scalable log operation and scalable directory operation, you also need to create the following file:

- Log group management file
- Log files for the user log group (log management file, temporary log file, and archive log file)
- RDB directory file for the user log group

■ Creating a log group management file

When adopting scalable log operation, first create a log group management file. Use the "M" option of the "rdblog" command. The log group management file is created in the raw device specified with RDBLOGGROUPMANAGE in the RDB configuration parameter file.

```
$ rdblog -M
```

■ Creating a log management file

Create a log management file in the raw device of the shared disk device that is specified with RDBLOGMANAGE in the RDB configuration parameter file.

Create a log management file by using the "l" option of the "rdblog" command.

```
$ rdblog -l
```

■ Creating a temporary log file

A temporary log file needs to be created before RDB startup. This setting is required. If omitted, you cannot start RDB.

Use the "G" option and the "t" option of the "rdblog" command to create a temporary log file.

Note that a temporary log file can be created on the same raw device as that on which the log management file is stored.

Example

When the BI log area is 30 MB, the AI log area is 30 MB, the number of transaction entries is 20, and the log index area is to be created in /dev/FJSVmphd/rdisk/mphd2048s1:

```
$ rdblog -G -t /dev/FJSVmphd/rdisk/mphd2048s1 -in -in 30M 30M 20
```



See

Specify 16 GB or less in the BI and AI log area sizes of the temporary log file.

■ Creating an archive log file

To enable error recovery by applying an archive log, create two or more archive log files in advance.

◆ Initial creation of the archive log file

Use the “G” option and the “a” option of the “rdblog” command for the initial creation of the archive log file.

Example

When an archive file of 2 MB is to be created in /dev/FJSVmphd/rdisk/mphd2048s3:

```
$ rdblog -G -a /dev/FJSVmphd/rdisk/mphd2048s3 2M
```

◆ Adding an archive log file

After completing the initial creation of the archive log file, add the archive log file. Use the “U” option and the “a” option of the “rdblog” command. At this time, the size of the archive log file cannot be specified. Regardless of the size of the specified raw device, the value at initial creation is used.

An archive log file is added even when RDB is activated.

Example

When the archive file is to be created in /dev/FJSVmphd/rdisk/mphd2048s4 and /dev/FJSVmphd/rdisk/mphd2048s5:

```
$ rdblog -U -a /dev/FJSVmphd/rdisk/mphd2048s4  
$ rdblog -U -a /dev/FJSVmphd/rdisk/mphd2048s5
```

■ Creating an RDB dictionary

The RDB dictionary is created to configure a database environment. Use the “rdbcrdic” command to create an RDB dictionary. Specify a raw device name when you execute the “rdbcrdic” command to create the database environment.

After creating an RDB dictionary, acquire the saved data to enable subsequent error recovery of the RDB dictionary.



See

For details on how to acquire the save data, see the “SymfoWARE(R) Server RDB Operation Guide.”

Example

When an RDB dictionary of 60 MB is to be created in /dev/FJSVmphd/rdisk/mphd2048s6:

```
$ rdbcrdic -r /dev/FJSVmphd/rdisk/mphd2048s6 -a 60M
```



Point

If an error occurs in the system file such as log management, temporary log, archive log,

RDB dictionary, or RDB directory file, you need to stop the RDB system for recovery. It is recommended that you duplicate the RDB system files.

When the RDB dictionary is created, both the RDB directory files for the database and for the RDB dictionary are automatically created in the raw device that is specified in the RDB-configured parameter file.



See

For details on how to specify the “rdbcrdic” command, see the “rdbcrdic” command page.

■ **Creating a log file for a user log group**

When adopting scalable log operation, create the following log files for the user log group:

- Log management file for the user log group
- Temporary log file for the user log group
- Archive log file for the user log group

These files are created by adding the “g” option to the options of the “rdblog” command.



See

For details on how to specify the “rdblog” command, see the “rdblog” command page.

■ **Creating an RDB directory for user log group**

When adopting scalable directory operation is to be performed, create an RDB directory file for each user log group. Use the “G” option of the “rdbscldir” command.

If an RDB directory file is not created even in one user log group, you cannot start Symfoware/RDB.

Example

When an RDB directory file is to be created in /dev/FJSVmphd/rdsk/mphd2049s1:

```
$ rdbscldir -G -g grp1 /dev/FJSVmphd/rdsk/mphd2049s1
```



See

For details on how to specify the “rdbscldir” command, see the “rdbscldir” command page.

17.3.7 Declaring Hot Standby

When adopting the hot standby operation, you need to configure the RDB environment first, and then declare the hot standby on the operating node by using the “mon” option of the “rdbhsuty” command.

Example

Declaring hot standby

```
$ rdbhsuty -mon
```



See

For details on how to specify the “rdbhsuty” command, see the “rdbhsuty” command page.

17.3.8 Deactivating Gds Resources

There are two methods of deactivating the Gds resources, namely, that using the GUI and that

using CLI.

- GUI (Cluster Admin is used.)
- CLI (clstprsc(1M) command is used.)

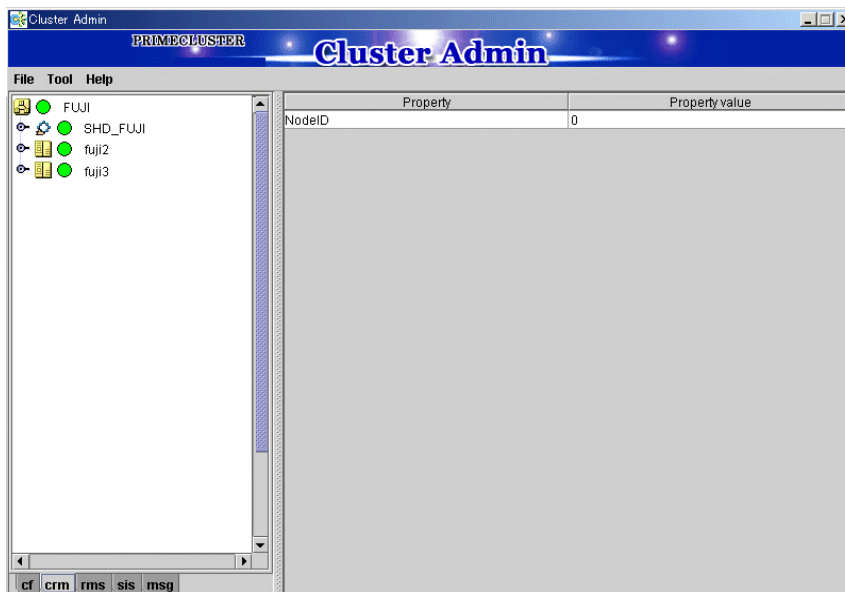
The method using Cluster Admin is explained here. For details on how to use the “clstartsc(1M)” command, see the “clstartsc(1M)” command page.

◆ Procedure

1. Display the CRM main window of Cluster Admin.



See 17.3.5 "Activating Gds Resources".



2. Select a Gds resource on the crm tree view and then right-click. Choose *Stop* from the popup menu that appears.

The Gds resource is deactivated.

17.3.9 Registering RDB Resources

As a resource that constitutes the cluster system, register the RDB system. RDB operates based on this RDB system.

To register the RDB system resource, use the “a” option in the “rdbhrsc” command. You can also register the resource on a remote node by specifying the node identifier of the node to be registered in the “n” option of the “rdbhrsc” command. When RDA-SV is to be used at the same time, specify ON in the “RDASV” option.



For details on how to specify the “rdbhrsc” command, see the “Symfoware Server RDB Command Reference.”

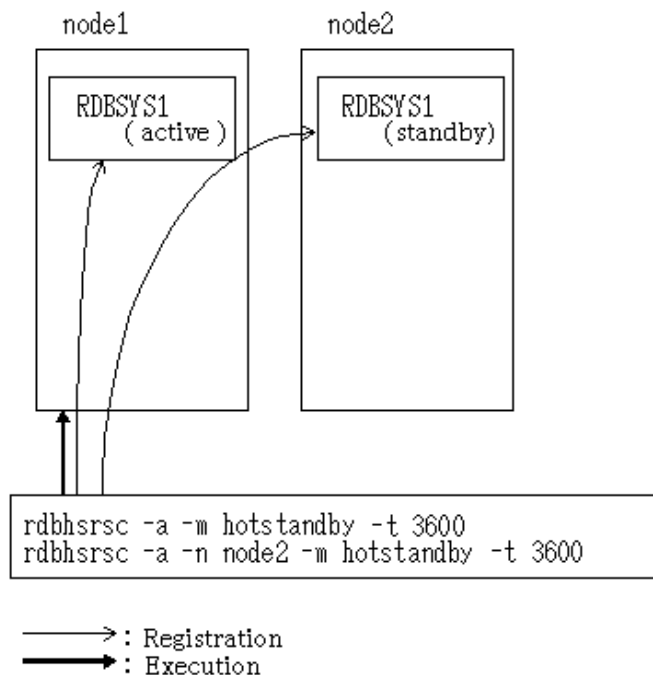


Note

The “rdbhsrsc” command can be executed only with the system administrator access privilege (route).

Example

When the RDB resource is to be registered on node1 (hot standby operation):



The registered RDB resource names are as follows:

Operation mode	Resource name
Operation with RDB system name required	RDB system name
Operation with RDB system name not required	RDBII

For operation that requires an RDB system name, use the RDB system name that is specified with the environment variable RDBNAME. Confirm the name is correct, and then register the resource.

■ **Notes on process monitoring interval and timeout interval**

When the resource is registered, you can set up a process monitoring interval using the “i” option and the timeout interval using the “t” option. With Symfoware, the process for monitoring the Symfoware server process checks, at specified intervals, whether there has been no response from the server process within the timeout interval (hereafter referred to as no response) or to detect systemdown. The timeout interval refers to the time that must elapse prior to the server process recognizing a no-response state when there is no response from the server process. If “no response” is detected, the process for monitoring the Symfoware server process assumes that there was no response with the specified timeout interval, and the RDB system switches to the standby node. When setting the timeout interval, you need to consider the followings:

- Assumed response time
How long it requires for the system to wait for a response.
- Time until system error is judged
When the response takes a longer time than the assumed response time, how long it

requires for the process for monitoring the Symfoware server process to determine a system failure.

An example timeout interval is shown below:

Example

Estimation of the timeout interval when the system response time is assumed to be 10 seconds, and the required time to determine a system failure is assumed to be 10 minutes (600 seconds):

$\text{Timeout interval (610 seconds)} =$ $\text{Assumed system response time (10 seconds) + time until system error is judged (600 seconds)}$
--

Since it is highly likely that “no response” is detected, you are recommended to specify a maximum value for the timeout interval (3600 seconds) to disable the no-response monitoring.

- Unexpected CUP load
- Mistake of estimating timeout interval

It is necessary to examine the following when determining whether to enable or disable the no-response monitoring:

- When there is no response from the Symfoware server process, the response to the database access cannot be assured. So, it is preferable to cause a failover.
- When there is no response from the Symfoware server process, the response to the database access cannot be assured. But it is preferable to continue operation within the supported range instead of causing a failover.

Although it is difficult to figure out the time interval, users are recommended to specify the maximum value 3600 seconds. This setting will make it difficult to detect that the Symfoware server process hangs, however, if the no-response monitoring is disabled, the normal RDB system will never be judged as no-response state due to overload.

Note that, if the no-response state continues even after one hour has passed, the cluster application is switched to the standby node.

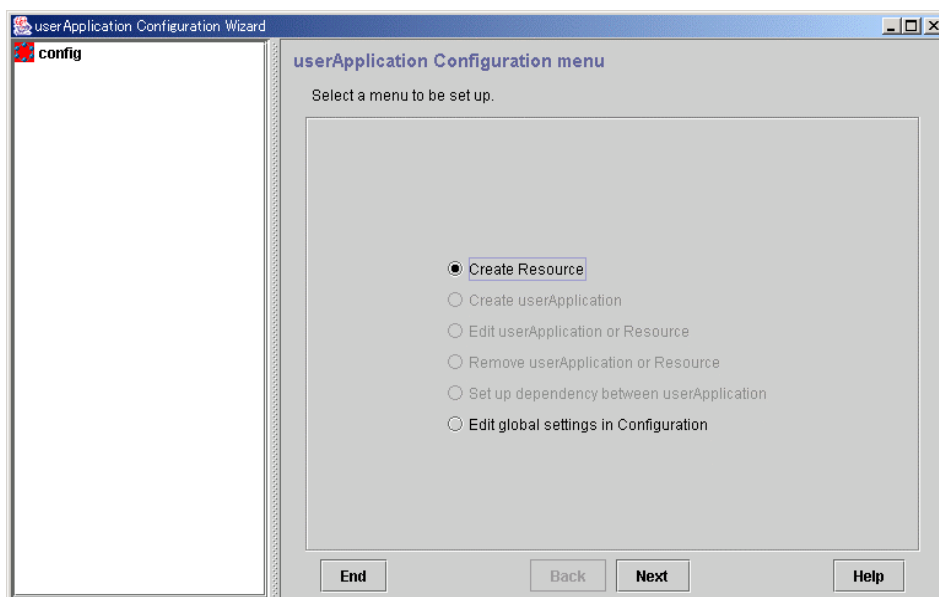
17.3.10 Creating a Cluster Application

Add RDB system or Symfoware procedure resources to the cluster application that has disk resources. To register a disk in the cluster application, use the “userApplication Configuration Wizard” according to the following steps:

■ **1) Opening the "userApplication Configuration Wizard" screen**

1. Select *userApplication Configuration Wizard* on the "Global Cluster Service" screen.

userApplication Configuration Wizard screen



■ 2) Setting the resources

◆ When using a disk resource

Set up the disk resource.

Repeat resource setting as many times as the number of disk units to be used.



Note

If you want to handle two or more disk units as a single group, first set up the group in the initial GDS setup.

For information on setting, see 6.2.2.2 "Setting Up a Shared Disk".

● Procedure

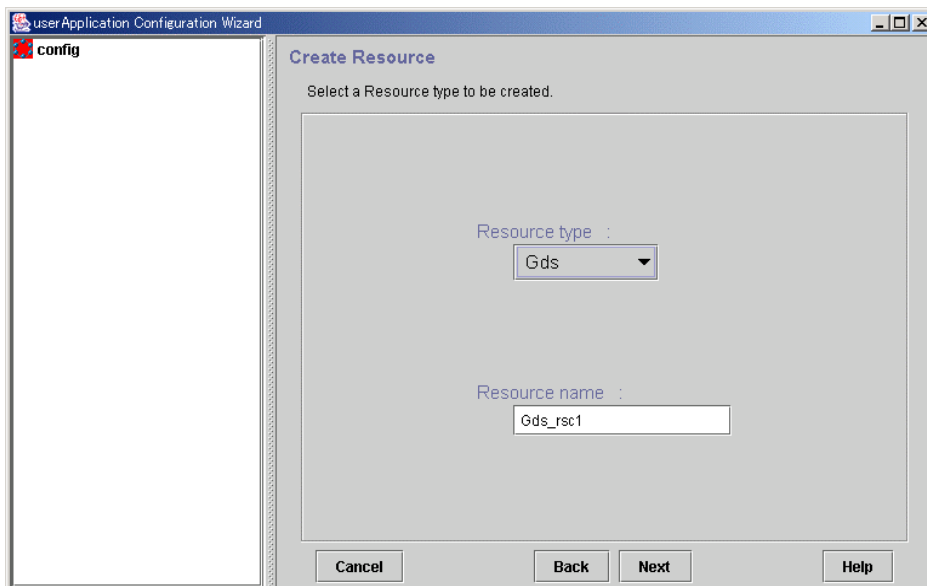
1. Open the resource setup screen.
Select *Create Resource* from the top menu of userApplication Configuration Wizard and set up the resource the cluster application.
2. Set up the resource name.
Set up the Resource type and Resource name on the "Create Resource" screen.

Resource type:

Select *Gds*.

Resource name:

Specify the name of the disk resource to be created. The resource name is optional.



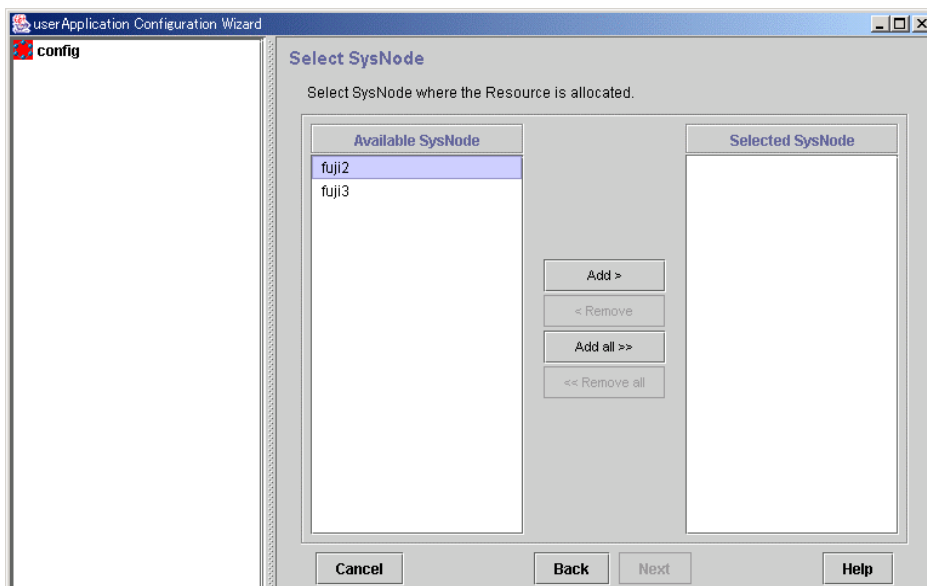
3. Set up the nodes.
On the "Select SysNode" screen, set the node in which resources are to be set to the "Selected SysNode" list.

Available SysNode:

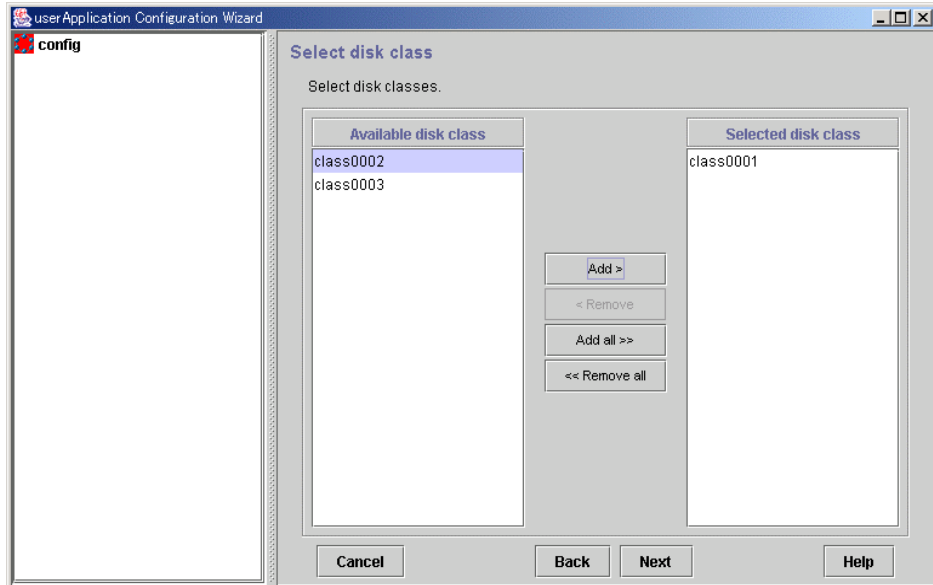
All the cluster nodes are displayed.

Selected SysNode:

Node to which resources are to be set.



4. Select a disk class.
On the "Select disk class" screen, set the disk class in the "Selected disk class" list.

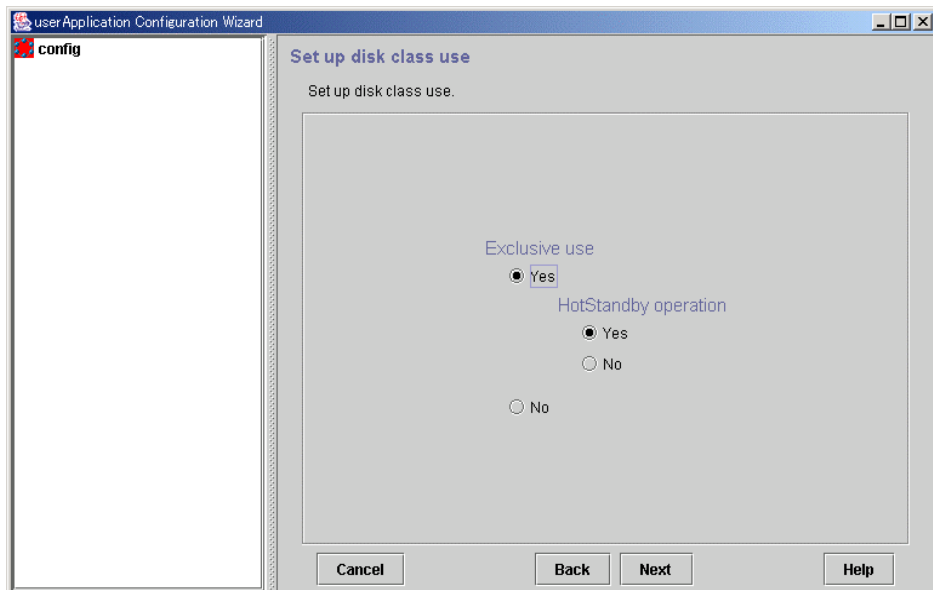


[See](#)

For details, see “Selecting a disk class” in 6.6.1.3 “Creating a Gds resource”.

- 5. Set up the usage of the disk class.

Select “Exclusive use” from “Set disk class use” and then click the Yes button. Then, select “Hot Standby operation” and click the Yes button. (**Shared and simultaneous access**)



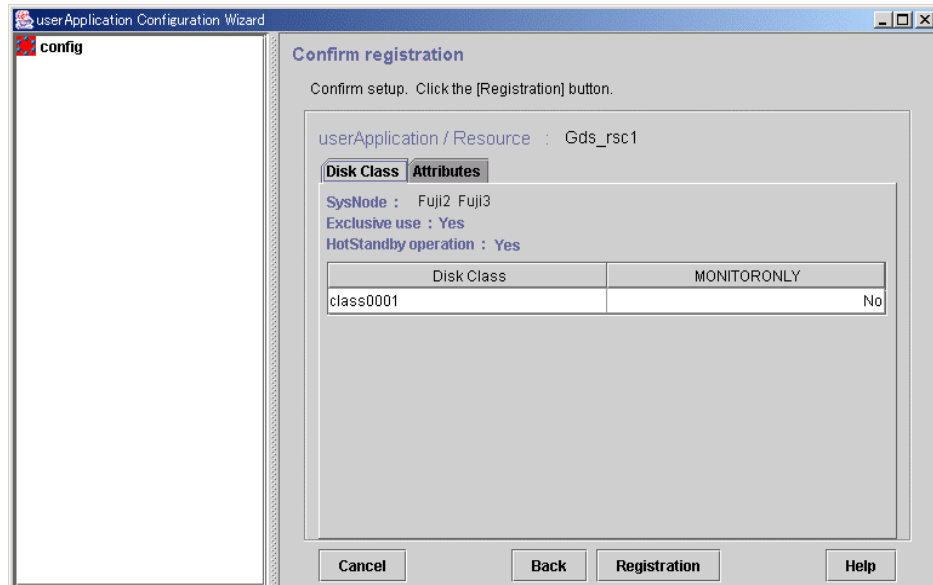
[See](#)

For details, see “Setting the disk class usage” in 6.6.1.3 “Creating a Gds resource”.

For the standby operation, you can set up a switching disk. For example, there is a disk that contains intermediate save file of the “rdbgcdsi” command, reorganization control file of the “rdbgcdsi” command, and a variety of files used with the RDB command.

To enable use as a switching disk, click Yes from “Exclusive use” and then click the No button from “Hot Standby operation.”

6. Confirm/register the registration information of the Gds resource.
 On the " Confirm registration " screen, if the settings are correct, click the "Registration" button to register the settings.
 If the settings are incorrect, click the "Back" button and then correct the settings.



For details, see "Confirming the Gds resource registration information" in 6.6.1.3 "Creating a Gds resource".

◆ When using an RDB resource

Create a Symfoware online/offline script resource.

● Procedure

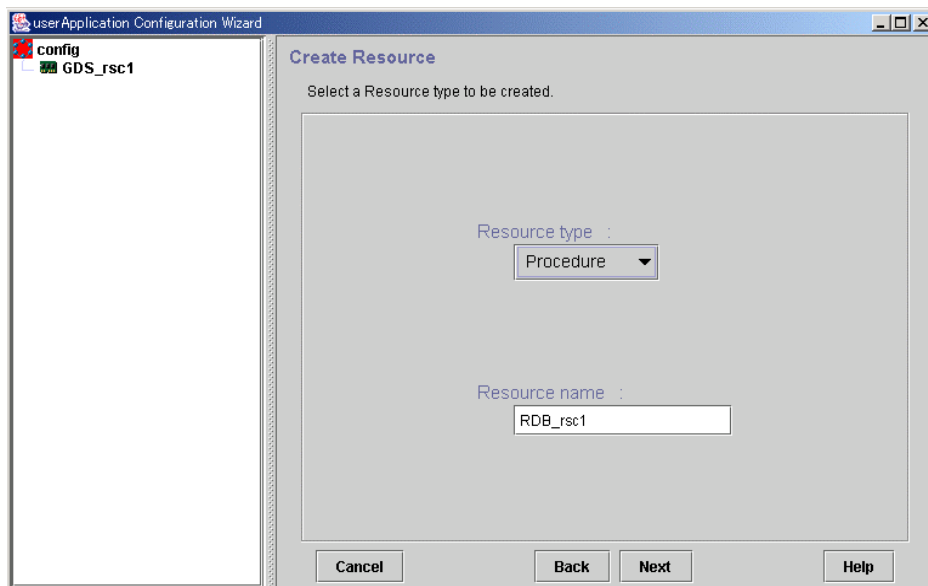
1. Open the resource setup screen.
 Select *Create Resource* from the top menu of the userApplication Configuration Wizard and then set up the resource for the cluster application.
2. Set up the resource name.
 Set up the Resource type and Resource name on the "Create Resource" screen.

Resource type:

Select *Procedure*.

Resource name:

Specify the name of the disk resource to be created. The resource name is optional.



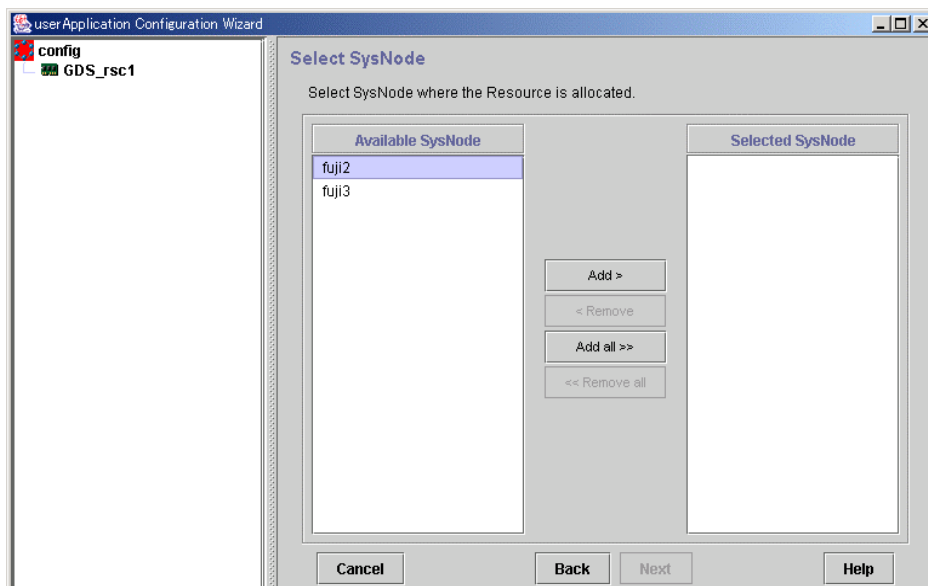
3. Set up nodes.
On the "Select SysNode" screen, set the node in which resources are to be set to the "Selected SysNode" list.

Available SysNode :

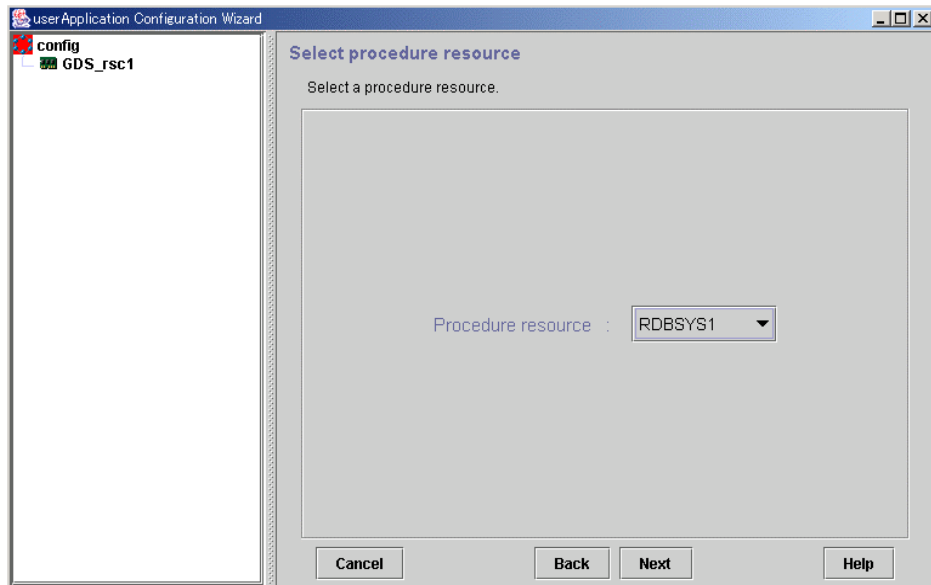
All the cluster nodes are displayed.

Selected SysNode :

Node to which resources are to be set.



4. Select a procedure class.
Set up a procedure class on the "Select procedure class" screen.

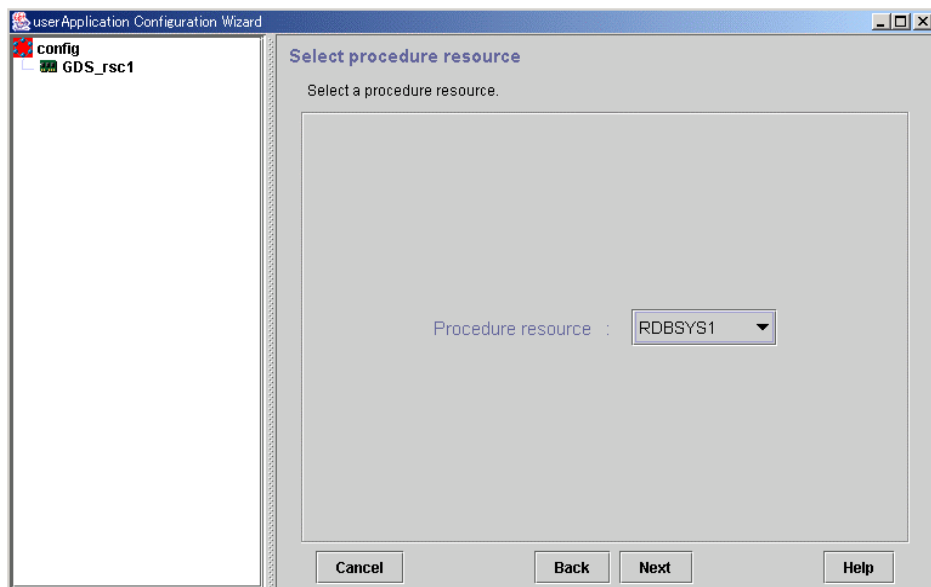


Procedure class:

Select *SymfoRDB_FSUNrdb2b*.

5. Select a procedure resource.

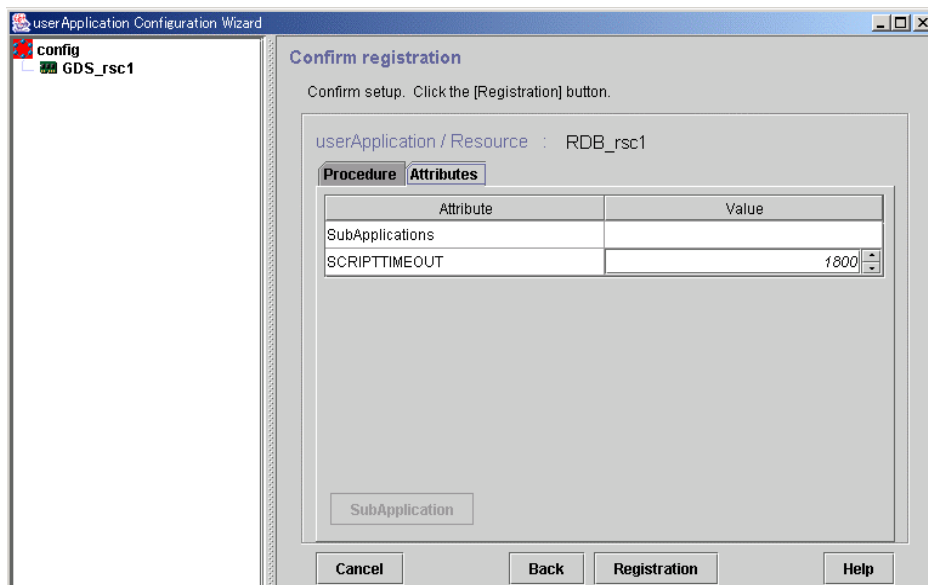
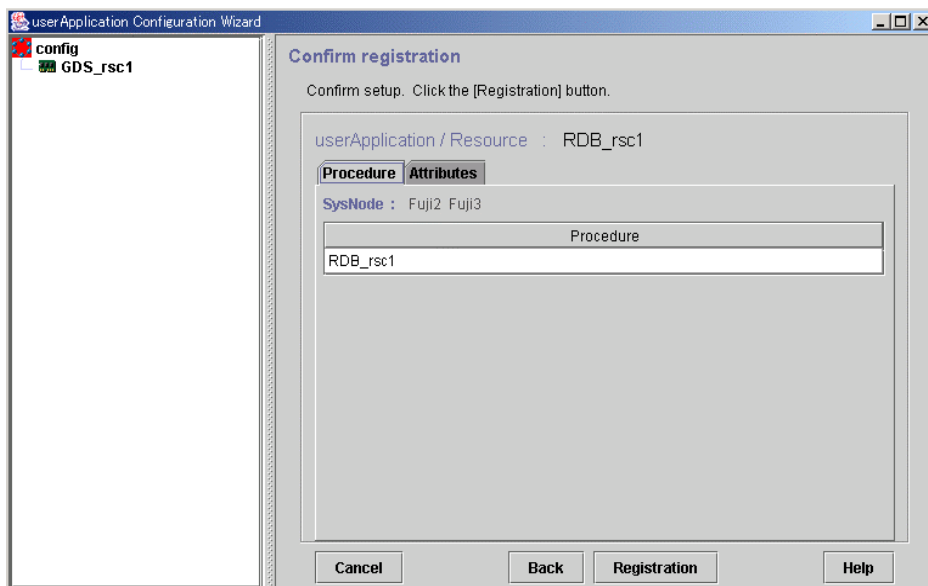
Select an RDB resource as the procedure resource to be created.



6. Confirm/register the registration information of the procedure resource.

On the "Confirm registration" screen, if the settings are correct, click the "Registration" button to register the settings.

If the settings are incorrect, click the "Back" button and then correct the settings.

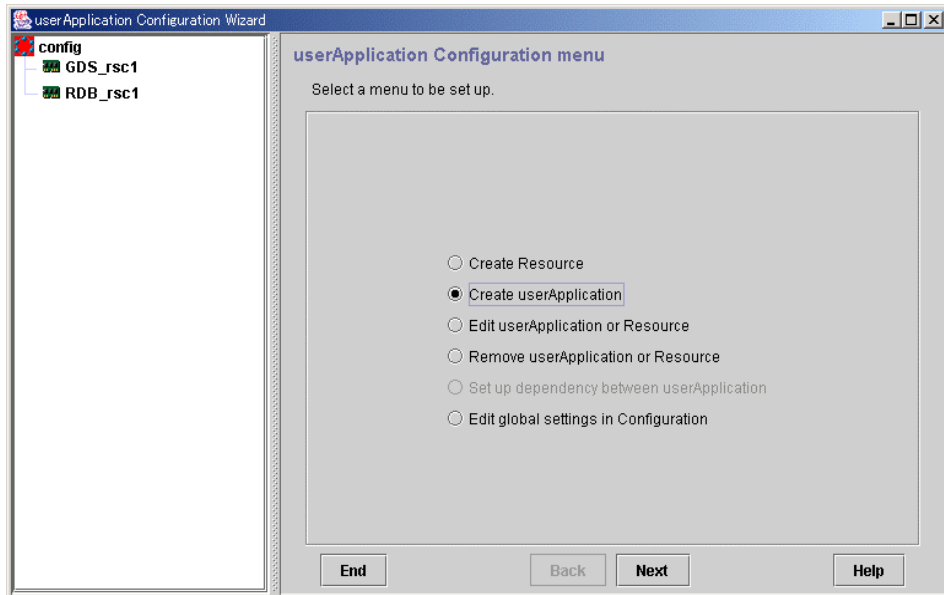


■ **3) Creating a cluster application**

Create a cluster application by using the resources set up in 2).

● **Procedure**

1. Open the cluster application creation screen.
Select *Create userApplication* from the top menu of the userApplication Configuration Wizard and then start creating a cluster application.



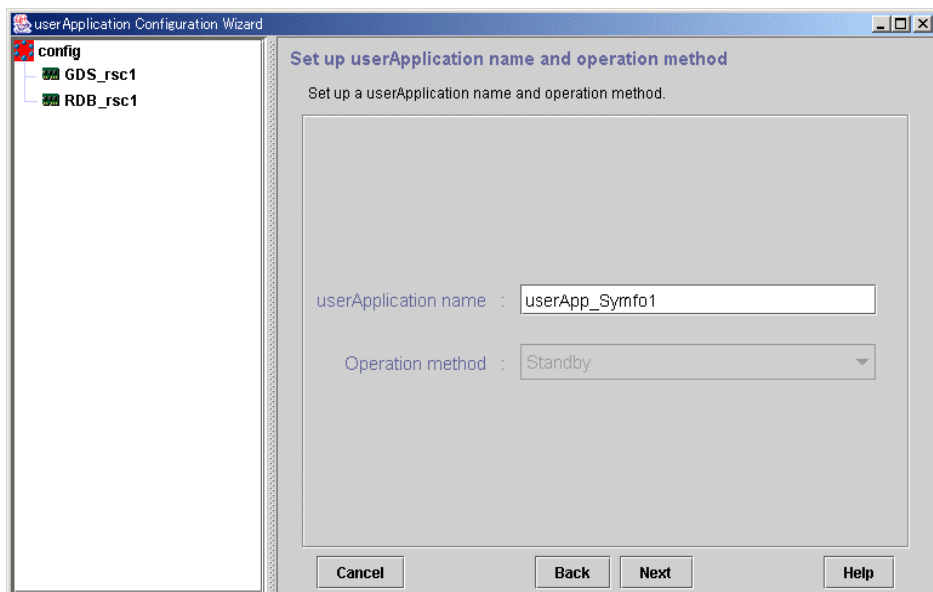
2. Set up the userApplication name and operation mode.
On the "Set up userApplication name and operation method" screen, set up the name and operation mode for the standby cluster application.

userApplication name:

Specify the cluster application name to be registered. The resource name is optional.

Operation mode:

Standby is selected.



3. Set up nodes.
On the "Select SysNode" screen, set the node in which cluster application is to be set to the *Selected SysNode* list.



Note

Nodes are set up as an operating node and standby nodes by the order set up in "Selected SysNode". The top node is an operating node in the initial setting.

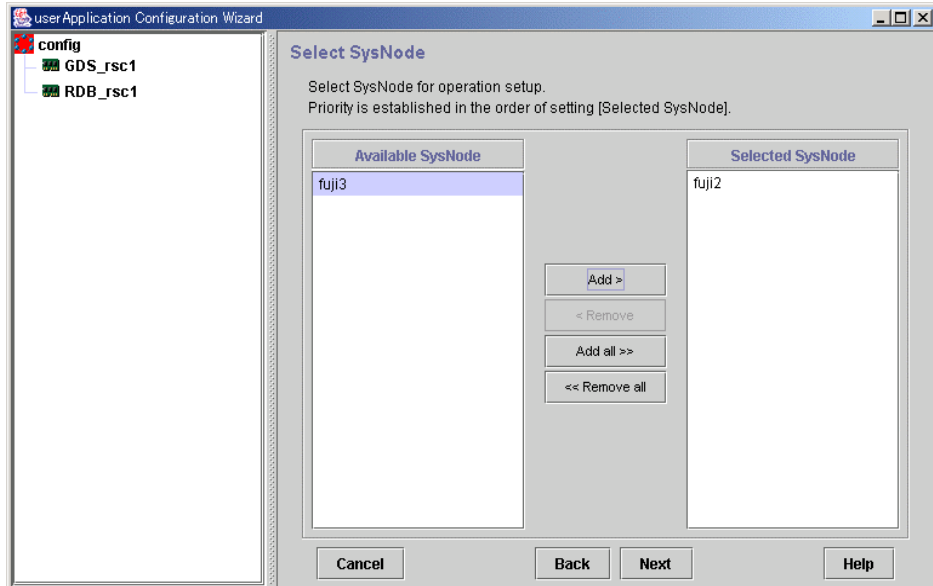
Available SysNode :

Of the nodes belonging to the specified RMS Configuration, currently available

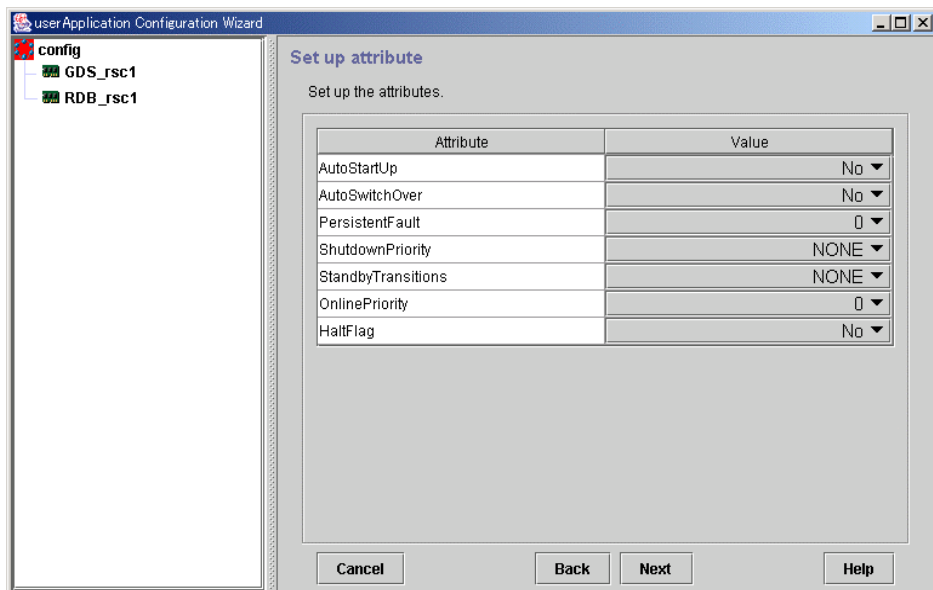
nodes are displayed.

Selected SysNode :

Nodes that use a cluster application as the operation system.

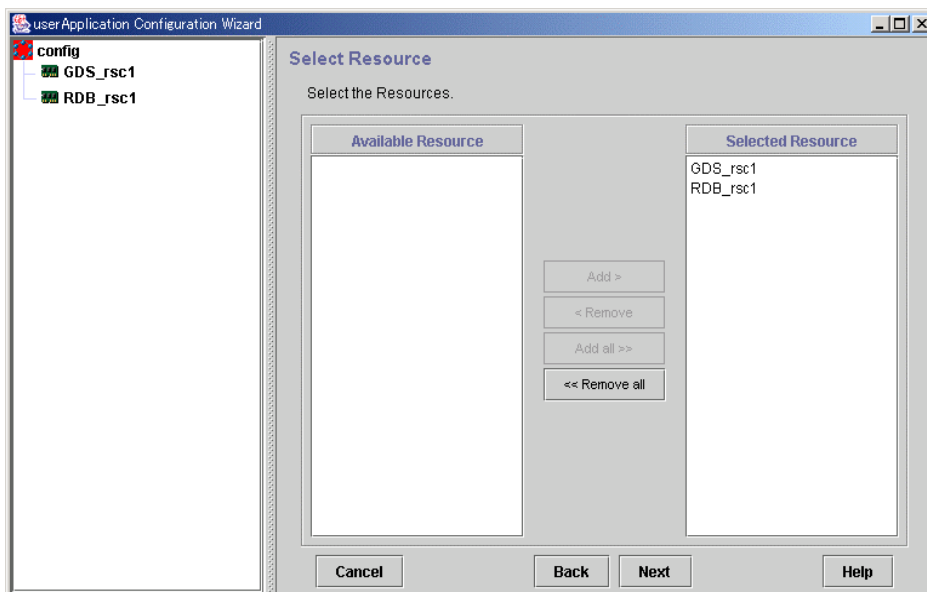


4. Set up the attribute of the cluster application.
On the “Set up attribute” screen, set up the attribute of the cluster application.

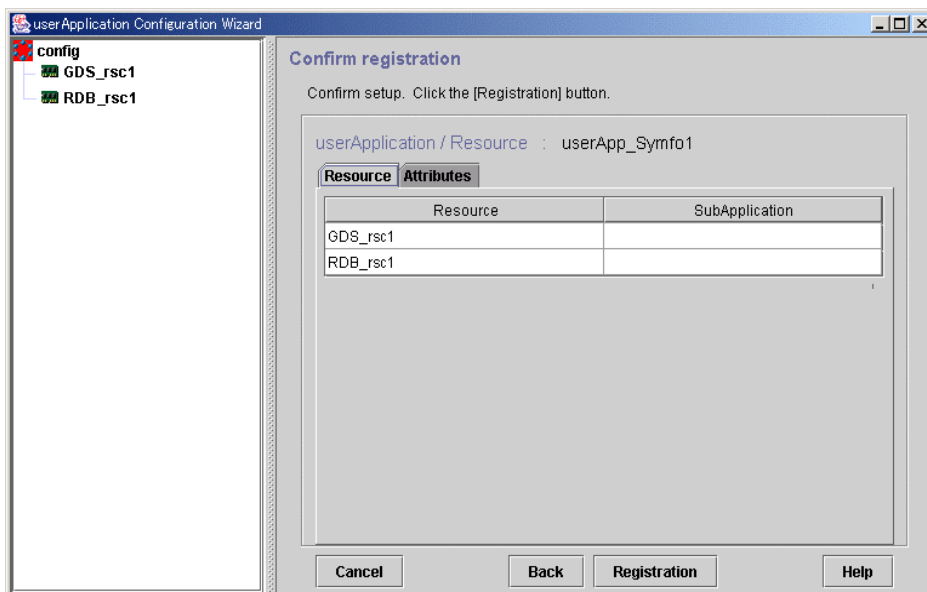


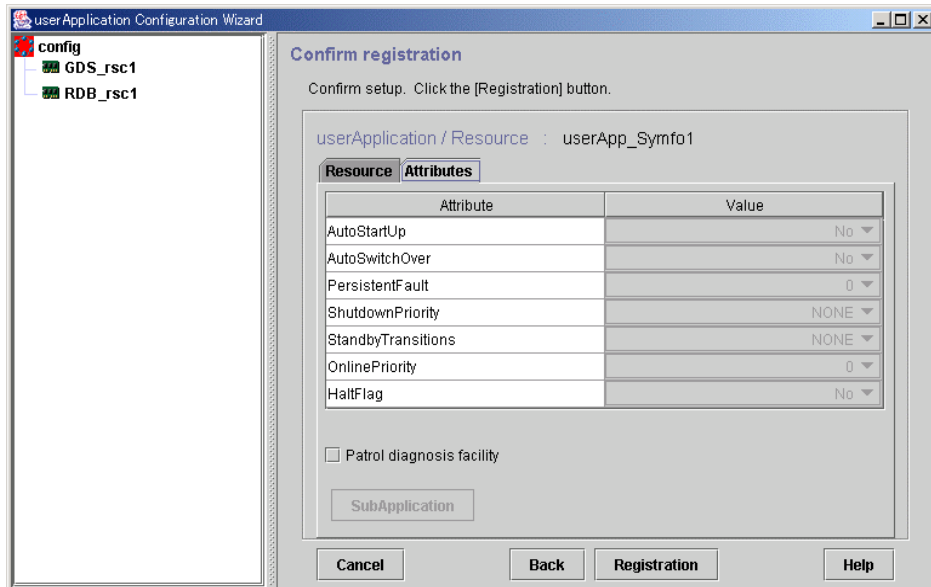
For details on each attribute, see 6.6.5 "Explaining the Attributes".

5. Select a resource to be used in the cluster application.
On the “Select subApplication” screen, set up a resource in the cluster application.
Select a disk resource for the cluster application from the “Available Resource” list and then add it to the “Selected Resource” list.



6. Confirm/register the registration information for the cluster application.
 On the " Confirm registration " screen, if the settings are correct, click the "Registration" button to register the settings.





When operating on an N:1 standby system, keep the top menu of userApplication Configuration Wizard displayed because the dependency of the cluster applications will subsequently be set up.

17.3.11 Setting Up Exclusive Relationships Between Cluster Applications

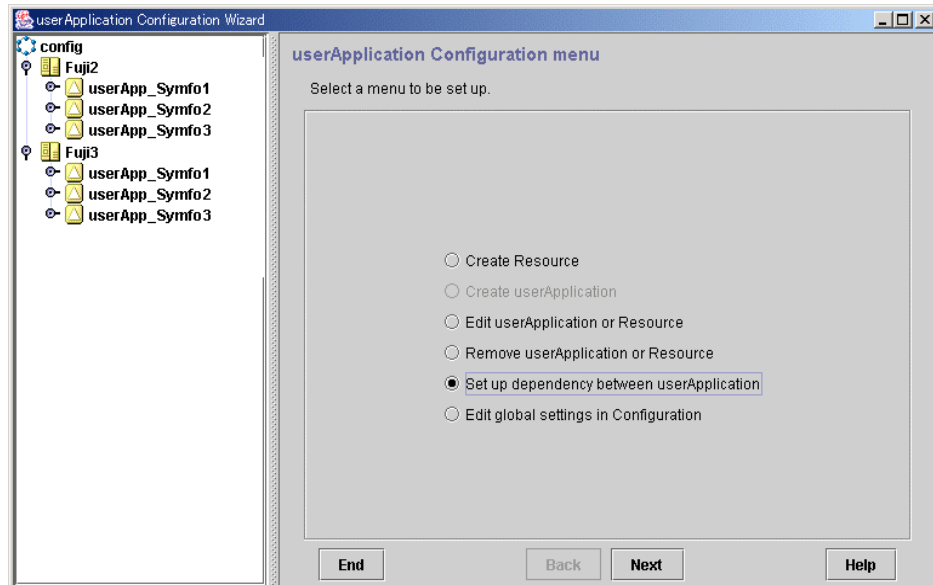
To enable operation on an N:1 standby system, set up and register exclusive relationships between cluster applications according to the following steps.

- **Set up exclusive relationships between cluster applications**

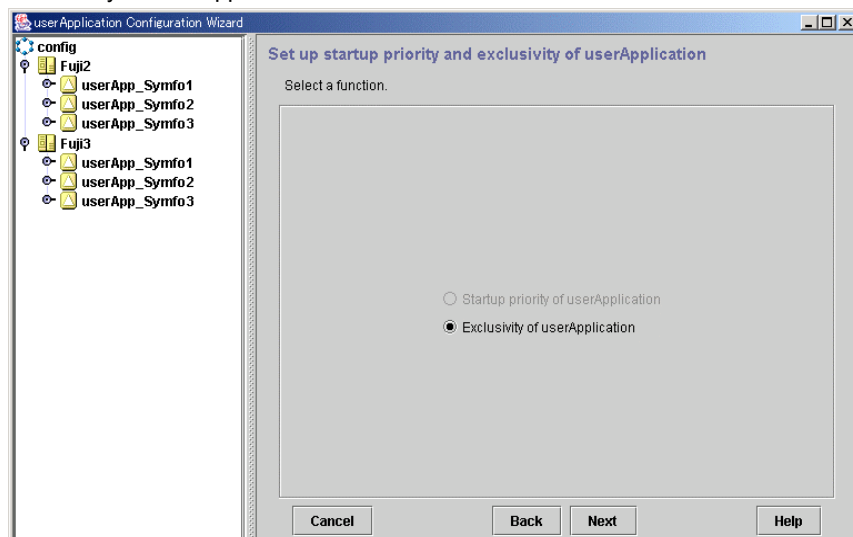
Open the "userApplication Configuration Wizard" screen.

- ◆ **Procedure**

1. Start the cluster application dependency setup screen.
Select *Set up dependency between userApplication* on the top menu of userApplication Configuration Wizard and then set up the cluster application dependency.

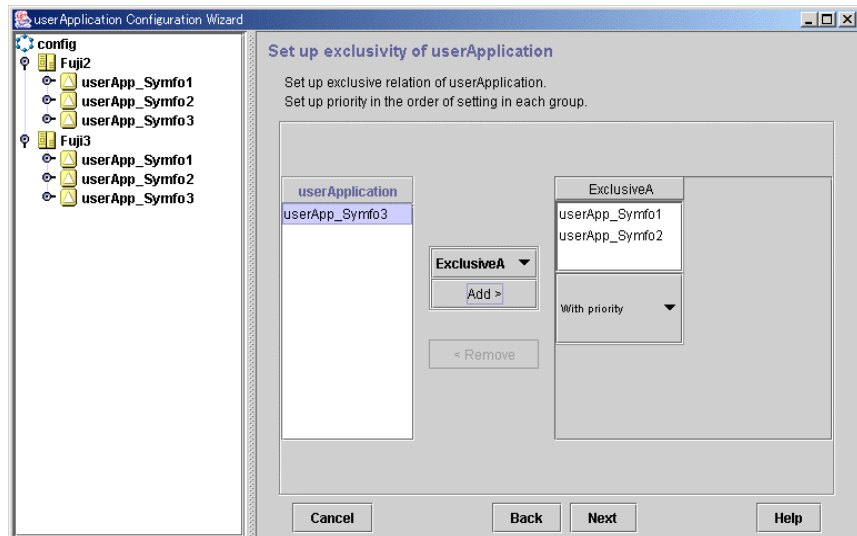


2. Set up the exclusive relationships between cluster applications.
 - 1) Select the *Exclusivity of userApplication* menu on "Set up startup priority and exclusivity of userApplication."



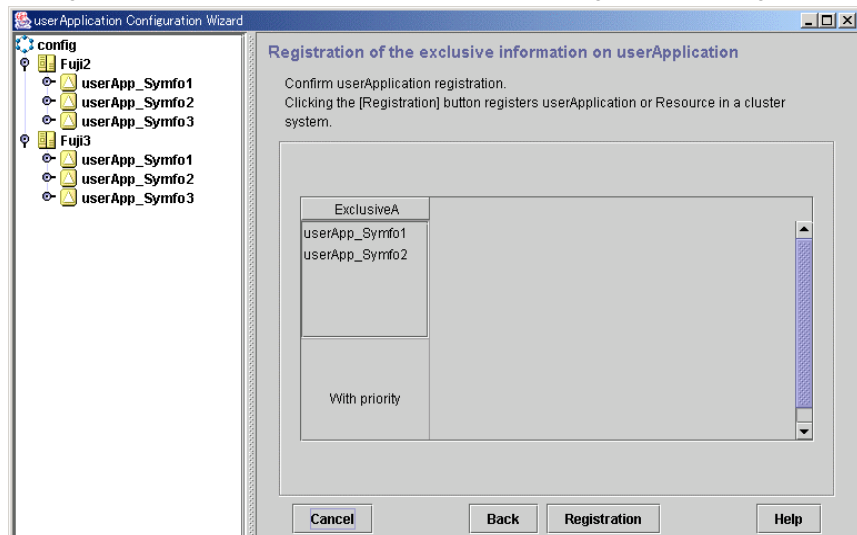
- 2) Set up exclusive relationships.

Set up exclusive relationships between cluster applications on the "Set up exclusivity of userApplication" screen.



3) Confirm/register exclusive relationships.

On the "Registration of the exclusive information on userApplication" screen, if the settings are correct, click the "Registration" button to register the settings.



3. Exit userApplication Configuration Wizard.

Click the "End" button on the "userApplication Configuration Wizard" screen to return to the "Global Cluster Services" screen.

17.3.12 Starting a Cluster Application

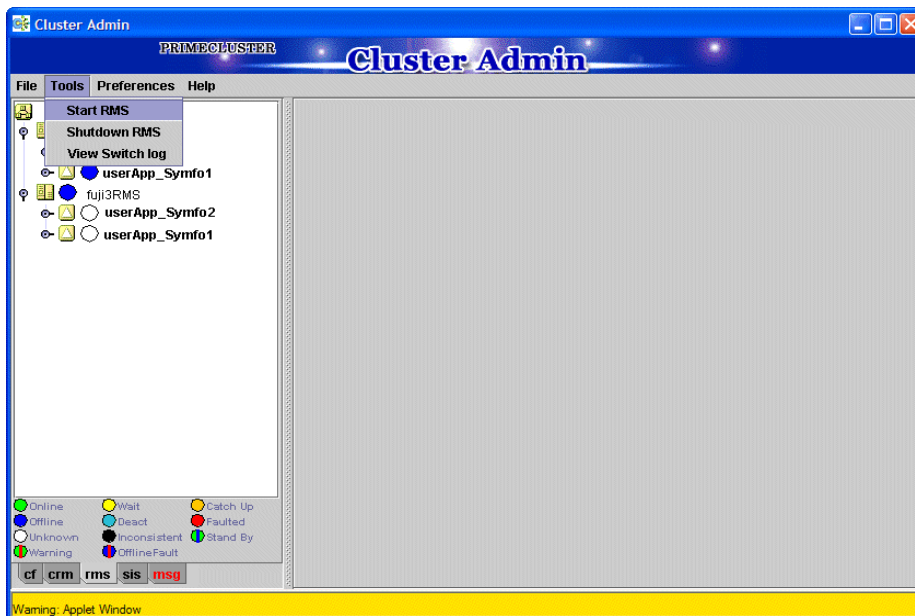
To enable hot standby operation, you need to start the cluster application first according to the following steps:

◆ **Procedure**

1. Display the "Cluster Admin" screen.
Select *Cluster Admin* screen from the "Global Cluster Services" screen.
2. Start RMS.
Click the "rms" tab on the "Cluster Admin" screen to display the RMS main window. Then, select the "Tool - Launch RMS" menu.
3. Start the cluster application.
For details on how to start a cluster application, see 7.2.2.1 "Starting a Cluster Application".

4. Confirm the starting message.
The Symfoware starting message will be output to the message log file of each node.
Confirm that the cluster application is normally started.

Cluster Admin screen



17.3.13 Checking the Operation

Once a cluster application startup has been done, you can operate the cluster application. Users are recommended to confirm that the environment setup is properly done, and the cluster application is normally running by causing failover and built-in.

17.4 Failover Maintenance and Management

This section explains the maintenance and management of a system for hot standby operation as follows:

- Changing System Files
- Changing to Scalable Log Operation
- Changing the Scalable Log Environment

17.4.1 Changing System Files

The types of system files, the operations for changing each system file, and the status of the operable RDB systems are shown below:

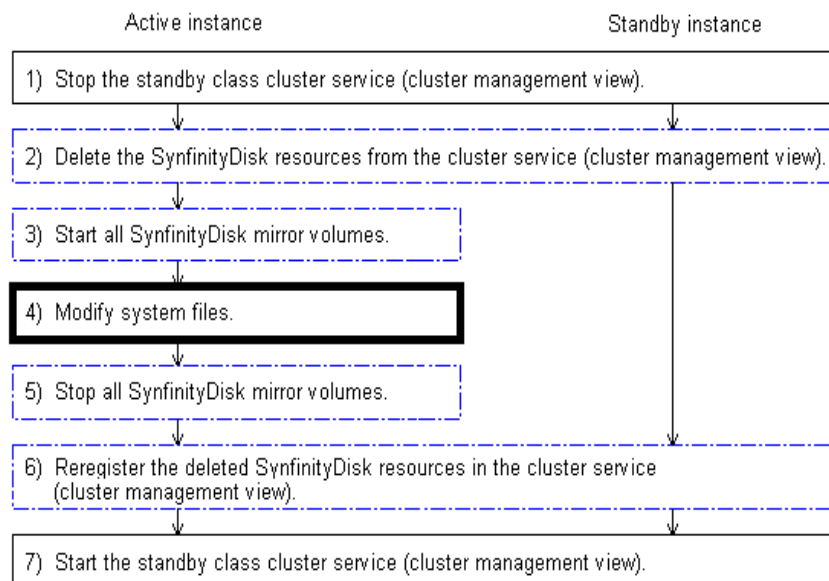
File	Modification operation	RDB state	
		Startup	Stop
RDB dictionary	Reorganization	×	○
	Allocation of additional area	×	○
	Increasing the size	×	○
RDB directory file	Increasing the size	×	○
Log management file	Change of location	×	○
Temporary log file	Setting value change (recovery log size, BI log area size, AI log area size, and transaction entry count)	×	○
	Media change (regeneration)	×	○
Archive log file	Addition	○	○
	Deletion	×	○

○ : Executable
 × : Not executable

To make modifications other than adding an archive log file, you need to stop the RDB system first. In fact, the ongoing operations should be stopped completely.

■ Flow of the system file change procedure

The flow of the main procedure for changing the system files is shown below. The portions shown by broken lines indicate the procedure to take when the system file to be changed is allocated to GDS.



◆ Procedure

1. Stop the cluster application for maintenance.
Stop the cluster application, in which the RDB system is registered, by using the “-d” option of the “hvutil(1M)” command.
2. Activate the Gds resource.
Activate the Gds resource by using the CRM main window of Cluster Admin or executing the “clstartsc(1M)” command.
3. Change the system files.
Change the system files.
4. Deactivate the Gds resource.
Deactivate the Gds resource by using the CRM main window of Cluster Admin or executing the “clstopsc(1M)” command.
5. Cancel the maintenance stop for the cluster application.
Cancel the maintenance stop for the cluster application by using the RMS main window of Cluster Admin or the “-a” option of the “hvutil(1M)” command.
6. Start the cluster application.
Start the cluster application by using the RMS main window of Cluster Admin or executing the “hvswitch(1M)” command.



See

For details on GDS, see the “*PRIMECLUSTER Global Disk Services Configuration and Administration Guide*.”

17.4.1.1 Procedure for changing the RDB dictionary

■ Reallocation

An empty area may be generated within the system table of the RDB dictionary when the database definition change is repeated. In this case, the area for the system table can be used effectively by reallocating the area within the system table.

Apply the following procedure for the active RDB system:

◆ **Procedure**

1. Stop the cluster application for maintenance.
Use the “-d” option of the “hvutil(1M)” command.
2. Confirm that the RDB has been stopped normally.
A message indicating that RDB has been stopped will be output to the message log file of each node in which the RDB is allocated.
3. Activate the Gds resource.
4. Acquire the save data for the RDB dictionary and the RDB directory file.
Save the RDB dictionary and the raw device of the RDB directory file by executing the “dd” command in the event of a failure during reconfiguration.
5. Start the RDB.
Use the “rdbstart” command.
6. Set up the rules for using the RDB dictionary reference/update suppression.
Use the “-rrw” option and the “-z” option of the “rdbtr” command.
7. Reconfigure the RDB dictionary.
Use the “-r” option of the “rdbgcdic” command.
 - If processing ends normally, go to Step 12.
 - If processing ends abnormally (due to insufficient memory), go to Step 8.
 - If processing ends abnormally (due to an input or output failure, or other failures) go to Step 9.
8. Set aside enough memory.
9. Execute reconfiguration of the RDB dictionary again.
 - If processing ends normally, go to Step 12.
 - If processing ends abnormally (due to insufficient memory), go to Step 8.
 - If processing ends abnormally (due to an input or output failure, or other failures), go to Step 10.
10. Stop the RDB.
Use the “rdbstop” command.
11. Correct the errors.
12. Restore the RDB dictionary and the RDB directory file from the saved data.
Execute the “dd” command. Return to Step 5.
13. Cancel the rules for using reference/update suppression of the RDB dictionary.
Use the “-rrw” option and the “-z” option of the “rdbtr” command.
14. Stop the RDB.
Use the “rdbstop” command.
15. Start the RDB. (Operation check)
Use the “rdbstart” command.
16. Stop the RDB. (Operation check)
Use the “rdbstop” command.
17. Deactivate the Gds resource.
18. Cancel the maintenance stop for the cluster application.
Use the RMS main window of Cluster Admin or the “-a” option of the “hvutil(1M)” command.
19. Start the cluster application.
Use the RMS main window of Cluster Admin or execute the “hvswitch(1M)” command.
20. Acquire the saved data for the RDB dictionary.
Use the “rdbdmpdic” command.
21. Restart the operation.

■ **Estimating the expandability of the RDB dictionary**

The size of the RDB dictionary area can become insufficient in the course of database operation. If this occurs, operation stops, so it is necessary to comprehend the situation to cope with the

situation in advance. Thus, after the database definition has been changed, acquire the activity ratio of the RDB dictionary. Based on the information find the changes in the activity ratio and then predict the expandability by executing the "rdbprdic" command. For details on how to specify the "rdbprdic" command, see the "rdbprdic" command page.

The output format of the "rdbprdic" command is explained as follows:

◆ Output format of the "rdbprdic" command

Based on the information that is output by executing the "rdbprdic" command, determine whether to allocate additional RDB dictionary or expand capacity.

The output format of the "rdbprdic" command is shown below:

```

$ rdbprdic

Database space  : RDB[[ SYSTEMD[IC
Device         : /dev/FJ[SVm[phd/r[ds[sk/m[phd2048s6      ①
Size          : 10240 K                                ②
Static allocate size
  total       : 5120 K                                  ③
Dynamic allocate size
  total       : 3072 K                                  ④
Free size
  total       : 2048 K                                  ⑤
System table used rate
  max        : 80 % ( 1024 K)                          ⑥ ⑦
  total      : 60 % ( 8192 K)                          ⑧ ⑨

```

- ① Name of raw device on which the RDB dictionary was created
- ② Total size of the RDB dictionary (unit: kilobytes)
- ③ Size allocated to system tables with the rdbprdic command (unit: kilobytes)
- ④ Total size added to system tables with the rdbprdic command (unit: kilobytes)
- ⑤ Amount of unused RDB dictionary space (unit: kilobytes)
- ⑥ Utilization rate of system table with the heaviest usage in the RDB dictionary
- ⑦ Size of system table with the heaviest usage in the RDB dictionary (unit: kilobytes)
- ⑧ Utilization rate of total system table area
- ⑨ Total size of all system tables (unit: kilobytes)

● Approximate standard for additional allocation and capacity expansion

Based on the maximum activity ratio (output format [6]) of the system table output with the "rdbprdic" command and the activity ratio of the entire RDB dictionary, you can determine whether to allocate additional RDB dictionary or expand capacity. An approximate standard for judgment is given here.

If the database is defined or deleted frequently, much free space might be included in the system table. So you need to reallocate the RDB dictionary first. If the result of reallocation is one of the following, you can allocate RDB dictionary or expand capacity.

If the area activity ratio ([6]) of a certain system table is large, you need to allocate RDB dictionary or expanding capacity.

- If the activity ratio ([8]) of the entire RDB dictionary is small, allocate RDB dictionary.
- If the activity ratio ([8]) of the entire RDB dictionary is great, expand capacity.

■ Additional allocation

If, as a result of estimating the expandability of the RDB dictionary, you determine that the area of a certain system table is insufficient, it will be necessary to allocate an additional RDB dictionary. Upon allocating the additional RDB dictionary, the proportion of free space in each system table must be equalized by allocating an additional system table area and then distributing that area appropriately for each system table.

You need to allocate an additional RDB dictionary for the operating RDB system according to the

following procedure.

◆ **Procedure**

1. Stop the cluster application for maintenance.
Stop the cluster application, in which the RDB system is registered, by using the “-d” option of the “hvutil(1M)” command.
2. Confirm that the RDB has been stopped normally.
A message indicating that the RDB has been stopped will be output to the message log file of each node in which the RDB is allocated.
3. Acquire the save data of the RDB dictionary and the RDB directory file.
To guard against the occurrence of an error during additional allocation, save the RDB dictionary and raw device of the DRB directory file.
Save the RDB dictionary and the raw device of the RDB directory file.
4. Allocate the additional RDB dictionary.
Use the “-a” option of the “rdbaldic” command.
 - If the processing ends normally, go to Step 7.
 - If the processing ends abnormally, go to Step 5.
5. Correct the errors.
6. Restore the RDB dictionary and the RDB directory file from the save data.
Execute the “dd” command. Return to Step 4.
7. Start the RDB. (Operation check)
Use the “rdbstart” command.
8. Stop the RDB. (Operation check)
Use the “rdbstop” command.
9. Cancel the maintenance stop for the cluster application.
Use the RMS main window of Cluster Admin or the “-a” option of the “hvutil(1M)” command.
10. Start the cluster application.
Use the RMS main window of Cluster Admin or the “hvswitch(1M)” command.
11. Acquire the saved RDB dictionary data.
Use the “rdbdmpdic” command.
12. Restart the operation.

■ **Capacity expansion**

As a result of estimating the expandability of the RDB dictionary, if you determine the area of the entire RDB dictionary is insufficient, you need to increase the capacity. First, prepare a new raw device with large space. Then, copy the RDB dictionary to the raw device and set up the device name in RDBDIRSPACE in the RDB-configured parameter file of the operating or standby RDB system.

You need to expand capacity for the operating RDB system according to the following procedure:

◆ **Procedure**

1. Stop the cluster application for maintenance.
Stop the cluster application, in which the RDB system is registered, by using the “-d” option of the “hvutil(1M)” command.
2. Confirm that the RDB has stopped normally.
A message indicating that the RDB has stopped will be output to the message log file of each node in which the RDB is allocated.
3. Acquire the saved RDB dictionary data and the RDB directory file.
Save the RDB dictionary and the raw device of the RDB directory file by executing the “dd” command.
4. Prepare a new raw device and increase the capacity of the RDB dictionary.

Increase the capacity of the RDB dictionary by using the “-a” option and the “-e” option of the “rdbaldic” command.

- If processing ends normally, go to Step 7.
- If processing ends abnormally, go to Step 5.

5. Correct the errors.
6. Restore the RDB dictionary and the RDB directory file from the saved data.
Execute the “dd” command. Return to Step 4.
7. Start the RDB. (Operation check)
start the RDB.
8. Stop the RDB. (Operation check)
Use the “rdbstop” command.
9. Cancel the maintenance stop for the cluster application.
Use the RMS main window of Cluster Admin or the “-a” option of the “hvutil(1M)” command.
10. Start the cluster application.
Use the RMS main window of Cluster Admin or execute the “hvswitch(1M)” command.
11. Acquire the saved RDB dictionary data.
Use the “rdbdmpdic” command.
12. Restart the operation.

17.4.1.2 Procedure for changing the RDB directory

■ Estimating the expandability of the RDB directory file

Additional RDB directory files for the user log group are automatically allocated in the course of database operation. However, when the memory has been exhausted, additional allocation is disabled, and RDB directory file areas might become insufficient. If this occurs, operation stops. Since it is necessary to comprehend the situation in advance to allow you to cope with such an error, you need to acquire the activity ratio of the RDB directory file and estimate the expandability.

Output the active ratio of the RDB directory file area by using the “r” option of the “rdbprdic” command. For details on how to specify the “rdbprdic” command, see the “rdbprdic” command page.

The output format of the “rdbprdic” command is explained below:

◆ Output format of “rdbprdic” command

Determine whether the capacity of the RDB directory file should be expanded based on the information output by the “rdbprdic” command.

The output format of the “rdbprdic” command is shown below:

```

$ rdbprdic -r

Directory file space
Device       : /dev/FJ5Vnphd/rdsk/nphd2048s7      ①
Size        : 102400K                          ②
Allocate size
  total     : 2048 K                            ③
Free size
  total     : 100352K                          ④
Used rate
  total     : 1 % ( 16 K)                      ⑤ (⑥)

```

- ① Name of raw device on which the RDB directory file was created
- ② Total size of the raw device (unit: kilobytes)
- ③ Size allocated to the raw device for the RDB directory (unit: kilobytes)
- ④ Amount of unused raw device size (unit: kilobytes)
- ⑤ Utilization rate of RDB directory file
- ⑥ Amount of RDB directory file space used (unit: kilobytes)

- **Approximate standard of expansion opportunity**

If the value of the unused size ([4]) of the raw device is small, the capacity of the RDB directory file might become insufficient. However, this will not occur if the activity ratio of the RDB directory file ([5]) is small.

- **Capacity expansion**

As a result of estimating the expandability of the RDB dictionary file, if you determine the area of the entire RDB dictionary file is insufficient, you need to increase the capacity. First, prepare a new raw device with large space. Then, copy the RDB dictionary to the raw device and set up the device name in RDBDIRSPACE in the RDB-configured parameter file of the operating or standby RDB system.

You need to expand capacity for the operating RDB system according to the following procedure. Note that the RDBDIRSPACE setting should be done on the operating and standby RDB system.

- ◆ **Procedure**

1. Stop the cluster application for maintenance.
 - Stop the cluster application in which the RDB system is registered, by using the “-d” option of the “hvutil(1M)” command.
2. Confirm that the RDB has stopped normally.
 - A message indicating that the RDB has stopped will be output to the message log file of each node in which the RDB is allocated.
3. Activate the Gds resource.
4. Acquire the data saved from the RDB directory file.
 - Save the raw device of the RDB directory file prior to attempting capacity expansion by executing the “dd” command.
5. Restore the RDB directory file to the capacity expansion destination.
 - Restore the to the raw device by executing the “dd” command.
 - If processing ends normally, go to Step 7.
 - If processing ends abnormally, go to Step 6.
6. Correct the errors. Return to Step 4.
7. Set up RDBDIRSPACE included in the RDB configuration parameter file.
 - Using the “vi” editor, change the absolute path name of RDBDIRSPACE on the active

and standby RDB systems, to the name of the raw device of the capacity expansion destination.

8. Start the RDB. (Operation check)
Use the "rdbstart" command to start the RDB.
9. Stop the RDB. (Operation check)
Execute the "rdbstop" command.
10. Deactivate the Gds resource.
11. Cancel maintenance stop for the cluster application.
Use the RMS main window of Cluster Admin or the "-a" option of the "hvutil(1M)" command.
12. Start the cluster application.
Use the RMS main window of Cluster Admin or execute the "hvswitch(1M)" command.
13. Restart the operation.

■ Estimating the expandability of the RDB directory file for a user log group

Additional RDB directory files for the user log group are automatically allocated in the course of database operation. However, when the memory has been exhausted, additional allocation is disenabled, and RDB directory file areas might become insufficient. If this occurs, operation stops. It is necessary to comprehend the situation in advance to allow you to cope with such an error.

Since it is necessary to comprehend the situation in advance to allow you to cope with such an error, you need to acquire the activity ratio of the RDB directory file for a user log group and estimate the expandability.

Output the active ratio of the RDB directory file area by using the "V" option and the "g" option of the "rdbscldir" command. For details on how to specify the "rdbscldir" command, see the "rdbscldir" command page.

The output format of the "rdbscldir" command is explained below:

◆ Output format of "rdbscldir" command

Determine whether the capacity of the RDB directory file for a user log group should be expanded based on the information output by the "rdbscldir" command.

The output format of the "rdbscldir" command is shown below:

```

$ rdbscldir -V -g grp1

RDB[[ rdbscldir DATE:2001/07/21 TIME: 16/30/31

LogGroup          Status  DBspace  Size(Used rate)  Directory file path
①                ②      ③        ④(⑤)            ⑥
grp1              normal  Exist    1024K( 23%)     /dev/FJ5Vmphd/rdisk/mphd2049s7

DBspace Information
Inventory control DB .DBSP_1
Inventory control DB .DBSP_2

```

- ① Registered log group name
- ② State of the RDB directory file for user log groups
normal: File can be used.
inhibit: Access to the file is disabled.
- ③ Indicates whether there is a database space the relevant log group is being used.
Exist: Such a space exists.
Not Exist: Such a space does not exist.
- ④ Size allocated to the raw device for the RDB directory files for user log groups (unit: kilobytes)
- ⑤ Utilization rate of the RDB directory file for user log groups
- ⑥ Path name of the RDB directory file for user log groups

- **Approximate standard for expandability**

The capacity of the RDB directory file might become insufficient under the following conditions:

- When the difference between the entire size of the allocated raw device and the size of the RDB directory file for a user log group ([4]) is small; and
- When the activity ratio ([5]) of the RDB directory file for user log group is high.

- **Capacity expansion of the RDB directory file for a user log group**

As a result of estimating the expandability of the RDB dictionary file, if you determine the area of the entire RDB dictionary file is insufficient, you need to increase the capacity. First, prepare a new raw device with large space. Then, copy the RDB dictionary to the raw device and set up the device name in RDBDIRSPACE in the RDB-configured parameter file of the operating or standby RDB system by using the “A” option and the “g” option of the “rdbscldir” command.

You need to expand capacity for the operating RDB system according to the following procedure:

- ◆ **Procedure**

1. Stop the cluster application for maintenance.
Stop the cluster application, in which the RDB system whose system file is to be changed is registered, by using the “-d” option of the “hvutil(1M)” command.
2. Confirm that the RDB has stopped normally.
A message indicating that the RDB has been stopped will be output to the message log file of each node in which the RDB is allocated.
3. Acquire the saved RDB directory file data for the user log group.
Save the raw device of the RDB directory file by executing the “dd” command.
4. Restore the RDB directory file for the user log group to the capacity expansion destination.
Restore the save data to the raw device by executing the “dd” command.
 - If processing ends normally, go to Step 6.
 - If processing ends abnormally, go to Step 5.
5. Correct the errors.
Return to Step 4.
6. Reregister the raw device as the creation destination path name of the RDB directory file for the user log group.
Use the “-A” option and the “-g” option of the “rdbscldir” command.
7. Confirm that the raw device has been correctly reregistered.
Use the “-V” option and the “-g” option of the “rdbscldir” command.
8. Start the RDB. (Operation check)
Execute the “rdbstart” command.
9. Stop the RDB. (Operation check)
Execute the “rdbstop” command.
10. Cancel the maintenance stop for the cluster application.
Use the RMS main window of Cluster Admin or the “-a” option of the “hvutil(1M)” command.
11. Start the cluster application.
Use the RMS main window of Cluster Admin or execute the “hvswitch(1M)” command.
12. Restart the operation.

17.4.1.3 Procedure for changing the log management file

- **Changing the allocation destination**

Changing the allocation destination of the log management file is one of the modifications of the

environment. You can change the allocation destination by executing the “rdblog” command. If the log management file and the temporary log file are created in the same raw device, Symfaware/RDB must have stopped normally.

For scalable log operation, change the allocation destination for the relevant log group. Take the following steps on the operating RDB system; You need to change the allocation destination for the operating RDB system according to the following procedure:

◆ Procedure

1. Stop the cluster application for maintenance.
Stop the cluster application, in which the RDB system is registered, by using the “-d” option of the “hvutil(1M)” command.
2. Confirm whether the RDB has stopped normally.
A message indicating that the RDB has been stopped will be output to the message log file of each node in which the RDB is allocated.
3. Activate the Gds resource.
4. Confirm the allocation destination of the temporary log file.
Use the “rdblog” command. Use the options as follows:
 - Other than scalable log operation: The “-V” option and the “-t” option
 - Scalable log operation: The “-V” option, “-t” option, and the “-g” option
5. Confirm the allocation destination of the archive log file.
Use the “rdblog” command. Use the options as follows:
 - Other than scalable log operation: The “-V” option and the “-a” option
 - Scalable log operation: The “-V” option, “-a” option, and the “-g” option
 Go to the following procedure:
 - Other than scalable log operation or in the case of a system log group: Go to Step 6.
 - Scalable log operation: Go to Step 7.
6. Specify a new allocation destination for the log management file in RDBLOGMANAGE of the RDB configuration parameter file.
7. Recreate the log management file.
Use the “rdblog” command. Use the options as follows:
 - Other than scalable log operation or in case of system log group: The “-l” option
 - User log group: The “-l” option, the “-r” option, and the “-g” option
8. Reregister all archive log files.
Use the “-A” option and the “-a” option of the “rdblog” command.
9. Confirm that all the archive log files have been registered normally.
Use the “rdblog” command. Use the options as follows:
 - Other than scalable log operation: The “-V” option and the “-a” option
 - Scalable log operation: The “-V” option, the “-a” option, and the “-g” option
 Go to Step 10 when the log management file and the temporary log file, which were created on the same raw device, are to be created on different raw devices or when the log management file and the temporary log file, which were created on different raw devices, are to be created on the same raw device.
In all cases other than the above, go to Step 11.
10. Reregister the temporary log file.
Use the “-A” option and the “-t” option of the “rdblog” command. Go to Step 12.
11. Recreate the temporary log file.
Use the “-G” option, “-t” option and “r” option of the “rdblog” command.
12. Confirm that the temporary log file has been correctly registered or created.
Use the “rdblog” command. Use the options as follows:

- Other than scalable log operation: The “-V” option and the “-t” option
 - Scalable log operation: The “-V” option, the “-t” option and the “-g” option
13. Start the RDB. (Operation check)
Execute the “rdbstart” command.
 14. Stop the RDB. (Operation check)
Execute the “rdbstop” command.
 15. Deactivate the Gds resource.
 16. Cancel the maintenance stop for the cluster application.
Use the RMS main window of Cluster Admin or the “-a” option of the “hvutil(1M)” command.
 17. Start the cluster application.
Use the RMS main window of Cluster Admin or execute the “hvswitch(1M)” command.
 18. Restart the operation.

17.4.1.4 Procedure for changing the temporary log file

■ Changing the setup value

You can avoid errors and improve performance by changing the volume of the recovery logs, the size of the temporary log file, and the number of transaction entries that were specified at temporary file creation. Use the “-U” option of the “rdblog” command.

You need to check the temporary log file status first.

For scalable operation, change the setup by specifying the log name with the “-g” option of the “rdblog” command.

Take the following steps on the operating RDB system.

◆ Procedure

1. Stop the cluster application for maintenance.
Stop the cluster application, in which the RDB system is registered, by using the “-d” option of the “hvutil(1M)” command.
2. Confirm that the RDB has stopped normally.
A message indicating that the RDB has stopped will be output to the message log file of each node in which the RDB is allocated.
3. Activate the Gds resource.
4. Confirm the status of the temporary log file.
Confirm that the status of the temporary log file (Status) is unused (---) by using the “-V” and “-t” option of the “rdblog” command. If the status indicates that it is being used (OPERATING), the RDB has not been stopped normally. In this case, first start the standby class service, stop the service again and then restart the operation from Step 2. If the status is abnormal (trouble), an error in the temporary log file is indicated. In such a case, restore the temporary log file.
5. Change the setup value of the temporary log file.
Use the “-U” option and “-t” option of the “rdblog” command. For information on how to change each value, see “RDB Operations Guide.”
6. Confirm that the attribute of the temporary log file has been changed normally.
Use the “-U” option and “-t” option of the “rdblog” command.
7. Start the RDB. (Operation check)
Use the “rdbstart” command.
8. Stop the RDB. (Operation check)
Execute the “rdbstop” command.
9. Deactivate the Gds resource.
10. Cancel the maintenance stop for the cluster application.

Use the RMS main window of Cluster Admin or the “-a” option of the “hvutil(1M)” command.

11. Start the cluster application.

Use the RMS main window of Cluster Admin or execute the “hvswitch(1M)” command.

12. Restart the operation.

■ Changing the medium

The load imposed on the raw devices can be distributed by creating a log index area, a BI log area, and an AI log area, which are specified when the temporary log files are created, in different raw devices. When the raw devices are to be changed, recreate the temporary log files. For this purpose, you need to prepare a new raw device first. Also, check the temporary log file status. Use the “-G” option, “-t” option, and “-r” option of the “rdblog” command to change the temporary log files.

Note and confirm the status of the temporary log file before changing the medium.

◆ Procedure

1. Stop the cluster application for maintenance.
Stop the cluster application, in which the RDB system is registered, by using the “-d” option of the “hvutil(1M)” command.
2. Confirm that the RDB has stopped normally.
A message indicating that the RDB has been stopped will be output to the message log file of each node to which the RDB is allocated.
3. Confirm the status of the temporary log file.
Confirm that the status of the temporary log file (Status) is unused (---) by using the “-V” option and the “-t” option of the “rdblog” command. If the status indicates that it is being used (OPERATING), the RDB has not been stopped normally. In this case, first start the standby class service, stop the service again and then restart the operation from Step 2.
If the status is abnormal (trouble), an error in the temporary log file is indicated. In such a case, restore the temporary log file.
4. Recreate the temporary log file.
Specifying the raw device of the change destination using the “-G” option, “-t” option, and “-r” option of the “rdblog” command.
5. Confirm that the temporary log file has been normally created.
Use “-V” option and “-t” option of the “rdblog” command.
6. Start the RDB. (Operation check)
Use the “rdbstart” command.
7. Stop the RDB. (Operation check)
Use the “rdbstop” command.
8. Cancel the maintenance stop for the cluster application.
Use the RMS main window of Cluster Admin or the “-a” option of the “hvutil(1M)” command.
9. Start the cluster application.
Use the RMS main window of Cluster Admin or execute the “hvswitch(1M)” command.
10. Restart the operation.

17.4.1.5 Procedure for changing the archive log file

■ Addition

You can add an archive log file even while the RDB system is running. You don't have to stop

the ongoing operations.

First, you need to prepare a raw device. Change the medium of the archive log files by using the “-U” option of the “rdblog” command.

For scalable log operation, specify a log group name by using the “-g” option of the “rdblog” command to change the medium.

You need to add an archive log file for the operating RDB system according to the following procedure:

◆ **Procedure**

1. Add the archive log file.
Specify a raw device by using the “-U” option and “-a” option of the “rdblog” command.
2. Confirm that the archive log file has been normally added.
Use the “-V” option and “-a” option of the “rdblog” command.

■ **Deletion**

You can delete unnecessary archive log files by using the “-D” option of the “rdblog” command.

For scalable log operation, specify a log group name using the “-g” option of the “rdblog” command to change the medium.

You need to delete unnecessary archive log files for the operating RDB system according to the following procedure:

◆ **Procedure**

1. Stop the cluster application for maintenance.
Stop the cluster application, in which the RDB system is registered, by using the “-d” option of the “hvutil(1M)” command.
2. Confirm that the RDB has been stopped normally.
A message indicating that the RDB has been stopped will be output to the message log file of each node in which RDB is allocated.
3. Activate the Gds resource.
4. Confirm the state of the archive log file.
Use the “-V” option and “-a” option of the “rdblog” command.
5. Save all archive log files.
Save all archive log files whose states (Status) are save wait (full), being used (using), and forcible switch (switch) in Step 3.
If an archive log file whose state (Status) is archive log error (inh) is included, it indicates that an error has occurred in the archive log file. Restore the archive log file before attempting to change the file.
6. Delete unnecessary archive log files.
Use the “-D” option and “-a” option of the “rdblog” command.
7. Confirm that the archive log file has been normally deleted.
Use the “-V” option and “-a” option of the “rdblog” command
8. Start the RDB. (Operation check)
Execute the “rdbstart” command.
9. Stop the RDB. (Operation check)
Execute the “rdbstop” command.
10. Deactivate the Gds resource.
11. Cancel the maintenance stop for the cluster application.
Use the RMS main window of Cluster Admin or the “-a” option of the “hvutil(1M)” command.
12. Start the cluster application.
Use the RMS main window of Cluster Admin or execute the “hvswitch(1M)” command.

13. Restart the operation.

17.4.2 Changing to Scalable Log Operation

Take the following steps to change from non-scalable log operation to scalable log operation:

1. Stop Symfoware/RDB
2. Edit an RDB configuration parameter file
3. Create a log group management file
4. Add a user log group



See

For details on how to add a user log group, see 17.3.6 “Creating the RDB Environment” and 17.4.3.1 “Adding a user log group”.

◆ Procedure

1. Stop the cluster application for maintenance.
Stop the cluster application, in which the RDB system is registered, by using the “-d” option of the “hvutil(1M)” command.
2. Confirm whether the RDB has stopped normally.
A message indicating that the RDB has been stopped will appear in the message log file for each node in which RDB is allocated.
3. Edit the RDB configuration parameter file.
To create a log group management file, specify the allocation destination of the log group management file in RDBLOGGOUPTMANAGE.
4. Create a log group management file.
Use the “-M” option of the “rdblog” command.
5. Add a user log group.
Execute the “rdblog” command.
6. Start the RDB. (Operation check)
Execute the “rdbstart” command.
7. Stop the RDB. (Operation check)
Execute the “rdbstop” command.
8. Cancel the maintenance stop for the cluster application.
Use the RMS main window of Cluster Admin or the “-a” option of the “hvutil(1M)” command.
9. Start the cluster application.
Use the RMS main window of Cluster Admin or execute the “hvswitch(1M)” command.
10. Restart the operation.



Note

The raw device of the log group management file allocation destination should not overlap a raw device in which existing RDB system resources (RDB dictionary, RDB directory files, database space, log management files, temporary log files, and archive log files) are allocated.

17.4.3 Changing the Scalable Log Environment

The addition of a user log group and the deletion of an existing user log group are one of the modifications of the scalable log environment.

To add or delete a user log group, execute the “rdbscldir” and the “rdblog” commands. For details on how to specify the “rdbscldir” and the “rdblog” command, see the “rdbscldir” and the “rdblog” command pages.

17.4.3.1 Adding a user log group

The procedure for adding a user log group is outlined below:

1. Stop Symfoware/RDB
2. Create a log management file for a user log group
3. Create a temporary log file for a user log group
4. Create an archive log file for a user log group
5. Create an RDB directory file for a user log group when adopting a scalable directory operation.



See

For details on how to add a user log group, see 17.3.6 “Creating the RDB Environment”.

17.4.3.2 Deleting a user log group

The procedure for deleting a user log group is outlined below:

1. Confirm and delete the database space that uses a user log group
2. Stop Symfoware/RDB
3. Delete the RDB directory file for the user log group when a scalable directory operation is being performed
4. Delete an archive log file for the user log group
5. Delete the temporary log file for the user log group
6. Delete the user log group
7. Confirm the user log group

◆ Procedure

1. Stop the cluster application for maintenance.
Stop the cluster application, in which the RDB system is registered, by using the “-d” option of the “hvutil(1M)” command.
2. Confirm the database space that uses a user log group.
 - Other than scalable directory operation: Use the “rdbprt” command.
 - Scalable directory operation: Use the “-V” option and the “-g” option of the “rdbscldir” command.
3. Delete the database space that uses a user log group.
Use the “rdbddlex” command.
4. Confirm that the RDB has stopped normally.
A message indicating that the RDB has stopped will be output to the message log file of each node in which the RDB is allocated.
5. In the case of scalable directory operation, delete the RDB directory file for the user log

group.

Use the “-D” option and “-g” option of the “rdbscldir” command.

6. Delete the archive file for the user log group.
Use the “-D” option, “-a” option, and “-g” option of the “rdblog” command.
7. Delete the temporary log file for the user log group.
Use the “-D” option, “-t” option, and “-g” option of the “rdblog” command.
8. Delete the user log group.
Use the “-D” option, “-l” option, and “-g” option of the “rdblog” command.
9. Start the RDB. (Operation check)
Execute the “rdbstart” command.
10. Stop the RDB. (Operation check)
Execute the “rdbstop” command.
11. Cancel the maintenance stop for the cluster application.
Use the RMS main window of Cluster Admin or the “-a” option of the “hvutil(1M)” command.
12. Start the cluster application.
Use the RMS main window of Cluster Admin or execute the “hvswitch(1M)” command.
13. Restart the operation.

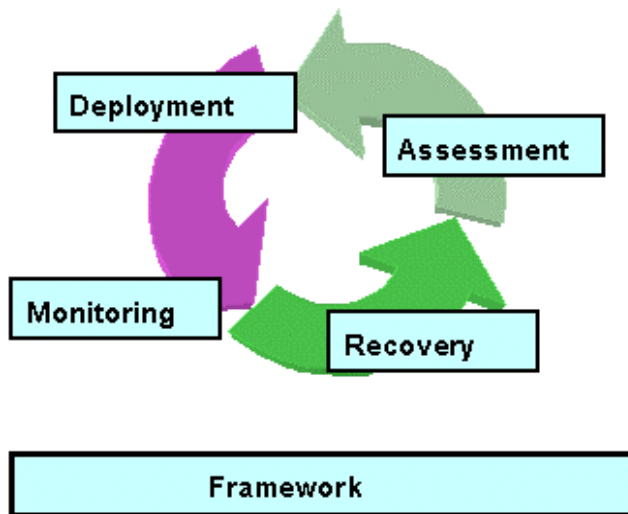
Chapter 18 Systemwalker CentricMGR

18.1 Functional Overview

Systemwalker CentricMGR is a software product that acts as the integrative infrastructure for the management of an information system. It provides life cycle management of IT resources such as networks, hardware, OS, applications, and users that consist of the system according to the policy based management.

■ Life cycle management

Systemwalker CentricMGR controls the life cycle of IT resources. It provides an effective operation management by categorizing the IT resources into the following 4 phases:



- **Deployment**

Refers to the phase in which IT resources and transactions are installed on the system and set up. The resources to be used for the information system are deployed and applied.

- **Monitoring**

Refers to the phase in which the performance of IT resources and failures are monitored.

- **Recovery**

Refers to the phase in which corrective action is taken in the event of a failure. Troubleshooting and recovery are performed.

- **Assessment**

Refers to the phase in which the stability of operation is evaluated. The service level is evaluated and analyzed from operation information of IT resources. Performance bottlenecks are detected, and capacity planning is done.

- **Framework**

The “framework” refers to the operation management infrastructure that is used to share information between the functions of the life cycle and to enable seamless functional cooperation. The framework collects the configuration information for the entire information system, such as the network, hardware, OS, applications and others, and maintains the integrated management of the configuration information.

18.1.1 Overview of Cluster System Support

Systemwalker CentricMGR enables the integrated management of a cluster system. Systemwalker CentricMGR monitors that the entire cluster system is normally running. Also, Systemwalker CentricMGR eliminates downtime caused by node-down, and provides a highly reliable system by performing quick recovery at failover.

18.1.2 Supported Modes

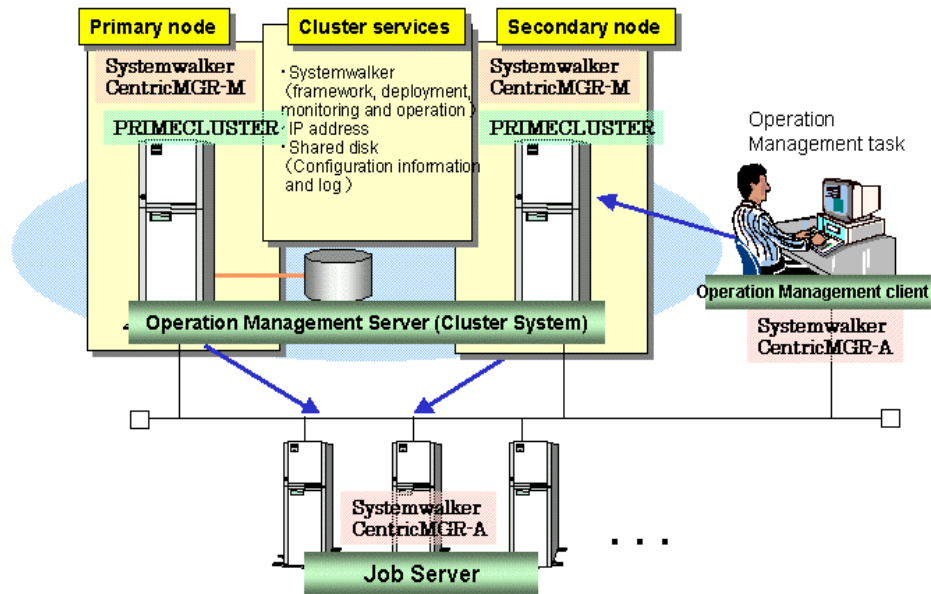
Systemwalker CentricMGR supports a 1:1 standby operation mode using IP address takeover. For details, see the Table 11-1 "PRIMECLUSTER Product List."

18.2 Standby class

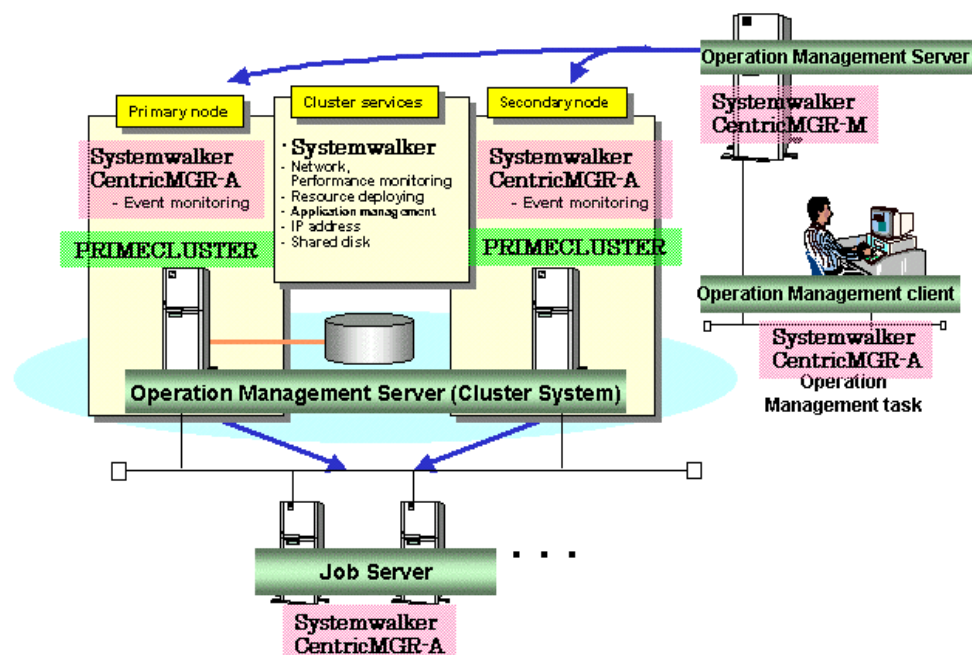
18.2.1 System Configuration

Systemwalker CentricMGR enables a user to use an operation management server, section management server, or job server in a cluster system. The system configuration of using each type of server is illustrated below:

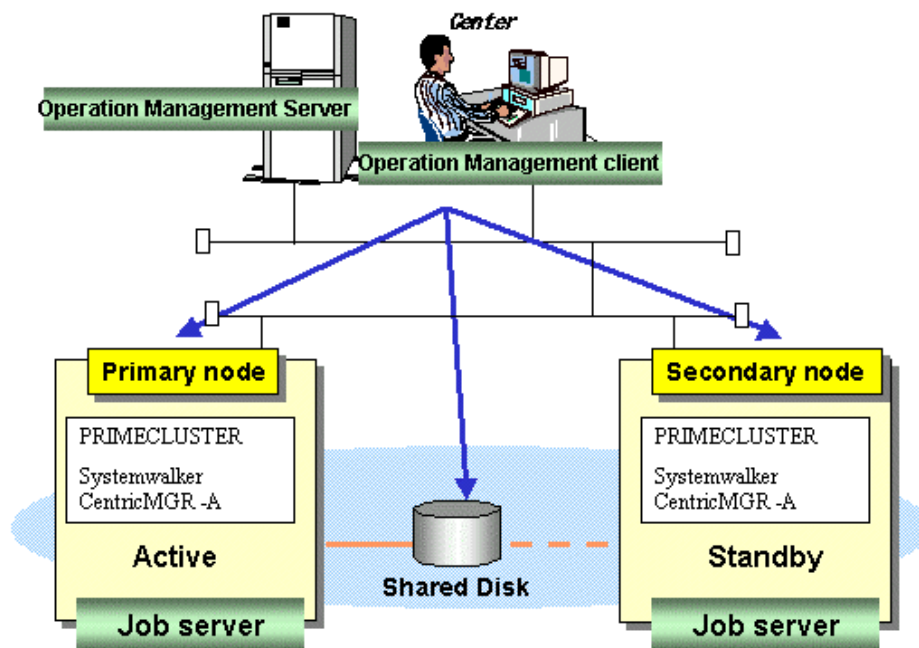
■ Operation Management Server



■ Section Management Server



■ Job server

**18.2.2 Environment Setup**

For details, see the "Systemwalker CentricMGR Customization Guide."

Chapter 19 Systemwalker OperationMGR

19.1 Functional Overview

Systemwalker OperationMGR supports the following functions:

■ Automation of routine system operation and management

By installing Systemwalker OperationMGR, routine system operation and management can be automated as follows:

● Automatic control of power on/off

Power to the server can be automatically turned on/off. Power on/off of the server is conducted according to a time schedule that is defined in advance. Also, power to the server can be automatically turned on when a client starts.

Note that this function is enabled only for Solaris OE servers that are running Systemwalker OperationMGR UNIX version.

● Automatic activation of the services/applications

When the server is booted, services and applications are activated in the order in which they are registered. You can change the services and applications on any given day.

Note that this automatic activation of the services can be used only when the connected server is for the Windows version.

● Automatic execution of a routine batch job

If you register the times and dates at which a routine batch job is run, the routine batch job is automatically executed according to that schedule. If an error occurs in a routine batch job, it can be corrected automatically without the intervention of the operator.

● Scheduling file compression and transfer

The commands used for file compression and transfer are provided as job-associated commands. If you register these files with the job scheduler, you can execute these commands by scheduling.

■ Monitoring and operating a job on the screen

By installing Systemwalker OperationMGR, you can confirm the job execution status at a glance because the job status is displayed in different colors. You can monitor jobs running not only on a single system but also those running on multiple systems.

Moreover, you can operate a job while monitoring its status.

■ Control of job execution according to the system operation and status

Systemwalker OperationMGR enables you to control the job execution, as follows:

● Control of job execution environment

Jobs can be executed efficiently by adjusting the job execution environments such as the execution order and the number of jobs that can be executed simultaneously.

● Job execution with networked servers

Jobs can be executed on any server connected to the network.

● Control of networked clients

You can provide clients that are connected over the network with controls such as power-on and file transfer.

19.1.1 Overview of Cluster System Support

Systemwalker OperationMGR provides high availability batch jobs and enables a high-reliability transaction system by running on a cluster system.

19.1.2 Supported Modes

Systemwalker OperationMGR supports the following operation modes:

- 1:1 standby
- N:1 standby
- Two-node mutual standby

For details, see the Table 11-1 "PRIMECLUSTER Product List".

19.2 Standby Classes

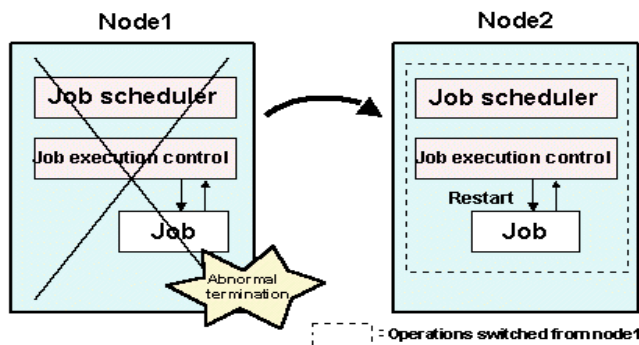
19.2.1 System Configuration

Systemwalker OperationMGR enables the entire servers, schedule server, execution server, and schedule server + execution server to operate on a cluster system in 1:1 standby, N:1 standby, or two-node mutual standby operation mode.

Each cluster system configuration when the entire Systemwalker OperationMGR servers are set up in a cluster configuration is outlined below:

■ 1:1 standby

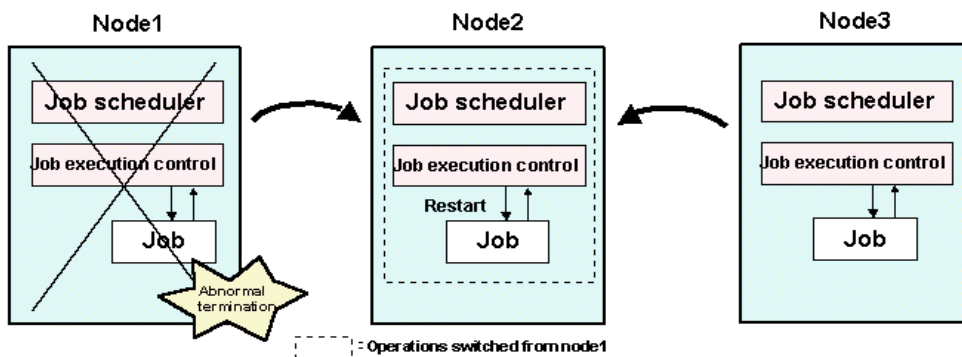
The following figure shows an example in which node 1 operates as an active and node 2 operates as a standby:



If an error occurs in node 1, ongoing operations are switched to node 2.

■ N:1 standby

The following figure shows an example in which node 1 and node 3 are active and node 2 operates as a standby. The following shows an example where an error occurs on node 1. Even if an error occurs on node 3, ongoing operations are switched to node 2.

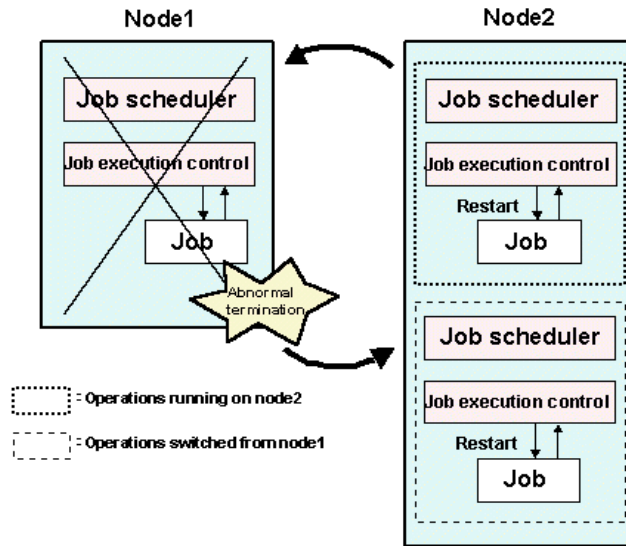


If an error occurs on node 1 or node 3, ongoing operations are switched to node 2. If errors occur on two or more nodes, the transaction running on the node on which the error occurred first is taken over by the standby node. However, the transactions of the nodes on which the

errors occurred subsequently will not be taken over.

■ **Two-node mutual standby**

The following figures shows an example in which node 1 and node 2 execute their transactions while each operates as a standby for the other. The following shows an example where an error has occurred on node 1. If an error occurs on node 2, ongoing operations are switched to node 1.



For details, see the “Systemwalker OperationMGR Installation Guide.”

19.2.2 Environment Setup

For details, see the “Systemwalker OperationMGR Installation Guide.”

Chapter 20 Systemwalker WebMGR

20.1 Functional Overview

Systemwalker WebMGR provides the functions that are required for supporting the integrated management of a Web system, ranging from SLA operation to the marketing strategies.

- **Monitoring, evaluation, and prediction of the Web system service level**
By accessing services such as HTTP/HTTPS, CGI, ASP, Servlet, and JSP to collect information on the throughput and the operation status, you can monitor, evaluate, and predict the service levels.
From the user's point of view, you can collect and evaluate service level information such as response/page download performance and the operating ratio.
- **Analysis of the state of use**
You can optimize business performance because customer needs can be comprehended and Web page configurations can be evaluated by analyzing the usage of the Web server.
- **Revision monitoring**
You can check for invalid corrections or revisions of the contents on the Web server.

20.1.1 Overview of Cluster System Support

Systemwalker WebMGR supports 1:1 standby and provides commands and state transition procedures to be built on a cluster system.

20.1.2 Supported Modes

For details, see the Table 11-1 "PRIMECLUSTER Product List."

20.1.3 Notes

None

20.2 Standby Classes

20.2.1 System Configuration

For details, see “15.7 Operation in a Cluster Environment” in the “Systemwalker WebMGR” manual.

20.2.2 Notes

None

Appendix A PRIMECLUSTER System Design Worksheets

A.1 Worksheet Purpose

The PRIMECLUSTER System Design Worksheets allow you to determine necessary parameters before you configure the PRIMECLUSTER system. Filling out all items in the worksheet will enable you to proceed smoothly with the PRIMECLUSTER installation work.

The worksheets consist of the following:

- **Overall Design Worksheet**

This worksheet is used to design basic items for the PRIMECLUSTER system.

- **CE Instruction Worksheet**

This worksheet compiles necessary information for installation and configuration, and is used to communicate instructions to the Fujitsu technician (CE).

- **Cluster Installation Environment Setup Worksheet**

This worksheet is used to configure an environment before the installation of Solaris OE, PRIMECLUSTER, and other required and related software, and the configuration of the PRIMECLUSTER system using Web-Based Admin View.

For the installation of each software product, you can select either installing on each node using an installation script or using the One Shot Installer to automatically install software on all nodes.



[See](#)

For details on each installation method, see the *"PRIMECLUSTER Installation Guide."*

This section identifies the worksheet for preparing and organizing necessary information for each installation method. This worksheet will enable a smooth installation.

- **Kernel Parameter Worksheet**

This worksheet allows you to determine the fundamental PRIMECLUSTER values for estimating the kernel parameters. After installing the Solaris OE software and PRIMECLUSTER packages, configure the new values for the kernel parameters, as necessary.

- **Cluster Configuration Worksheet**

This worksheet organizes the necessary items for configuring the PRIMECLUSTER system with Web-Based Admin View. Using this worksheet and determining the parameter values beforehand will enable you to smoothly set up operations using Web-Based Admin View.

- **Cluster Application Configuration Worksheets**

When building a cluster application, use these worksheets to design how the application should operate. There are individual worksheets for configuring RMS, GFS, GLS, GDS, and cluster applications.

- **Cluster Application Setting Worksheet**

This worksheet is used for configuring cluster applications and resources.

A.2 Notes on Worksheet Creation

Note the following points when creating PRIMECLUSTER design worksheets.

- Specify appropriate values in the blank sections of each design sheet. For instructions on specifying each item, see the point explanations.
- Items marked with are selection items. Select one of the items written in the box.
- Items marked with are selection items. You can select multiple items written in the box.
- Different values can be specified depending on the model in which PRIMECLUSTER is to be installed. Read the point explanations before specifying values.

A.3 Overall Design Worksheet

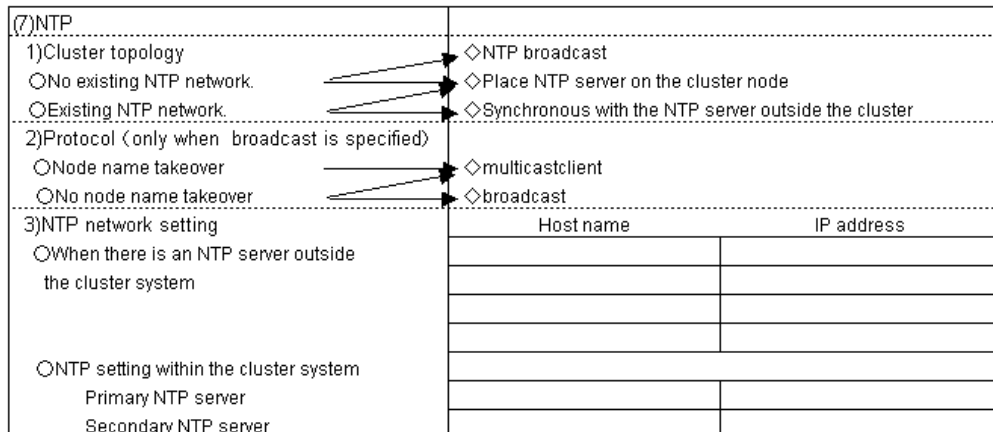
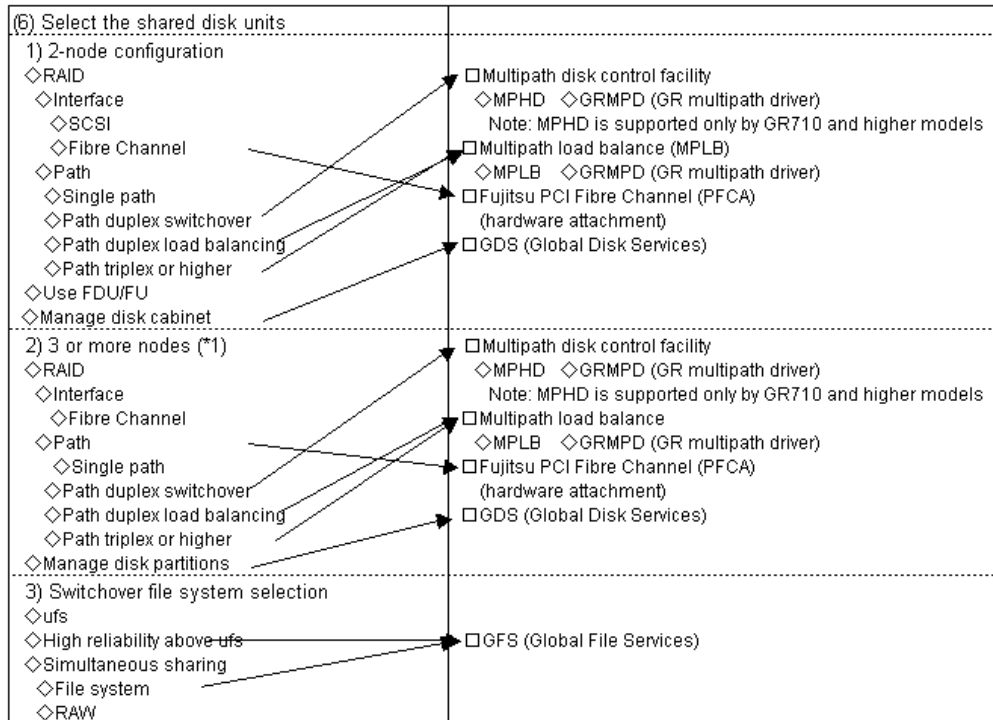
Select the operation mode of the cluster system.



See

See A.11 "System Design Examples" when determining values for the setup items in the Overall Design Worksheet.

Cluster :	System requirement	Selective product/function/configuration
Cluster system topology		
(1) Installation objective		<input type="checkbox"/> Standby operation
<input type="checkbox"/> Improvement of availability		<input type="checkbox"/> 1:1 standby
<input type="checkbox"/> Improvement of performance		<input type="checkbox"/> Mutual standby
(2) Operation after failover		<input type="checkbox"/> N:1 standby
<input type="checkbox"/> Degenerate operation enabled		<input type="checkbox"/> Cascade operation
<input type="checkbox"/> Degenerate operation disabled		<input type="checkbox"/> Scalable operation (RAC only)
(3) Intersystem shared DB		
<input type="checkbox"/> Provided		
<input type="checkbox"/> Not provided		
(4) Node count		
<input type="checkbox"/> 2 nodes		
<input type="checkbox"/> 3 or more nodes		
(5) Web-Based Admin View operation modes		
<input type="checkbox"/> 2-layer model		<input type="checkbox"/> 1 PC required
<input type="checkbox"/> Integrated console management		<input type="checkbox"/> RC2000 *Required on the PC
<input type="checkbox"/> 3-layer model		<input type="checkbox"/> Operation management server and 1 PC required
<input type="checkbox"/> Integrated console management		<input type="checkbox"/> RC2000 *Required on the management server or PC



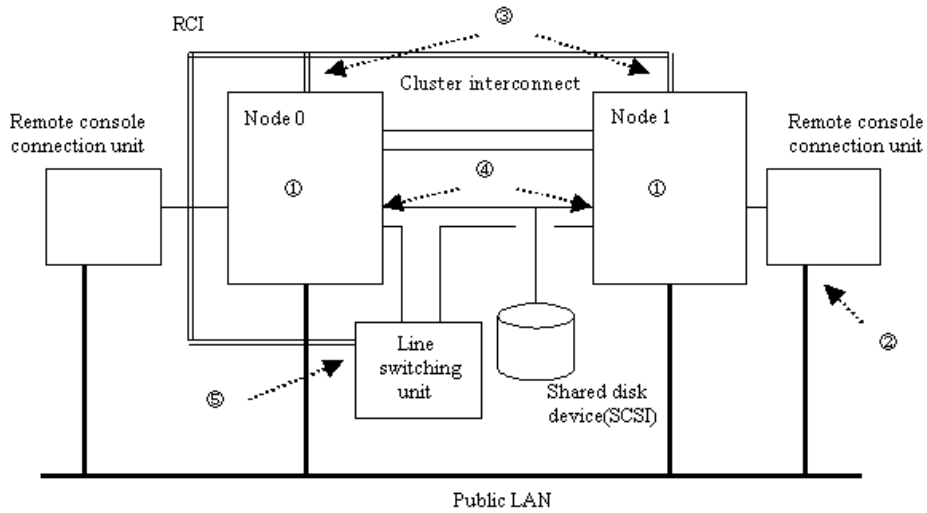
*1: For the configuration with three or more nodes, the available shared disks are limited to disk array units that have an FC interface. In addition, the disk array units must be connected to all nodes.

In this chart, ISV products (Veritas, Emulex, EMC PowerPath) should be mentioned.

A.4 CE(FE for North America) Instruction Worksheet

The CE Instruction Worksheet indicates information required for hardware installation for a Fujitsu customer engineer (CE). This worksheet is also used for specifying information that was configured by the CE.

Fill in the necessary information, and submit to the CE.



(1) Configuration of each machine model

· PRIMEPOWER 800

(Basic Cabinet)

(Expansion Cabinet)

Partition name (node name)	Partition name (node name)

· PRIMEPOWER 1000

(Basic Cabinet)

(Expansion Cabinet)

Partition name (node name)	Partition name (node name)

· PRIMEPOWER 2000

(Basic Cabinet)

(Expansion Cabinet1)

<p style="text-align: center;">Partition name (node name)</p> <div style="border: 1px solid black; height: 150px; margin: 5px 0;"> <p>.....</p> <p>.....</p> <p>.....</p> <p>.....</p> <p>.....</p> <p>.....</p> </div>	<p style="text-align: center;">Partition name (node name)</p> <div style="border: 1px solid black; height: 150px; margin: 5px 0;"> <p>.....</p> <p>.....</p> <p>.....</p> <p>.....</p> <p>.....</p> <p>.....</p> </div>
---	---

(Expansion Cabinet2)

(Expansion Cabinet3)

<p style="text-align: center;">Partition name (node name)</p> <div style="border: 1px solid black; height: 150px; margin: 5px 0;"> <p>.....</p> <p>.....</p> <p>.....</p> <p>.....</p> <p>.....</p> <p>.....</p> </div>	<p style="text-align: center;">Partition name (node name)</p> <div style="border: 1px solid black; height: 150px; margin: 5px 0;"> <p>.....</p> <p>.....</p> <p>.....</p> <p>.....</p> <p>.....</p> <p>.....</p> </div>
---	---

(2) Node name	(3) IP address of remote console (4) RCI address of node (PRIMEPOWER only)	(5) RCI address of line switching unit (Only for PRIMEPOWER when line switching unit is used)	(6) SCSI initiator ID (PRIMEPOWER only)
[00]	___* ___* ___* ___* Default		6
[01]	___* ___* ___* ___* Default		7
[02]	___* ___* ___* ___* Default		6
[03]	___* ___* ___* ___* Default		7
[04]	___* ___* ___* ___* Default		6
[05]	___* ___* ___* ___* Default		7
[06]	___* ___* ___* ___* Default		6
[07]	___* ___* ___* ___* Default		7

[08]	__* __* __* __		6
	Default		
[09]	__* __* __* __		7
	Default		
[10]	__* __* __* __		6
	Default		
[11]	__* __* __* __		7
	Default		
[12]	__* __* __* __		6
	Default		
[13]	__* __* __* __		7
	Default		
[14]	__* __* __* __		6
	Default		
[15]	__* __* __* __		7
	Default		

□ Shared RAID unit				
RAID No. :	Model:			
(7) LU configuration	LU number	RAID group	RAID level	
	0	0		
	1	1		
	2	2		
	3	3		
	4	4		
	5	5		
	6	6		
	7	7		
	8	8		
	9	9		
	10	10		
	11	11		
	12	12		
	13	13		
	14	14		
	15	15		
	16	16		
	17	17		
	18	18		
	19	19		
	20	20		
	21	21		
	22	22		
	23	23		
	24	24		
	25	25		
	26	26		
	27	27		
	28	28		
	29	29		
	30	30		
	31	31		
32	32			
(8) Controller	Host name/IP address, net mask		SCSI adapter to be connected	
			Server to be connected	Slot number
	Controller __	__ . __ . __ . __ ()		
	Controller __	__ . __ . __ . __ ()		
	Controller __	__ . __ . __ . __ ()		
Controller __	__ . __ . __ . __ ()			

The worksheet should be for each RAID unit. For example, if there are 4 units, you need to prepare 4 worksheets.

Instructions for fill-in

- (2) and (3) are information for CE.
- CE needs to set up (4), (5), and (6).
- RAID 0, 1, or 5 is filled in for how RAID level is stored in the disk in the LU configuration. Normally, RAID5 is filled in.
- When FibreChannel is used, it is not necessary to fill in "SCSI adapter to be connected" of (8) Controller.

A.5 Cluster Installation Environment Worksheet

The Cluster Installation Environment Worksheet organizes items related to installation and initial configuration of Solaris OE software, PRIMECLUSTER, required and related software. Create the Cluster Installation Environment Worksheet and the Solaris OE Installation Worksheet.

The Cluster Installation Environment Worksheet contains initial configuration items related to the entire PRIMECLUSTER system. If you are using the One Shot Installer, respond to queries from One Shot Installer. If you are not using One Shot Installer, configure a system on each node according to the information specified here.

In the Solaris OE Installation Worksheet, specify the configuration items for installing Solaris OE software on each node including the installation server when using One Shot Installer.

Cluster system name:		Cluster Installation Environment Worksheet			
Node name:					
Settings		Notes			
(1) Software to be installed	<input type="checkbox"/> Optional software	<input type="checkbox"/> RAID Disk Driver (HDDV): Depends on hardware configuration <input type="checkbox"/> Fibre Channel driver: Depends on hardware configuration <input type="checkbox"/> Multi-path disk control (MPHD) <input type="checkbox"/> Multipath load balance (MPLB) <input type="checkbox"/> GRMPD (GR multipath driver)			
(2) Version of Solaris	◇8 ◇9	Use the same version on all nodes.			
(3) Partition information		Logical path	Size	Configuration should be synchronized on all nodes	
	/				
	swap				
	/usr				
	/var				
	/opt				
(4) System locale	◇ C ◇ Ja ◇ Other ()				
(5) Time zone	◇ Japan ◇ Other ()				
(6) Node information	Node name IP MAC				
(7) Web-Based Admin View					
	Node name	IP	Access I/F	Http port number	RMI port number
Primary management server	_____	_____	_____	_____	_____
Secondary management server	_____	_____	_____	_____	_____

■ **Solaris OE Installation Worksheet**

Specify information needed for installing the Solaris OE software in nodes. Refer to the worksheet created here when installing various software programs to each node individually and when building the installation server.

In a cluster system, the items other than the host names and IP addresses of the individual nodes have the same values in all nodes.



For details of each item, see the "Solaris X Information Library."

Setting item	Setting value	Remarks
Select a Language	0) English	This item is displayed only for the English version of Solaris. If the environment is not a Japanese language environment, select 0 (English).
Select a Locale	0) USA - English (ASCII only)	This item is displayed only for the English version of Solaris. If the environment is not a Japanese language environment, select 0 (English).
What type of terminal are you using?		Set this item based on the terminal emulator. Select vt52 for using Windows telnet.
Host Name		Specify the node name of each node recorded on the initial setup worksheet.
Network Connectivity	Yes	Specify Yes.
Primary Network Interface	_____	Specify the network interface connected to the public LAN.
IP address		Specify the node name of each node recorded on the initial setup worksheet.
Name Service	None	Specify None.
Subnets	Yes/No	Specify Yes if the public LAN is part of the subnet.
Netmask	____.____.____.____	If Yes is selected for Subnets, set the net mask of the subnet.
Time Zone		Specify the default time zone.
Data and Time		The initial setup tool matches the date and time of other nodes to the date and time set for the installation server. Set the correct date and time.
Solaris Interactive Installation	Initial	Select Initial.
Allocation Client Services?	Continue	Select Continue.
Select Languages	ja, _____	Select the required language. For a Japanese language environment, you also need to select ja.
Select Software	Entire Distribution	Select Entire Distribution.
Select Disks		Select the disk on which Solaris is installed.
Preserve Data?	Continue	Select Continue.
Automatically Layout File Systems?	Manual Layout	Select Manual Layout. Set so that the disk slice configuration of all nodes is the same.
Customize Disk		Select Manual Layout, so the disk slice configuration is synchronized on all nodes.
Mount Remote File System?	Continue	Select Continue.
Reboot After Installation?	Auto Reboot	Select Auto Reboot to automatically restart after installation is done.

A.6 Kernel Parameter Worksheet

When you build the PRIMECLUSTER system, the default values for the kernel parameters of the Solaris OE may be inadequate. The Kernel Parameter Worksheet shows the kernel parameter values used for PRIMECLUSTER. If the values have been set in /etc/system, you need to edit the values (Defined values + kernel parameter values used for PRIMECLUSTER). If the values have not been set, you need to set the values (Solaris OE default values + the kernel parameter values used for PRIMECLUSTER.)

The kernel parameter values differ depending upon:

- CF configuration
- RMS configuration
- Using GFS
- Using GLS



See

- For details of the kernel parameters and instructions on changing parameter values, see "Solaris System Administration" in *"Solaris X System Administrator Collection Vol. 1."*
- For information on the default values of the Solaris OE, see the *"Solaris Tunable Parameters Reference Manual."*



Note

- The values used by products and user applications that operate in the PRIMECLUSTER system must also be included in the kernel parameter values.
- To enable values that have been changed, you must restart the system after the installation.
- If a kernel parameter value is already maximized, the change will not be added to the system.

A.6.1 CF Configuration

■ When the resource database is used

The table below shows the kernel parameter values that are required in the CF configuration when the resource database is used.

Kernel parameter	Recommended value/minimum value	Comments (parameter description)
semsys:semifn_semmni	20	Value required for resource database
semsys:semifn_semmns	30	Value required for resource database
semsys:semifn_semmnu	30	Value required for resource database Note: Set same value as the calculated semsys:semifn_semmns value.
shmsys:shminfo_shmmax	4194304 *	Value required for resource database
shmsys:shminfo_shmseg	30	Value required for PRIMECLUSTER system
shmsys:shminfo_shmmni	30	Value required for resource database

*

Change the shmsys:shminfo_shmmax value required by the cluster system to the value shown below.

Estimate the number of cluster system resources according to the following equation:

Number of resources = (a) + (b)

(a) Number of disks in shared system devices x (number of shared nodes + 1) x 2

(b) Total number of local disks (number of local disks in all cluster configuration nodes)

Value required for resource database = 1048576 + 2776 x number of resources

— If the value calculated above is larger than the installation default value of PRIMECLUSTER (4194304):

shmsys:shminfo_shmmax = Value required for resource database

- If the value calculated above is smaller than the installation default value of PRIMECLUSTER (4194304):
shmsys:shminfo_shmmax = 4194304
(The installation default value of PRIMECLUSTER is used.)



Note

For system expansion, if you increase the number of nodes and logical disks, you need to re-estimate the resources and restart each node in the cluster system.

■ RCI monitoring agent setup

The table below shows values for the kernel parameters that are required for RCI monitoring agent setup.

To set up RCI monitoring agent on PRIMEPOWER 800, 900, 1000, 1500, 2000, or 2500, you must set the monitoring timeout duration via SCF/RCI, according to the number of partitions (including partitions that are not in the cluster).

Kernel parameter	Recommended value/minimum value	Remarks (parameter description)
FJSVscf2:scf_rdctrl_sense_wait	**	Monitoring timeout time via SCF/RCI (for PRIMEPOWER 800, 1000, and 2000)
FJSVscf3:scf_rdctrl_sense_wait	**	Monitoring timeout time via SCF/RCI (for PRIMEPOWER 900, 1500, and 2500)

**

Calculation of the monitoring timeout duration

Since the monitoring timeout duration is set in microsecond units, use the value obtained by multiplying the value calculated below by 1000000.

2 or fewer partitions: 2 seconds

3 or more partitions: (1 + 0.5 x number of partitions) seconds

Example) If PRIMEPOWER 1000 has two partitions

FJSVscf2:scf_rdctrl_sense_wait = 2 seconds = 2000000 μs

Example) If PRIMEPOWER 1500 has three partitions

FJSVscf3:scf_rdctrl_sense_wait = 1 + 0.5 x 3 = 2.5 seconds = 2500000 μs

A.6.2 RMS Configuration

The table below shows the values of the kernel parameters required for the RMS configuration.

Kernel parameter	Recommended value/minimum value	Comments (parameter description)
msgsys:msgmax	16384	
msgsys:msgtql	65535	
msgsys:msgmnb	4194304	
msgsys:msgmni	8192	



Note

If you uninstall the RMS package from /etc/system by executing the "pkgrm(1M)" command, you need to restart the system after uninstallation.

A.6.3 Using GFS

If you plan to use a GFS Local File System, you must adjust the kernel parameters again.



See

See "9.2.3 Tuning Parameters" in the *"PRIMECLUSTER Global File Services Configuration and Administration Guide."*

A.6.4 Using GLS

The table below shows values for the kernel parameters required for when Global Link Services (GLS) is used.

Kernel parameter	Recommended value/minimum value	Comments (parameter description)
shmsys:shminfo_shmmax	5120	Maximum size of a shared memory segment
shmsys:shminfo_shmmni	2	Maximum number of shared memory segments
semsys:seminfo_semmni	1	Maximum number of semaphore identifiers
semsys:seminfo_semmns	1	Maximum number of semaphores in the system

The system default values are necessary for the other kernel parameters.

The values shown above are necessary regardless of whether the GLS environment is set up.

A.7 Cluster Configuration Worksheet

The Cluster Configuration Worksheet is required building a cluster.

Use this worksheet to organize the items before using Web-Based Admin View to set up the PRIMECLUSTER system.



See

For information on the setup items for this worksheet, see Chapter 5 "Building a Cluster." Also see the A.11.1 "Cluster Building Worksheet" in the A.11 "System Design Examples."

Item		Setting	Remarks	
Shared disk unit: Type 1	Interface			
	Path			
	File system selection			
Shared disk unit: Type 2	Interface			
	Path			
	File system selection			
NTP	Operation mode			
	Protocol (only when broadcast is specified)			
	Network configuration	External NTP	Host name	
			IP address	
			Host name	
	NTP server settings in cluster	Primary NTP	Host name	Set either "External NTP servers" or "NTP server settings in clusters."
			IP address	
Secondary NTP		Host name		
		IP address		
Operation management topology	Web-Based Admin View operation mode			
	Public LAN layer			
	Primary management server IP			
User group	Secondary management server IP			
	Group name	User name		
	◇ wvroot			
	◇ clroot			
	◇ cladmin			
		◇ clmon		

Cluster name					
Node information	CIP	Number of subnets			
		Subnet IP			
		Net mask			
	Node 1	Node name (uname -n)			
		CF node name			
		Public LAN	Network interface name	IP address	
				Net mask	
				Gateway	
				weight	Node weight (priority if Split-Brain occurs) used by SF Note: See setup policy for live priority if Split-Brain occurs.
		Cluster interconnect	Path 0 NIC name		
			Path 1 NIC name		
		RCCU	IP address	(Only when RCCU is used)	
		Node in CF quorum set		◇ [Yes] ◇ No	Do not change the default setting.
	Node 2	Node name (uname -n)			
		CF node name			
		Public LAN	Network interface name	IP address	
				Net mask	
				Gateway	
				weight	Node weight (priority if Split-Brain occurs) used by SF Note: See setup policy for live priority if Split-Brain occurs.
		Cluster interconnect	Path 0 NIC name		
		Path 1 NIC name			
RCCU		IP address	(Only when RCCU is used)		
Node in CF quorum set		◇ [Yes] ◇ No	Do not change the default setting.		
CF remote service usage		<input type="checkbox"/> cfcop (CF file copy) <input type="checkbox"/> cfsh (CF remote command execution)			
IP interconnect setup		◇ [Not used] ◇ Used (IP interconnect count) IP interface:			
CIP		◇ [Used by RMS] ◇ Not used by RMS Suffix:			
Cluster resource management	Hardware device to be registered in the resource database		<input type="checkbox"/> Network device *1 <input type="checkbox"/> Line switching unit *2 <input type="checkbox"/> Disk unit *3		
			*1) Required when public LAN takeover is used *2) Required when line takeover is used *3) Required when GDS and GFS are used		
Shutdown facility (SF)	Node elimination method		<input type="checkbox"/> RCI <input type="checkbox"/> RCCU		
			RCI monitoring agent Console monitoring agent		

Note: Values enclosed in brackets ([]) are default values.



See

For information on the "Live priority setting policy when Split-Brain occurs" in the Remarks column for weight, see "Live Priority" in 5.2.2 "Setting Up the Shutdown

Facility."

A.8 Cluster Application Configuration Worksheets

Use the Cluster Application Configuration Worksheet to organize the items before building a cluster application.

The following worksheets are required for building a cluster application.

- A.8.1 GFS Local File System Setup Worksheet
- A.8.2 GLS Setup Worksheet
- A.9 GDS Setup Worksheets
- A.10 Cluster Application Setup Worksheets



See

For information on the setup items for this worksheet, see Chapter 6 "Building Cluster Applications."

A.8.1 GFS Local File System Setup Worksheet

If you plan to use a GFS (Global File Services) Local File System, use the GFS Local File System Setup Worksheet to organize the input items beforehand.



See

For information on the setup items in this worksheet, see 6.3 "Initial GFS Setup." Also see A.11.2 "GFS Local File System Setup Worksheet" in A.11 "System Design Examples."

Item		Setting
GFS Local File System settings		Device name
		Mount point
		Device name
		Mount point

A.8.2 GLS Configuration Worksheet

If you will be using Global Link Services (GLS), use the GLS Configuration Worksheet to organize the input items beforehand.

This section describes the worksheet settings for the following typical duplexing modes:

- NIC switching mode (logical IP takeover)
- Fast switching mode



See

- For configuration instructions for other duplexing modes, see "Appendix B Examples of Setting Up" in the *"PRIMECLUSTER Global Link Services Configuration and Administration Guide: Redundant Line Control Function"* and "Chapter 3 Configuration" in the *"PRIMECLUSTER Global Link Services Configuration and Administration Guide: Multipath Function."*
- For information on the items in this sheet, see the explanation at the bottom of the sheet and 6.1 "Initial GLS Setup." Also see A.11.3 "GLS Setup Worksheet" in A.11 "System Design Examples."

■ NIC Switching Mode (Logical IP Takeover)

Item		Setting	
GLS settings	Switching mode	◆ NIC switching mode (logical IP takeover) ◇ Fast switching mode	
	Takeover virtual interface name		
	Takeover virtual IP address (or host name)		
	Subnet mask		
	Node name (1)		
	Configuration information	Virtual interface name	
		Primary physical interface name	
		Secondary physical interface name	
		Physical IP address (or host name)	
	Monitoring destination information	Logical IP address (or host name)	
		IP address (or host name) of primary monitoring destination	
	Monitoring destination information	IP address (or host name) of secondary monitoring destination	
		Optional function	◇ Disable ◇ Enable Set to standby NIC Local MAC address ()
	Node name (2)		
	Configuration information	Virtual interface name	
		Primary physical interface name	
		Secondary physical interface name	
		Physical IP address (or host name)	
	Monitoring destination information	Logical IP address (or host name)	
		IP address (or host name) of primary monitoring destination	
Monitoring destination information	IP address (or host name) of secondary monitoring destination		
	Optional function	◇ Disable ◇ Enable Set to standby NIC Local MAC address ()	

[Setup items]

- Switching mode

Specify a redundant operation type for GLS; Fast switching mode, NIC (Network Interface Card) switching mode, or RIP mode.

Add d (logical IP takeover of the NIC switching mode) to the "-m" option of the "hanetcnfig create" command.

- Takeover virtual interface name
Specify the name of the virtual interface for cluster switchover.
The virtual interface is automatically created under the name of shaX:NN (X and NN are numbers) as a result of executing the “hanethvrsc create” command.
- Takeover virtual IP address (or host name)
Specify the IP address (or host name) for cluster switchover.
The same logical IP address (or host name) that was set in nodes (1) and (2) is set as a result of executing the “hanethvrsc create” command.
- Subnet mask
Specify the subnet mask value corresponding to the takeover virtual IP address in the “/etc/inet/netmasks” file.
This value is used for a physical IP and logical IP.
If subnet is not used, you don’t need to specify the value.
- Virtual interface name
Specify the virtual interface name to be assigned to the physical interface to be duplexed.
Specify shaX (X is a number) to the “-n” option of the “hanetconfig create” command.
Set the same name for node (1) and node (2).
- Primary physical interface name
Specify the name of the interface to be first activated among the duplexed physical interfaces (e.g. hme1, qfe1, etc.)
Specify the name to the “-t” option of the “hanetconfig create” command.
- Secondary physical interface name
Among the duplexed physical interfaces, specify the name of the interface to be activated after switchover from the primary physical interface. Specify the name to the “-t” option of the “hanetconfig create” command.
- Physical IP address (or host name)
Specify the physical IP address (or host name) to be assigned to the physical interface to be duplexed.
Specify the value to the “-e” option of the “hanetconfig create” command.
Specify different values for node (1) and node (2).
- Logical IP address (or host name)
Specify the logical IP address (or host name) to be assigned to the physical interface to be duplexed.
Specify the value to the “-i” option of the “hanetconfig create” command. Specify the same value for node (1) and node (2).
- Primary monitoring-destination IP address (or host name)
Specify the IP address (or host name) of the switching hub to be monitored when the primary physical interface is used.
Specify the value to the “-p” option of the “hanetpoll create” command.
- Secondary monitoring-destination IP address (or host name)
Specify the IP address (or host name) of the switching hub to be monitored when the secondary physical interface is used.
Specify the value to the “-p” option of the “hanetpoll create” command.
- Standby NIC patrol
When monitoring the standby NIC, specify p for standby patrol (automatic switchback in the event of a failure) or q for standby patrol (immediate automatic switchback) to the –m option of the “hanetconfig create” command.
You need to specify the local MAC address to the “-a” option.
Specify the different local MAC address values for node (1) and node (2).

■ Fast Switching Mode

Item		Setting	
GLS settings	Switching mode	◇NIC switching mode (logical IP takeover) ◆Fast switching mode	
	Takeover virtual interface name		
	Takeover virtual IP address (or host name)		
	Subnet mask		
	Node name (1)		
	Configuration information	Virtual interface name	
		Physical interface name (1)	
		Physical interface name (2)	
		Virtual IP address (or host name)	
		Subnet mask	
		Physical IP address (or host name) (1)	
		Subnet mask	
		Physical IP address (or host name) (2)	
	Subnet mask		
	Node name (2)		
	Configuration information	Virtual interface name	
		Physical interface name (1)	
		Physical interface name (2)	
		Virtual IP address (or host name)	
		Subnet mask	
Physical IP address (or host name) (1)			
Subnet mask			
Physical IP address (or host name) (2)			
Subnet mask			

[Setup items]

- Switching mode
 - Specify a redundant operation type for GLS; Fast switching mode, NIC (Network Interface Card) switching mode, or RIP mode.
 - Add t (fast switching mode) to the "-m" option of the "hanetcnfig create" command.
- Takeover virtual interface name
 - Specify the name of the virtual interface for cluster switchover.
 - The virtual interface is automatically created under the name of shaX:NN (X and NN are numbers) as a result of executing the "hanethvrsccreate" command.
- Takeover virtual IP address (or host name)
 - Specify the IP address (or host name) for cluster switchover.
 - Specify the value to the "-i" option of the "hanethvrsc create" command.
- Subnet mask
 - Specify the subnet mask value corresponding to the takeover virtual IP address in the "/etc/inet/netmasks" file.
 - This value should be the same as the virtual IP for the subnet mask.
 - If subnet is not used, you don't need to specify the value.
- Virtual interface name
 - Specify the virtual interface name to be assigned to the physical interface to be duplexed.
 - Specify shaX (X is a number) to the "-n" option of the "hanetconfig create" command.
 - Set the same name for node (1) and node (2).
- Physical interface name (1) and (2)
 - Specify the name of the interface to be first activated among the duplexed physical interfaces (e.g. hme1, qfe1, etc.)
 - Specify the name to the "-t" option of the "hanetconfig create" command.
- Virtual IP address (or host name)
 - Specify the virtual IP address (or host name) to the "-i" option of the "hanetconfig create" command.
 - Specify different values for node (1) and node (2).
- Subnet mask
 - Specify the subnet mask value corresponding to the takeover virtual IP address in the

“/etc/inet/netmasks” file.

This value should be the same as the virtual IP for the subnet mask.

If subnet is not used, you don't need to specify the value.

- Physical IP address (or host name) (1) and (2)

Specify the physical interface name to be assigned to the physical interface to be duplexed.

Create the “/etc/hostname. physical interface name” file and specify the IP address (or host name) in the file.

This value should be different than other IP.

- Subnet mask

Specify the subnet mask value corresponding to the physical IP address in the “/etc/inet/netmasks” file.

If subnet is not used, you don't need to specify the value.

A.9 GDS Setup Worksheets

Two types of GDS Setup Worksheets are System Disk Mirror Set up for setting up system disk mirroring and GDS Configuration for setting up shared disks.



See

- Before setting up the GDS configuration, you need to know basic information from reading “*PRIMECLUSTER Global Disk Services Guide*.”
- For information on the items in this worksheet, see 6.2.2 “Setting Up the GDS Configuration.”



Note

The class name should be unique in the cluster system.

A.9.1 System Disk Mirror Setup Worksheet

Use the System Disk Mirror Setup Worksheet to organize items before mirroring the system disk.



See

- Before setting up the GDS configuration, you need to know basic information from reading “*PRIMECLUSTER Global Disk Services Guide*.”
- For information on the items in this worksheet, see 6.2.2.1 “Setting Up System Disk Mirroring.” Also see A.11.4 “System Disk Mirror Setup Worksheet” in A.11 “System Design Examples.”

■ System Disk Mirror Setup Worksheet

Item		Setting	
System disk mirror settings	Node name		
	Class name		
	Group name		
	Mount point		
	Physical disk name		
	Mirror disk name		
	Spare disk name		
	Node name		
	Class name		
	Group name		
	Mount point		
	Physical disk name		
	Mirror disk name		
	Spare disk name		

A.9.2 Shared Disk Setup Worksheet

If you are setting up shared disks, you must determine the GDS configuration beforehand. Use the Shared Disk Setup Worksheet to organize the GDS configuration beforehand.



See

- Before setting up the GDS configuration, you need to know basic information from reading "*PRIMECLUSTER Global Disk Services Guide.*"
- For information on the items in this worksheet, see 6.2.2.2 "Setting Up Shared Disks." Also see A.11.5 "GDS Configuration Worksheet" in A.11 "System Design Examples."

■ GDS Configuration Worksheet

		Item		Setting		
GDS configuration	Class 1	Class name				
		Class scope (node name)				
		Node 1				
		Node 2				
		Spare disk 1 (*1)	SDX disk name			
			Physical disk name in node 1			
			Physical disk name in node 2			
		Single disk 1 (*2)	SDX disk name			
			Physical disk name in node 1			
			Physical disk name in node 2			
			Single volume 1	Volume name		
				Size		
			Single volume 2	Volume name		
				Size		
		Single disk 2 (*2)	SDX disk name			
			Physical disk name in node 1			
			Physical disk name in node 2			
			Single volume 1	Volume name		
				Size		
			Single volume 2	Volume name		
Size						
	Disk 1 to be connected to group (*3)	SDX disk name				
		Physical disk name in node 1				
		Physical disk name in node 2				
	Disk 2 to be connected to group (*3)	SDX disk name				
		Physical disk name in node 1				
		Physical disk name in node 2				
	Low-order group 1 (*4)	Group name				
		Group type				
		Stripe width (*6)				
		Disk /low-order group name	Disk /low-order group 1			
			Disk /low-order group 2			
	Low-order group 2 (*4)	Group name				
		Group type				
		Stripe width (*6)				
		Disk /low-order group name	Disk /low-order group 1			
Disk /low-order group 2						

		Highest-order group 1 (*5)	Group name			
			Group type			
			Stripe width (*6)			
			Disk /low-order group name	Disk	Disk /low-order group 1	
				Disk	Disk /low-order group 2	
			Volume 1	Volume name		
				Size		
		Volume 2	Volume name			
			Size			
		Highest-order group 2 (*5)	Group name			
			Group type			
			Stripe width (*6)			
			Disk /low-order group name	Disk	Disk /low-order group 1	
				Disk	Disk /low-order group 2	
Volume 1	Volume name					
	Size					
Volume 2	Volume name					
	Size					

	Class 2	Class name				
		Class scope (node name)	Node 1			
			Node 2			
		Spare disk 1 (*1)	SDX disk name			
			Physical disk name in node 1			
			Physical disk name in node 2			
		Single disk 1 (*2)	SDX disk name			
			Physical disk name in node 1			
			Physical disk name in node 2			
			Single volume 1	Volume name		
				Size		
			Single volume 2	Volume name		
		Size				
		Single disk 2 (*2)	SDX disk name			
			Physical disk name in node 1			
			Physical disk name in node 2			
			Single volume 1	Volume name		
				Size		
		Single volume 2	Volume name			
			Size			
		Disk 1 to be connected to group (*3)	SDX disk name			
			Physical disk name in node 1			
			Physical disk name in node 2			
		Disk 2 to be connected to group (*3)	SDX disk name			
			Physical disk name in node 1			
			Physical disk name in node 2			

		Low-order group 1 (*4)	Group name		
			Group type		
			Stripe width (*6)		
			Disk /low-order group name	Disk /low-order group 1	
				Disk /low-order group 2	
		Low-order group 2 (*4)	Group name		
			Group type		
			Stripe width (*6)		
			Disk /low-order group name	Disk /low-order group 1	
				Disk /low-order group 2	
		Highest-order group 1 (*5)	Group name		
			Group type		
			Stripe width (*6)		
Disk /low-order group name	Disk /low-order group 1				
	Disk /low-order group 2				
Volume 1	Volume name				
	Size				
Volume 2	Volume name				
	Size				

		Highest-order group 2 (*5)	Group name		
			Group type		
			Stripe width (*6)		
			Disk /low-order group name	Disk /low-order group 1	
				Disk /low-order group 2	
			Volume 1	Volume name	
				Size	
			Volume 2	Volume name	
				Size	

- (*1) This item can be defined only if mirroring is performed.
- (*2) This item must be defined only if a single volume is to be created.
- (*3) This item must be defined only if mirroring, striping, or concatenation is performed.
- (*4) This item must be defined only if the groups are to be arranged into a hierarchy.
- (*5) This item must be defined only if mirroring, striping, or concatenation is performed.
- (*6) This item must be defined only if the group type is stripe.

A.10 Cluster Application Worksheets

The Cluster Application Worksheets are necessary for setting up cluster applications and resources.

The following worksheets are available:

- ◆ **Resource configuration:**
 - Cmdline Resource Worksheet
 - Fsystem Resource Worksheet
 - Gds (Global Disk Services) Resource Worksheet
 - Gls (Global Link Services) Resource Worksheet
 - Takeover Network Resource Worksheet
 - Procedure Resource Worksheet
 - Process Monitoring Resource Worksheet
 - Line Switching Unit Resource Worksheet
- ◆ **Cluster application configuration:**
 - Cluster Application Setup Worksheet
- ◆ **Exclusive relationship configuration for cluster applications:**
 - Cluster Application Exclusion Setup Worksheet
- ◆ **Global Settings in Configuration Setup:**
 - Configuration Global Settings Setup Worksheet



For information on the items in this worksheet, see 6.6 "Setting Up Cluster Applications."

A.10.1 Cmdline Resource Worksheet

The Cmdline Resource Setup Worksheet is used for configuring a Cmdline resource.



For information on the items in this worksheet, see 6.6.1.1 "Creating Cmdline Resources."

Item			Setting value	
Cmdline resource	Active node candidate SysNode			
	Resource name			
	Resource operation	Attribute	InParallel	<input type="checkbox"/> Yes <input type="checkbox"/> [No]
			NeedAll	<input type="checkbox"/> Yes <input type="checkbox"/> [No]
		Association	SubApplication	
	Script to be controlled	Object	Start script	
			Stop script	
			Check script	
	Flag		NULLDETECTOR	<input type="checkbox"/> Yes <input type="checkbox"/> [No]
			ALLEXITCODES	<input type="checkbox"/> Yes <input type="checkbox"/> [No]
			LIEOFFLINE	<input type="checkbox"/> Yes <input type="checkbox"/> [No]
			CLUSTEREXCLUSIVE	<input type="checkbox"/> [Yes] <input type="checkbox"/> No
			AUTORECOVER	<input type="checkbox"/> [Yes] <input type="checkbox"/> No
		MONITORONLY	<input type="checkbox"/> Yes <input type="checkbox"/> [No]	
		STANDBYCAPABLE	<input type="checkbox"/> Yes <input type="checkbox"/> [No]	
		REALTIME	<input type="checkbox"/> Yes <input type="checkbox"/> [No]	
	TIMEOUT	(Range: 45 to 31535999) [300]		

Note: Values enclosed in brackets ([]) are default values.

A.10.2 Fsystem Resource Worksheet

The Fsystem Resource Worksheet is used for configuring an Fsystem resource.



See

For information on the setup items in this worksheet, see 6.6.1.2 "Creating Fsystem Resources."

Item			Setting value	
Fsystem resource	Active node candidate	SysNode		
	Resource name			
	Resource operation	Attribute	NeedAll	<input type="checkbox"/> [Yes] <input type="checkbox"/> No
			Timeout	(Range: 45 to 3600) [180]
	Mount point to be controlled 1	Object	Mount point	
		Flag	AUTORECOVER	<input type="checkbox"/> [Yes] <input type="checkbox"/> No
			SHARE	<input type="checkbox"/> Yes <input type="checkbox"/> [No]
	Mount point to be controlled 2	Flag	NFSLOCKFAILOVER	<input type="checkbox"/> Yes <input type="checkbox"/> [No]
			Object	Mount point
		Mount point to be controlled 3	Flag	AUTORECOVER
	SHARE			<input type="checkbox"/> Yes <input type="checkbox"/> [No]
	NFSLOCKFAILOVER		<input type="checkbox"/> Yes <input type="checkbox"/> [No]	

Note: Values enclosed in brackets ([]) are default values.



Note

Before you can set the NFSLOCKFAILOVER to Yes, you need to select Yes for NFS Lock Failover and then specify the Lock information directory name for the Global setting in the configuration.

For information on the Global Settings in the Configuration, see A.10.11 "Configuration Global Settings Worksheet."

A.10.3 Gds Resource Worksheet

The Gds Resource Worksheet is used for configuring a Gds (Global Disk Services) resource.



For information on the setup items in this worksheet, see 6.6.1.3 "Creating Gds Resources."

Item			Setting value	
Gds resource	Active node candidate	SysNode		
	Resource name			
	Resource operation	Attribute	Use	Exclusive use <input type="checkbox"/> [Enable] Hot Standby operation <input type="checkbox"/> Enable <input type="checkbox"/> [Disable] <input type="checkbox"/> Disable
			AutoRecover	<input type="checkbox"/> Yes <input type="checkbox"/> [No]
			Timeout	(Range: 5 to 3600) [1800]
	Disk class to be controlled 1	Object	Disk Class	
		Flag	MONITORONLY	<input type="checkbox"/> Yes <input type="checkbox"/> [No]
	Disk class to be controlled 2	Object	Disk Class	
		Flag	MONITORONLY	<input type="checkbox"/> Yes <input type="checkbox"/> [No]
	Disk class to be controlled 3	Object	Disk Class	
Flag		MONITORONLY	<input type="checkbox"/> Yes <input type="checkbox"/> [No]	

Note: Values enclosed in brackets ([]) are default values.

A.10.4 GIs Resource Worksheet

The GIs Resource Worksheet is used for configuring a GIs (Global Link Services) resource.



See

For information on the setup items in this worksheet, see 6.6.1.4 "Creating GIs Resources."

Item			Setting value	
GIs resource	Active node candidate	SysNode		
	Resource name			
	Resource operation	Attribute	Timeout	(Range: 5 to 300) [60]
		Association	SubApplication	
	Takeover IP address to be controlled 1	Object	Takeover IP address(IPv4)	
			Takeover IP address(IPv6)	
		Flag	AUTORECOVER	<input type="checkbox"/> Yes <input type="checkbox"/> [No]
	Takeover IP address to be controlled 2	Object	Takeover IP address(IPv4)	
			Takeover IP address(IPv6)	
		Flag	AUTORECOVER	<input type="checkbox"/> Yes <input type="checkbox"/> [No]
	Takeover IP address to be controlled 3	Object	Takeover IP address(IPv4)	
			Takeover IP address(IPv6)	
		Flag	AUTORECOVER	<input type="checkbox"/> Yes <input type="checkbox"/> [No]

Note: Values enclosed in brackets ([]) are default values.

A.10.5 Takeover Network Resource Worksheet

The Takeover Network Resource Worksheet is used for configuring a takeover network resource.



See

For information on the items in this worksheet, see 6.6.1.5 "Creating Takeover Network Resources."

Item			Setting value	
Takeover IP address resource	Active node candidate	SysNode		
	Resource name			
	Takeover network type		<input type="checkbox"/> [IP address takeover] <input type="checkbox"/> Node name takeover + IP address	
	Network interfaces	Node 1 ()		
		Node 2 ()		
		Node 3 ()		
		Node 4 ()		
	Resource operation	Attribute	NeedAll	<input type="checkbox"/> [Yes] <input type="checkbox"/> No
			Timeout	(Range: 45 to 3600)
		PingHost		
Association	SubApplication			
Takeover IP address to be controlled	Object	Host name		
		IP address		
		Net mask		
	Flag	BASE	<input type="checkbox"/> [virtual] <input type="checkbox"/> base	
		AUTORECOVER	<input type="checkbox"/> [Yes] <input type="checkbox"/> No	
		PingHost		

Note: Values enclosed in brackets ([]) are default values.

A.10.6 Procedure Resource Worksheet

The Procedure Resource Worksheet is used for configuring a procedure resource.



For information on the items in this worksheet, see 6.6.1.6 "Creating Procedure Resources."

Item			Setting value
Procedure resource	Active node candidate	SysNode	
	Resource name		
Resource operation	Attribute	SCRIPTTIMEOUT	(Range: 45 to 31535999) [1800]
	Association	SubApplication	
Procedure resource to be controlled	Procedure class		◇Application ◇BasicApplication ◇SystemState2 ◇SystemState3 ◇()
		Procedure resource	

Note: Values enclosed in brackets ([]) are default values.

A.10.7 Process Monitoring Resource Worksheet

The Process Monitoring Resource Worksheet is used for configuring a process monitoring resource.



See

For information on the items in this worksheet, see 6.6.1.7 "Creating Process Monitoring Resources."

Item			Setting value	
Process resource	Active node candidate	SysNode		
	Resource name			
	Resource operation	Attribute	InParallel	<input type="checkbox"/> Yes <input type="checkbox"/> [No]
			NeedAll	<input type="checkbox"/> Yes <input type="checkbox"/> [No]
		Association	SubApplication	
	Command path to be controlled	Object	Start command path	
			Stop command path	
			Monitored process is in different process group from parent process	If "Yes," check "Process is a daemon."
		Attribute	Restart count for monitored process	(Range: 0 to 99) [3]
		Restart interval for monitored process	(Range: 0 to 3600) [3]	

A.10.8 Line Switching Unit Resource Worksheet

The Line Switching Unit Resource Worksheet is used for configuring a line switching unit resource.



See

For information on the items in this worksheet, see 6.6.1.8 "Creating Line Switching Unit Resources."

Item		Setting value
SH_SWLine resource	Active node candidate	SysNode
	Resource name	
	Control target	Line switching unit resource

Note: Values enclosed in brackets ([]) are default values.

A.10.9 Cluster Application Worksheet

The Cluster Application Worksheet is used for configuring a cluster application.



For information on the items in this worksheet, see 6.6.2 "Creating Cluster Applications."

Item		Setting value	Remarks (value specified with GUI/CUI)			
Cluster application settings	Configuration name		config	Fixed		
	Cluster application name					
	Active node	SysNode (Priority 1: High)				
		SysNode (Priority 2)				
		SysNode (Priority 3)				
		SysNode (Priority 4: Low)				
	Attribute	Start	Active node at startup	OnlinePriority	◇ [According to cluster application] ◇ Active node when RMS stopped	[0] 1
			Automatic startup	AutoStartUp	◇ [Manual] ◇ Automatic	[No] Yes
	Switchover	Switchover operation	AutoSwitchOver	◇ [Manual] ◇ Automatic (more than one of the following can be selected) <input type="checkbox"/> At node failure <input type="checkbox"/> At resource failure <input type="checkbox"/> When RMS stops	[No] HostFailure ResourceFailure ShutDown	
					Standby	Trigger to be Standby
	Operation in the event of a failure	Operation when RMS fails to control 2	HalfFlag	◇ [Do not forcibly stop node] ◇ Forcibly stop node		
		Handling of failed node	PersistentFault	◇ [Use if fault is not detected when RMS is restarted] ◇ Use after operator clears fault	[0] 1	
		Operation if cluster interconnect fails	ShutdownPriority	◇ [NONE] ◇ Priority ()	[NONE] Priority (0 to MAXINT) * Higher number indicates higher priority. * See setup policy for live priority if Split-Brain occurs.	
	Configuration	Resource			Specified resource name	
		Patrol diagnosis		◇ Required ◇ [Not required]	Check [Do not check]	

Note: Values enclosed in brackets ([]) are default values.



For information on the "Live priority configuring policy when Split-Brain occurs" in the Remarks column for Shutdown Priority, see "Live Priority" in 5.2.2 "Setting Up the Shutdown Facility."

A.10.10 Cluster Application Exclusion Worksheet

The Cluster Application Exclusion Worksheet is used for configuring exclusion relationships between cluster applications.



See

For information on the items in this worksheet, see 6.6.3 "Setting Up Dependency Relationships Between Cluster Applications."

		Item	Setting value
Dependency relationship settings for cluster applications	Exclusion group 1	Group name	Exclusive
		Cluster application name 1	(Priority:)
		Cluster application name 2	(Priority:)
		Cluster application name 3	(Priority:)
		Cluster application name 4	(Priority:)
	Exclusion group 2	Group name	Exclusive
		Cluster application name 1	(Priority:)
		Cluster application name 2	(Priority:)
		Cluster application name 3	(Priority:)
		Cluster application name 4	(Priority:)
	Exclusion group 3	Group name	Exclusive
		Cluster application name 1	(Priority:)
		Cluster application name 2	(Priority:)
		Cluster application name 3	(Priority:)
		Cluster application name 4	(Priority:)
	Exclusion group 4	Group name	Exclusive
		Cluster application name 1	(Priority:)
		Cluster application name 2	(Priority:)
		Cluster application name 3	(Priority:)
		Cluster application name 4	(Priority:)

A.10.11 Configuration Global Settings Worksheet

This worksheet is used for configuring the Global Settings in the Configuration.



For information on the setup items in this worksheet, see 6.6.4 "Editing global settings in Configuration."

Item		Setting value	
Global Settings in the Configuration	PreCheck Timeout	(Range: 5 to 2147483647) [300]	
	First Available Detector	(Range: 0 to127) [0]	
	Last Available Detector	(Range: 0 to127) [127]	
	NFS Lock Failover	◇Yes ◇[No]	
	Lock information directory	*1)Only if Yes is selected above []	
Detector Details	Monitoring Intervals	hvdet_execbin Used for ops, rtp	(Range: 5 to 2147483647) [10]
		hvdet_ckhost Used for ops, rtp.	(Range: 5 to 2147483647) [10]
		hvdet_ddm Used for Ddm (invalid under Solaris OE).	(Range: 5 to 2147483647) [19]
		hvdet_glbassrt Used for Used for ops.	(Range: 5 to 2147483647) [10]
		hvdet_gmount Used for Fsystem.	(Range: 5 to 2147483647) [10]
		hvdet_icmp Used for Ipaddress.	(Range: 5 to 2147483647) [10]
		hvdet_locassrt Used for userApplication.	(Range: 5 to 2147483647) [10]
		hvdet_lvm Used for Lvm (invalid under Solaris OE).	(Range: 5 to 2147483647) [18]
		hvdet_nfs Used for Fsystem.	(Range: 5 to 2147483647) [10]
		hvdet_rcfs Rcfs.	(Range: 5 to 2147483647) [9]
		hvdet_rcvm Rcvm.	(Range: 5 to 2147483647) [33]
		hvdet_read Used for Rawdisk.	(Range: 5 to 2147483647) [10]
		hvdet_srdf Used for Srdf.	(Range: 5 to 2147483647) [60]
		hvdet_stopclnt Used for Fsystem.	(Range: 5 to 2147483647) [10]
		hvdet_system Used for Cmdline, Fsystem, userApplication.	(Range: 5 to 2147483647) [10]
		hvdet_vwm Used for Vwm.	(Range: 5 to 2147483647) [30]
		ForeignDetectors Used for foreign-code.	(Range: 5 to 2147483647) [30]
		Log level (MemoryLevel)	(Range: 0 to 2147483647) [1]
		Detector logging	(Range: 0 to 2147483647) [0]

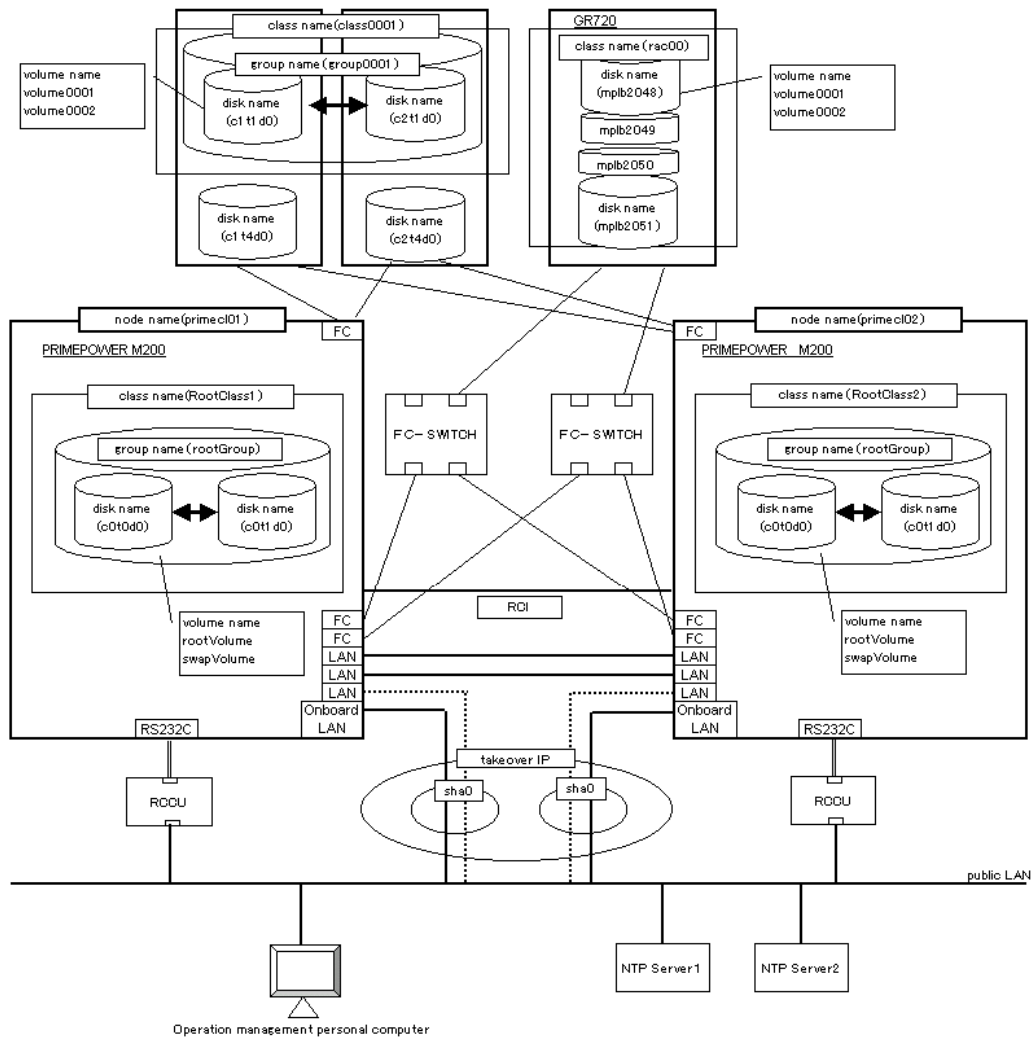
*1) Values enclosed in brackets ([]) are default values.
 Note: If the settings for items other than NFS Lock Failover need to be changed, please contact Fujitsu systems engineer (SE). However, no changes may be necessary for the normal operation.

A.11 System Design Examples

This section shows design examples of the PRIMECLUSTER system. Refer to these examples when designing the PRIMECLUSTER system.

■ System configuration

System configuration example



Note: The NTP server should be set to one of the following operation mode;

- Maintains time that is reliable for special hardware devices such as time units and GPS units.
- Uses another server that maintains time that is reliable for special hardware devices such as time units and GPS units, and uses NTP for time synchronization.

■ Used hardware

- PRIMEPOWER 200 x 2
- Expansion file unit x 2
- Remote console unit (RCCU) x 2
- Fibre channel switch (SN200) x 2
- Fast Ethernet card x 6
- Fibre channel card x 6
- Disk array unit (GR720) x 1

- Operation management personal computer x 1

■ **Used software**

- Solaris 8 OE
- Solaris 8 OE PTF (R02021)
- Solaris OE Unbundled PTF (R02021) (for PRIMEPOWER)
- Enhanced Support Facility 2.0
- PRIMECLUSTER 4.1A10 Enterprise Edition
- Multipath Disk Control 2.0
- Multipath Control Load Balance Option 2.1
- Fujitsu PCI Fibre Channel 2.2
- Netscape Communicator 4.7x (installed in the operation management personal computer)
- Java(TM) 2 Runtime Environment Standard Edition v1.3.1 (installed in the operation management personal computer)

■ **System disk settings**

node:primecl01	Physical disk name	Slice number	Slice name	Size (MB)
	c0t0d0	0	/	15374
		1	swap	2048
		2	backup	17423
node:primecl02	Physical disk name	Slice number	Slice name	Size (MB)
	c0t0d0	0	/	15374
		1	swap	2048
		2	backup	17423



Note

If GDS is used for system disk mirroring, one slice number in the system disk and at least 32 megabytes of free area (or swap area) are used.

You need to consider the resources used by GDS when designing the system.

■ **Shared disk array settings**

Device name: GR720 (FC)	Number of LU	Number of RAID groups	RAID level	Size
	4	1	5	248.2 GB
Device name: Expansion file unit (FC) x 2	—	—	—	18.2 GB



Note

To use the disk array units on UNIX, you need to format them by executing the “format (1M)” command.

When formatting the disk array units as part of the cluster system configuration work, you need to estimate the formatting time.

A.11.1 Cluster Building Worksheet

Shown below is an example of creating the Cluster Building Worksheet.

Item				Setting		
Shared disk unit: Type 1	Interface			GR720		
	Path			Fibre channel		
	File system selection			multipath		
				GFS Local File System		
Shared disk unit: Type 2				Expansion file unit		
	Interface			SCSI		
	Path			single		
	File system selection			GFS Local File System		
NTP	Operation mode			-		
				-		
	Protocol (only when broadcast is specified)			-		
				-		
	Network configuration	NTP servers	Host name		pclntp1	
			IP address		10.34.214.100	
			Host name		pclntp2	
			IP address		10.34.214.101	
	NTP server settings in cluster	Primary NTP server	Host name		-	
			IP address		-	
Secondary NTP server		Host name		-		
		IP address		-		
Operation management mode	Operation mode of Web-Based Admin View			2 layers		
	Public LAN					
	Primary management server IP			10.34.214.181		
	Secondary management server IP			10.34.214.182		
User group				Group name	User name	
				◆wroot	root	
				◆clroot	root	
				◇cladmin		
				◇clmon		
Cluster name				PRIMECLUSTER		

Node information	CIP	Subnet count				
		Subnet IP		192.168.1.0		
		Netmask		255.255.255.0		
	Node 1	Node name (uname -n)		primecl01		
		CF node name		primecl01		
		Public LAN	Network interface name		hme0/hme3	
			IP address		10.34.214.181	
			Netmask		255.255.255.0	
			Gateway		-	
		Cluster interconnect	Path 0 NIC name		/devhme1	
			Path 1 NIC name		/devhme2	
		Weight		2		
		RCCU	IP address		10.34.214.183	
		Node is part of CF quorum set		◆ [Yes] ◇ No		
	Node 2	Node name (uname -n)		primecl02		
		CF node name		primecl02		
		Public LAN	Network interface name		hme0/hme3	
			IP address		10.34.214.182	
			Netmask		255.255.255.0	
			Gateway		-	
		Cluster interconnect	Path 0 NIC name		/devhme1	
			Path 1 NIC name		/devhme2	
		Weight		2		
RCCU		IP address		10.34.214.184		
Node is part of CF quorum set		◆ [Yes] ◇ No				
Use of CF remote services		<input type="checkbox"/> cfcp (CF file copy) <input type="checkbox"/> cfsh (CF remote command execution)				
Set up IP interconnects		<input type="checkbox"/> [No] <input type="checkbox"/> Yes _____ (Quantity) IP interface:				
CIP		<input type="checkbox"/> [Used by RMS] <input type="checkbox"/> Not used by RMS Suffix:				
Cluster resource management facility	Hardware device to be registered in the resource database		<input checked="" type="checkbox"/> Network devices (*1) <input checked="" type="checkbox"/> Line switching units (*2) <input checked="" type="checkbox"/> Disk units (*3)			
Shutdown facility (SF)	First shutdown procedure for node		<input checked="" type="checkbox"/> RCI <input type="checkbox"/> RCCU			

Note: Values enclosed in brackets (f1) are default values.

In each node, specify /etc/inet/ntp.conf as shown below.

```
server 10.34.214.100
server 10.34.214.101
server 127.127.1.0

fudge 127.127.1.0 stratum 9

enable auth monitor
disable pll
driftfile /etc/ntp/ntp.drift
statsdir /var/ntp/ntpstats/
filegen peerstats file peerstats type day enable
filegen loopstats file loopstats type day enable
filegen clockstats file clockstats type day enable
```

For detailed instructions on specifying /etc/inet/ntp/conf, see the online manual by executing the

“xntpd(1M)” command.

A.11.2 GFS Local File System Setup Worksheet

Shown below is an example of creating the GFS Local File System Setup Worksheet.

Item		Setting
GFS Local File System setup	Device name	class0001:volume0001
	Mount point	/disk1
	Device name	class0001:volume0002
	Mount point	/disk2

A.11.3 GLS Setup Worksheet

Shown below are examples of creating the GLS Setup Worksheet.

■ NIC Switching Mode (Logical IP Takeover)

Item		Setting	
GLS setup	Switching mode	◆NIC switching mode (logical IP takeover) ◇Fast switching mode	
	Takeover virtual interface name	sha0:65	
	Takeover virtual IP address (or host name)	10.34.214.185	
	Subnet mask	255.255.255.0	
	Node name (1)	primecl01	
	Configuration information	Virtual interface name	sha0
		Primary physical interface name	hme0
		Secondary physical interface name	hme3
		Physical IP address (or host name)	10.34.214.181
		Logical IP address (or host name)	10.34.214.185
	Monitoring destination information	Primary monitoring destination IP address (or host name)	10.34.214.188
		Secondary monitoring destination IP address (or host name)	10.34.214.189
	Optional function	Backup NIC patrol ◇Disable ◆Enable Set to backup NIC. Local MAC address (02:00:00:00:00:01)	
	Node name (2)	primecl02	
	Configuration information	Virtual interface name	sha0
		Primary physical interface name	hme0
		Secondary physical interface name	hme3
		Physical IP address (or host name)	10.34.214.182
		Logical IP address (or host name)	10.34.214.185
	Monitoring destination information	Primary monitoring-destination IP address (or host name)	10.34.214.188
Secondary monitoring-destination IP address (or host name)		10.34.214.189	
Optional function	Backup NIC patrol ◇Disable ◆Enable Set to backup NIC Local MAC address (02:00:00:00:00:02)		

■ **Fast Switching Mode**

Item		Setting	
GLS setup	Switching mode	◇ NIC switching mode (logical IP takeover) ◆ Fast switching mode	
	Takeover virtual interface name	sha0:65	
	Takeover virtual IP address (or host name)	10.34.214.185	
	Subnet mask	255.255.255.0	
	Node name (1)	primecl01	
	Configuration information	Virtual interface name	sha0
		Physical interface name (1)	hme0
		Physical interface name (2)	hme3
		Virtual IP address (or host name)	10.34.214.181
		Subnet mask	255.255.255.0
		Physical IP address (or host name) (1)	10.34.215.181
		Subnet mask	255.255.255.0
		Physical IP address (or host name) (2)	10.34.216.181
	Subnet mask	255.255.255.0	
	Node name (2)	primecl02	
	Configuration information	Virtual interface name	sha0
		Physical interface name (1)	hme0
		Physical interface name (2)	hme3
		Virtual IP address (or host name)	10.34.214.182
		Subnet mask	255.255.255.0
Physical IP address (or host name) (1)		10.34.215.182	
Subnet mask		255.255.255.0	
Physical IP address (or host name) (2)		10.34.216.182	
Subnet mask	255.255.255.0		

A.11.4 System Disk Mirror Setup Worksheet

Shown below is an example of creating the System Disk Mirror Setup Worksheet.

Item		Setting	
System disk mirroring setup	Node name	primecl01	
	Class name	Group name	rootGroup
		Mount point	/, /swap, /usr, /opt
		Physical disk name	c0t0d0
		Mirror disk name	c0t1d0
		Spare disk name	-
	Node name	primecl02	
	Class name	Group name	rootGroup
		Mount point	/, /swap, /usr, /opt
		Physical disk name	c0t0d0
		Mirror disk name	c0t1d0
		Spare disk name	-

A.11.5 GDS Configuration Worksheet

Shown below are examples of creating the GDS Configuration Worksheet.

■ **System configuration example**

For a system configuration example, set up the worksheet as shown below.

		Item	Setting		
GDS configuration	Class 1	Class name	rac00		
		Class scope (node name)	Node 1	primecl01	
			Node 2	primecl02	
		Single disk 1	SDX disk name	diskmplb0001	
			Physical disk name in node 1	mplb2048	
			Physical disk name in node 2	mplb2048	
			Single volume 1	Volume name	volume0001
				Size	1024 MB
			Single volume 2	Volume name	volume0002
		Size		1024 MB	
		Single disk 2	SDX disk name	diskmplb0002	
			Physical disk name in node 1	mplb2049	
			Physical disk name in node 2	mplb2049	
		Single disk 3	SDX disk name	diskmplb0003	
			Physical disk name in node 1	mplb2050	
			Physical disk name in node 2	mplb2050	
	Single disk 4	SDX disk name	diskmplb0004		
		Physical disk name in node 1	mplb2051		
		Physical disk name in node 2	mplb2051		
	Class 2	Class name	class0001		
		Class scope (node name)	Node 1	primecl01	
			Node 2	primecl02	
		Spare disk 2	SDX disk name	-	
			Physical disk name in node 1	-	
			Physical disk name in node 2	-	
		Disk 1 connected to group	SDX disk name	disk010001	
			Physical disk name in node 1	c1t1d0	
			Physical disk name in node 2	c1t1d0	
		Disk 1 connected to group	SDX disk name	disk020001	
			Physical disk name in node 1	c2t1d0	
			Physical disk name in node 2	c2t1d0	
		Highest-order group 1	Group name	group0001	
Group type			mirror		
Stripe width (*6)			-		
Disk/low-order group name			Disk/low-order group 1	disk010001	
			Disk/low-order group 2	disk010002	
Volume 1			Volume name	volume0001	
			Size	1024 MB	
Volume 2			Volume name	volume0002	
	Size	1024 MB			

Examples of creating the GDS Configuration Worksheet are provided below.

■ **Example 1. Managing a disk as a single disk:**

In this example, single volumes Volume1 and Volume2 are created in physical disk c3t4d5.

Item		Setting		
Class 1	Class name		Class1	
	Class scope (node name)	Node 1	Node1	
		Node 2	Node2	
	Single disk 1	SDX disk name		Disk1
		Physical disk name in node 1		c3t4d5
		Physical disk name in node 2		c2t3d4
		Single volume 1	Volume name	Volume1
			Size	1024 blocks
		Single volume 2	Volume name	Volume2
	Size		1024 blocks	

■ **Example 2. If a disk is not mirrored but may be changed to a mirror configuration later:**

In this example, mirror group Group1, which consists only of physical disk c3t4d5, is created, and single volumes Volume1 and Volume2 are created in Group1.

Since Group1 consists of only one disk, Volume1 and Volume2 are not mirrored. If another disk is added to Group1, then Volume1 and Volume2 can be changed to a mirror configuration.

Item		Setting		
Class 1	Class name		Class1	
	Class scope (node name)	Node 1	Node1	
		Node 2	Node2	
	Disk 1 connected to group	SDX disk name		Disk1
		Physical disk name in node 1		c3t4d5
		Physical disk name in node 2		c2t3d4
	Highest-order group 1	Group name		Group1
		Group type		mirror
		Stripe width		-
		Disk/low-order group name	Disk/low-order group 1	Disk1
		Volume 1	Volume name	Volume1
			Size	1024 blocks
		Volume 2	Volume name	Volume2
Size	1024 blocks			

■ **Example 3. If disk mirroring is to be executed:**

In this example, mirror group Group1, which consists of physical disks c3t4d5 and c4t5d6, is created, and mirrored volumes Volume1 and Volume2 are created in Group1.

Item		Setting		
Class 1	Class name		Class1	
	Class scope (node name)	Node 1	Node1	
		Node 2	Node2	
	Spare disk 1	SDX disk name		Disk3
		Physical disk name in node 1		c1t2d3
		Physical disk name in node 2		c2t2d2
	Disk 1 connected to group	SDX disk name		Disk1
		Physical disk name in node 1		c3t4d5
		Physical disk name in node 2		c2t3d4
	Disk 2 connected to group	SDX disk name		Disk2
		Physical disk name in node 1		c4t5d6
		Physical disk name in node 2		c3t3d3
	Highest-order group 1	Group name		Group1
		Group type		mirror
		Stripe width		-
		Disk/low-order group name	Disk/low-order group 1	Disk1
			Disk/low-order group 2	Disk2
		Volume 1	Volume name	Volume1
			Size	1024 blocks
		Volume 2	Volume name	Volume2
Size	1024 blocks			

■ **Example 4. If disk striping is to be executed:**

In this example, striping group Group1, which consists of physical disks c3t4d5 and c4t5d6, is created, and striped volumes Volume1 and Volume2 are created in Group1.

Item		Setting		
Class 1	Class name		Class1	
	Class scope (node name)	Node 1	Node1	
		Node 2	Node2	
	Disk 1 connected to group (*3)	SDX disk name		Disk1
		Physical disk name in node 1		c3t4d5
		Physical disk name in node 2		c2t3d4
	Disk 2 connected to group (*3)	SDX disk name		Disk2
		Physical disk name in node 1		c4t5d6
		Physical disk name in node 2		c3t3d3
	Highest-order group 1	Group name		Group1
		Group type		stripe
		Stripe width		32
		Disk/low-order group name	Disk/low-order group 1	Disk1
			Disk/low-order group 2	Disk2
		Volume 1	Volume name	Volume1
			Size	1024 blocks
		Volume 2	Volume name	Volume2
Size	1024 blocks			

■ **Example 5. If disk concatenation is to be executed:**

In this example, concatenation group Group1, which consists of physical disks c3t4d5 and c4t5d6, is connected, and volumes Volume1 and Volume2 are created in Group1.

Item		Setting		
Class 1	Class name		Class1	
	Class scope (node name)	Node 1	Node1	
		Node 2	Node2	
	Disk 1 connected to group (*3)	SDX disk name		Disk1
		Physical disk name in node 1		c3t4d5
		Physical disk name in node 2		c2t3d4
	Disk 2 connected to group (*3)	SDX disk name		Disk2
		Physical disk name in node 1		c4t5d6
		Physical disk name in node 2		c3t3d3
	Highest-order group 1	Group name		Group1
		Group type		concat
		Stripe width		-
		Disk/low-order group name	Disk/low-order group 1	Disk1
			Disk/low-order group 2	Disk2
		Volume 1	Volume name	Volume1
			Size	1024 blocks
Volume 2		Volume name	Volume2	
	Size	1024 blocks		

■ **Example 6. If disk striping and mirroring are to be executed:**

In this example, mirror group Group1, which consists of striping group Group2 and striping group Group3 is created, and volumes Volume1 and Volume2 are created in Group1. Striping group Group2 consists of physical disks c3t4d5 and c4t5d6, and striping group Group3 consists of physical disks c3t4d6 and c4t5d7.

Item		Setting		
Class 1	Class name		Class1	
	Class scope (node name)	Node 1	Node1	
		Node 2	Node2	
	Spare disk 1	SDX disk name		Disk5
		Physical disk name in node 1		c1t2d3
		Physical disk name in node 2		c2t2d2
	Disk 1 connected to group	SDX disk name		Disk1
		Physical disk name in node 1		c3t4d5
		Physical disk name in node 2		c2t3d4
	Disk 2 connected to group	SDX disk name		Disk2
		Physical disk name in node 1		c4t5d6
		Physical disk name in node 2		c3t3d3
	Disk 3 connected to group (*3)	SDX disk name		Disk3
		Physical disk name in node 1		c3t4d6
		Physical disk name in node 2		c2t3d5
	Disk 4 connected to group	SDX disk name		Disk4
		Physical disk name in node 1		c4t5d7
		Physical disk name in node 2		c3t3d4
	Low-order group 1	Group name		Group2
		Group type		stripe
		Stripe width		32
		Disk/low-order group name	Disk/low-order group 1	Disk1
			Disk/low-order group 2	Disk2
	Low-order group 2	Group name		Group3
		Group type		stripe
		Stripe width		32
		Disk/low-order group name	Disk/low-order group 1	Disk3
Disk/low-order group 2			Disk4	
Highest-order group 1	Group name		Group1	
	Group type		mirror	
	Stripe width		-	
	Disk/low-order group name	Disk/low-order group 1	Group2	
		Disk/low-order group 2	Group3	
	Volume 1	Volume name	Volume1	
		Size	1024 blocks	
Volume 2	Volume name	Volume2		
	Size	1024 blocks		

Appendix B Manual Pages

This appendix provides online manual page lists for CCBR, CF, CIP, operator intervention, PAS, the cluster resource management facility, RMS, shutdown facility (SF), monitoring agent (MA), SIS, tracing failed resource, Web-Based Admin View, procedure resource, process monitoring feature, and the RMS wizards.

To view a manual page, enter the following command:

```
$ man man_page_name
```

Note:

To view these manual pages, you must set the MANPATH environment variable so that /etc/opt/FJSVcluster/man is included.

To print a hard copy of a manual page, enter the following command:

```
% man man_page_name | col-b | lpr
```

B.1 CCBR

System administrator

Command	Function
cfbackup(1M)	Creates a backup copy of all the cluster configuration information related to the PRIMECLUSTER nodes.
cfrestore(1M)	Restores the cluster configuration information stored on the PRIMECLUSTER node.

B.2 CF

System administrator

Command	Function
cfconfig(1M)	Configures or deconfigures a node for a PRIMECLUSTER cluster.
cfset(1M)	Applies or modifies /etc/default/cluster.config entries into the CF module.
cftool(1M)	Prints the node communications state of a node or the cluster.

B.3 CIP

System administrator

Command	Function
cipconfig(1M)	Starts or stops CIP 2.0.
ciptool(1M)	Retrieves CIP information about local and remote nodes in the cluster.

File format

Command	Function
cip.cf(4)	CIP configuration file format

B.4 Operator Intervention

System administrator

Command	Function
clreply(1M)	Responds to an operator intervention request message.

B.5 PAS

System administrator

Command	Function
mipcstat(1M)	MIPC statistics
clmstat(1M)	CLM statistics

B.6 Cluster Resource Management Facility

System administrator

Command	Function
clautoconfig(1M)	Executes automatic resource registration.
clbackuprdb(1M)	Saves the resource database.
clexec(1M)	Executes a remote command.
cldeldevice(1M)	Deletes a resource that was registered during automatic resource registration.
clinitreset(1M)	Reset the resource database.
clinitscript(1M)	Reports the connection confirmation results for shared disk units.
clrestorerdb(1M)	Restores the resource database.
clsetacparam(1M)	Checks the connections of shared disk units and sets up the operation for automatic resource registration.
clsetparam(1M)	Displays and changes the resource database operation environment.
clsetup(1M)	Sets up the resource database.
clspconfig(1M)	Sets up the operation of patrol diagnosis.
clsptl(1M)	Executes patrol diagnosis.
clstarttrsc(1M)	Activates a resource (GDS only).
clstoprsc(1M)	Deactivates a resource (GDS only).
clsyncfile(1M)	Distributes a file between cluster nodes.

User command



Point

There is also a clgettree command in the Web-Based System Administration tool WSA.

Command	Function
clgettree(1)	Outputs tree information for the resource database.

B.7 RMS

System administrator

Command	Function
hvassert (1M)	Asserts (tests for) an RMS resource state.
hvcn (1M)	Start the RMS configuration monitor.
hvconfig (1M)	Displays or saves the RMS configuration file.
hvdisp (1M)	Displays RMS resource information.
hvdist (1M)	Distributes RMS configuration files.
hvdump (1M)	Collects debugging information about RMS.
hvgdmake (1M)	Compiles an RMS custom detector.
hvlogclean (1M)	Clean the RMS log files.
hvlogcontrol (1M)	Controls the size of the log disk.
hvrcllev (1M)	Changes the default startup execution level of RMS.
hvshut (1M)	Shuts down RMS.
hvswitch (1M)	Switches control of an RMS user application resource to another host.
hvthrottle (1M)	Prevents multiple RMS scripts from running simultaneously.
hvutil (1M)	Manipulates the availability of an RMS resource.
SA_pprci (PRIMEPOWER only)	Uses the RCI interface to shut down an agent.

File format

Command	Function
config.us	Format of the RMS node configuration file
hvenv.local (4)	RMS local environment configuration file
hvgdstartup	RMS general-purpose detector startup file

B.8 Shutdown Facility (SF)

System administrator

Command	Function
sdtool (1M)	Interface tool for Reliant Cluster shutdown daemon
rcsd (1M)	Shutdown daemon for Reliant Cluster shutdown manager
rcsd.cfg (4M)	Configuration file for Reliant Cluster shutdown daemon
SA_wtinps.cfg (4M)	Configuration file for WTI NPS shutdown agent
SA_sunF.cfg (4M)	Configuration file for sunF system controller shutdown agent
SA_sspint.cfg (4M)	Configuration file for Sun E10000 shutdown agent
SA_scon.cfg (4M)	Configuration file for SCON shutdown agent
SA_pprci.cfg (4M)	Configuration file for RCI shutdown agent (only for PRIMEPOWER)
SA_rps.cfg (4M)	Configuration file for shutdown agent that uses remote power switch (RPS)
SA_rccu.cfg (4M)	Configuration file for RCCU shutdown agent

B.9 Monitoring Agent (MA)

System administrator

Command	Function
clrcimonctl (1M)	Displays, starts, stops, and restarts the operation of the RCI asynchronous monitoring daemon.
clrccumonctl (1M)	Displays, starts, stops, and restarts the operation of the console asynchronous monitoring daemon.

B.10 SIS

System administrator

Command	Function
dtcpadmin(1)	Starts the SIS administration utility.
dtcpd(1)	Starts the SIS daemon for configuring VIPs.
dtcpdbg(1)	Displays SIS debugging information.
dtcpstat(1)	Displays state information on SIS.

B.11 Tracing Failed Resource

System administrator

Command	Function
cldispfaultrsc(1M)	Outputs a list of the current failed resources.

B.12 Web-Based Admin View

System administrator

Command	Function
fjsvwvbs(1M)	Stops Web-Based Admin View.
fjsvwvcnf(1M)	Starts, stops, or restarts the web server for Web-Based Admin View.
wvCntl(1M)	Starts, stops, or gets debugging information for Web-Based Admin View.
wvGetparam(1M)	Displays the Web-Based Admin View environment variables.
wvSetparam(1M)	Sets the Web-Based Admin View environment variables.
wvstat(1M)	Displays the operating state of Web-Based Admin View.

B.13 Procedure Resource

System administrator

Command	Function
claddprocrsc(1M)	Registers an application resource that uses a state transition procedure.
cldelproc(1M)	Deletes a state transition procedure.
cldelprocrsc(1M)	Deletes an application resource that uses state transition procedure.
clgetproc(1M)	Gets a state transition procedure.
clsetproc(1M)	Registers a state transition procedure.
clsetprocrsc(1M)	Changes the registered information of an application resource that uses a state transition procedure.

User command

Command	Function
cldspproc(1)	Outputs information on the resource that uses the state transition procedure.

B.14 Process Monitoring Feature

System administrator

Command	Function
clmonproc(1M)	Requests the process monitoring facility to monitor a process.

B.15 RMS Wizards

RMS Wizards and RMS Application Wizard

The manual for the RMS wizards is stored on the CD-ROM SMAWRhvd0 package as an html document. If you install this package, the manual will be saved in the following directory:

`/usr/opt/reliant/htdocs.solaris/wizards.en`

Appendix C Troubleshooting

This appendix explains how to collect troubleshooting information if an error occurs in the PRIMECLUSTER system.

C.1 Collecting Troubleshooting Information

If an error occurs in the PRIMECLUSTER system, collect the information required for the error investigation from all nodes that constructs the cluster and the cluster management servers. Then, contact your customer support representative.

1. PRIMECLUSTER investigation information
 - Use fjsnap to collect information.
 - Retrieve the system dump.

If a hardware error, an operating system error, a panic, or a login failure occurs, collect the followings:

 - System dump
 - SCF* dump

* SCF: System Control Facility
 - Collect the Java Console on the clients.

See "Appendix B.2.2 Java console" in the "*PRIMECLUSTER Web-Based Admin View Operation Guide*."
 - Collect a hard copy of the client screens.

See "Appendix B.2.3 Screen hard copy" in the "*PRIMECLUSTER Web-Based Admin View Operation Guide*."
 - If a client is using RC2000, collect RC2000 information for the client.

See "D.2 Collecting Troubleshooting Information" in the "*RC2000 User's Guide*."
2. Investigation information for the failed application
3. Error reproduction procedure manual if the error can be reproduced



Information

- When reporting a problem, collect the information required for an error investigation. If you do not provide information for problem checking and error reproduction execution, it may take a long time to reproduce and diagnose the problem or it may become impossible to do so.
- Collect investigation material promptly from all nodes of the PRIMECLUSTER system. Necessary information may become lost if a long time elapses after the error occurs. This applies especially to information collected by fjsnap.
- If a node was forcibly terminated, execute sync in OBP mode, and collect a system dump.

C.1.1 Executing the fjsnap Command

The "fjsnap" command is a system information tool of the Solaris OE, and it comes with the FJSVsnap Expanded Support Function Package. This tool enables you to collect information for troubleshooting if a failure occurs in the PRIMECLUSTER system.

The procedure for executing the fjsnap command is described below.

1. Log in with system administrator authority.
2. Execute the "fjsnap" command.

```
/opt/FJSVsnap/bin/fjsnap -h output
```

or

```
/opt/FJSVsnap/bin/fjsnap -a output
```

- If `-a` is specified, the amount of data becomes large because all detailed information is collected. If `-h` is specified, only cluster control information is collected.
- Specify a file name or an output file name (`/dev/rmt/0`) to output information. The specified name is the file to which collected information is output when the “fjsnap” command is executed.



See

For details on the “fjsnap” command, see the “README.ja” file, which is the README file included in the “FJSVsnap” package.



Information

Execution timings for the fjsnap command

- For problems that occur during operation, for example, if an error message is output, execute the “fjsnap” command immediately after the problem occurs.
- If the “fjsnap” command cannot be executed because the system hangs, collect a system dump. Then start the system in single user mode, and execute the “fjsnap” command.
To collect the system dump, press the REQUEST switch or input the abort key sequence (for example, Break signal) to forcibly stop the node to OBP mode, and then execute “sync.” For detailed instructions on forcibly stopping the node to OBP mode, see the PRIMEPOWER user’s guides and the “Solaris System Management” manual of the Solaris OE.
- After an error occurs, if a node restarts automatically (the node could not be started in single-user mode) or if the node is mistakenly started in multi-user mode, execute the “fjsnap” command.
- If investigation information cannot be collected because the “fjsnap” command results in an error or the “fjsnap” command does not return, then collect a system dump.

C.1.2 System dump

If a system dump is collected when a node is in a panic, obtain the system dump as investigation information. The system dump is written into the dump file during node startup. The default storage directory is `/var/crash/node_name`.

C.1.3 SCF Dump

Collect a SCF dump if conditions like those listed below occur:

- Message 7003 or 7004 is output.
- The SCF driver outputs a message.



See

For information on the messages that the SCF driver outputs, see the “*Enhanced Support Facility User’s Guide*.”

◆ Collecting the SCF dump

The SCF RAS monitoring daemon that received the error notification from SCF stores the SCF dump to the "/var/opt/FJSVhwr/scf.dump" file. Collect the entire directory of this file according to the following operation.

```
# cd /var/opt
# tar cf /tmp/scf.dump.tar ./FJSVhwr
```

C.2 Troubleshooting

C.2.1 GUI in General

This section explains how to take corrective actions for problems that may occur while you are using the GUI.

If you find no relevant descriptions in this chapter, see also "B.1 Corrective action" in the "*PRIMECLUSTER Web-Based Admin Operation Guide*."

Symptom: When disk class creation, deletion, or name change is executed on the GDS screen, the message, "An error occurred in the log monitoring facility in node *XXXX* Monitoring stops. After confirming that the node is active, update to the latest information." or "0007 The connection to the management server is disconnected. Attempt to connect to the active management server?" is displayed. Web-Based Admin View is disconnected.

Corrective action

This error might be due to a JavaVM related problem. Close the browser, and then display the screen again.

If you are using the ClusterAdmin screen, close the screen first, and create or delete a disk class or change the disk class name to avoid this error. If the same error occurs frequently even after closing the ClusterAdmin screen, contact your Fujitsu engineer.

C.3 Detecting a Failed Resource

If a failure occurs in a resource, you can specify the resource by referring to the following:

- The message displayed if a failure occurs in the resource
- List of currently failed resources
- Failed resource list screen



Note

To use the history function of the failed resource, the resource database must be set up correctly. Also, the "PersistentFault" attribute of userApplication must be set to yes(1). For information on the resource database settings, see the "*PRIMECLUSTER Cluster Foundation Configuration and Administration*."

The operator intervention function and the failed resource history function are both dependent on the “clwatchlogd” daemon. This daemon can be started automatically with the “rc” script in multi-user mode. The “clwatchlogd” daemon uses the “RELIANT_LOG_PATH” environment variable of RMS. The value of this variable is set when the “rc” script starts up for the first time.

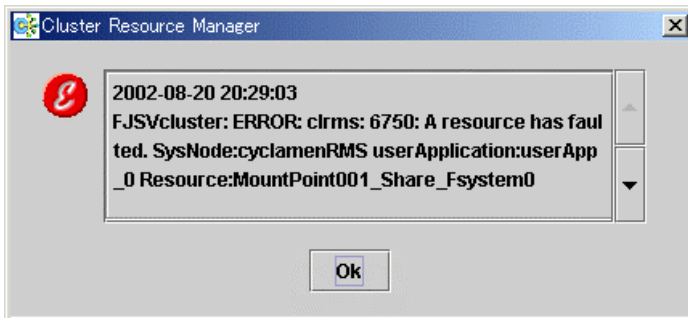
When this value is changed, you need to send the “SIGHUP” signal to clwatchlogd. When clwatchlogd receives this signal, clwatchlogd acquires the latest value of RELIANT_LOG_PATH. After completing the above processing, start RMS.

This manual is installed in the /etc/opt/FJSVcluster/man directory.

Before executing the “man (1)” command, add this directory to the beginning of MANPATH. Usually, a directory name is added to the line beginning with “setenv MANPATH” within the “.cshrc” file or the line beginning with “export MANPATH” within the “.profile” file.

C.3.1 Failed Resource Message

If a resource failure or recovery is detected, a message screen pops up as the Cluster Admin popup screen. An example failed resource message screen is shown below:



Note

If a message frame title says “Cluster resource management facility,” refer to the following:

- H.5 "Cluster Resource Management Facility Messages"
- D.5 "Failed Resource and Operator Intervention Messages (GUI)"
- D.7 "Shared Disk Connection Confirmation Messages"
- D.8 "Patrol Diagnosis Messages"

The severity icon is defined as follows:

Icon	Meaning
	Notice
	Warning
	Error
	Other

Respond to the failed resource message screen as follows:

◆ **Procedure**

1. Click on the OK button to respond to the message.
2. Click the up arrow mark or down arrow mark to go to the previous or next message.

Then, a message appears to remind you that you have not yet entered a response or confirmed the displayed message.

If you subsequently enter a response, the message is cleared and the next message appears. If the next message does not appear and the message prior to that for which a response was entered is still available, that message will appear. If there is any message for which confirmation or a response has not yet been entered, the message screen closes. For information on the message contents, refer to “Failed Resource and Operator Intervention Messages” and for information on how to display previous messages, refer to “Resource Fault History.”



Note

If you close Web-Based Admin View or Cluster Admin after this message is displayed, a fault resource message with the same contents will not be displayed. Therefore, you are recommended to confirm the message contents if a fault resource message is displayed for the first time. After you have closed the message, refer to the fault history on the “Resource Fault History” screen. For information on the message display language, refer to “Setting up the language of Web-Based Admin View” in 4.1.3 “Initial Setup of Web-Based Admin View.”

If the Cluster Admin screen is not displayed on the client PC when the fault resource message is displayed, the message is transmitted only to the client to which the management server was first connected.

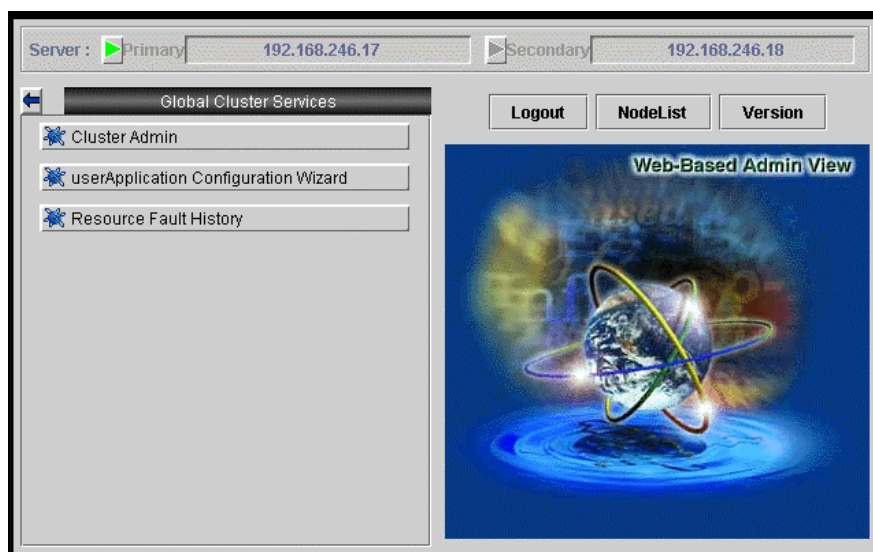
Each management server administers its fault resource messages. If you change the management server after confirming the message, the same message will be displayed again. To delete these messages, select *Cluster Admin* by using the GUI of *Web-Based Admin View* after closing *Cluster Admin*, and then open *Cluster Admin* again.

C.3.2 Resource Fault History

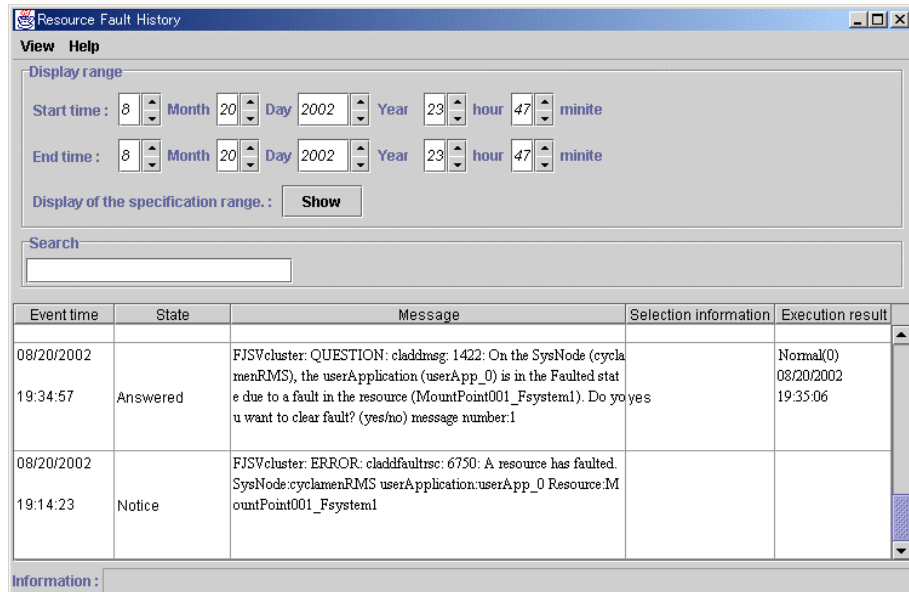
Display the “Resource Fault History” screen, in which the resource fault history is displayed, in the following procedure.

◆ **Procedure**

1. Open the “Web-Based Admin View” screen and then select *Global Cluster Services*.
2. Choose *Resource Fault History*.



The "Resource Fault History" will be displayed.



Note

The "Resource Fault History" cannot be displayed automatically. To display the latest history information, select *View* → *Update* menu.

■ **Menu of the fault resource list screen**

The "Resource Fault History" screen contains the following menu items:

Menu	Function
View -> Update latest information	The duration is initialized to the present time and date. A maximum of 100 of the latest history resources are displayed.
View -> Fault Resource List	A list of resources in which failures are present are displayed (see C.3.3 "Fault Resource List").
View -> Exit	The "Resource Fault History" screen is cleared.
Help -> Help	The GUI help screen is displayed.

■ **Setting the range of time**

A fault resource history listing can be displayed by specifying a date and time.

- *Start time* – A start time is set up.
- *End time* – An end time is set up.

If you click the *View* button after setting up the required values, a maximum of 100 of the most recently failed resources within the specifiable range can be displayed.

■ **Search with a keyword**

The fault resource history list can be narrowed by specifying "*Keyword*".

If a duration is set, the history of up to the 100 latest failed resources that satisfy both conditions can be displayed.

■ **How to read the list**

The following information is displayed on the "Resource Fault History" screen.

- Occurrence time — The time at which the RMS detected a resource failure is displayed.
- Status — One of the following statuses is indicated.
 - Responded – The operator has already responded the message.

- Not responded – The operator has not responded to the message for which a response is required.
- Responding – The operator is currently responding to the message.
- Confirm – Notification message for which no response is required.
- Message – The message is displayed.
- Selection information – Operator intervention message information from the client that is connected to the management server is displayed. If the message is canceled or if a response to the message is entered by executing the “creply(1M)” command, nothing will be displayed.
- Execution result – The result and time of the response processing are displayed.

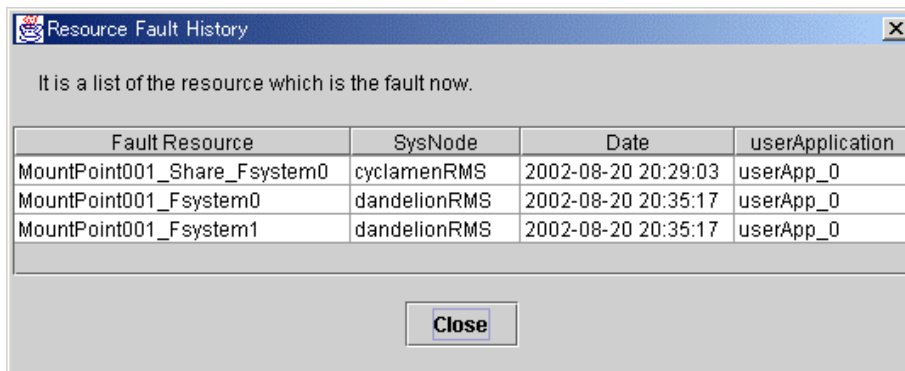
■ Information field

The information related to error detection during the acquisition or read-in of the history files is displayed. The following items will be displayed:

- Processing – History data is being collected from the management server.
- An error is included in the specified duration. – The specified duration is incorrect. Correct it and then click the *View* button.
- Part of the data acquisition failed. – Parts of the history files could be damaged. This will not disrupt ongoing operation, but the corrupted data will not be displayed.

C.3.3 Fault Resource List

If you select *View* → *Fault Resource List* on the “Resource Fault History” screen, the fault resource list is displayed as follows:



Fault Resource	SysNode	Date	userApplication
MountPoint001_Share_Fsystem0	cyclamenRMS	2002-08-20 20:29:03	userApp_0
MountPoint001_Fsystem0	dandelionRMS	2002-08-20 20:35:17	userApp_0
MountPoint001_Fsystem1	dandelionRMS	2002-08-20 20:35:17	userApp_0

The following information is displayed on the fault resource list screen:

- Fault resource – The name of the fault resource is displayed.
- SysNode – The SysNode to which the fault resource belongs is displayed.
- Fault time – The date and time at which the RMS detected a resource failure is displayed.
- userApplication – The name of userApplication to which the failed resource belongs is displayed.

If you click *Close*, the failed resource list screen is closed.

The list of resources that are currently in the failed state can be displayed by executing the “cldisefaulttrsc(1M)” command.

Appendix D Messages

This appendix explains the following messages:

- D.1 Messages Related to CF (The reference sections are indicated.)
- D.2 Messages Related to RMS (The reference sections are indicated.)
- D.3 Messages Related to CRM View (The reference sections are indicated.)
- D.4 Messages Related to Line Switching Unit
- D.5 Failed Resource and Operator Intervention Messages (GUI)
- D.6 Failed Resource and Operator Intervention Messages (CLI)
- D.7 Shared Disk Connection Confirmation Messages
- D.8 Patrol Diagnosis Messages
- D.9 userApplication Configuration Wizard GUI Messages
- D.10 Procedure Resource Messages
- D.11 Process Monitoring Messages

D.1 Messages Related to CF

The message related to Cluster Foundation (CF) are shown below.

You can refer to the corrective action by taking the following steps:

■ Procedure

1. Find the same display format as that of the displayed message.
2. Confirm the relevant table in "Display format" and then derive the columns of "Reference location in CF Configuration and Administration" from the following information that appears.
 - Operation/state
Operation/state when the message was displayed
 - Message details
"Command name," "error code," "message number," etc. included in the displayed message
3. Refer to the relevant "Reference location in CF Configuration and Administration" and, once you have confirmed the message, take corrective action.

■ Display format 1

command-name : *message*

command-name:

Command name

message:

Message (condition, message number, reason, and other information are included)

Operation/state		<i>command-name</i> : <i>message</i>	Reference location in CF Configuration and Administration
Operation	Command		
Cluster node configuration	cfconfig command	cfconfig: <i>message</i>	11.1 cfconfig Messages
CIP2.0 start/stop	cipconfig command	cipconfig: <i>message</i>	11.2 cipconfig Messages
Node communication state output	cftool command	cftool: <i>message</i>	11.3 cftool Messages
cluster.config application	cfset command	cfset: <i>message</i>	11.4 cfset Messages
	newng command	newng: <i>message</i>	11.5 newng Messages

Operation/state		<i>command-name : message</i>	Reference location in CF Configuration and Administration
Operation	Command		
	showng command	showng: <i>message</i>	11.6 showng Messages
	deleteng command	deleteng: <i>message</i>	11.7 deleteng Messages
	detailing command	detailing: <i>message</i>	11.8 detailing Messages
	changeng command	changeng: <i>message</i>	11.9 changeng Messages
	descng command	descng: <i>message</i>	11.10 descng Messages
	rcqconfig command	rcqconfig: <i>message</i>	11.11 rcqconfig Messages
	rcquery command	rcquery: <i>message</i>	11.12 rcquery Messages
CF execution		CF: <i>message</i>	11.13 CF Runtime Messages

■ **Display format 2**

FJSVcluster:*severity:program:message-number:message*

severity:

Indicates the message severity level.

There are 4 message severity levels: Stop (HALT), Information (INFORMATION), Warning (WARNING), Error (ERROR). For details, see the table below.

program:

Indicates the name of the program that outputs this message.

message-number:

Indicates the message number.

message:

Indicates the message text.

details:

Indicates the detailed classification code.

Operation	<i>message-number</i>	Reference location in CF Configuration and Administration
Cluster resource management facility	0100-2	12.17.1.2.1 HALT Messages
	2100, 2200-5, 3200-6	12.17.1.2.2 INFO Messages
	4250, 5200	12.17.1.2.3 Warning Messages
	6000-10, 6021, 6025, 6200-4, 6206-23, 6226, 6250, 6300, 6302-3, 6600-4, 6606-8, 6611, 6614-16, 6653, 6661, 6665, 6668, 6675, 6680, 6900-7, 6910-11, 7500-22, 7535-40, 7542-43, 7545-6	12.17.1.2.4 Error Messages
Asynchronous monitoring	3040-5	12.19.1 Information Messages
	5001	12.19.2 Warning Messages
	????, 6000, 6004, 7003-4, 7040-2, 7200-2	12.19.3 Error Messages

Operation	<i>message-number</i>	Reference location (this manual)
Line switching unit	4000-5999 ????, 6000-7999	D.4 Messages Related to Line Switching Unit

■ Display format 3

(SMAWsf, *number1*, *number2*) : *message*

number1, *number2* :

Message number

message :

Message

Operation	(<i>number1-number2</i>)	Reference location in CF Configuration and Administration
Shutdown facility	(10, 2)-(10, 12) (10, 15)-(10, 17), (10, 19), (10, 20) (10, 23), (10, 101) (30, 2)-(30, 10), (30, 12)-(30, 17) (50, 3)-(50, 4), (50, 6), (50, 9)	11.18 Shutdown Facility

■ Display format (GUI)

The messages that are displayed when the following operation is performed with the GUI are related:

Operation	<i>message-number</i>	Reference location in CF Configuration and Administration
Cluster resource management facility	0700, 0702-5, 0707-13	11.17.2 INFO messages
	0760-1, 0763-9, 0773-5	11.17.4 Error messages

■ Display format (others)

If neither of the above display formats is related, refer to the following:

- 11.14 CF Reason Code Table
- 11.15 Error messages for different systems

D.2 Messages Related to RMS

The messages related to RMS are shown below.

You can refer to the corrective action by taking the following steps:

■ Procedure

1. Find the same display format as that of the displayed message.
2. Confirm the relevant table in “Display format” and then derive the “Reference location,” which is included in the RMS Configuration and Administration in this manual, from the following information that is displayed.
 - Operation/state
Operation/state that was implemented when the message was displayed
 - Message details
“Command name,” “error code,” “message number,” etc. included in the displayed message
3. Refer to the relevant “Reference location” and, once you have confirmed the target message, apply corrective action.

■ Display format 1

EJSVcluster : security : program : message-number : message

security:

Indicates the message severity level.

There are four message severity levels: Stop (HALT), Information (INFORMATION), Warning (WARNING), Error (ERROR). For details, see the table below.

program:

Indicates the name of the resource database program that output this message.

message-number:

Indicates the message number.

message:

Indicates the message text.

Operation	message-number	Reference location in RMS configuration and administration
Failed resource and operator intervention	1421-1423 2620, 2621, 2622, 2700, 2701, 6000-6004, 6009, 6208, 6615, 6616 6651, 6750, 6751-6755	D.6 Failed Resource and Operator Intervention Messages (CLI)
Shared disk unit	2914 6807, 6836	D.7 Shared Disk Connection Confirmation Messages
Patrol diagnosis	3050-3053 6690-6692 7050-7056	D.8 Patrol Diagnosis Messages

■ Display format 2

(err-code, message-number) : message

err-code :

error code

message-number :

Message number

message :

Message			
Operation/state	err-code	message-number	Reference location in RMS configuration and administration
switchlog	ADC	1, 2, 3, 4, 5, 15, 17, 18, 20, 25, 27, 30, 31, 32, 33, 34, 35, 37, 38, 39, 41, 43 44, 45, 46, 47, 48, 49, 57, 58, 59, 60, 61, 62, 63, 68	5.11 Errors in the Switchlog
	ADM	55, 57, 58, 59, 60, 62, 63, 70, 95, 96	
	BAS	2, 3, 6, 14, 15, 16, 17, 18, 19, 25, 26, 27, 29, 30, 31, 32, 36	
	BM	8, 52, 54, 68, 73, 74	
	CML	11, 12, 17, 18, 19, 20, 21	
	CRT	1, 2, 3, 4, 5	
	CUP	2, 3, 5, 7, 8	
	DET	1, 3, 4, 5, 6, 7, 12, 13, 24, 26, 28, 34	
	GEM	4	
	INI	1, 9	
	NOD	6, 7, 8, 9, 10-13, 16, 20, 21, 26, 28, 29, 30, 31, 34, 38, 40	
	QUE	13	
	SCR	8, 9, 20	
	SWT	4, 20, 25, 26, 45	
	SYS	1, 8, 13, 14, 15, 17, 48-50, 84, 90, 93, 94, 97, 98	
	UAP	1, 5, 6, 7, 8, 9, 15, 16, 19, 21, 22, 23, 24, 27, 28, 29, 32, 33, 35, 41, 42	
	US	5, 6, 31	
	WLT	1, 3, 5	
	WRP	3, 4, 9, 11, 12, 14, 15, 16, 17, 28-35	
	Dynamic reconfiguration	ADC	
ACM		3, 4, 5, 6-9, 11, 12-16, 17-28, 30-34, 37, 38-54, 75-79, 81-91, 98, 99, 100	
BM		13-21, 23-26, 29, 42, 46, 59, 71, 72, 75, 80, 81	
CTL		1	
RMS error *	ADC	16, 21, 69	5.13 Fatal Messages
	ADM	1, 2	
	BM	3, 49, 51, 58, 67, 82, 89	
	CML	14	
	CMM	1-3	
	DET	8-9, 16, 18	
	INI	4, 7, 10, 11-14	
	MIS	4	
	QUE	1-2, 5, 6, 11, 12	
	SCR	4, 5, 10, 12, 13, 15, 18	
	SYS	33, 52	

Operation/state	<i>err-code</i>	<i>message-number</i>	Reference location in RMS configuration and administration
	UAP	36	
	US	1	

* RMS fails to start, or RMS stops during operation when a failure occurs.

■ **Display format (GUI)**

Messages related GUI operation:

Operation	<i>message-number</i>	Reference location in RMS configuration and administration
Failed resource and operator intervention messages	0701, 0766, 0767, 0790, 0791, 0792, 0765	D.5 Failed Resource and Operator Intervention Messages (GUI)

■ **Display format (others)**

If neither of above display formats is related, refer to the following in the RMS Configuration and Administration:

- 5.15 Additional Messages

D.3 Messages Related to CRM View

This section explains the messages of the line switching unit.

The message format is as follows:

■ Display format

If a message is displayed during operation on CRM view or if the frame title in the message dialog box is "Cluster resource management facility" is displayed.

■ Reference manual

See the following for an explanation of the above display format:

- This manual
 - H.5 "Cluster Resource Management Facility Messages"
 - D.5 "Failed Resource and Operator Intervention Messages (GUI)"
 - D.7 "Shared Disk Connection Confirmation Messages"
 - D.8 "Patrol Diagnosis Messages"

D.4 Messages Related to Line Switching Unit

This section explains the messages of the line switching unit.

The message format is as follows:

FJSVcluster:security:program:message-number:message (details)

security :

Indicates the severity level of the message.

The severity levels of the message output by the line switching unit are classified into three types, namely, information (INFORMATION), warning (WARNING), and error (ERROR). For details, refer to the following table.

program :

Indicates the name of the program that outputs this message.

message-number :

Indicates the message number.

message :

Indicates the message text.

details :

Indicates the detailed classification code.

Number	Severity level	Meaning
4000-5999	Warning (WARNING)	A message providing notification of an error that is not so serious and which does not cause the abnormal end of a line switching unit.
????,6000-7999	Error (ERROR)	The message providing notification of an error that is so serious as to cause the abnormal end of a line switching unit.

D.4.1 Warning Message

5100 An error was detected in the failover unit of the line switching unit. (RCI:addr

LSU:mask status:status type:type)**Corrective action:**

No corrective action is required because processing is retried. If, however, retries fail repeatedly and if this warning occurs frequently, contact your Fujitsu customer engineer (CE).

Supplement

An error was detected in the switching control board of the line switching unit.

addr: Indicates the RCI address of the line switching unit in which an error was detected.

mask: Indicates the LSU mask to be controlled.

status: Indicates the an internal status of the line switching unit by error type.

type: Indicates an error type.

- 3: Indicates that the reserved status was not canceled.
status: The reserved status of each LSU included in the switching unit is indicated by the value of the LSU mask.
0: Indicates that the LSU is in the released status.
1: Indicates that the LSU is in the reserved status.
- 4: Indicates that the connection has not changed.
status: The status of the connection of each LSU included in the switching unit is indicated by the LSU mask value.
0: Indicates that the LSU is connected to port 0.
1: Indicates that the LSU is connected to port 1.
- 5: Indicates that the reserved status could not be created.
status: The reserved status of each LSU included in the switching unit is indicated by the value of the LSU mask.
0: Indicates that the LSU is in the released status.
1: Indicates that the LSU is in the reserved status.

LSU mask value

```
LSU15 LSU14 LSU13 LSU12 ... LSU03 LSU02 LSU01 LSU00
0x8000 0x4000 0x2000 0x1000 ... 0x0008 0x0004 0x0002 0x0001
```

D.4.2 Error Messages

Note

If an error message is output, analyze the log of the time zone in which the message was output from the “/var/adm/messages” message to check if any other error message had been output before that. If you found another error message, you need to take corrective action for this error message first.

???? Message not found!!**Corrective action:**

The text of the message that is correspondent to the message number is not available. Contact your Fujitsu systems engineer (SE).

6001 Insufficient memory. (detail:code1-code2)**Corrective action:**

One of the following could be the case:

- The memory resources are insufficient.
- The kernel parameter has incorrect settings.

Collect information required for troubleshooting. See “10.3 Collecting troubleshooting

information" in the "*PRIMECLUSTER Cluster Foundation Configuration and Administration*."

Reexamine the estimation of the memory resources that are required for the entire system. For information on the amount of memory required for cluster control, see the "*PRIMECLUSTER Installation Guide*," which is provided with each product.

If you still have the problem, confirm that the kernel parameter setting is correct by referring to the A.6.1 "Kernel parameter worksheet for using the resource database."

Change the settings if necessary, and then reboot the system. If above actions do not help you solve the problem, contact your Fujitsu systems engineer (SE).

code1 and *code2* indicate the information required for troubleshooting.

6002 Insufficient disk or system resources. (detail:*code1-code2*)

Corrective action:

One of the following could be the case:

- The disk resources are insufficient.
- The kernel parameter has incorrect settings.

Collect the information required for troubleshooting. See "10.3 Collecting troubleshooting information" in the "*PRIMECLUSTER Cluster Foundation Configuration and Administration*."

Confirm that there is sufficient disk space to enable the operation of PRIMECLUSTER. If necessary, delete any unnecessary files to create sufficient free space and then restart the system. For information on the amount of required disk space, see the "*PRIMECLUSTER Installation Guide*," which is provided with each product.

If you still have the problem, confirm that the kernel parameter settings are correct by referring to the A.6.1 "Kernel parameter worksheet for using the resource database." Change the settings if necessary, and then reboot the system.

If above actions do not help you solve the problem, contact your Fujitsu systems engineer (SE).

code1 and *code2* indicate the information required for troubleshooting.

6003 Error in option specification. (option:*option*)

Corrective action:

Specify the option correctly, and then re-execute the operation.

option indicates an option.

6004 No system administrator authority.

Corrective action:

Re-execute the process with system administrator's authority.

6006 Required option *option* must be specified.

Corrective action:

Specify the option, and then re-execute the operation.

option indicates an option.

6007 One of the required options (*option*) must be specified.

Corrective action:

Specify the option, and then re-execute the operation.

option indicates an option.

7101 SCF cannot be accessed because it is in the busy state. (type:*type*)

Corrective action:

Leave the operation undone for several minutes, and then re-execute accessing.

type indicates information for research.

7102 SCF open failed. (errno:errno)

Corrective action:

Contact your Fujitsu customer engineer (CE) to check whether the SCF is operating normally.
errno indicates an error number.

7103 SCF access failed. (errno:errno)

Corrective action:

Contact your Fujitsu customer engineer (CE) to check whether the SCF is operating normally.
errno indicates an error number.

7104 The subclass of the line switching unit cannot be identified. (RCI:addr Subclass:no)

Corrective action:

A line switching unit whose subclass cannot be identified is connected.

- *addr*: Indicates the RCI address of the line switching unit.
- *no*: Indicates the subclass of the line switching unit.
 - 0x01: Indicates a 4-line switching unit.
 - 0x02: Indicates a 16-line switching unit.

Confirm if the line switching unit is a supported product.

7105 The specified line switching unit does not exist. (RCI:addr)

Corrective action:

No line switching unit that is specified with the RCI address exists.

Confirm with your Fujitsu customer engineer (CE) whether the RCI address of the specified line switching unit is correct or it is connected.

addr indicates an RCI address.

7106 The power to the line switching unit is not on, or the RCI cable has been disconnected. (RCI:addr)

Corrective action:

Confirm if the power of the specified line switching unit is turned on and that the RCI cable is not disconnected.

addr indicates the RCI address of the line switching unit.

7108 Reservation of the line switching device failed. (RCI:addr LSU:mask retry:no)

Corrective action:

Although *no* times of attempts were made to reserve the switching unit, which was specified with *mask* of the line switching unit that was specified with RCI address (*addr*), reservation failed.

Check whether the line switching unit has failed, whether the RCI connection has an error, and whether the power-supply voltage is abnormal. If errors occur frequently, contact your Fujitsu customer engineer (CE).

addr indicates the RCI address of the line switching unit, while *mask* indicates a mask that represents a switching unit of the line switching unit and *no* indicates the retry count until an error is displayed.

Maintenance information (for system administrators)

Determine whether the specified line switching unit has an error.

7109 An error was detected in the switching control board of the line switching unit.

(RCI:addr status:status type:type)**Corrective action:**

An error was detected in the switching control board of the line switching unit.

addr: Indicates the RCI address of the line switching unit in which an error was detected.

status: Indicates the internal status of the line switching unit by error type.

type: Indicates the error type.

- 1: Error in the switching control system (*status*: status 0)
 - status*: Indicates the value of status 0 (see below) of the line switching unit.
 - 0x80: QANS (0: normal, 1: abnormal)
Indicates that the switching line of QSC remains in the asserted state (abnormal) although other than switchover processing is being performed.
 - 0x40: QAST (0: normal, 1: abnormal)
Indicates that the switching line of QSC cannot be asserted during switchover processing. Once an abnormal state arises, that state remains until the power supply is turned off.
- 2: Power/circuit error (*status*: status 0)
 - status*: Indicates the value of status 0 (see below) of the line switching unit.
 - 0x10: QENA (0: normal, 1: abnormal)
Indicates the QSC switchover function enabled state. If this Bit is ON, it indicates that every connected QSC is abnormal.
 - 0x08: DCNV (0: normal, 1: abnormal)
Indicates that the output voltage of the DC-DC converter, which is mounted in the QSC, is normal. If this Bit is ON, it indicates that the output voltage of the DC-DC converter is abnormal.
Remark: This bit is enabled only for a 4-line switching unit.
 - 0x04: PW12
0 is indicated for a single power unit while 1 indicates two power units.
Remark: This bit is enabled only for a 16-line switching unit.
 - 0x02: PRY1 (0: normal, 1: abnormal)
 - 0x01: PRY0 (0: normal, 1: abnormal)
Indicates whether the power supply is normal/abnormal. (Normal means that power is supplied without any failure.)
Remark: This Bit is enabled only for a 16-line switching unit.
- 3: QSC connection error (*status*: status 1)
 - status*: Indicates the value of status 1 (see below) of the line switching unit.
 - 0x80: HSC (0: 4-line switching unit, 1: 16-line switching unit)
Indicates if a 16-line switching unit is used.
 - 0x20: QSC1 (slot 1 mounted)
 - 0x10: QSC0 (slot 0 mounted)
Indicates the slot in which the QSC (switching control board) is mounted. Values other than 0x10 and 0x20 indicate errors.
 - 0x02: OBSY
Indicates that the other side of the duplicated QSC is presently executing switchover processing (canceling of reserve, switchover command 0, and switchover command 1).

Check whether the line switching unit has a failure, if the RCI connection has an error, or whether the power-supply voltage is abnormal. If these errors occur frequently, contact your Fujitsu customer engineer (CE).

Maintenance information (for system administrators)

Check whether the specified line switching unit has an error.

**7110 An error was detected in the switching unit of the line switching unit. (RCI:addr
LSU:mask status:status type:type)****Corrective action:**

An error was detected in the switching unit of the line switching unit.

addr: Indicates an RCI address of the line switching unit in to be controlled.

mask: Indicates an LSU mask which is the target of control

status: Indicates the internal status of the line switching unit by error type (for research).

type: Indicates an error type.

- 1: Indicates an erroneous state.

status: Indicates the abnormal state of each LSU, which is included in the switching unit, as the value of LSU mask.

0: Indicates that the relevant LSU is normal.

1: Indicates that the relevant LSU is abnormal.

- 2: Indicates that a request of canceling switchover/reserve has been sent to the unconnected LSU.

status: Indicates whether each LSU that is included in the switching unit is connected using the value of the LSU mask.

0: Indicates that the LSU is unconnected.

1: Indicates that the LSU is connected.

LSU mask value

LSU15 LSU14 LSU13 LSU12 ... LSU03 LSU02 LSU01 LSU00

0x8000 0x4000 0x2000 0x1000 ... 0x0008 0x0004 0x0002 0x0001

Check whether the line switching unit has a failure, if the RCI connection has an error, or if the power-supply voltage is abnormal. If these errors occur frequently, contact your Fujitsu customer engineer (CE).

Maintenance information (for system administrators)

Check whether the specified line switching unit has an error.

7111 The cluster event control facility is not running. (detail:code1-code2)**Corrective action:**

Collect information for troubleshooting for all nodes, and then contact your Fujitsu systems engineer (SE). For details on how to collect information, see Appendix C "Troubleshooting."

Reboot the node in which the error occurred. If you need to stop the node, execute the "shutdown(1M)" command.

code1 and *code2* indicate information items for diagnosis.

7112 Communication failed in the cluster event control facility (detail:code1-code2)**Corrective action:**

Collect information for troubleshooting for all nodes, and then contact your Fujitsu systems engineer (SE). For details on how to collect information, see Appendix C "Troubleshooting."

Reboot the node in which an error occurred. If you need to stop the node, execute the "shutdown(1M)" command.

code1 and *code2* indicate the information required for troubleshooting.

7113 Cluster event control facility: internal error. (detail:code1-code2)**Corrective action:**

Copy this message, collect debugging information, and then contact your Fujitsu systems engineer (SE). For details on how to collect debugging information, see Appendix

C "Troubleshooting."

After collecting debugging information from all nodes, reboot the node in which the error occurred. To stop the node, use the shutdown(1M) command.

code1 and *code2* indicate the information required for troubleshooting.

7116 Port number information is not set for resource SWLine. (rid:rid)

Corrective action:

Set u the port number attribute (port) of the line switching unit used for the resource SWLine.

rid indicates the resource ID of SWLine in the line switching unit.

7117 The port number specified for resource SWLine is incorrect. (rid:rid port:port)

Corrective action:

Set up the correct port number.

rid indicates the resource ID of the SWLine in the line switching unit while *port* indicates a port number.

7119 The LSU mask information has not been set for the shared resource SH_SWLine.

(rid:rid)

Corrective action:

Set up the mask (Isu_mask) attribute of the switching unit used for the shared resource SH_SWLine.

rid indicates the resource ID of the shared resource SH_SWLine in the line switching unit.

7121 The parent resource of the shared resource SH_SWLine is other than shared resource SH_SWU. (rid:rid)

Corrective action:

Re-create the shared resource SH_SWLine as a child resource of shared resource SH_SWU.

rid indicates the resource ID of the shared resource SH_SWLine in the line switching unit.

7122 The RCI address information has not been set for shared resource SH_SWU.

(rid:rid)

Corrective action:

Set up the RCI address attribute (addr) of the line switching unit used for the shared resource SH_SWU.

rid indicates the resource ID of the shared resource SH_SWLine in the line switching unit.

7125 The resource ID of the node connected to the specified port *no* (rid: *rid*) is incorrect.

Corrective action:

For the resource ID of the node that is connected to the specified port of the line switching unit, an incorrect resource ID of other than a node or nonexistent resource ID is specified. Set up the correct resource ID.

no indicates a port number in the line switching unit while *rid* indicates the resource ID.

7126 The resource ID (*rid*) of the same node is specified for ports 0 and 1.

Corrective action:

The same resource ID cannot be specified for port 0 and port 1 in the line switching unit. The same node cannot be specified as the operating and standby node.

Set up the correct resource ID of the node.

rid indicates the resource ID of the specified node.

7130 The specified resource ID (*rid*) cannot be deleted because it is being used.

Corrective action:

The specified resource ID cannot be deleted because it has been used for GDS

Confirm the resource ID to be deleted, and then set up the correct resource ID.

rid indicates the resource ID.

7131 The specified resource ID (*rid*) is not present in the shared resource class (*class*).

Corrective action:

Set up the correct resource ID.

rid indicates a resource ID while *class* indicates the class name of the shared resource class.

7132 The specified resource name (*name*) is not present in the shared resource class

(*class*).

Corrective action:

Set up the correct resource ID.

name indicates a resource name while *class* indicates the class name of the shared resource class.

<h2>D.5 Failed Resource and Operator Intervention Messages (GUI)</h2>

This section explains the messages of the failed resource and operator intervention. The message is displayed on the GUI:

D.5.1 Information Messages

0701 There are no failed resources.

Content:

No failed resource was found in the results of output with the “*cldispfaulttrsc*” command.

D.5.2 Error Messages

0766 The command terminated abnormally.

Content:

The “*cldispfaulttrsc*” command or the “*clreply*” command ended abnormally.

Corrective action:

Follow the corrective action shown in the message.

0767 Command execution failed.

Content:

The “clreply” command cannot be executed while accessing the node.

Corrective action:

If SysNode that cannot be referenced in the detailed information appears, you can respond to the operator intervention message by executing the “clreply” command on SysNode. To respond through with the GUI, restart Web-Based Admin View on SysNode.

In all other cases, restart Web-Based Admin View on the node that serves as the management server of Web-Based Admin View. For information on how to restart Web-Based Admin View, see “6.2 Restart” in the “Web-Based Admin View Operation Guide.”

If the failure cannot be solved, collect maintenance information and then contact your Fujitsu systems engineer (SE).

For details on the maintenance information, see “B.2 Troubleshooting information collection” in the “PRIMECLUSTER Web-Based Admin View Operation Guide.”

0790 An error occurred while collecting the fault resources.

Content:

Node connection failed while the resource data was being collected.

Corrective action:

Reboot the management server of Web-Based Admin View for the affected client. For details, see the “PRIMECLUSTER Web-Based Admin View Operation Guide.”

If the problem still cannot be solved, collect maintenance information and then contact your Fujitsu systems engineer (SE). For details on maintenance information, see “B.2 Troubleshooting information collection” in the “PRIMECLUSTER Web-Based Admin View Operation Guide.”

0791 You do not have the access authority to respond to this message.

Content:

The user account that logged on to Web-Based Admin View does not have the execute permission to respond to this operator intervention message.

Corrective action:

Log out from Web-Based Admin View. Retry to log in as root or as a user belonging to wvroot, clroot, or cladmin, and then respond to the operator intervention message.

0792 The error occurred while accessing the management server. Select [Continue], and then end the Resource Fault History.

Content:

An error occurred while accessing the management server of Web-Based Admin View.

Corrective action:

Click the *Continue* button to close the “Fault Resource List” screen. If the network between the browser and the management server is merely temporarily disconnected, select the *Continue* button to close the “Fault Resource List” screen. (For example, you need to select *Connect* when rebooting or when a LAN cable is temporarily disconnected). If a message output by Web-Based Admin View is displayed, follow the instructions for that message. If no message is output by Web-Based Admin View, choose *Fault Resource List* from the top menu to restart.

If the problem cannot be corrected by clicking the *Continue* button to reconnect, collect the maintenance information and then contact your Fujitsu systems engineer (SE). For information on collecting maintenance information, see “B.2 Troubleshooting information collection” in the “PRIMECLUSTER Web-Based Admin View Operation Guide.”

0765 Communication with the management server failed.**Content:**

A communication error occurred between the browser and the Web-Based Admin View management server. This error occurs when the client's browser attempts to respond to an operator intervention message.

Corrective action:

Click *OK* to close the error message screen.

If an error occurs even when you re-execute, use the "clreply" command to reply. If a message that is output by Web-Based Admin View is displayed, follow the instructions for that message.

If the problem cannot be solved through the above method, collect the maintenance information and then contact your Fujitsu systems engineer (SE). For information on collecting maintenance information, see "B.2 Troubleshooting information collection" in the "PRIMECLUSTER Web-Based Admin View Operation Guide."

For details on messages 0001 to 0099, see "Appendix A Message" in the "PRIMECLUSTER Web-Based Admin View Operation Guide."

D.6 Failed Resource and Operator Intervention Messages (CLI)

This section explains the messages of the failed resources and of operator intervention. These messages are displayed by executing the "CLI" command. The message format is as follows:

FJSVcluster: *type:program:message number:message type*

Message types are as shown below:

- QUESTION – Indicates a message for which operator intervention is required (numbers 1000 to 1999).
- INFORMATION – Indicates a message in which information such as the operation state is shown (numbers 2000 to 3999).
- ERROR – Indicates an error that caused an abnormal end (numbers 6000 to 7977, or "????" that indicates an unknown message number).

program

Indicates the program that has output the message.

message number

Indicates the message number.

message

Indicates the message text.

D.6.1 Operator Intervention Messages

1421 The userApplication " *userApplication* " did not start automatically because not all of the nodes on which it can run are online. Do you want to force the userApplication online on the SysNode " *SysNode* "? Message No.:*number*

Do you want to proceed? (no/yes) Warning:Forcing a userApplication online ignores

potential error conditions. Used improperly, this can result in data corruption. You should not use it unless you are certain that the `userApplication` is not running anywhere in the cluster.



Note

If this message is output to the console and `/var/adm/messages`, “month day time node name” might be output to the beginning of the second and subsequent lines of the message independently of the text of the message. You can ignore it.

Corrective action:

This operator intervention message is displayed when `userApplication` cannot be online because RMS is inactive on some of the nodes that are designed to execute applications. Use the `clreply` command to respond from the command prompt (see “Manual Pages”).

If you select yes, the operator intervention function will execute the “`hvswitch`” command and `userApplication` will go online. Confirm whether `userApplication` is in the online state by using Cluster Admin or executing the “`hvdisp`.” (For details on the “`hvswitch`” command and the “`hvdisp`” command, see “Manual Pages”).

If you select no, the RMS command that is used to change the `userApplication` state cannot be executed.

`userApplication` indicates `userApplication` that is not online in any node.

`SysNode` indicates `SysNode` on which `userApplication` will be online if you select yes.

`number` indicates a message number.

1422 On the `SysNode " SysNode "`, the `userApplication " userApplication "` is in the failed state due to a fault in the resource "`resource`". Do you want to clear the fault?

Message No.:*number*

Do you want to proceed? (yes/no)

Corrective action:

Confirm that the resource indicated by `resource` has recovered. If you need to reply from CLI, execute the “`clreply`” command.

If you select yes, the operator intervention function will execute the “`hvutil`” command by specifying the clear option in the “`hvutil`” command and also brings `userApplication` Offline. Confirm that `userApplication` has gone Offline by executing the “`hvdisp`” command.

If you select no, the operator intervention function does not execute the RMS command to bring `userApplication` Offline.

`SysNode` indicates the name of `SysNode` on which the failure occurred. `userApplication` indicates the name of `userApplication` in which the failure occurred. `resource` indicates the name of the resource that caused a failure in `userApplication`. `number` indicates a message number.

1423 On the `SysNode " SysNode "`, the `userApplication " userApplication "` has the faulted resource "`resource`". The `userApplication " userApplication "` did not start automatically because not all of the nodes on which it can run are online. Do you want to

force the userApplication online on the SysNode " SysNode "?

Message No.:*number*

Do you want to proceed? (no/yes) **Warning:**Forcing a userApplication online ignores potential error conditions. Used improperly, this can result in data corruption. You should not use it unless you are certain that the userApplication is not running anywhere in the cluster.



Note

If this message is output to the console and /var/adm/messages, "month day time node name" might be output to the beginning of the second and subsequent lines of the message independently of the text of the message. You can ignore it.

Corrective action:

Confirm that the resource indicated by *resource* has recovered. If you need to reply from CLI, execute the "clreply" command.

If you select yes, the operator intervention function will execute the "hvswitch" command and userApplication will go Online. Confirm that userApplication has gone Offline by executing the "hvdisp" command.

If you select no, the operator intervention function will not execute the RMS command to bring userApplication Online.

SysNode indicates the name of SysNode in which the failure occurred. *userApplication* indicates the name of userApplication in which the failure occurred. *resource* indicates the name of the resource that caused the failure in userApplication. *number* indicates the message number.

D.6.2 Information Messages

2620 On the SysNode " SysNode "; the userApplication " *userApplication* " transitioned to state *state* . Therefore, message " *number* " has been canceled.

Content:

Since the userApplication state has changed, the message has been cancelled. You do not need to respond to the operator intervention message.

SysNode indicates the name of SysNode in which the userApplication state has been changed. *state* indicates the userApplication state. *number* indicates the message number.

2621 The response to the operator intervention message " *number* " was action.

Content:

The response to the operator intervention message has been made.

number indicates the number of the operator intervention message to which you responded. *action* indicates with or without response by yes or no.

2622 There are no outstanding operator intervention messages.**Content:**

There is no operator intervention messages that have yet to be processed.

2700 The resource failure has been recovered. SysNode:SysNode**userApplication:userApplication Resource:resource****Content:**

The resource recovered from the failure.

SysNode indicates the name of SysNode whose resource has been recovered. *userApplication* indicates the name of the userApplication to which the recovered resource belongs. *resource* indicates the name of the resource that has recovered from the error state.

2701 A failed resource has recovered. SysNode:SysNode**Content:**

SysNode that was in the Faulted state due to a node panic entered the Online state.

SysNode indicates a recovered SysNode.

D.6.3 Error Messages

6000 An internal error occurred. (function:function detail :code1-code2-code3-code4)**Content:**

An internal error occurred in the program. *function*, *code1*, *code2*, *code3*, and *code4* indicate the debugging information for error diagnosis.

Corrective action:

Collect the debugging information. Then, contact your Fujitsu systems engineer (SE). See “11.3 Collecting Troubleshooting Information” in the “PRIMECLUSTER Cluster Foundation Configuration and Administration.”

code1, *code2*, *code3*, and *code4* indicate the information that is required by your Fujitsu systems engineer (SE).

6001 Insufficient memory. (detail:code1-code2)**Content:**

The memory resources of the node are insufficient to output this message. *code1* and *code2* indicate the debugging information.

Corrective action:

Recheck the memory resources. If the problem still cannot be solved, collect debugging information, and then contact your Fujitsu systems engineer (SE). See “11.3 Collecting Troubleshooting Information” in the “PRIMECLUSTER Cluster Foundation Configuration and Administration.”

code1 and *code2* indicate the debugging information required for your Fujitsu systems engineer (SE).

6002 Insufficient disk or system resources. (detail:code1-code2)**Content:**

The disk resources or system resources of the node are insufficient to output this message.

code1 and *code2* indicate debugging information.

Corrective action:

Recheck the usable capacity of the disk resource and the system resource. If the problem still

cannot be solved, collect debugging information, and then contact your Fujitsu systems engineer (SE). See “11.3 Collecting Troubleshooting Information” in the “PRIMECLUSTER Cluster Foundation Configuration and Administration.”

code1 and *code2* indicate the debugging information required for Fujitsu systems engineer (SE).

6003 Error in option specification. (option:option)

Content:

The specification of the CLI option is disabled.

Corrective action:

Specify a correct option, and then re-execute the command.

option indicates an option of the command.

6004 No system administrator authority.

Corrective action:

Re-execute the command with system administrator authority.

6009 If option *option1* is specified, option *option2* cannot be specified.

Content:

Two options specified with the command conflict.

Corrective action:

Re-execute the command by specifying either one of the options.

6208 Access denied (command).

Corrective action:

Collect debugging information and then contact your Fujitsu systems engineer (SE). See “11.3 Collecting Troubleshooting Information” in the “PRIMECLUSTER Cluster Foundation Configuration and Administration.”

target indicates a command name.

6615 The cluster configuration management facility is not running.(detail:code1-code2)

Corrective action:

Reboot the node on which this message is displayed and then reactivate the resource database. If this message appears again, collect debugging information and then contact your Fujitsu systems engineer (SE). See “11.3 Collecting Troubleshooting Information” in the “PRIMECLUSTER Cluster Foundation Configuration and Administration.”

code1 and *code2* indicate the debugging information required for your Fujitsu systems engineer (SE).

6616 Cluster configuration management facility: error in the communication routine.(detail:code1-code2)

Corrective action:

Collect debugging information, and then contact your Fujitsu systems engineer (SE). See “11.3 Collecting Troubleshooting Information” in the “PRIMECLUSTER Cluster Foundation Configuration and Administration.”

code1 and *code2* indicate the debugging information required for your Fujitsu systems engineer (SE).

6651 The specified instruction contains an error.

Content:

This message will not be displayed on a client system on which a browser is active. This message is displayed on the standard output when you respond to the operator intervention message with the CLI command (clreply). If a string other than yes or no is to be entered, this message will be displayed.

Corrective action:

Specify the option correctly, and then re-execute the processing.

6750 A resource has failed. SysNode:SysNode userApplication:userApplication**Resource:resource****Corrective action:**

Confirm the state of userApplication in which the corrected resource is registered by using the RMS main window or executing the "hvdisp(1M)" command. You can also confirm the userApplication state by responding to the operator intervention message that is displayed after RMS is started. If userApplication is Faulted, you need to clear the Fault by using the RMS main window or specifying the "-c" option of the "hvutil(1M)" command.

SysNode indicates the name of SysNode in which a resource has failed. userApplication indicates the name of userApplication to which the failed resource belongs. resource indicates the name of the resource that has failed.

6751 A SysNode has failed. SysNode:SysNode**Corrective action:**

Respond to the operator intervention message that is displayed after the node is started or confirm the state of userApplication running on the node in which the failure occurred, by using the RMS main window or executing the "hvdisp(1M)" command. If userApplication is Faulted, you need to clear the Fault by using the RMS main window or specifying the "-c" option of the "hvutil(1M)" command.

SysNode indicates the SysNode in which a failure occurred.

6752 The processing was canceled due to the following error.**Error message from RMS command****Content:**

If you execute the RMS command (hvdisp) to enable the history function for the failed resource or the operation intervention function, and this fails, an error message will be displayed. Examine this error message and, after taking an appropriate correction, execute the required processing again.

Corrective action:

Confirm the contents of this message and, after taking the required corrective action, re-execute the processing.

6753 Failed to process the operator intervention message due to the following error.(message number: *number* response: *action* command : *command*)**Error message from RMS command****Content:**

Since the RMS command ended abnormally, the operator intervention function for the message failed.

Corrective action:

Note the contents of this message and, after applying an appropriate correction, re-execute the

required processing.

number indicates the operator intervention message for which processing failed. *action* indicates the first response to the message from the operator with either yes or no. *command* indicates the RMS command which ended abnormally. “Error message from RMS command” indicates an error message that the RMS command transmits when a standard error occurs.

6754 The specified message number (*number*) does not exist.

Corrective action:

This message is output in the following situations:

- The operator specified a nonexistent message number when executing the “clreply” command. This problem can be solved by specifying a message number that is included in the unfinished message list.
- The message for which a response was entered has been canceled. This occurs when the message gets old since the application state has been changed. You do not have to take any action.
- The operator intervention function has automatically replaced the message for which a response has been entered with other message. For example, when the operator intervention function’s message number 1422 is replaced by the message number 1423 and vice versa. In such a case, the operator intervention function responds to the first message, displays another message, and advises a user that the message number has been changed.

number indicates the number of operator intervention messages.

6755 Failed to respond to the operator intervention message due to the SysNode

(*SysNode*) stop.(message number:*number* response : *action*)

Content:

Since the node indicated by SysNode has stopped, the response to the operator intervention message failed.

Corrective action:

Reboot the node, and then confirm that RMS is running.

SysNode indicates the SysNode name of the node that is stopped. *number* indicates the number of the operator intervention messages that failed to respond. *action* indicates the operator’s response by yes or no.

D.7 Shared Disk Connection Confirmation Messages

This section explains the messages displayed by confirming the shared disk connection.

The message is displayed in the syslogd(1M) and the CRM main window in the following cases:

- When a new shared disk device is detected
- When an error is detected in the shared disk device

The message format is as follows:

```
FJSVcluster:type:program:message number:message
type
```

The message types are shown below:

- INFORMATION – A message indicating information (2000 to 3999).
- ERROR – A message indicating an error in the shared disk device (6000 to 7999 or “????” that shows an unknown message number).

program

Indicates the program from which the message is output.

message number

Indicates the message number.

message

Indicates the message text.



Note

If a message other than those described in this chapter is output, see H.5 "Cluster Resource Management Facility Messages."

D.7.1 Information Message

2914 A new disk device(*disk*) was found.

Corrective action:

Register a new detected shared disk device (*disk*) in the resource database by executing the "clautoconfig(1M)" or using the CRM main window. For details on the "clautoconfig(1M)" command, see the manual pages of "clautoconfig (1M)."

disk indicates a newly detected shared disk device.

D.7.2 Error Messages

6807 Disk device (NodeID *NodeID*, *disk*) cannot be detected.

Content:

The power to the disk unit may not be turned on or the disk may be disconnected. If an attempt is made to start userApplication, userApplication may not start normally.

Two messages, namely, this message and that of message number 6836 may be displayed depending on connection.

Corrective action:

Confirm that the power to the shared disk device is turned on and that the shared disk device is connected correctly. If power is not being supplied to the shared disk device, stop the node, turn on the power to the shared disk device, and then boot the node. If the connection of the shared disk device is incorrect, stop the node, rectify the connection, and then boot the node.

NodeID indicates the identification number of the node to which the disk unit was connected while *disk* indicates the shared disk that could not be detected.

6836 The disk device (NodeID *NodeID*, *disk*) has changed.

Content:

The wiring of the shared disk device could be incorrect. If an attempt is made to launch the userApplication in the current state, userApplication may not start up normally.

Two messages, namely, this message and that of message number 6807 may be displayed depending on connection.

Corrective action:

Confirm that the shared disk device is connected correctly. If the connection is incorrect, stop the node, correct the connection, and then boot the node.

NodeID indicates the node identification number to which the shared disk device is connected while *disk* indicates the shared disk in which an error has been detected.

D.8 Patrol Diagnosis Messages

This section explains the messages displayed by running patrol diagnosis facility.

The message is displayed in the “syslogd(1M)” command and the CRM main window in the following cases:

- When patrol diagnosis starts and ends
- If the hardware recovers after the operation for recovery from hardware failure
- When an error is detected as a result of patrol diagnosis

The message format is as follows:

```
FJSVcluster:type:program:message number:message
type
```

The type of message is shown below:

- INFORMATION – A message indicating information (2000 to 3999).
- ERROR – A message indicating an error in patrol diagnosis (6000 to 7999 or “???” that shows an unknown message number).

program

Indicates the program from which the message is output.

message number

Indicates the message number.

message

Indicates the message text.



Note

If a message other than that included in this chapter is displayed, see H.5 "Cluster Resource Management Facility Messages."

D.8.1 Information Messages

3050 Patrol monitoring started.

3051 Patrol monitoring stopped.

3052 Diagnostic access to broken LAN device succeeded. (device:*altname* rid:*rid*)

Supplement

altname indicates the interface name of the specified LAN device while *rid* indicates its resource ID.

3053 Diagnostic access to broken DISK device succeeded. (device:*altname* rid:*rid*)

Supplement

altname indicates the device name of the shared device that is operating normally while *rid* indicates its resource ID.

D.8.2 Error Messages

6690 The specified userApplication or resource is not monitored. (*resource*)

Corrective action:

userApplication or the resource is not registered as it is monitored by the patrol diagnosis. Reexamine the configuration of the patrol diagnosis by referring to 6.7 "Setting Up Patrol Diagnosis."

The specified userApplication or resource will be output to *resource*.

6691 The userApplication cannot do the patrol monitoring because of *status* .

Corrective action:

Specify userApplication that is in the following state, and then re-execute:
Standby, Offline, Faulted, Deact

The state of userApplication will be output to *status*.

6692 Patrol monitoring timed out.

Corrective action:

Confirm that power is being supplied to the node on which patrol is enabled. Power on the node if necessary, and then re-execute.

Confirm that RMS is activated.

If RMS is not activated, start the RMS with Cluster Admin or the "hvcm(1M)" command and then re-execute operation.

7050 Diagnostic access to LAN device failed. (node:*node* device:*altname* rid:*rid* detail:*code*)

Corrective action:

Take corrective action by referring to 7.4.2 "Corrective Action when Patrol Diagnosis Detects a Fault."

The interface name of the LAN device for which a failure is diagnosed is output with *altname*. *node*, *rid*, and *code* indicate the information required for debugging.

7051 Diagnostic access to LAN device terminated abnormally. (node:*node* device:*altname* rid:*rid* detail:*code*)

Corrective action:

Collect debugging information, and then contact your Fujitsu systems engineer (SE). See "11.3 Collecting Troubleshooting Information" in the "PRIMECLUSTER Cluster Foundation Configuration and Administration."

An interface name of the LAN device for which a failure is diagnosed is output with *altname*. *node*, *rid*, and *code* indicate debugging information.

7052 Diagnostic access to DISK device failed. (node:*node* device:*altname* rid:*rid* detail:*code*)

Corrective action:

Take corrective action by referring to 7.4.2 "Corrective Action when Patrol Diagnosis Detects a Fault."

A device name for which a failure is diagnosed is output with *altname*. *node*, *rid*, and *code*

indicate debugging information.

7053 Diagnostic access to DISK device terminated abnormally. (node:node device:*altname* rid:*rid* detail:*code*)

Corrective action:

Collect debugging information, and then contact your Fujitsu systems engineer (SE). See “11.3 Collecting Troubleshooting Information” in the “PRIMECLUSTER Cluster Foundation Configuration and Administration.”

A shared device name for which a failure is diagnosed is output with *altname*. *node*, *rid*, and *code* indicate debugging information.

7054 Cannot open shared disk device for diagnostic access. (node:node device:*altname* rid:*rid* detail:*code*)

Corrective action:

Specify the available hardware in which patrol diagnosis is enabled. See 6.7 "Setting Patrol Diagnosis."

The device name that could not found can be output with *altname*. *node*, *rid*, and *code* indicate debugging information.

7055 Cannot open LAN device for diagnostic access. (node:node device:*altname* rid:*rid* detail:*code*)

Corrective action:

Specify the available hardware in which patrol diagnosis is enabled. See 6.7 "Setting Patrol Diagnosis."

The interface name of the LAN device that could not be found can be output with *altname*. *node*, *rid*, and *code* indicate debugging information.

7056 Diagnostic access to LAN device failed due to improper activation flag setting.(node:node device:*altname* rid:*rid* detail:*code*)

Corrective action:

The flag used when the LAN device is activated is in the inadequate state such as not UP and not BROADCAST. After confirming the system configuration, activate the device correctly. Confirm the flag by executing the “ifconfig(1M)” command.

- UP must be set.
- BROADCAST must be set.
- LOOPBACK must not be set.
- POINTOPOINT must not be set.
- NOARP must not be set.

The network device name, which is in the inadequate state, can be output with *altname*. *node*, *rid*, and *code* indicates debugging information.

D.9 userApplication Configuration Wizard GUI Messages

This section explains the messages of the userApplication Configuration Wizard GUI.

D.9.1 Information messages

0801 : Do you want to exit userApplication Configuration Wizard GUI?

Corrective action:

To exit the userApplication Configuration Wizard GUI, select *Yes*. If you do not want to exit the GUI, select *No*.

0802 : Do you want to cancel the setup process?

Corrective action:

To interrupt the process being operated by the userApplication Configuration Wizard GUI, select *Yes*. To cancel the interruption, select *No*.

0803 : Do you want to register setup in a cluster system?

Corrective action:

To register the setup information to the system, select *Yes*. If you do not want to register the setup information to the system, select *No*.

0805 : GUI is generating RMS Configuration.

Corrective action:

This message is automatically cleared when RMS Configuration generation is completed. Wait until this message is cleared.

0807 : Do you want to remove only selected userApplication (*userApplication name*)?

Do you want to remove all the resources under userApplication?

Corrective action:

To delete only userApplication, select *userApplication only*. To delete all resources under userApplication as well, select *All*. To cancel the deletion, select *Cancel*. "*userApplication name*" represents the name of userApplication to be deleted.

0808 : Do you want to remove only selected Resource (*resource name*) and all the resources under Resource?

Corrective action:

To delete the resource indicated by "*resource name*" in the message and the resources under that resource, select *Yes*. If you do not want to delete the resources, select *No*.

0810 : Node name takeover is registered or removed in userApplication. You need to restart SysNode to enable or disable takeover network. Restart SysNode after completing setup.

Corrective action:

As soon as the setup process is completed, restart all SysNode that contain userApplication for which node name takeover was set.

0813 : GUI is reading RMS Configuration.

Corrective action:

The userApplication Configuration Wizard GUI collects RMS Configuration information.
The GUI cannot be closed until the process in the GUI ends.

0814 : GUI is saving RMS Configuration in a system.

Corrective action:

The userApplication Configuration Wizard GUI collects RMS Configuration information.
The GUI cannot be closed until the process in the GUI ends.

0815 : GUI is generating RMS Configuration.

Corrective action:

The userApplication Configuration Wizard GUI collects RMS Configuration information.
The GUI cannot be closed until the process in the GUI ends.

0816 : Do you want to generate RMS Configuration?

Corrective action:

If you want the userApplication Configuration Wizard GUI to generate RMS Configuration information, select *Yes*. If you do not want the GUI to generate the information, select *No*.

0817 : Do you want to distribute RMS Configuration?

Corrective action:

If you want the userApplication Configuration Wizard GUI to distribute RMS Configuration information, select *Yes*. If you do not want the GUI to distribute the information, select *No*.

D.9.2 Warning Messages

0830 : Since other client is using userApplication Configuration Wizard GUI or the hww(1M), GUI cannot be started.

Corrective action:

Check whether the userApplication Configuration Wizard GUI has already been started in another client or whether another client is using the “hww” command. After the other operation is completed, start the GUI or command again.

Even if the Web browser or the cluster management server of Web-Based Admin View is restarted while the GUI is being displayed, this message may be displayed at the next startup. If this is the case, wait about five minutes, and then restart the Web browser and the GUI.

0832 : Cluster resource management facility is not running. Since a list of candidate interfaces cannot be obtained, GUI is terminated.

Corrective action:

The GUI was terminated because a candidate list could not be obtained when a disk class, procedure, or takeover network resource for Global Disk Services (GDS) was being created. Initialize the resource database, register the automatic resource, specify the Gds and procedure settings, and then restart the GUI.

0833 : RMS is running. Since Configuration might not be saved, GUI is terminated.

Corrective action:

RMS is running. You might fail to generate or distribute the configuration information that you were trying to create or modify. Stop RMS, and then re-execute the operation.

0834 : An invalid character is included.**Corrective action:**

A userApplication name, a resource name, a script name, or a script path includes an disabled character. Reenter the correct value.

0835 : Removing resource (*resource name*) will concurrently remove userApplication (*userApplication name*). Do you want to continue?**Corrective action:**

The system is about to delete all resources under userApplication. To delete userApplication indicated by "*userApplication name*" in the message and all resources under userApplication, select Yes. If you do not want to execute deletion processing, select No.

0836 : A name is not entered.**Corrective action:**

Enter the userApplication name, the resource name, or the script name.

0837 : A value is invalid.**Corrective action:**

The number that was entered for TIMEOUT or net mask is a disabled value. Enter an appropriate value.

0838 : The specified takeover IP address is not available.**Corrective action:**

Enter another takeover IP address.

0839 : There is an incorrect setup.**Corrective action:**

Change the attribute (that has the incorrect data), and continue the operation.

0840 : The takeover network name has been defined. Do you want to use the following definitions?**Corrective action:**

Information on the takeover network is already specified in the `/usr/opt/reliant/etc/hvipalias` file. To use the values that were set, select Yes.

If you select No, the userApplication Configuration Wizard GUI re-creates the takeover network information in the previous file and in `/etc/inet/hosts`. In this case, the takeover network information can be deleted automatically from `/usr/opt/reliant/etc/hvipalias` and `/etc/inet/hosts` when the `Ipaddress` resource is deleted.

0841 : There is an attribute different than the ones of other resources. Do you want to continue?**Corrective action:**

Check that the displayed attribute values are correct. If you select Yes, the specified attribute will be set.

0848 : The file name is not specified.

Corrective action:

Enter the path of the reference file.

0849 : A required setup is missing.

Corrective action:

Set the required items in the screen.

0852 : It is not a proper combination.

Corrective action:

You need to set two or more userApplication for one exclusion group.

0856 : The selected userApplication or Resource cannot be edited.

Corrective action:

Change the userApplication name or resource name, and execute the setup process again.

0857 : The specified takeover Ipaddress or host name has been used.

Corrective action:

Enter another IP address or host name.

0859 : Invalid file name or path.

Corrective action:

Enter another reference file path.

0860 : The specified file exists. Do you want to replace it?

Corrective action:

The file to be created already exists. If you select *Yes*, the existing file will be replaced. If you select *No*, the existing file will not be replaced.

0861 : The specified interface is different. Do you want to set up IP address?

Corrective action:

The IP address segment that is assigned to the network interface card (NIC) for the takeover network is different. To continue the setup with the assigned IP address segment, select *Yes*. To select the NIC again, select *No*.

0866 : The file system has been used.

Corrective action:

The file system that you tried to create is already being used. Set another device path and mount point.

0867 : Since a list of candidate interfaces cannot be obtained. The process is exited.

Corrective action:

Candidate interfaces to be set to the resource could not be obtained. Check whether interfaces were previously registered to the cluster resource management facility, and then re-execute the operation.

0868 : It is not an executable file.

Corrective action:

The specified file is not executable. Use another file, or add an execute permission to the file.

D.9.3 Error messages

0880 : A non-classified error occurred.

Corrective action:

An error occurred in the userApplication Configuration Wizard GUI.

Collect Java console information, detailed error information, and maintenance information, and contact a Fujitsu technician (SE).

For maintenance information, see Appendix C "Troubleshooting."

0881 Connection to the server failed.

Corrective action:

An internal server contradiction or an event that caused a network disconnection between the Web browser and the cluster management server (restart, shutdown, emergency stop, LAN cable disconnection) may have occurred.

If a Web-Based Admin View message is displayed, take corrective action for that message.

If a Web-Based Admin View message is not displayed, respond to this message and restart the userApplication Configuration Wizard.

If the problem cannot be resolved by the action described above, collect Java console information, detailed error information, and maintenance information, and contact your Fujitsu system engineer.

For maintenance information, see Appendix C "Troubleshooting."

0882 A non-supported package is installed. Check the version.

Corrective action:

A package having a different version from the package version required by the userApplication Configuration Wizard GUI is installed in the cluster node. See the information that was output to (detailed information), and reinstall the correct package of the cluster node.

0883 Since the specified file is in the non-supported format, it cannot be edited.

Corrective action:

The file cannot be edited because it is not a Bourne, C, or Korn shell file. Specify another file.

0886 : Since a list of candidate interfaces that can set in Resource. The process is exited.

Corrective action:

A candidate list of the information to be set to Resource could not be obtained. Check whether the cluster resource management facility is operating, whether automatic resource registration was executed, and whether Gds and GIs have been set up. If any of these setup operations has not been completed, correct them, and execute the process again.

0888 : The command is abnormally terminated.

Corrective action:

Execute the command again, and if you still have the same problem, collect Java console information, detailed error information, and maintenance information, and then contact your

Fujitsu system engineer.

The message that is output from the command may contain the "FJSVcluster" keyword and a message number. In this case, take corrective action described in H.5 "Cluster Resource Management Facility Messages."

For maintenance information, see Appendix C "Troubleshooting."

0889 : The command execution failed.

Corrective action:

Execute the command again, and if you still have the same problem, collect Java console information, detailed error information, and maintenance information, and then contact a Fujitsu technician (SE).

For maintenance information, see Appendix C "Troubleshooting."

0890 The SysNode for executing a command cannot be found.

Corrective action:

When the three-layer configuration of Web-Based Admin View is used, no cluster node, which can be accessed from the management server, can be found. The operating status of Web-Based Admin View can be confirmed by executing `/etc/opt/FJSVwvbs/etc/bin/wvstat`.

If the problem cannot be improved when the environment of Web-Based Admin View has no problem, collect Java console information, detailed error information, and maintenance information, and then contact your Fujitsu systems engineer (SE).

For maintenance information, see Appendix C "Troubleshooting."

0891 Reading of the RMS Configuration failed.

Corrective action:

The RMS configuration information cannot be analyzed.

If `userApplication` or `Resource` is not created, change to other Configuration information.

If the problem cannot be improved, collect Java console information, detailed error information, and maintenance information, and then contact your Fujitsu systems engineer (SE).

For maintenance information, see Appendix C "Troubleshooting."

0893 : RMS Configuration generation failed.

Corrective action:

Start the operation again from the beginning.

If the problem is not resolved by the above action, collect Java console information, detailed error information, and maintenance information, and then contact your Fujitsu system engineer.

For maintenance information, see Appendix C "Troubleshooting."

0895 : RMS Configuration distribution failed.

Corrective action:

Check the following:

1. Whether there are resources that are not related to any `userApplication`
2. Whether there is `userApplication` that does not have any resources

If one or both of the above conditions are found, delete any unnecessary `userApplication` and resources. If none of the above conditions is found, do the operation again from the beginning.

If an error still occurs, collect Java console information, detailed error information, and maintenance information, and then contact your Fujitsu system engineer. For maintenance information, see Appendix C "Troubleshooting."

D.9.4 Messages of the wgcncfclient Command

The message of the “wgcncfclient” command is displayed in the format shown below:

```
wgcncfclient: ERROR: message number: message
```

A list of messages is given below:

0001: Illegal option.

Corrective action:

Confirm how to specify these options and option arguments, and then execute the command correctly.

0002: No system administrator authority.

Corrective action:

Execute the command with system administrator authority.

0003: File not found. (file:file-name)

Corrective action:

The operation environment file does not exist.
Re-install the “FJSVwvucw” package.

0004: Editing of the file failed.

Corrective action:

This message could be output when the state of the system is unstable such as when there is insufficient memory.

If this message is displayed for any other reason, follow the instructions given as the corrective action.

If the same error is output even when you re-execute the command, collect the debugging information and then contact your Fujitsu system engineer.

0005: Unknown keyword. (keyword:keyword)

Corrective action:

Confirm the specified keyword, and then execute the command with the correct keyword.

0006: The distribution of the file failed.

Corrective action:

Confirm that CRM is running on all cluster nodes including the node on which the command was executed. Activate CRM on all nodes if necessary, and then execute the command.

Check whether the state of any cluster node is unstable because of insufficient memory, and then re-execute the command. If you specify the “-v” option at this time, you can determine the node on which the failure occurred.

If the same error is output again, collect debugging information and then contact your Fujitsu systems engineer.

0007: The cluster configuration management facility is not running.

Corrective action:

Confirm that CRM is running on all cluster nodes including the node on which the command was executed. Activate CRM on all nodes if necessary, and then execute the command. Normally, a distribution failure could not occur when CRM is running on all nodes. Check whether the

state of any cluster node is unstable because of insufficient memory. Correct the problem if necessary, and then execute the command again.

If you specify the “-v” option at this time, you can determine the node on which a failure occurred. If the same error is output repeatedly, collect debugging data and then contact your Fujitsu system engineer.

0009: The command received a signal.

Corrective action:

A signal is received during the execution of the command.

If the same error is output again when you re-execute, collect debugging data and then contact your Fujitsu system engineer.

0000: Message not found!!

Corrective action:

An unexpected error occurred.

If the same error is output again when you re-execute, collect debugging data and then contact your Fujitsu system engineer.

D.10 Procedure Resource Messages

This section explains the messages that may be displayed when a cluster application uses a procedure resource.

The messages are output to syslogd(1M) with the following format:

FJSVcluster:*type:program:message number:message*

type

Indicates the type of message as follows:

- INFO – Displays information (numbers 1000 to 1999).
- ERROR – Indicates an error (numbers 6000 to 7999).

program

Identifies the program that produced the message.

message number

Identifies the message by a number.

message

This is the actual message text.



Note

If a message that is not shown in this section is output, see H.5 "Cluster Resource Management Facility Messages."

D.10.1 Error Messages

6002 Insufficient disk or system resources. (detail:code1-code2)

Insufficient disk or system resources. (detail:code1-code2)

Corrective action:

The disk or system resources are insufficient for system operation.

code1 and *code2* indicate the information required for troubleshooting.

See the installation guide and check that there is space available in the required directories. If

there is insufficient area, delete unnecessary files to secure more area.

If the problem cannot be resolved by this action, collect debugging information, and then contact your Fujitsu system engineer. For details on collecting debugging information, see Appendix C "Troubleshooting."

6617 The specified state transition procedure file does not exist.

Corrective action:

Specify the state transition procedure file correctly, and then re-execute.

If the problem cannot be solved with this corrective action, collect debugging information and then contact your Fujitsu systems engineer (SE). For details on collecting debugging information, see Appendix C "Troubleshooting."

6618 The state transition procedure file could not be written. A state transition procedure file with the same name already exists.

Corrective action:

To overwrite the state transition procedure file, specify the "-o" option and then re-execute.

6619 The state transition procedure file could not be written. There was an error in the resource class specification.

Corrective action:

Specify the resource class correctly, and then re-execute. The available resource classes are file names under /etc/opt/FJSVcluster/classes.

Confirm that the character string specified as the resource class contains no errors.

**6621 Could not perform file operation on state transition procedure file.
(detail:code1-code2)**

Corrective action:

- Confirm the disk resource from which the state transition procedure is retrieved or the node resource of the file system is sufficient by executing the "df(1M)" command. Correct the insufficient resource problem or change the location from which the state transition procedure is retried, and do the operation again.
- Confirm the disk resource on which the cluster system is installed or the node resource of the file system is sufficient by executing the "df(1M)" command. Correct the insufficient resource problem, and do the operation again.

If the problem cannot be solved even by applying with the corrective actions, collect debugging information and then contact your Fujitsu systems engineer (SE). For details on debugging information, see Appendix C "Troubleshooting."

code1 indicates debugging information while *code2* indicates error number.

6623 Cannot delete the specified state transition procedure file.

Corrective action:

You can delete only the state transition procedure file that was defined by a user. For information on how to delete it, refer to the manual of the product that provides the state transition procedure file.

6624 The specified resource does not exist in cluster service. (resource:resource

rid:rid)

The specified resource does not exist in the cluster service. (resource: resource rid:rid)

Corrective action:

A procedure resource that is registered to the cluster application is not in the resource database. This message is not output if the cluster application was registered by using the userApplication Configuration Wizard(GUI) and executing the "hvw(1M)" command. However, if this occurs, collect debugging information and contact your Fujitsu system engineer. For details on collecting debugging information, see Appendix C "Troubleshooting."

If hvw(1M) was used to register the procedure resource to the cluster application by FREECHOICE, check that the procedure resource displayed in the message text is not registered to the resource database by executing the "clgettree(1)" command. For details on the "clgettree(1)" command, see the manual page for clgettree(1M).

If the procedure resource is not registered to the resource database, register the procedure resource displayed in the message to the resource database. See "PRIMECLUSTER Products,"

If the procedure resource is registered to the resource database, collect debugging information and contact your Fujitsu system engineer. For details on collecting debugging information, see Appendix C "Troubleshooting."

Resource indicates the resource name that is not registered to the resource database, and *rid* indicates the resource ID of the resource that is not registered to the resource database.

6680 The specified directory does not exist.

Corrective action:

Specify a correct directory, and then re-execute.

6817 An error occurred during state transition procedure execution. (error procedure:procedure detail:code1-code2-code3-code4-code5-code6-code7)

An error occurred during state transition procedure execution. (error procedure:procedure detail:code1-code2-code3-code4-code5-code6-code7)

Corrective action:

Collect debugging information and contact your Fujitsu system engineer. For details on collecting debugging information, see Appendix C "Troubleshooting."

procedure indicates the state transition procedure in which the error occurred. If the state transition procedure indicated by *procedure* was created, see the subsequent information, and correct the state transition procedure.

code1, *code2*, *code3*, *code4*, *code5*, and *code6* indicate the state transition instruction that resulted in an error. *code7* represents debugging information.

- code1: the first argument (state transition instruction type)
- code2: the second argument (cluster service instance type)
- code3: the third argument (state transition instruction timing)
- code4: the fourth argument (resource ID)
- code5: the fifth argument (state transition event type)
- code6: the sixth argument (state transition event detail)

error indicates the error cause. The error causes include the following:

- procedure file exit error

[Error cause details]

The possible causes are as follows:

- The state transition procedure (*procedure*) is not a Bourne shell script.
- The state transition processes for the individual arguments (*code1* to *code6*) of the state transition procedure (*procedure*) returned an error. The control program of the procedure resource determines the success or failure of the state transition processes based on the exit code (exit function) of the state transition procedure.

Exit code 0: The control program determines that the state transition process is normal.

Exit code other than 0: The control program determines that the state transition process failed.

[Corrective action]

Take the following actions:

- Obtain the state transition procedure, and check that the state transition procedure (*procedure*) is a Bourne shell script. If the procedure is not a Bourne shell script, specify the following in the first line of the state transition procedure, and then register the state transition procedure again:

```
#!/bin/sh
```

To obtain the state transition procedure, execute the “clgetproc(1M)” command. To register the state transition procedure, execute the “clsetproc(1M)” command. For details on each command, see the corresponding manual page.

- Check the return value of the state transition process for each argument (*code1* to *code6*). If there is no process that sets up an exit code (exit function), you need to add this exit code process. If there is no process, the execution result of the last command in the state transition procedure becomes the return value.

If the problem is not resolved by the above action, contact your Fujitsu system engineer.

D.11 Process Monitoring Messages

2206 The process (*count: appli*) was restarted.

Content:

The process monitoring function detected that a process being monitored had stopped and restarted the process.

count indicates the restart count of the process to be monitored. *appli* indicates the absolute path name of the restarted process.

Corrective action:

Message 2207 is output before this message.

See the explanation of message 2207.

2207 Process (*appli*) has stopped.

Content:

This message warns that a process being monitored by the process monitoring feature was stopped, but not by the “clmonproc” command.

appli indicates the absolute path name of the monitored process that has been stopped.

Corrective action:

If the process was stopped because of an error, search for the cause by checking the process specification or core file error. The core file is written to the current directory of the process. If the file is written-enabled, the normal access control is applied. The core file is not generated for the process that has an effective user ID different than the actual user ID. For detailed investigations, contact the creator of this process.

6000 An internal error occurred. (function:*function* detail:*code1-code2-code3-code4*)

Content:

An internal error occurred in the program. *function*, *code1*, *code2*, *code3*, and *code4* represent debugging information.

Corrective action:

Collect debugging information, and contact your Fujitsu system engineer. See Appendix C "Troubleshooting."

6001 Insufficient memory. (detail:*code1-code2*)

Content:

The memory resource is smaller than the size required for PRIMECLUSTER operation. *code1* and *code2* indicate the information required for troubleshooting.

Corrective action:

Copy this message, and collect debugging information. For details on collecting debugging information, see Appendix C "Troubleshooting." Review the memory resource estimate. For information on the memory size required by PRIMECLUSTER, see the "*Installation Guide*." If the problem cannot be resolved by this action, contact your Fujitsu system engineer.

6002 Insufficient disk or system resources. (detail:*code1-code2*)

Content:

The disk or system resources are less than the amount required for PRIMECLUSTER operation. *code1* and *code2* indicate the information required for troubleshooting.

Corrective action:

Collect debugging information, and contact your Fujitsu system engineer. See Appendix C "Troubleshooting." and Appendix A "PRIMECLUSTER System Design Worksheets," and review the estimates for the disk and system resources (kernel parameters). If the kernel parameters were changed, restart the node in which the kernel parameters were changed. If this problem cannot be resolved by this action, contact your Fujitsu system engineer.

6003 Error in option specification. (option:*option*)

Content:

The option that was specified to *option* contains an error.

Corrective action:

Specify the option correctly, and re-execute the command.

6004 No system administrator authority.

Content:

The user who executed the process does not have the system administrator authority.

Corrective action:

Re-execute the process with the system administrator authority.

6006 The required option *option* must be specified.

Content:

Specify the required option indicated by *option*.

Corrective action:

Specify the option correctly, and re-execute the operation.

6007 One of the required options (option) must be specified.

Content:

Specify one of the required options indicated by *option*.

Corrective action:

Specify the option correctly, and re-execute the operation.

6008 If option *option1* is specified, option *option2* is required.

Content:

When option *option1* is specified, option *option2* is required.

Corrective action:

Specify the options correctly, and re-execute the operation.

6010 If any one of the options *option1* is specified, option *option2* cannot be specified.

Content:

If one of the options *option1* is specified, option *option2* cannot be specified.

Corrective action:

Specify the options correctly, and re-execute the operation.

6602 The specified resource does not exist. (detail:code1-code2)

Content:

The specified resource does not exist. *code1* and *code2* *code2* indicate the information required for troubleshooting.

Corrective action:

Specify the resource correctly, and re-execute the operation.

6655 Use the absolute path to specify the option (*option*).

Content:

Specify the option *option* with the absolute path name.

Corrective action:

Specify the option correctly, and re-execute the operation.

6657 The specified resource is not being monitored. (detail:code)

Content:

The specified resource is not being monitored. *code* represents debugging information.

Corrective action:

No action is necessary.

6658 The specified process does not exist. (pid:pid)

Content:

The specified process does not exist. *pid* represents the process ID of the specified process.

Corrective action:

Specify the process ID correctly, and re-execute the operation.

6659 The specified command does not exist. (command:command)

Content:

The specified command does not exist. *command* represents the specified command.

Corrective action:

Specify the command with a full path name, and then re-execute the operation.

6662 A timeout occurred in process termination. (detail:code1-code2)

Content:

The process did not terminate within the termination wait time of the process.

code1 and *code2* indicate the information required for troubleshooting.

Corrective action:

Search for a cause. For information on the investigation, contact the creator of the process.

6780 Cannot request to the process monitoring daemon.

Content:

The “clmonproc” command failed to request start or stop monitoring the process monitoring function.

Corrective action:

The daemon process for the process monitoring function might not be running. Check the “prmd” process by executing the “ps” command. If the “prmd” process does not exist, execute `/etc/init.d/clprmd start` to recover the process. If the “prmd” process exists, execute `/etc/init.d/clprmd stop` and then `/etc/init.d/clprmd start`, to recover the process.

6781 The process (*appli*) cannot be monitored because the process hasn't made a process group at starting.

Content:

A process to be monitored by specifying the “-g” option in the “clmonproc” command must satisfy the condition “process ends immediately after descendent processes are generated.” However, the parent process did not end even after the specified time (default 10 seconds) elapsed after the process was started. If the system continues to monitor the process in this condition, the load on the system is getting high, so the process was removed from the processes to be monitored by the process monitoring function.

appli indicates the absolute path name of the monitored process.

Corrective action:

Take one of the following actions:

1. Do not monitor descendent processes. Do not specify the “-g” option in the “clmonproc” command.
2. If the monitored process can be changed, do not change the process group in the descendent processes, and do not specify the “-g” option in the “clmonproc” command.
3. If processes were generated, end the parent process immediately. Set up the process so that the first child process that is generated becomes the process leader immediately after it operates.

6782 The process(*appli*) was not able to be executed. (errno:*error*)

Content:

The command that was specified with the “-a” option of the “clmonproc” command could not be executed.

appli indicates the absolute path name of the process that has failed startup. *error* indicates the detailed code.

Corrective action:

Check whether the command that was specified with the “-a” option of the “clmonproc” command can be executed. Execute the command, and check whether an error occurs. If this message is output again even if the command could be executed, contact your Fujitsu system engineer (SE).

Since *errno* is output as a detail code, the Fujitsu SE should investigate the cause from this message information. For example, if *errno* is 13 (EACCES), the most likely cause is that the command path that was specified in the “-a” option of the “clmonproc” command does not have execute permission.

Appendix E Using SynfinityCluster Products in PRIMECLUSTER

Target users:

Users who use SynfinityCluster products

This appendix describes the required information for applying a SynfinityCluster-related topic in a reference manual to PRIMECLUSTER. The information focuses on the following points:

- Terminology
- Manual series
- Building procedure

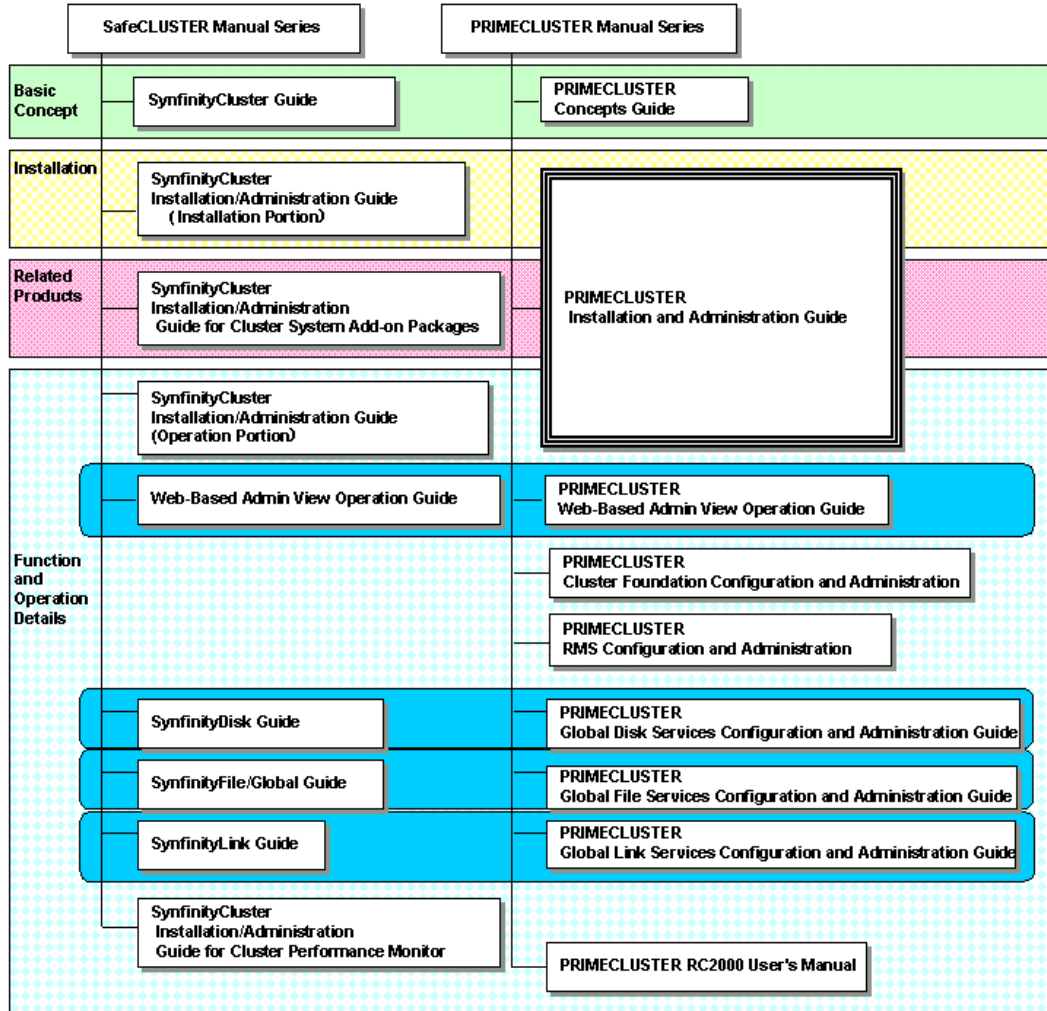
E.1 Terminology

The terms of SynfinityCluster and PRIMECLUSTER are as follows:

SynfinityCluster	PRIMECLUSTER
Cluster services	Cluster applications, userApplication
SynfinityCluster agent products	PRIMECLUSTER products
State Transition Procedure	Online/Offline scripts
Cluster Service Instance	None (Expressions such as active node and standby node are used instead.)
Cluster Domain	None
Node	Node or Host
Failover	Switch Over (Switchover or Failover)
Private LAN	Interconnect
Standby Patrol	Patrol diagnosis
Public LAN Takeover	Network Takeover
Console Function	RC2000
Monitoring Function	RMS Monitoring Function
SynfinityLink	GLS (Global Link Services)
SynfinityDisk, SynfinityDisk/Global	GDS (Global Disk Services)
SynfinityFile, SynfinityFile/Global	GFS (Global File Services)

E.2 Manual Series

The manual series for SynfinityCluster and PRIMECLUSTER are shown below.



Manual list and manual uses

PRIMECLUSTER manual	Use	Reference
PRIMECLUSTER Installation/Administration Guide (This Manual)	This manual is a general guide for all PRIMECLUSTER operations (installation, design, and maintenance). The manual also explains differences between PRIMECLUSTER and SynfinityCluster, the predecessor product, and information on PRIMECLUSTER products.	Installation - Design to maintenance
PRIMECLUSTER Concepts Guide	This manual allows readers to learn basic knowledge (technology, architecture, functions, etc.) related to each cluster system.	Design
PRIMECLUSTER Cluster Foundation Configuration and Administration	This manual describes theory to setup information related to the Cluster Foundation (CF) functions.	Installation to operations
PRIMECLUSTER RMS Configuration and Administration	This manual describes theory to setup information related to the RMS functions.	Installation to operations
PRIMECLUSTER Web-Based Admin View Operation Guide	This manual describes theory to setup information related to Web-Based Admin View.	Installation to operations
PRIMECLUSTER Global Disk Services Configuration and Administration Guide	This manual describes information on Global Disk Services (GDS).	Installation to operations
PRIMECLUSTER Global File Services Configuration and Administration Guide	This manual describes information on Global File Services (GFS).	Installation to operations
PRIMECLUSTER Global Link Services Configuration and Administration Guide: Redundant Line Control Function	This manual describes information related to the transmission path duplexing function of Global Link Services (GLS).	Installation to operations
PRIMECLUSTER Global Link Services Configuration and Administration Guide: Multipath Function	This manual describes information related to the multipath function of Global Link Services (GLS).	Installation to operations
RC2000 User's Guide	This manual presents an overview of RC2000 and describes the RC2000 functions.	Installation to maintenance

E.3 Building Procedure

This section compares the PRIMECLUSTER operation procedures and the SynfinityCluster operation procedures.

E.3.1 Software Installation

The installation methods for the cluster products and related software are shown below.

Installation method

Operation	SynfinityCluster	PRIMECLUSTER
Installation using a custom jumpstart	Installation using custom Jumpstart	One Shot Installer
Installation in each node	Installation in node units	CLI Installer (installation using an installation script)

E.3.2 Initial Cluster Setup

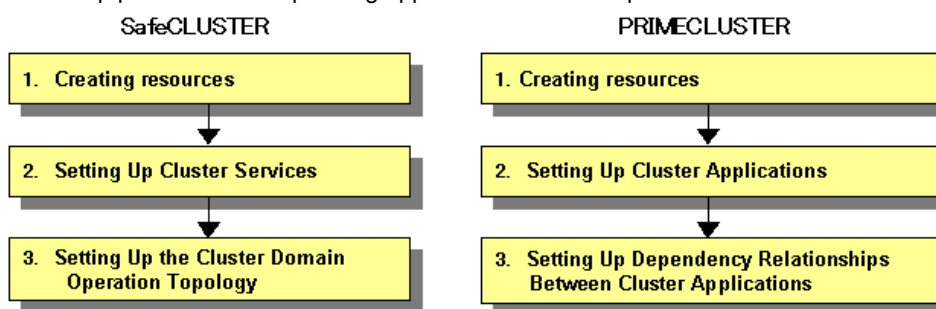
The initial setup procedures for the cluster products are shown below.

Initial setup procedure of the cluster

Operation	SynfinityCluster	PRIMECLUSTER
Initial setup of the cluster system	Setting up cluster configuration information and the resource database Cluster operation management view (GUI) <i>SynfinityCluster initial setup</i>	5.2 "Initial Clustr Setup" 5.2.3 "Initial Setup of the Cluster Resource Management Facility"
	Setting up cluster configuration information Setting up a private LAN	5.2.1 "Setting Up CF and CIP" (CF Wizard used)
	Setting up console asynchronous monitoring	5.2.2 "Setting Up the Shutdown Facility"
	Setting up optional hardware resources	5.2.2 "Setting Up the Shutdown Facility"
	Setting up shared disk units	5.4 "Setting Up Shared Disk Connection Confirmation"
	Changing the operation environment for standby patrol	6.7 "Setting Up Patrol Diagnosis"

E.3.3 Application Setup

The setup procedures for operating applications with each product are shown below.



◆ **Setting up resources**

Create the elements used by cluster services (cluster application in PRIMECLUSTER) as resources.

Operation	SynfinityCluster	PRIMECLUSTER
Setting up the takeover network	<i>Set Cluster Operation</i> GUI Setting up a takeover network	6.6.1.5 "Creating Takeover Network Resources"
Setting up state transition processing (script) of an application	<i>Set Cluster Operation</i> GUI <i>Set State Transition Procedure of Set Application Resource</i>	F.1 "Registering a Procedure Resource" 6.6.1.6 "Creating Procedure Resources" Note: This function is for making a SynfinityCluster product compatible for use in PRIMECLUSTER.
Using scripts and commands as resources	—	6.6.1.1 "Creating Cmdline Resources"
Mount information for shared disks	Manual	6.6.1.2 "Creating Fsystem Resources"
Setting up shared disks	<i>Set Cluster Operation</i> GUI Shared resource units	6.6.1.3 "Creating Gds Resources"
Setting up high availability resources	Manual operation of SynfinityLink (CLI)	6.6.1.4 "Creating Gls Resources"

◆ **Setting up services**

Services that operate in the cluster are provided for switchover units. These services are called "cluster services" in SynfinityCluster and "cluster applications" in PRIMECLUSTER.

Operation	SynfinityCluster	PRIMECLUSTER
Setting the application startup priority	<i>Set Cluster Operation GUI</i> <i>Set Cluster Service - Set Application Start/Stop Priority</i> menu items	"Resource association"
Setting a disk group	<i>Set Cluster Operation GUI</i> <i>Set Cluster Service-Set Group</i> menu items	GDS GUI
Setting the type of shared disk device	<i>Set Cluster Operation GUI</i> <i>Set Cluster Service-Set Shared Disk Unit by Use</i> menu items	6.6.1.3 "Creating Gds Resources"

◆ **Setting up Inter-service relationships**

Operation	SynfinityCluster	PRIMECLUSTER
Setting a launch priority	<i>Set Cluster Domain Operation Mode-Set Cluster Service Startup Priority</i> menu items	-
Setting a low job priority	<i>Set Cluster Domain Operation Mode-Set Cluster Service Application Priority/Exclusive Relationship</i> menu items	-
Setting an exclusive relationship	<i>Set Cluster Domain Operation Mode-Set Cluster Service Application Priority/Exclusive Relationship</i> menu items	"userApplication Configuration Wizard" menu- <i>Set Dependency Relationship Between userApplications-Set userApplication exclusion</i> 6.6.3.1 "Setting Exclusive Relationships Between Cluster Applications"Applications"

E.3.4 Operations

The operations of each cluster product are shown below.

◆ **System state monitoring**

Operation	SynfinityCluster	PRIMECLUSTER
Start the operation management screen	From the top menu of the cluster operation management view, select <i>SynfinityCluster</i> and then select <i>Cluster Operation Management</i> .	From the top menu of Web-Based Admin View, select <i>Global Cluster Services</i> and then select <i>Cluster Admin</i> .
Configuring the operation management screen	<ul style="list-style-type: none"> ● Node view Display a hierarchical list of the resources (system resources) as seen from a node. ● Service view Display a hierarchical configuration of the cluster resources. 	<ul style="list-style-type: none"> ● CF GUI ● CRM main window (displays only resources related to hardware) ● RMS main window ● MSG main window

◆ **When the resource state changes**

Operation	SynfinityCluster	PRIMECLUSTER
Checking resource errors	<ul style="list-style-type: none"> ● Message ● Node View ● Service View 	<ul style="list-style-type: none"> ● Message ● Resource Fault History screen ● Failed resource list

Operation	SynfinityCluster	PRIMECLUSTER
Patrol diagnosis	1. Detection by standby patrol 2. Confirmation with messages	1. Detection by patrol diagnosis 2. Confirmation with messages and CRM main window

Appendix F Registering, Changing, and Deleting State Transition Procedure Resources for SynfinityCluster Compatibility

Operation target:

The procedures described here are necessary only if you will be using products that have been migrated from SynfinityCluster.

To use a procedure resource in a cluster application, you must register the procedure resource before setting up the cluster application.

This appendix explains how to register, change, and delete procedure resources.

F.1 Registering a Procedure Resource

This section explains how to register a procedure resource.

Take the following steps to register a procedure resource on all nodes where the procedure resource needs to be registered.

Operation Procedure:

1. Log in with the system administrator authority to the node in which the procedure resource is to be registered.
2. Execute the "clsetproc(1M)" command to register the state transition procedure.



See

For details on the "clsetproc(1M)" command, see the manual page.



Example

To register the "/tmp/program" state transition procedure as program (file name) to the BasicApplication class

```
# /etc/opt/FJSVcluster/bin/clsetproc -c BasicApplication -m  
program /tmp/program
```



Point

To overwrite a state transition procedure that is already registered, specify the -o option.

3. Registering the procedure resource

Execute the "claddprocrsc(1M)" command to register the procedure resource.



See

For details on the claddprocrsc(1M) command, see the manual page for claddprocrsc (1M).



Example

When registering a procedure resource, this procedure resource has to meet the following conditions;

- The resource key of the procedure resource is SDISK,
- The procedure name is program,
- This procedure resource uses the state transition procedure registered in the BasicApplication class,
- The procedure resource is registered in the node (NODE1), and
- The state transition procedure receives the requests of START RUN AFTER and STOP RUN BEFORE

```
# /etc/opt/FJSVcluster/bin/claddprocrsc -k SDISK -m program -c
BasicApplication -s NODE1 -K AFTER -S BEFORE
```

F.2 Changing a Procedure Resource

This section explains how to change a procedure resource.

■ Changing a state transition procedure

Take the following steps to change the state transition procedure on all nodes where it needs to be changed.

Operation Procedure:

1. Log in with the system administrator authority to the node in which the state transition procedure is to be changed.
2. Execute the "clgetproc(1M)" command to retrieve the state transition procedure.



See

For details on the "clgetproc(1M)" command, see the manual page.



Example

When retrieving a state transition procedure, this procedure resource has to meet the following conditions;

- The state transition procedure is retried to the "/tmp" directory.
- The file name registered in the BasicApplication class is program

```
# /etc/opt/FJSVcluster/bin/clgetproc -c BasicApplication -f
/tmp/program program
```

3. Modifying the state transition procedure
Using a text editor such as vi(1), modify the state transition procedure that was retrieved in Step 2.
4. Registering the state transition procedure
For instruction on registering the procedure, see Step 2 of F.1 "Registering a Procedure Resource."

■ Changing registration information of a procedure resource

Take the following steps to change the registration information of the procedure resource on all nodes where the state transition procedure needs to be changed.

Operation Procedure:

1. Log in with the system administrator authority to the node in which the state transition procedure of the procedure resource is to be changed.

- Execute the "clsetprocrsc(1M)" command to change the registration information of the procedure resource.



See

For details on the "clsetprocrsc(1M)" command, see the manual page.



Example

When adding the requests of START RUN BEFORE state transition to the procedure resource that meet the following conditions;

- The resource key of the procedure resource is SDISK,
- This procedure resource uses the state transition procedure registered in the BasicApplication class,
- The procedure resource is registered in the node (NODE1), and
- The state transition procedure receives the requests of START RUN AFTER and STOP RUN BEFORE

```
# /etc/opt/FJSVcluster/bin/clsetprocrsc -n SDISK -c
BasicApplication -s NODE1 -K BEFORE,AFTER -S BEFORE
```

F.3 Deleting a Procedure Resource

Take the following steps to delete a procedure resource on all nodes where the procedure resource needs to be changed.

Operation Procedure:

- Log in with the system administrator authority to the node from which the procedure resource is to be deleted.
- Execute the "cldelprocrsc(1M)" command to delete the procedure resource.



See

For details on the "cldelprocrsc(1M)" command, see the manual page.



Example

When deleting a procedure resource, the procedure resource needs to meet the following conditions;

- The resource key of the procedure resource is SDISK,
- This procedure resource uses the state transition procedure registered in the BasicApplication class, and
- The node identification name is NODE1

```
# /etc/opt/FJSVcluster/bin/cldelprocrsc -n SDISK -c
BasicApplication -s NODE1
```

- Deleting the state transition procedure

If a state transition procedure becomes unnecessary after all procedure resources that use that state transition procedure have been deleted, execute the cldelproc(1M) command to delete the state transition procedure.



See

For details on the "cldelproc(1M)" command, see the manual page.



Example

When deleting a procedure resource, the procedure resource needs to meet the following conditions;

- The procedure name is program, and
- This procedure resource uses the state transition procedure registered in the BasicApplication class

```
# /etc/opt/FJSVcluster/bin/cldelproc -c BasicApplication program
```


Appendix G Registering SynfinityCluster-compatible Resources

This appendix explains how to register SynfinityCluster-compatible resources.
The procedures described here are necessary only when the following product is used:

- Interstage Traffic Director



See

See G.3 "Deleting a Cluster Service" only if the userApplication configuration was changed.

G.1 Registering a Cluster Service

If you used the CUI to set up userApplication, you need to register a SynfinityCluster-compatible cluster service and a cluster service instance resource to the Resource Database for the following product:

- Interstage Traffic Director



Note

- If you used the GUI to set up userApplication, the procedure below is unnecessary.
- If you are using the CUI to set up SynfinityCluster-compatible userApplication, see the following:

`"/opt/SMAW/SMAWRrms/htdocs.solaris/wizards.en/wizards/CRM.htm"`

Describe below is the procedure for registering a SynfinityCluster-compatible cluster service and a cluster service instance resource.

◆ Operation Procedure:



Note

Carry out Steps 1 and 2 in any one of the nodes that make up userApplication. The nodes refer to all nodes that were set to "Machines" in "(5)" of "CRM.htm."

1. Log in with the system administrator authority to any node of the cluster system.
2. Execute the "claddrsc(1)" command in the format shown below. If the registration is successful, the resource ID of the cluster service is output to standard output.

```
# /etc/opt/FJSVcluster/sys/claddrsc -c ClusterService -k  
ApplicationName-of-userApplication * -p 0 -t nocontroler -s -1 -d self  
-e service
```

* For "ApplicationName-of-userApplication," specify the application name of the user application that was set to "(4)" of "CRM.htm."

Example) If the application name of userApplication is "generic."

```
# /etc/opt/FJSVcluster/sys/claddrsc -c ClusterService -k generic -p
0 -t nocontroler -s -1 -d self -e service
100
```



Note

Carry out Steps 3 to 5 in all nodes that make up userApplication.

3. Log in with the system administrator authority to the node.
4. Obtain the node identification number of the local node.
Execute the clgetnode(1) command in the format shown below, and check the node identification number of the local node. If clgetnode(1) execution is successful, the node identification number of the local node is output to standard output.

```
# /etc/opt/FJSVcluster/bin/clgetnode -i
```

In the following example, the node identification number of the local node is "0."

```
# /etc/opt/FJSVcluster/bin/clgetnode -i
0
```

5. Register the cluster service instance resource.
Execute the claddrsc(1) command in the format shown below. If the registration is successful, the resource ID of the cluster service instance is output to standard output.

```
# /etc/opt/FJSVcluster/sys/claddrsc -c AndBinding -k
ApplicationName-of-userApplication (*) -p
resource-ID-of-cluster-service (**) -t nocontroler -s
node-identification-number-of-local-node (***) -d self -e service
```

* For "ApplicationName-of-userApplication," specify the application name of the user application that was set to "(4)" of "CRM.htm."

** For "resource-ID-of-cluster-service," specify the resource ID of the cluster service that was registered in Step 2.

*** For "node-identification-number-of-local-node," specify the node identification number that was obtained in Step 4 for the local node.

Example) If the application name of userApplication is "generic," the resource ID of the cluster service is "100," and the node identification number of the local node is "0."

```
# /etc/opt/FJSVcluster/sys/claddrsc -c AndBinding -k generic -p 100
-t nocontroler -s 0 -d self -e service
101
```



Note

Carry out Steps 6 and 7 in any one of the nodes that make up userApplication.

6. Log in with the system administrator authority to any one of the nodes that make up the cluster system.
7. Set up the operation sequence of the cluster service instances.
Execute the clsetinsorder(1M) command in the format shown below, and set the operation sequence of the cluster service instances.

```
# /etc/opt/FJSVcluster/bin/clsetinsorder -s
resource-ID-of-cluster-service(*) -r
resource-ID-of-cluster-service-instance ...(**) -S
```

* For "resource-ID-of-cluster-service," specify the resource ID of the cluster

service that was registered in Step 2.

- ** For "*resource-ID-of-cluster-service-instance*," specify the resource ID of the cluster service instance that was registered in Step 5 for each node. Specify the resource IDs of the cluster service instances in the "Machines" sequence that was set in "(5)" of "CRM.htm."

Example) If the resource ID of the cluster service is "100," and the Machines sequence is as follows: The resource ID of the cluster service instance in the narcissus node is "101" and the resource ID of the cluster service instance in the sweetpea node is "102."

```
Machines[0] narcissusRMS
Machines[1] sweetpeaRMS
```

```
# /etc/opt/FJSVcluster/bin/clsetinsorder -s 100 -r 101,102 -S
```

G.2 Associating Resources to a Cluster Service Instance

The SynfinityCluster-compatible cluster service instance needs to be associated with the following product:

- Interstage Traffic Director



Note

For products other than the above, the procedure for associating the product to a cluster service instance is unnecessary.

The procedure for associating the above product with a SynfinityCluster-compatible cluster service instance is described below.

◆ Operation Procedure:

1. Log in with the system administrator authority.
Log in with the system administrator authority to one of the nodes of the cluster system.



Note

Perform Step 2 only if userApplication was set up with the CUI and IP address takeover was set during userApplication setup. If userApplication was set up with the GUI or if IP address takeover was not set during userApplication setup, Step 2 is unnecessary.

2. Register the IP address takeover resources.
 - Execute the "clgettree(1)" command in the format shown below, and check the resource IDs of the PublicLAN resources in all nodes that execute IP address takeover. The resource class of PublicLAN resources is "Ethernet."

```
# /etc/opt/FJSVcluster/bin/clgettree
```

Example) In the following case, the resource ID of the PublicLAN resource in the narcissus node is "25" and the resource ID of the PublicLAN resource in the sweetpea node is "26."

```
# /etc/opt/FJSVcluster/bin/clgettree
```

```
Cluster 1 /
```

```

Domain 2 RC9
Shared 7 SHD_RC9
Node 3 narcissus ON
    Psd 21 hme1 ON
    Psd 22 hme2 ON
    Ethernet 25 hme0 ON
    DISK 19 c0t0d0 UNKNOWN
    SytemState2 40 FJSVndbs UNKNOWN
Node 5 sweetpea ON
    Psd 23 hme1 ON
    Psd 24 hme2 ON
    Ethernet 26 hme0 ON
    DISK 20 c0t0d0 UNKNOWN
    SytemState2 41 FJSVndbs UNKNOWN
    
```

- Execute the "clcreate-iprsc(1M)" command in the format shown below, and register the IP address takeover resources.

```

# /etc/opt/FJSVcluster/sys/clcreate-iprsc -p
resource-ID-of-PublicLAN-resource... (*1)
takeover-IP-address (*2)
    
```

*1 For "resource-ID-of-PublicLAN-resource...", specify the resource IDs of the PublicLAN resources of all nodes that were confirmed with the previous "clgettree(1)" command.

*2 For "takeover-IP-address," specify the takeover IP address that was specified during userApplication setup.

Example) If the resource IDs of the PublicLAN resources are "25," "26" and the takeover IP address is "192.168.246.1"

```

# /etc/opt/FJSVcluster/sys/clcreate-iprsc -p 25,26 192.168.246.1
    
```

3. Associate the resources to cluster service instances.

Associate the following resources to cluster service instances:

- IP address takeover resources (*1)
 - *1 If IP address takeover resources were registered in Step 2, associated them to cluster service instances.
- "Interstage Traffic Director" resources

- 1) Execute the clgettree(1) command in the format shown below, and check the resource IDs of the resources to be associated to cluster service instances. The resource class of IP address takeover resources is "IP_Address." The resource name of the Interstage Traffic Director resource is "FJSVndbs."

```

# /etc/opt/FJSVcluster/bin/clgettree
    
```

Example) For the "clgettree(1) command execution example" described below, the resource IDs for the IP address takeover and Interstage Traffic Director resources are as follows:

Node	Resource ID of IP address takeover resource	Resource ID of Interstage Traffic Director resource
narcissus	27	40
sweetpea	28	41

[clgettree(1) command execution example of the clgettree(1) command]

```

# /etc/opt/FJSVcluster/bin/clgettree
    
```

```

Cluster 1 /
    
```

```

Domain 2 RC9
Shared 7 SHD_RC9
    SHD_Host 29 192.168.246.1 UNKNOWN
        IP_Address 27 hme0:1 UNKNOWN narcissus
        IP_Address 28 hme0:1 UNKNOWN sweetpea
Node 3 narcissus ON
    Psd 21 hme1 ON
    Psd 22 hme2 ON
    Ethernet 25 hme0 ON
        IP_Address 27 hme0:1 UNKNOWN
    DISK 19 c0t0d0 UNKNOWN
    SytemState2 40 FJSVndbs UNKNOWN
Node 5 sweetpea ON
    Psd 23 hme1 ON
    Psd 24 hme2 ON
    Ethernet 26 hme0 ON
        IP_Address 28 hme0:1 UNKNOWN
    DISK 20 c0t0d0 UNKNOWN
    SytemState2 41 FJSVndbs UNKNOWN

```

- 2) Using the format shown below, execute the "clrepparent(1M)" command for each node in the userApplication configuration, and associate the IP address takeover and Interstage Traffic Director resource to cluster service instances.

```

# /etc/opt/FJSVcluster/sys/clrepparent -s
resource-IDs-of-IP-address-takeover-and-Interstage-Traffic
Director-resources(*1) -t
resource-ID-of-cluster-service-instance(*2)

```

- *1 Specify the resource IDs of the IP address takeover and Interstage Traffic Director resources that were obtained with the clgettree(1) command in each node.

*2

If userApplication was set up with the CUI

Specify the resource ID of the cluster service instance that was registered in each node according to Step 5 "Register the cluster service instance" in G.1 "Registering a Cluster Service."

If userApplication was set up with the GUI

Execute the "clgettree(1)" command in the format shown below, and check the resource ID of the cluster service instance in each node. The resource class for cluster service instances is "AndBinding." The node name to which the cluster service instance belongs is displayed at the end of the line for the "AndBinding" resource class.

```
# /etc/opt/FJSVcluster/bin/clgettree -s
```

In the following example, the resource ID of the cluster service instance in the narcissus node is "101," and the resource ID of the cluster service instance in the sweetpea node is "102."

```

# /etc/opt/FJSVcluster/bin/clgettree -s
Standby 68 Service1 STOP AVAILABLE
    AndBinding 101 Instance1_Of _narcissus STOP STOP(RUN)
narcissus
    AndBinding 102 Instance1_Of _sweetpea STOP STOP(RUN)
sweetpea

```

Example) When the resource ID of the cluster service instance in the narcissus node is "101" and the resource ID of the cluster service instance in the sweetpea node is "102" and the following resources are registered in each node:

Node	Resource ID of IP address takeover resource	Resource ID of Interstage Traffic Director resource
narcissus	27	40
sweetpea	28	41

```
# /etc/opt/FJSVcluster/sys/clrepparent -s 27,40 -t 101
```

```
# /etc/opt/FJSVcluster/sys/clrepparent -s 28,41 -t 102
```

G.3 Deleting a Cluster Service

This section describes the procedure to be performed in the following cases:

- If userApplication is deleted
- If the following product is installed:
 - Interstage Traffic Director

After carrying out the procedure indicated in this section, perform the G.1 "Registering a Cluster Service" and G.2 "Associating Resources to a Cluster Service Instance" operations in the following cases:

- If the number of nodes configuring userApplication is changed
- If the ApplicationName of userApplication is changed
- If a new IP address takeover is to be executed or if an IP address takeover is to be discontinued
- If a takeover IP address is changed

◆ Operation Procedure:

1. Log in with the system administrator authority.

Log in with the system administrator authority to one of the nodes of the cluster system.

2. Check the resource ID of the cluster service.

Execute the "clgettree(1)" command in the format shown below, and check the cluster service resource. The resource class of the cluster service is "Standby" or "Scalable." The cluster service is output in the first line.

```
# /etc/opt/FJSVcluster/bin/clgettree -s
```

Example) In the example below, the resource ID of the cluster service is "68."

```
# /etc/opt/FJSVcluster/bin/clgettree -s
```

```
Standby 68 Service1 STOP AVAILABLE
```

```
AndBinding 101 Instance1_Of _narcissus STOP STOP(RUN) narcissus
```

```
AndBinding 102 Instance1_Of _sweetpea STOP STOP(RUN) sweetpea
```

3. Delete the cluster service resource.

Execute the "cldelrsc(1M)" command in the following format, and delete the cluster service resource.

```
# /etc/opt/FJSVcluster/bin/cldelrsc -r
resource-ID-of-cluster-service(*1)
```

*1 For "resource-ID-of-cluster-service," specify the resource ID of the cluster service that was obtained in Step 2.

Example) To delete the cluster service that has resource ID "68."

```
# /etc/opt/FJSVcluster/bin/cldelrsc -r 68
```

4. Delete the IP address takeover resources.

- Execute the "clgettree(1)" command in the format shown below, and check the resource IDs of the IP address takeover resources. The resource classes of the IP address takeover resources are "SHD_Host" and "IP_Address." If resources of the "SHD_Host" and "IP_Address" resource classes are not output, the execution of the subsequent steps is unnecessary because there are no IP address takeover resources.

```
# /etc/opt/FJSVcluster/bin/clgettree
```

Example) In the following case, the resource IDs of the IP address takeover resources are "29," "27" and "28."

```
# /etc/opt/FJSVcluster/bin/clgettree
```

```
Cluster 1 /
  Domain 2 RC9
  Shared 7 SHD_RC9
    SHD_Host 29 192.168.246.1 UNKNOWN
      IP_Address 27 hme0:1 UNKNOWN narcissus
      IP_Address 28 hme0:1 UNKNOWN sweetpea
  Node 3 narcissus ON
    Psd 21 hme1 ON
    Psd 22 hme2 ON
    Ethernet 25 hme0 ON
      IP_Address 27 hme0:1 UNKNOWN
    DISK 19 c0t0d0 UNKNOWN
    SytemState2 40 FJSVndbs UNKNOWN
  Node 5 sweetpea ON
    Psd 23 hme1 ON
    Psd 24 hme2 ON
    Ethernet 26 hme0 ON
      IP_Address 28 hme0:1 UNKNOWN
    DISK 20 c0t0d0 UNKNOWN
    SytemState2 41 FJSVndbs UNKNOWN
```

- If the previous procedure indicates that there is an IP address takeover resource, execute the "cldelrsc(1)" command in the format shown below, and delete the IP address takeover resource. Execute this step only if there is an IP address takeover resource.

```
# /etc/opt/FJSVcluster/bin/cldelrsc -r
```

```
resource-ID-of-IP-address-takeover-resource(*1)
```

- *1 For "resource-ID-of-IP-address-takeover-resource," specify all resource IDs of IP address takeover resources that were obtained with the previous "clgettree(1)" command.

Example) If the resource IDs of the IP address takeover resources are "29," "27" and "28."

```
# /etc/opt/FJSVcluster/bin/cldelrsc -r 29,27,28
```


Appendix H Supplemental Information

H.1 Setting Up the Resource Database from the CRM Main Window

This section explains how to set the resource database that is managed by the cluster resource management facility (CRM).

The CRM setup involves the following operations:

Initial installation

Set up the resource database that is managed by CRM.

Automatic resource registration of devices

Register the hardware devices that are connected to the system to the resource database that is managed by CRM. (The hardware devices include shared disks, line switching units, and network interface cards.)



See

For details on the setup procedure, see 5.2.3 "Initial Setup of the Cluster Resource Management Facility."

H.2 Setting Up the SF Configuration

This section explains how to set up the SF configuration.

H.2.1 SF Preparations

Take the following procedure before you create the configuration file.

1. Check the system requirements.

Specifically, you need to follow operations below:

- Determine the functional requirements of the user.
- Determine how SF is to be used in cluster machine monitoring and shutdown processing.
- Determine the optimum shutdown agent.

2. Propose the configuration of the shutdown agent.

Specifically, you need to determine the following:

- Machines to be monitored by SF
- Shutdown agent

Determine the configuration design based on the intended use and the machine-specific requirements.

In addition, you need to determine details on monitoring by SF (including shutdown agent and usage sequence).

3. Define the shutdown agent (SA) to be set to SF.

You must define an SA to forcibly stop nodes if all cluster interconnects become disabled because the nodes that configure the cluster system hang or fail. When defining the SA, preferentially use SA_pprcip as much as possible because information for troubleshooting will remain if node elimination is done.

H.2.2 SF Configuration Files

The format of the [important] configuration file is described as a reference. Instructions on setting up the shutdown facility are explained in "8.4 Setting Up the Shutdown Facility."

Create the configuration file in the "/etc/opt/SMAW/SMAWsf" directory, and set the configuration file name to rcsd.cfg.

The format of the configuration file is as follows:

```
CFName[,weight=weight][,admnIP=myadmnIP):agent=SA_name,timeout=SA_timeo
ut{:agent=SA_name2,timeout=SA_timeout2:]
```

weight is an optional keyword. If this option is not specified, rcsd will be assigned a weight of 1. This keyword is optional so that existing configuration will still function as expected.

admnIP is an optional keyword, and *myadmnIP* is the IP address of the *CFName* machine in the administrative LAN. Although this keyword was also made optional for downward compatibility, this setting is required to avoid inappropriate cluster partitions. For *myadmnIP* specify an address that is not on the CIP interface.

CFName is the CF node name of the machine in the cluster.

agent and *timeout* are reserved words.

SA_name is the command name of the shutdown agent.

SA_timeout is the maximum time, in seconds, that is allowed for the shutdown agent to run before a failure occurrence is assumed.

The shutdown agent that is specified first in the configuration file becomes the preferred SA. If the preferred SA issues a shutdown request and the shutdown failure response is received, the second SA issues a shutdown request. This request/response pattern is repeated until a shutdown success response is received or all SAs have been tried. If SA is successful in shutting down a cluster node, then operator intervention is required and the node is left in the LEFTCLUSTER state.

The storage location of the log file is /var/opt/SMAWsf/log/rcsd.log. It is important that all cluster nodes use the same "rcsd.cfg" file. Care must be taken in administration to ensure this is true.

A file called rcsd.cfg.template is provided under the "/etc/opt/SMAW/SMAWsf" directory. This is a sample configuration file for the shutdown daemon based on fictitious machines and agents.

H.3 Setting Up the Alternate Keyboard Abort Sequence

Edit the "/etc/default/kbd" file by removing the comment symbol for the line that defines the keyboard abort sequence and setting the line to the alternate abort sequence. The line should appear as follows:

```
KEYBOARD_ABORT=alternate
```

H.4 SCF Dump

If following error occurs, collect SCF dump.

If message number 7003 or 7004 is output

If a message from the SCF driver is output

For details on the message numbers 7003 and 7004, see "12.19 Asynchronous Monitoring Messages" in "PRIMECLUSTER Cluster Foundation Configuration and Administration." For details on messages that are output from the SCF driver, see the "Enhanced Support Facility

User's Guide."

Dump collection procedure

The RAS monitoring daemon of SCF that received the error notification from SCF stores the SCF dump to `/var/opt/FJSVhwr/scf.dump`.

Collect this file together with the directory by executing the following:

```
# cd /var/opt
# tar cf /tmp/scf.dump.tar ./FJSVhwr
```

H.5 Cluster Resource Management Facility Messages

This section explains the cluster management facility messages. The messages are classified into the following types:

Messages displayed by the GUI

Messages displayed upon execution of the CLI command

H.5.1 GUI (Cluster Resource Management Facility)

The Cluster Resource Management Facility Messages are explained below. Each description explains the meaning of each message and the procedure to be applied to correct the problems:

■ Information Messages

0700 : The resource database is not configured. Please configure it by using [Tool] - [Initial setup] menu.

Corrective action:

Since the resource database has not been setup, the information is not displayed.

Choose *Tool* → *Initial setup* menu from the CRM main menu, and then set up the resource database.

0702 :The screen cannot be displayed from the main CRM window.

Corrective action:

The machine administration screen is not displayed from the cluster resource management facility main window. After closing the message dialog box by clicking the *OK* button, select the *Machine administration* menu from the *MISC* category at the top menu of Web-Based Admin View.

0703 :Do you want to start up resource_name (rid=rid) ?

Corrective action:

Click either of the following buttons, and then request to activate the selected resource:

Yes: Requests to activate the resource.

No: Does not request to activate the resource.

resource_name indicates a displayed resource name while *rid* indicates a resource ID.

0704 :Do you want to stop resource_name (rid= rid)

Corrective action:

Click either of the following buttons, and then request to deactivate the selected resource:

Yes: Requests to deactivate the resource.

No: Does not request to activate the resource.

resource_name indicates a displayed resource name while *rid* indicates a resource ID.

0705 :Do you want to diagnose *resource_name* (*rid=rid*) ?

Corrective action:

Click either of the following buttons, and then run a patrol diagnosis for the selected resource:

Yes: Runs a patrol diagnosis for the resource.

No: Does not run a patrol diagnosis for the resource.

resource_name indicates a displayed resource name while *rid* indicates a resource ID.

0707 :Do you want to begin the *proc* processing?

Corrective action:

Click either of the following buttons:

Yes: Executes the processing indicated by *proc*.

No: Terminates the operation.

The type of processing varies with the processing name displayed in *proc*, as follows:

Initial setup

The resource database is set up.

Automatic configure

The device is registered to the database.

0708 : *proc1* finished.

Corrective action:

The processing shown in *proc1* has been completed.

Press the *OK* button to close the message dialog box.

The type of processing varies depending on the processing name displayed in *proc1*, as follows:

Initial setup

The resource database is set up.

Automatic configure

The device is registered to the database.

0709 :The configuration change function cannot be used because it is being used by another task.

Corrective action:

This processing cannot be executed because the configuration change function is being used for other operation.

After closing the message dialog box by clicking the *OK* button, exit from the processing execution screen of the same client or the other client (Web browser). Then, re-execute the operation.

0710 :Processing cannot be ended because the following operation instruction is not completed.

Corrective action:

The operation is being requested (the command is being transmitted) to the cluster resource management facility. After a lapse of one or two minutes, re-select the *File* → *Exit* menu. If this error message appears again, close the browser once and then re-open it.

0711 :Can't get information from the resource database.

Corrective action:

The resource database cannot be obtained. Leave the operation undone keeping the screen displayed. Once the resource database has been obtained, the resource database information

will be displayed.

0712 :The resource database has already been configured.

Corrective action:

The resource database has been already set up. Confirm whether the cluster resource management facility has been activated. If it has not been activated, start the cluster resource management facility. If it has been activated, leave the operation undone as is. Click the *OK* button to close the message dialog box.

0713 :The node which completed the settings of resource database exists.

Corrective action:

A node in which the resource database is already set up is available. After closing the message dialog box by clicking the *OK* button, initialize the resource database. Then, re-execute the initial setup.

H.5.2 Error Messages

0760 : A requested operation failed. (Error Details)

Corrective action:

The operation instruction to be executed has failed. An error message of the cluster resource management facility will be displayed in Error Details. Take corrective action according to the instructions in the message. Click the *OK* button to close the message dialog box.

0761 : An internal contradiction occurred in the main CRM window. (Error Details)

Corrective action:

Either of the following symptoms might occur:

The Java execution environment in the Web browser failed to load the Java class files that constitute the cluster resource management facility, due to the load on the network.

A program inconsistency was detected in the CRM main window.

After closing the message dialog box by clicking the *OK* button, restart Web-Based Admin View. Then, restart the browser and re-execute the operation. For information on how to restart Web-Based Admin View, see "6.2 Restart" in the "*PRIMECLUSTER Web-Based Admin View Operation Guide*."

If this message is displayed, collect the Java console, a hard copy of the error dialog box, and debugging information, and then contact your Fujitsu system engineer (SE).

0763 : The operation cannot be executed because the resource database is not configured on all nodes, or all nodes are not communicating with Web-Based Admin View.

Corrective action:

The following symptoms might occur:

The cluster resource management facility has not yet been activated because all nodes are just been started.

None of the nodes are connected to Web-Based Admin View.

As the cluster resource management facility is being started, click the *OK* button to close the message dialog box, wait a short while, and then re-execute the operation. If the same symptom occurs, confirm whether the node power is on and whether the cluster resource

management facility is running normally on the nodes. Correct the problem if necessary, and restart Web-Based Admin View on the node on which the operation is to be executed. For information on how to start Web-Based Admin View, see “6.2 Restart” in the “*PRIMECLUSTER Web-Based Admin View Operation Guide*.”

If this error message is displayed again even after applying the above corrective action, collect the Java console, a hard copy of the erroneous dialog box, and debugging information, and then contact your Fujitsu system engineer (SE).

Click the *OK* button to close the message dialog box.

0764 : An I/O error occurred.

Corrective action:

Confirm whether the symptom conforms to any of the following descriptions:

- a. While the CRM main window was displayed, the operation to shut down the node was performed repeatedly.
- b. The operation has been requested from the CRM main window.
- c. A node or client machine is loaded, or the network is loaded.
- d. While the CRM main window was displayed, the CRM main window was initialized.

If any operation instruction is being requested, close the message dialog box by clicking the *OK* button, wait a short while (3 to 5 minutes), and then re-execute the operation request.

If no operation is being requested, close the message dialog box by clicking the *OK* button and then restart the browser.

If the above action fails to solve the problem, restart Web-Based Admin View on all nodes.

For information on how to restart Web-Based Admin View, see “6.2 Restart” in the “*PRIMECLUSTER Web-Based Admin View Operation Guide*.”

0765 : Communication with the management server failed.

Corrective action:

The management server might have been disconnected because of the events to disconnect the network such as rebooting, shutdown, emergency shutdown, or LAN cable disconnection). Otherwise, restarting of Web-Based Admin View is considered the cause.

After closing the message dialog box by clicking the *OK* button, restart the browser and then display the screen again.

If this error continues to occur, collect the Java console, a hard copy of the erroneous dialog box, and the debugging information, and then contact your Fujitsu system engineer (SE).

0766 : The command terminated abnormally. (Error Details)

Corrective action:

A message related to the cluster resource management facility is displayed in Error Details. Take corrective action according to the instructions in the message.

Click the *OK* button, and then close the message dialog box.

0767 : Command execution failed.

Corrective action:

The command that was being executed did not terminate within the specified time.

Collect the Java console, a hard copy of the error dialog box, and the debugging information, and then contact your Fujitsu system engineer (SE).

Click the *OK* button, and then end the message dialog box.

0768 : The processing for the *proc1* cannot finish normally.

Corrective action:

After you close the message dialog box by clicking the *OK* button, wait a short while and then

re-execute the operation.

If this error message continues to be displayed, collect the Java console, a hard copy of the error dialog box, and the debugging information, and then contact your Fujitsu system engineer (SE).

The processing to be executed varies with the processing name displayed in *proc1*.

- Initial setup
The resource database is set up.
- Automatic configure
The device is registered to the resource database.

0769 : The processing was aborted because it could not be done on all nodes. (Error Details)

Corrective action:

The command cannot be executed for the node that is displayed in Error Details.

After restarting Web-Based Admin View on that node, wait a short while and then re-execute. For details on restarting Web-Based Admin View, see “6.2 Restart” in the “*PRIMECLUSTER Web-Based Admin View Operation Guide*.”

If the same message continues to appear, reboot that node.

If all of above corrective actions fail, collect the Java console, a hard copy of the erroneous dialog box, and the debugging information, and then contact your Fujitsu system engineer (SE).

Click the *OK* button to close the message dialog box.

0773 : The initial setup of the resource database failed. (Error Details)

Corrective action:

The symptom can be classified into one of the following. Take corrective action according to the symptom.

The information on Web-Based Admin View has not yet been obtained to enable setup of the cluster resource management facility on the node that is displayed in Error Details.

Corrective action :

After closing the message dialog box by clicking the *OK* button, restart Web-Based Admin View on the node that is displayed in Error Details and then re-execute the operation instruction. For information on how to restart Web-Based Admin View, see “6.2 Restart” in the “*PRIMECLUSTER Web-Based Admin View Operation Guide*.”

As CF has not yet been configured, the resource database cannot be set up.

Corrective action:

After closing the message dialog box by clicking the *OK* button, configure the CF and then re-execute the operation request.

Collect the Java console, a hard copy of the error dialog box, and the debugging information, and then contact your Fujitsu system engineer (SE).

For other than the above, or if the same error continues to occur, collect the Java console, a hard copy of the erroneous dialog box, and the debugging information, and then contact your Fujitsu system engineer (SE).

0774 : Initial setup failed: the resource database could not be initialized.

Corrective action:

The startup processing of the initial setup failed.

Collect the Java console, a hard copy of the erroneous dialog box, and the debugging information.

After collecting the hard copy, click the *OK* button to close the message dialog box.

0775 : CF is not running, or CF is not configured.**Corrective action:**

Since CF is not configured or CF is stopped on any one of the nodes, the initial setup cannot be executed for the resource database. After you select the *cf* tab and display the CF main window, confirm the state of CF and then configure or start CF.

H.6 Monitoring Agent Messages

This section explains the messages output by monitoring agents.

The message format is shown below. The italic text indicates output content that varies depending on the message.

FJSVcluster:severity:program:message-number:message (details)

<i>severity</i>	Indicates the severity level of the message. The severity levels of the messages output by the monitoring facility of monitoring agents are classified into three types, namely, information (INFORMATION), warning (WARNING), and error (ERROR). For more details, refer to the following table:
<i>program</i>	Indicates the name of the program that outputs this message. DEV is output when monitoring agent is used.
<i>message-number</i>	Indicates the message number.
<i>message</i>	Indicates the text of the message.
<i>details</i>	Indicates the detailed classification code.

monitoring agent message type classification

Number	Severity level	Meaning
2000-3999	Information (INFORMATION)	A message notifying the user of information related to the operation status of the monitoring agent.
4000-5999	Warning (WARNING)	A message notifying the user of a slight error that is not so serious as to cause an abnormal end of monitoring agent.
????, 6000-7999	Error (ERROR)	A message notifying the user of a serious error that causes the abnormal end of monitoring agent.

H.6.1 Information Messages

3040 The console monitoring agent has been started. (*node:nodename*)

3041 The console monitoring agent has been stopped. (*node:nodename*)

3042 The RCI monitoring agent has been started.

3043 The RCI monitoring agent has been stopped.

3044 The console monitoring agent took over monitoring Node *targetnode*.

3045 The console monitoring agent cancelled to monitor Node *targetnode*.

H.6.2 Warning Messages

5001 The RCI address has been changed. (node:*nodename* address:*address*)

Corrective action:

A change in the RCI address has been detected. *nodename* indicates the name of the node on which RCI address has been changed. *address* indicates the RCI address that has been changed. Reexamine the RCI address setting for that node.

H.6.3 Error Messages



Note

If an error message is output, analyze the logs for the period during which the message was output from the "/var/adm/messages" file and confirm whether any other error messages were output before that. Take corrective actions for the errors according to the instructions in the message.

???? Message not found!!

Corrective action:

Text that is associated with the message number cannot be found. Copy this message and then contact your Fujitsu system engineer (SE).

6000 An internal error occurred. (function:*function* detail:*code1-code2-code3-code4*)

Corrective action:

Collect the debugging information, and then contact your Fujitsu system engineer (SE). See "11.3 Collecting Troubleshooting Information" in "PRIMECLUSTER Cluster Foundation Configuration and Administration."

6004 No system administrator authority.

Corrective action:

Other than system administrator authority is used for this operation. All work must be done with the system administrator authority.

7003 An error was detected in RCI. (node:*nodename* address:*address* status:*status*)

Corrective action:

An RCI failure was detected between the node that has displayed the message and the node described in the message. This failure is due to an incorrect setting of RCI connection or a system error.

Check whether the RCI cable is connected. If it is disconnected, take corrective action, and execute the following command on the node that output the message. Then, restart the RCI monitoring agent (MA).

```
# /etc/opt/FJSVcluster/bin/clrcimonctl restart
```

Restart the shutdown facility (SF) on the node that output the message.

```
# /opt/SMAW/bin/sdtool -r
```

If the RCI cable is correctly connected, the cause of the problem might be due to a hardware error in the RCI cable or the system control facility (hereafter referred to as SCF). Collect the SCF dump and debugging information, and then contact your Fujitsu system engineer and customer engineer. See "11.3 Collecting Troubleshooting Information" in "PRIMECLUSTER

Cluster Foundation Configuration and Administration."

The Fujitsu engineers shall restart the RCI monitoring agent (MA) and the shutdown facility (SF) by executing the above command after hardware restoration.

7004 The RCI monitoring agent has been stopped due to an RCI address error.

(node:nodename address:address)

Corrective action:

The RCI monitoring agent has been changed on other node while the RCI monitoring is running. Collect the SCF dump and debugging information, and then contact your Fujitsu system engineer and customer engineer. See "11.3 Collecting Troubleshooting Information" in "PRIMECLUSTER Cluster Foundation Configuration and Administration."

The Fujitsu engineers first confirm that the RCI address of *nodename* that is displayed in the message is correct by executing the following command on an optional node:

```
# /opt/FJSVmadm/sbin/setrci stat
```

If the RCI address is not correctly set up, they set up the RCI address again, referring to the local procurement procedure manual for Fujitsu customer engineers (CEs).

Then, they execute the following command on the node that output the message and restart the RCI monitoring agent (MA):

```
# /etc/opt/FJSVcluster/bin/clrcimonctl restart
```

Then, they restart the shutdown facility (SF) on the node that output the message.

```
# /opt/SMAW/bin/sdtool -r
```

7040 The console was disconnected. (node:nodename portno:portnumber detail:code)

Corrective action:

The remote console connection unit (RCCU) has been disconnected. Confirm the following:

Power is supplied to the remote console connection unit.

The light indicates that the HUB and LAN cable are connected to the port.

Whether the LAN cable is disconnected from the connector on the remote console connection unit or the connector on the HUB.

If either of above setup is incorrect, take corrective action, execute the following command on the node that output the message, and then restart the shutdown facility (SF):

```
# /etc/SMAW/bin/sdtool -r
```

If the connection still fails, a hardware error may have occurred such as in the network, remote console connection unit, or HUB. In such a case, contact your Fujitsu system engineer (SE).

If the error cannot be solved through the application of this corrective action, collect the debugging information, and then contact your Fujitsu system engineer (SE). See "11.3 Collecting Debugging Information."

7042 Connection to the console is refused. (node:nodename portno:portnumber detail:code)

Corrective action:

Connection to the console cannot be established during console monitoring agent startup. Confirm the following points:

Power is supplied to the remote console connection unit.

The light indicates that the HUB and LAN cable are connected to the port.

If the LAN cable is disconnected from the connector on the remote console connection unit or from the connector on the HUB.

If either of above setup is incorrect, take corrective action, execute the following command on the node that output the message, and then restart the shutdown facility (SF):


```
# /etc/SMAW/bin/sdtool -r
```

If connection cannot be established, a hardware error may have occurred such as in the network, the remote console connection unit, or HUB. In such a case, contact your Fujitsu customer engineer (CE).

If the error cannot be cleared despite the application of the above corrective action, collect the debugging information, and then contact your Fujitsu system engineer (SE). See "11.3 Collecting Troubleshooting Information" in "PRIMECLUSTER Cluster Foundation Configuration and Administration."

7200 The configuration file of the console monitoring agent does not exist.

(file:filename)

Corrective action:

No setup file for the console monitoring agent is found. Download the setup file displayed in the supplementary information, from other node that constructs the cluster, by using ftp and then allocate the setup file to the storage location. Set up the access privilege, which is the same as that for the other nodes, in the setup file. After allocating the setup file, reboot the system. If the setup files are not included in all the nodes that construct the cluster, collect the debugging information, and then contact your Fujitsu system engineer (SE). See "11.3 Collecting Troubleshooting Information" in "PRIMECLUSTER Cluster Foundation Configuration and Administration."

7201 The configuration file of the RCI monitoring agent does not exist. (file:filename)

Corrective action:

No setup file for the RCI monitoring agent is found. Download the setup file displayed in the supplementary information, from another node constructing the cluster by using ftp, and then allocate the setup file to the storage location. Set up the access privilege, which is the same as that for the other nodes, to the setup file. After allocating the setup file, reboot the system. If the setup file is not included in any of the nodes that construct the cluster, collect the debugging information, and then contact your Fujitsu system engineer (SE). See "11.3 Collecting Troubleshooting Information" in "PRIMECLUSTER Cluster Foundation Configuration and Administration."

7202 The configuration file of the console monitoring agent has an incorrect format.

(file:filename)

Corrective action:

The format of the setup file for the console monitoring agent includes an error. If the setup file name displayed in the supplementary information is SA_rccu.cfg, set up the shutdown facility from the configuration wizard of the shutdown facility (SF) again. In this case, confirm that the RCCU name has been entered. If this corrective action fails to solve the error, or if the setup file name displayed in the supplementary information is other than SA_rccu.cfg, collect the debugging information, and then contact your Fujitsu system engineer (SE). See "11.3 Collecting Troubleshooting Information" in "PRIMECLUSTER Cluster Foundation Configuration and Administration."

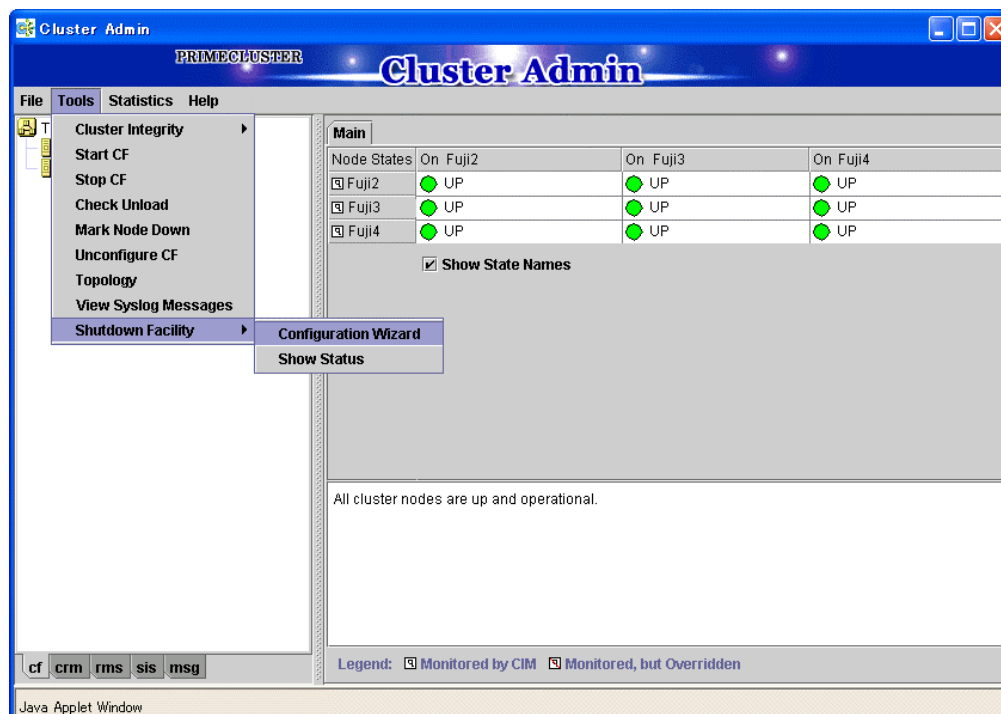
H.7 Setting Up the Shutdown Facility

This section describes how to use Cluster Admin and CLI to configure the Shutdown Facility (SF).

H.7.1 Starting Configuration Wizard

Use the *Tools* pull-down menu to select *Shutdown Facility*, and then choose *Configuration Wizard*. Figure H-1 shows how to invoke the Configuration Wizard.

Figure H-1: Opening the SF Configuration Wizard

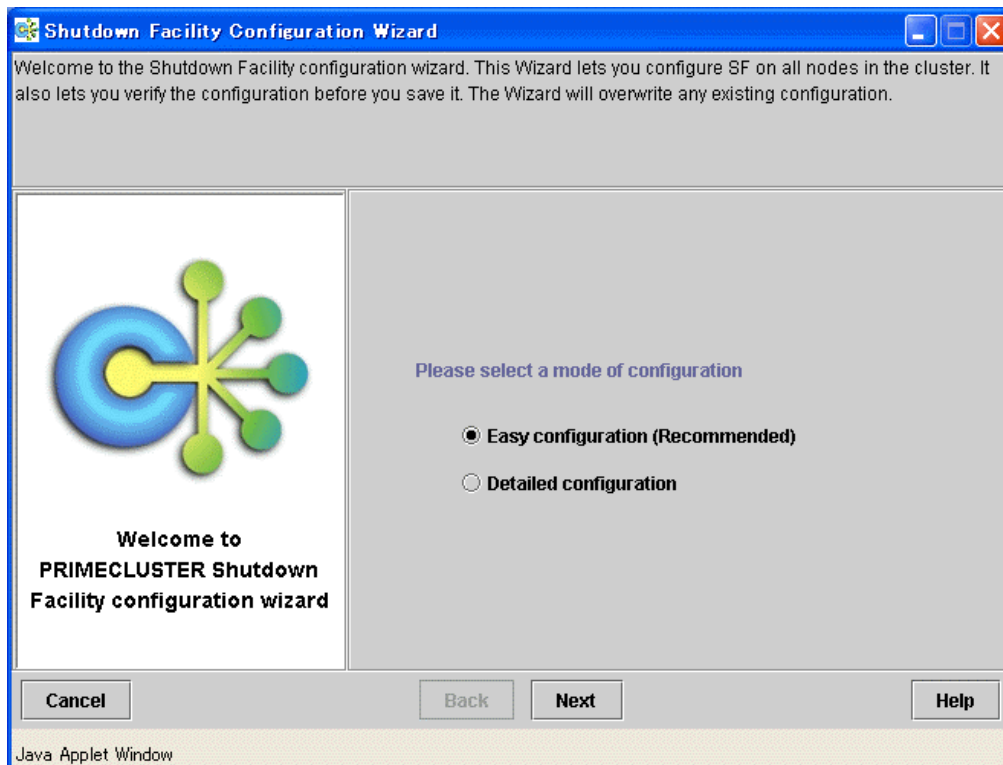


When the Configuration Wizard starts, the window shown in Figure H-2 appears. At this window, select the configuration setup mode. You can choose either the *Easy configuration (recommended)* mode or the *Detailed configuration* mode.

Easy configuration (recommended) allows you to set up the recommended SF configuration in PRIMECLUSTER. Normally, you would select *Easy configuration (recommended)*. Choose *Detailed configuration* if you want to add or delete a shutdown agent, change the configuration, or change the timeout value for a shutdown agent.

Choose *Easy configuration (recommended)* and click *Next*. If you select *Detailed configuration*, see "8.4.3 Detailed configuration."

Figure H-2: Selecting the configuration mode



H.7.2 Simple configuration (recommended)

At the window shown in Figure H-3, select *No SCON Configuration*, and then select the shutdown agents to be used. The shutdown agents to be used differ according to the PRIMEPOWER model. Check the hardware model, and configure the SF.

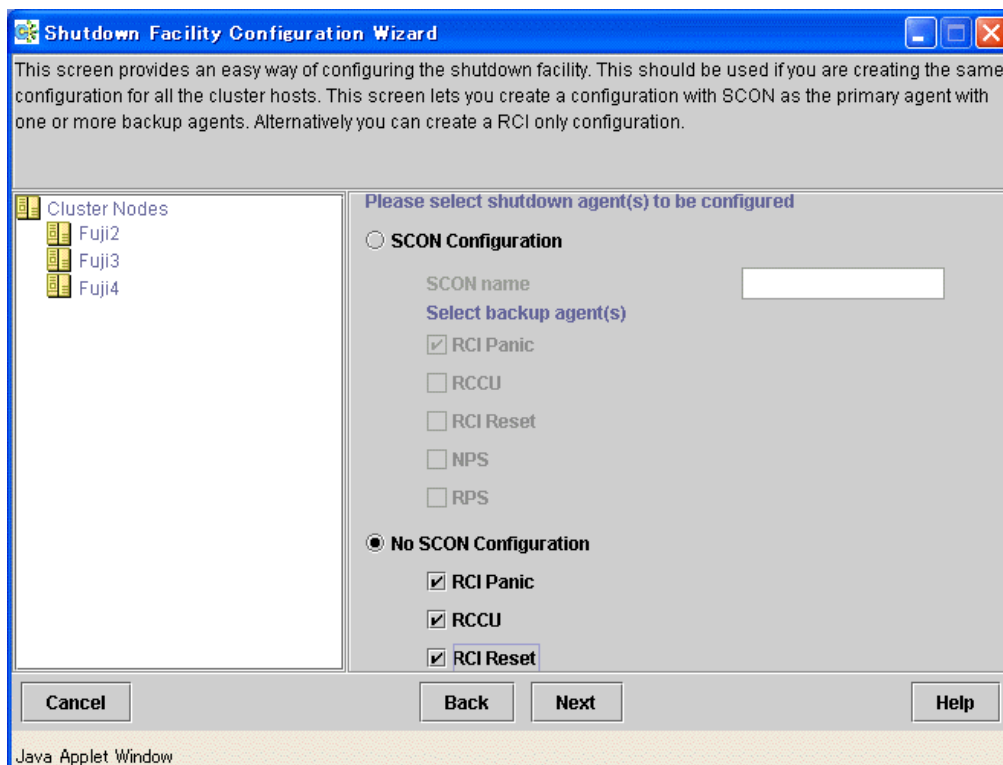
For PRIMEPOWER 200, 400, 600, 650, and 850:

Select all shutdown agents for RCI monitoring agent (RCI Panic and RCI Reset) and RCCU monitoring agent.

For PRIMEPOWER 800, 900, 1000, 1500, 2000, and 2500:

Select the shutdown agents for RCI monitoring agent (RCI Panic and RCI Reset).

Figure H-3: Selecting the shutdown agents to be used



Click *Next*.

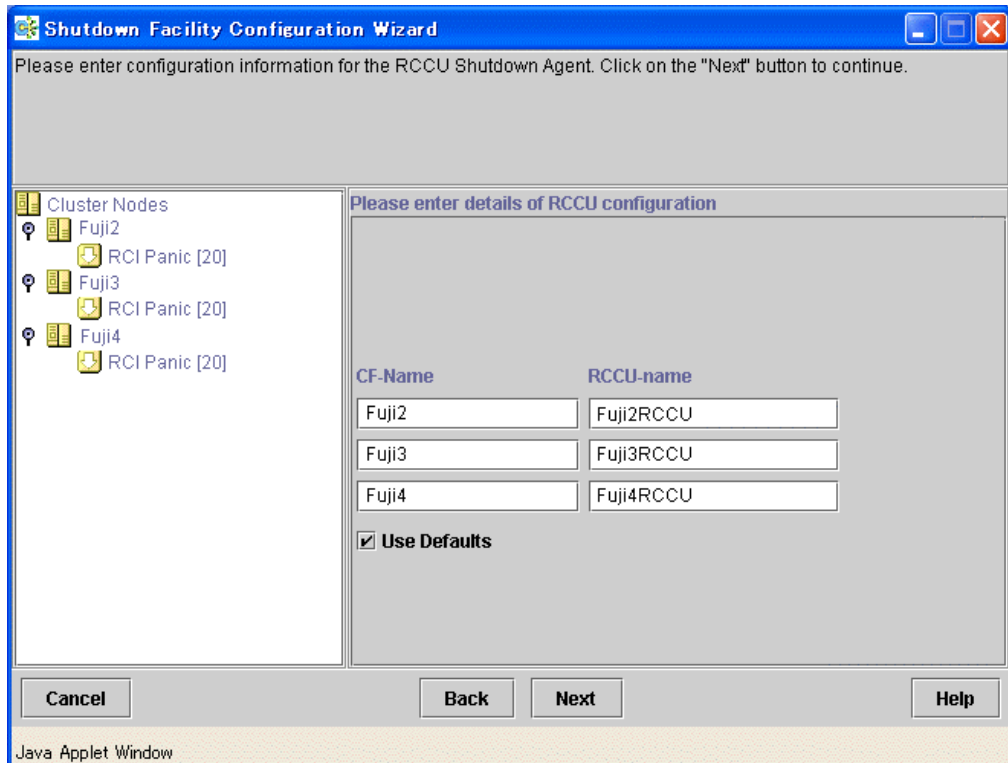
If you select the RCCU shutdown agent, you will be taken to the window for entering RCCU configuration information, which is shown in Figure H-4. At this window, you must enter the RCCU name. Enter the IP address of the RCCU or the RCCU host name that is specified in the `/etc/inet/hosts` file.



Note

Do not clear the *Use Defaults* checkbox, and do not change the CF name.

Figure H-4: RCCU configuration details



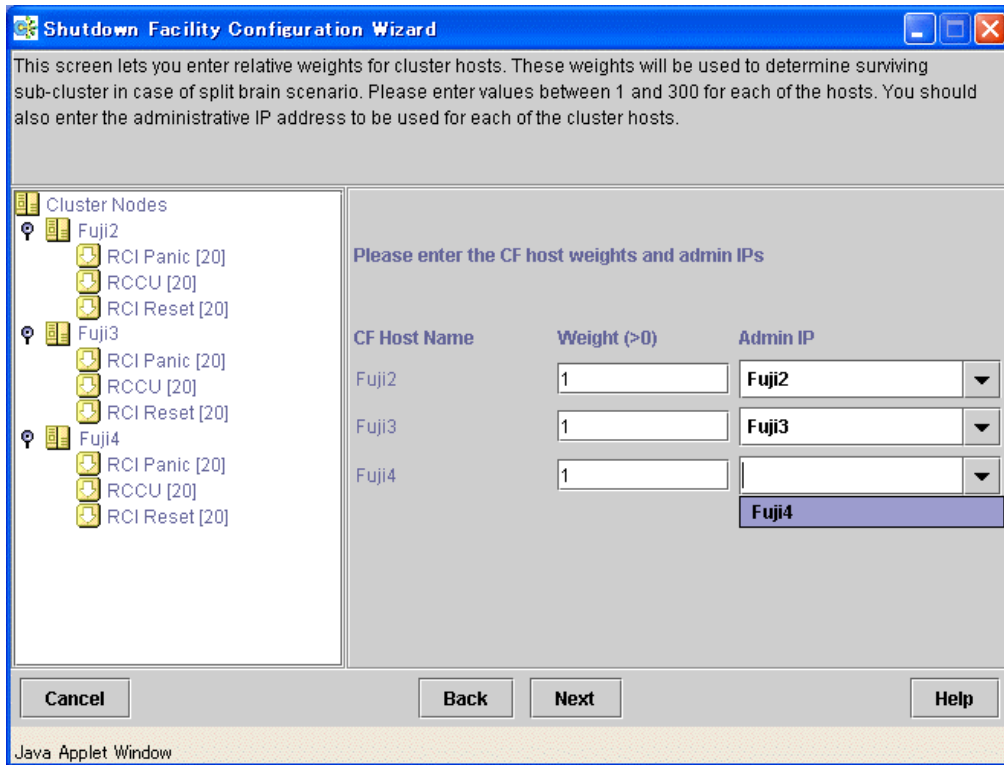
If you click *Next*, the window shown in Figure H-5 appears.

This window allows you to enter weights for the cluster nodes. These weights are used to identify the live priority of the surviving node group if a cluster partition occurs. If a cluster interconnect failure triggers a cluster partition, all nodes can still access the user resources. To ensure the data consistency in the user resources, you must determine which node groups should survive and which node groups should be forcibly terminated. In PRIMECLUSTER, the weights that are assigned to the individual node groups are called "live priority" values. As the node weight increases, the live priority becomes higher. Conversely, as the weight decreases, the live priority becomes lower.

You can enter a value from 1 to 300 for each node. You must also enter the administrative LAN IP address to be used by each node. Enter the IP address directory, or click the tab and set the host name that has been assigned to the administrative LAN IP address.

For details on the node weight, see 5.2.2 "Setting Up the Shutdown Facility."

Figure H-5: Entering host weights and administrative LAN IP addresses

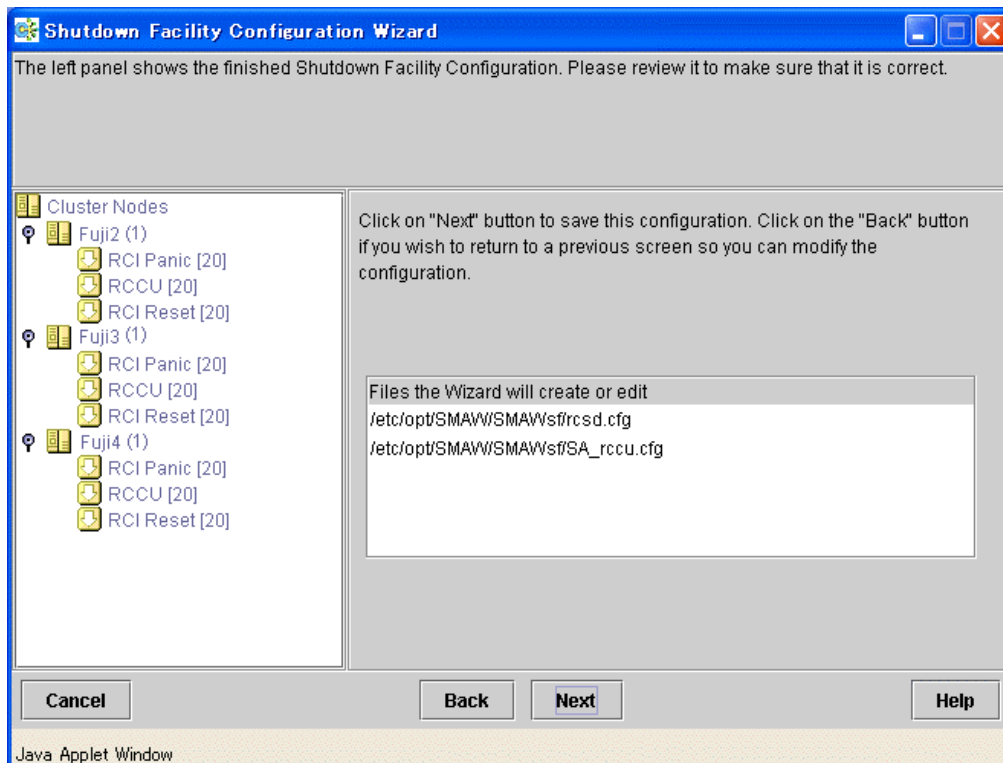


Click *Next* to display the completed SF configuration, as shown in the window in Figure H-6.

The left panel in the window displays the cluster nodes and shows the shutdown agents configured for each node. Click *Next* to save the configuration to a configuration file.

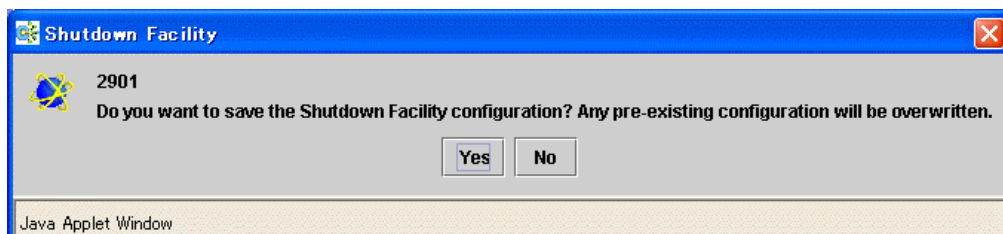
Click *Back* to change the configuration.

Figure H-6: Configuration files



Click *Next* to display the confirmation pop-up menu, which is shown in Figure H-7. Select *Yes* to save the configuration.

Figure H-7: Saving the SF configuration



When you save the configuration, the SF configuration window, which is shown in Figure H-8, appears. You can check the SF configuration of each node by selecting a node in this window.

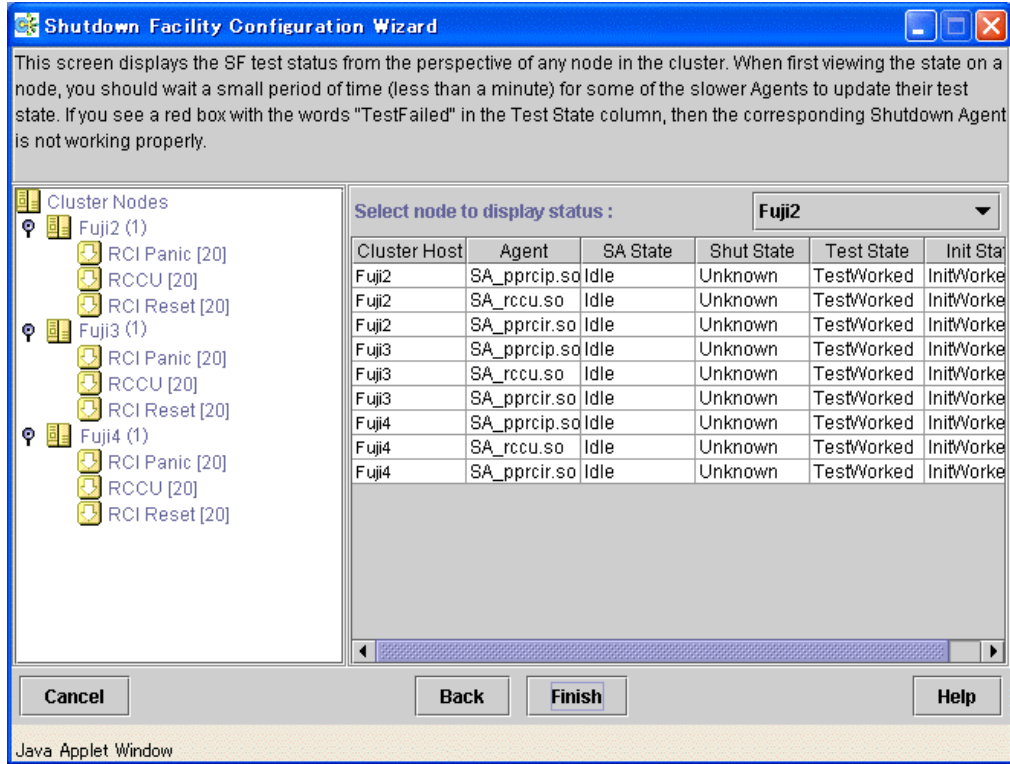
To display the SF configuration window, you may also use the *Tools* pull-down menu to select *Shutdown Facility*, and then choose *Show Status*.

The Init State column indicates whether the shutdown agent has been initialized. The Test State column indicates whether the path for shutting down the node in the event of a failure has been tested.

The Test State column will show *Unknown* if the path test has not been completed, but the value changes to *Test Worked* when the configured shutdown agent works normally. If the Init State column shows *Init Failed* even though SF configuration has been completed or if the Test Status column shows *Unknown* or *Test Failed*, there might be incorrect settings in the SF configuration or hardware products. Check whether an error message was output to the "error/var/adm/messages" file or the console output screen. Then if a message was output, take the action for that message. See "12.19 Monitoring Agent Messages." in "PRIMECLUSTER

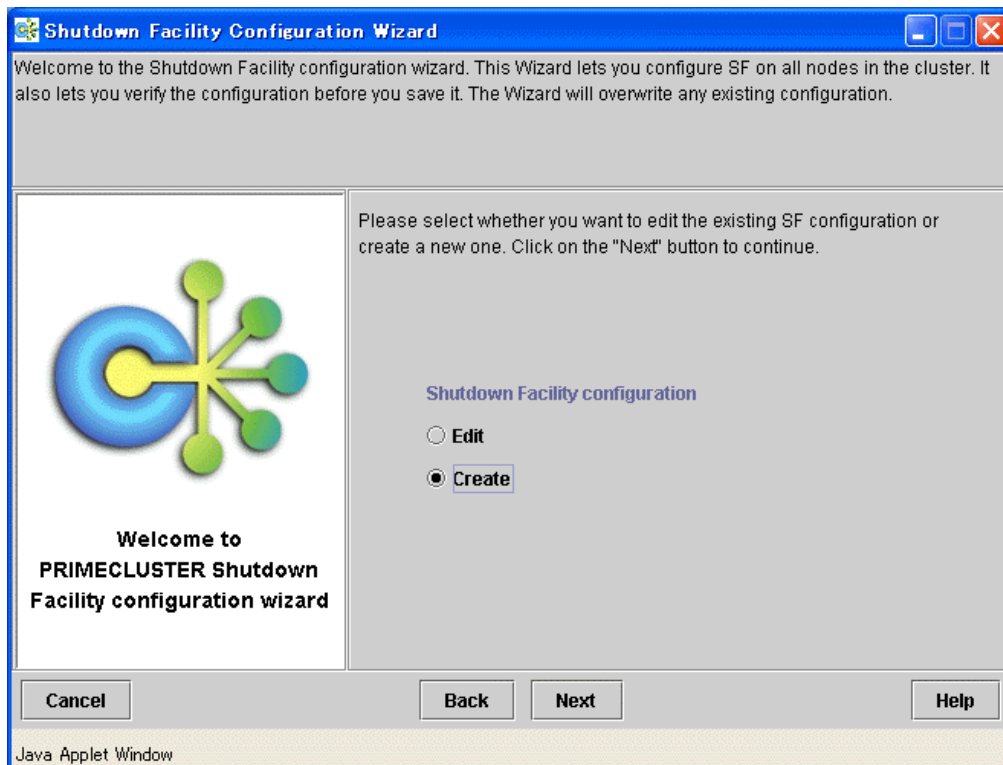
Cluster Foundation Configuration and Administration." The Shut State column displays Unknown when the system is operating normally. But if a node error occurs, and SF stops the node successfully, the status changes to KillWorked.

Figure H-8: Status of shutdown agents



To exit the Configuration Wizard, click *Finish*. Then when the pop-up window shown in Figure H-9 appears, click *Yes*.

Figure H-9: Exiting the Configuration Wizard

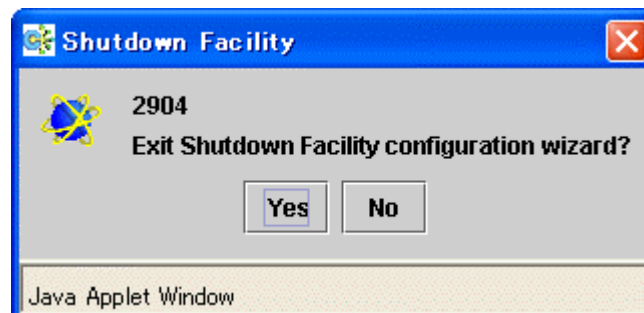


H.7.3 Detailed configuration

If you choose *Detailed configuration* at the configuration mode selection window shown in Figure H-2 and click *Next*, the configuration window for the detailed configuration mode, which is shown in Figure H-10 will appear.

At this window, choose *Edit existing Shutdown Facility configuration* to edit an existing configuration or choose *Create a new Shutdown Facility configuration* to create a new configuration.

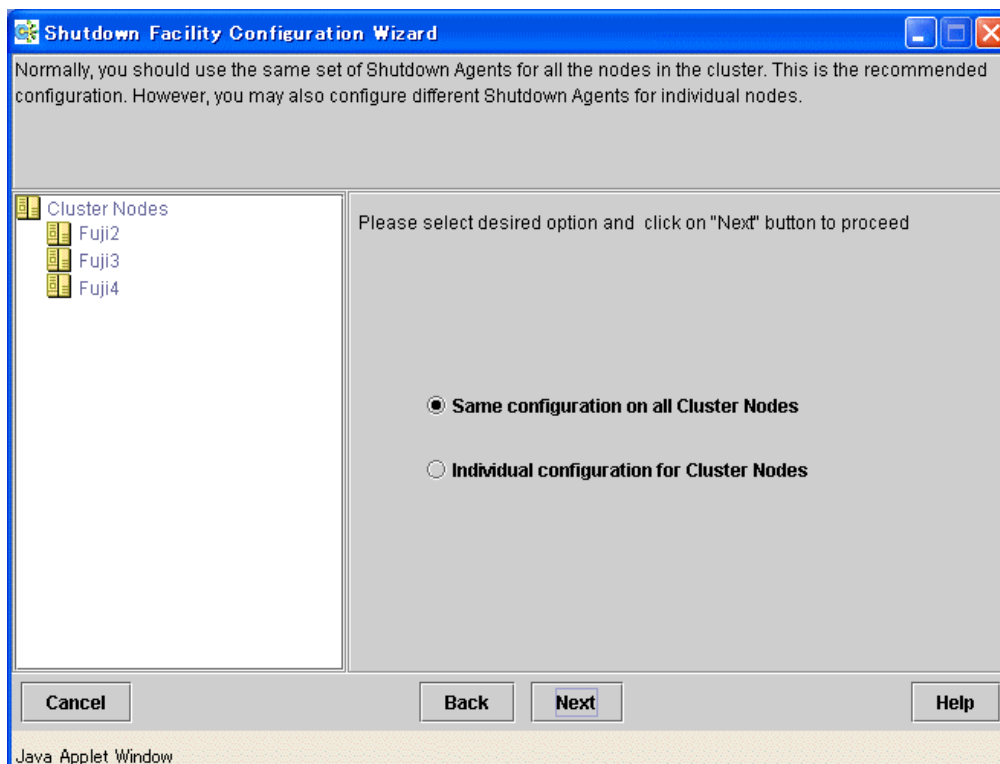
Figure H-10: Detailed mode of SF configuration



Choose *Create a new Shutdown Facility configuration* and click *Next*.

At the window shown in Figure H-11 select whether to use the same configuration for all cluster nodes or to use a different configuration for each node. Normally, you should use the same configuration for all nodes.

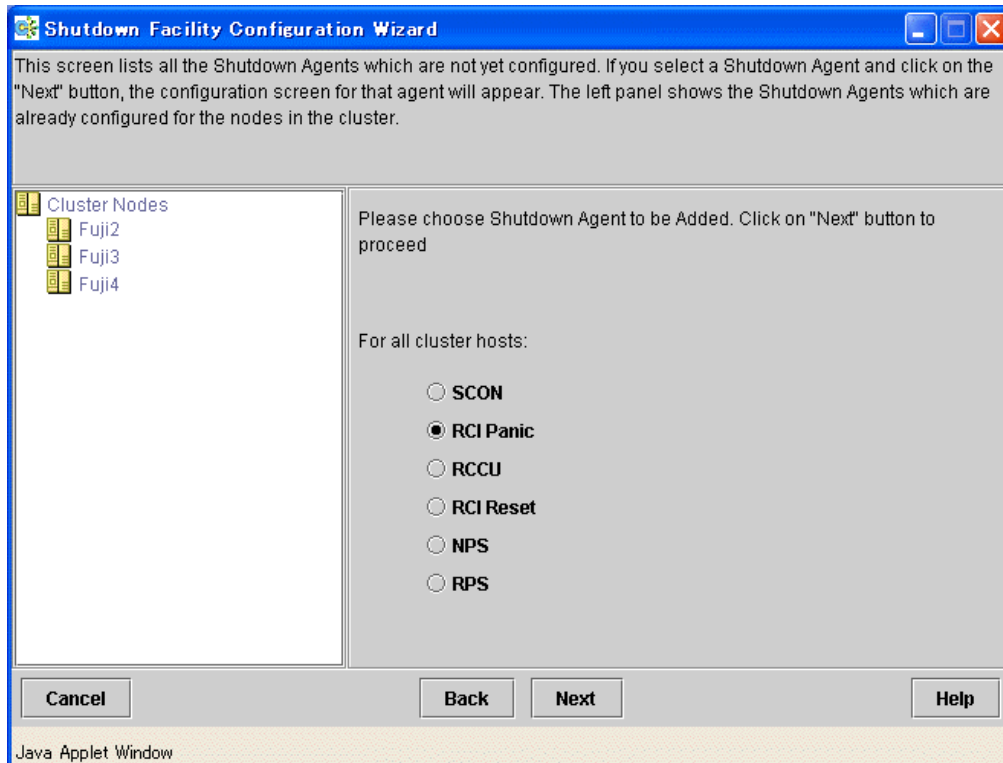
Figure H-11: Choosing the same SF configuration or different SF configurations for each node



Select *Same configuration on all Cluster Nodes* and click *Next*.

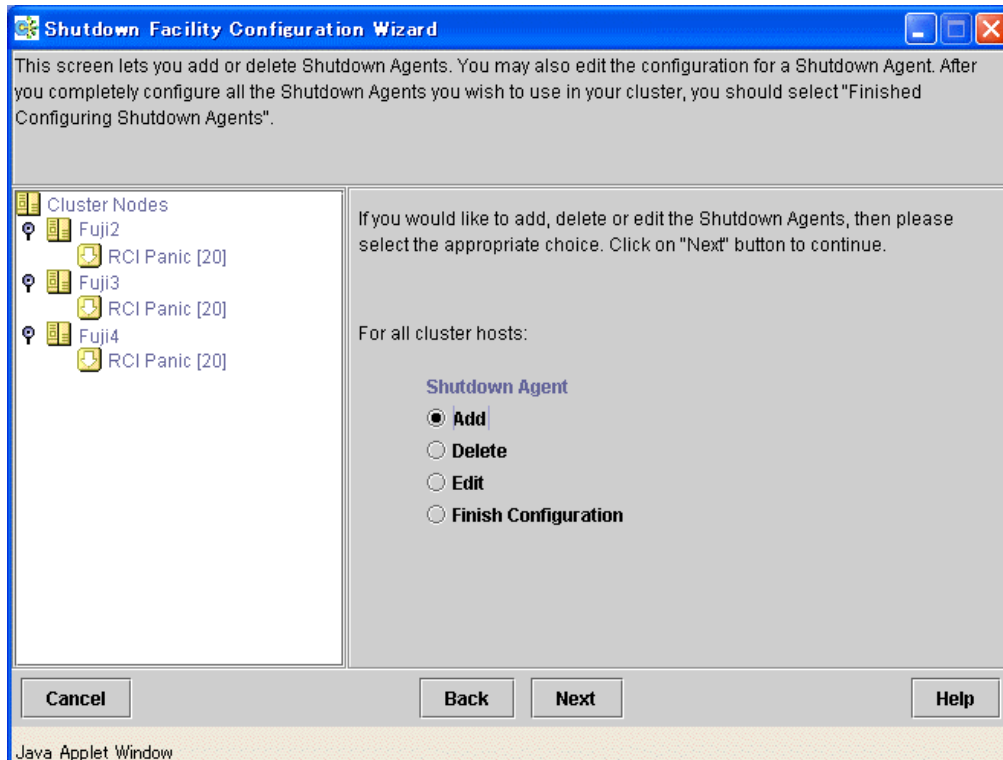
The window shown in Figure H-12 displays the shutdown agents that can be added. Of the displayed shutdown agents, those that are supported are RCI Panic, RCI Reset, and RCCU.

Figure H-12: Choosing the RCI Panic shutdown agent



If you select *RCI Panic* and click *Next*, the screen shown in Figure H-13 will appear.

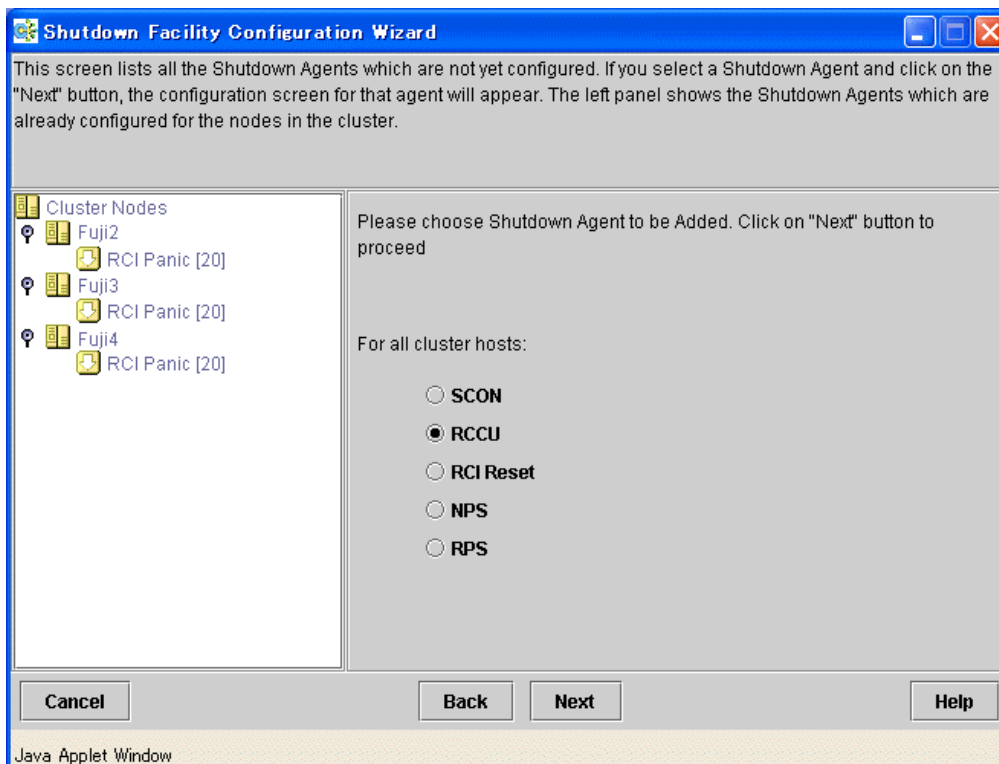
Figure H-13: Adding, deleting, or editing shutdown agents



Since another shutdown agent will be added, select *Add* and click *Next*.

The left panel in Figure H-14 displays the shutdown agents that are already configured.

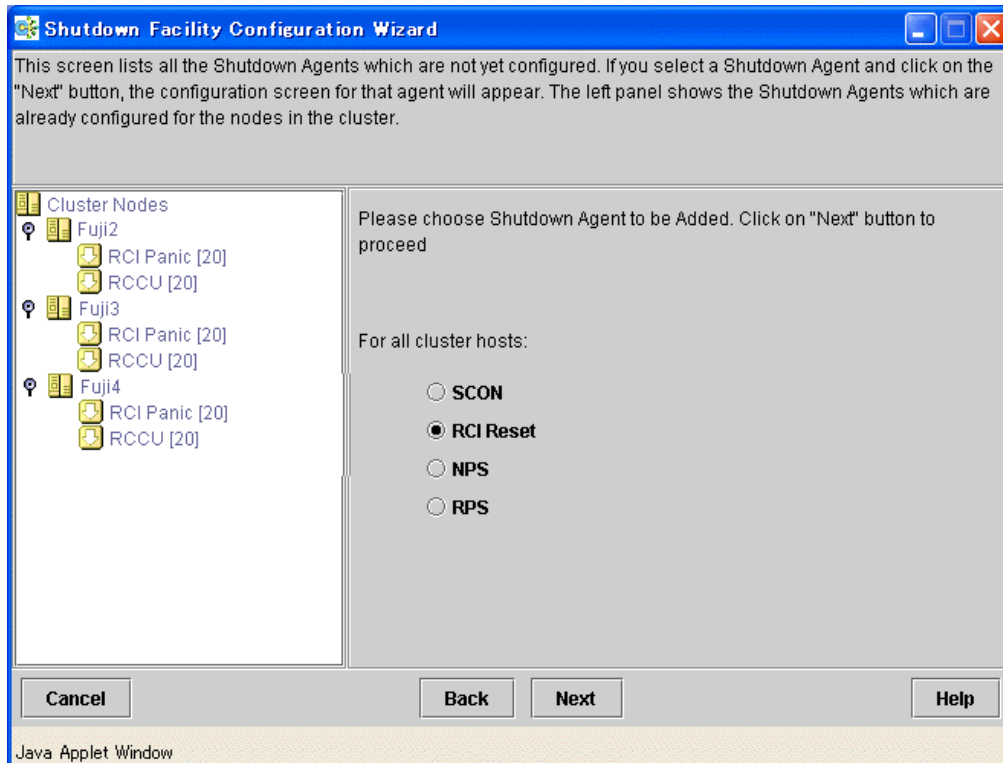
Figure H-14: Selecting the RCCU shutdown agent



Select *RCCU* and click *Next*.

If you select *RCCU* from the list and click *Next*, a detailed setup screen for the *RCCU* configuration, which is shown in Figure H-15 will appear. Enter the *RCCU* configuration information according to the explanation for Figure H-4

Figure H-15: Selecting the RCI Reset shutdown agent



Select *RCI Reset* and click *Next*.

If you configured a shutdown agent incorrectly, select *Delete* at the window shown in Figure H-16 and click *Next*. A window like the one shown in Figure H-17 will appear.

Figure H-16: Deleting a shutdown agent

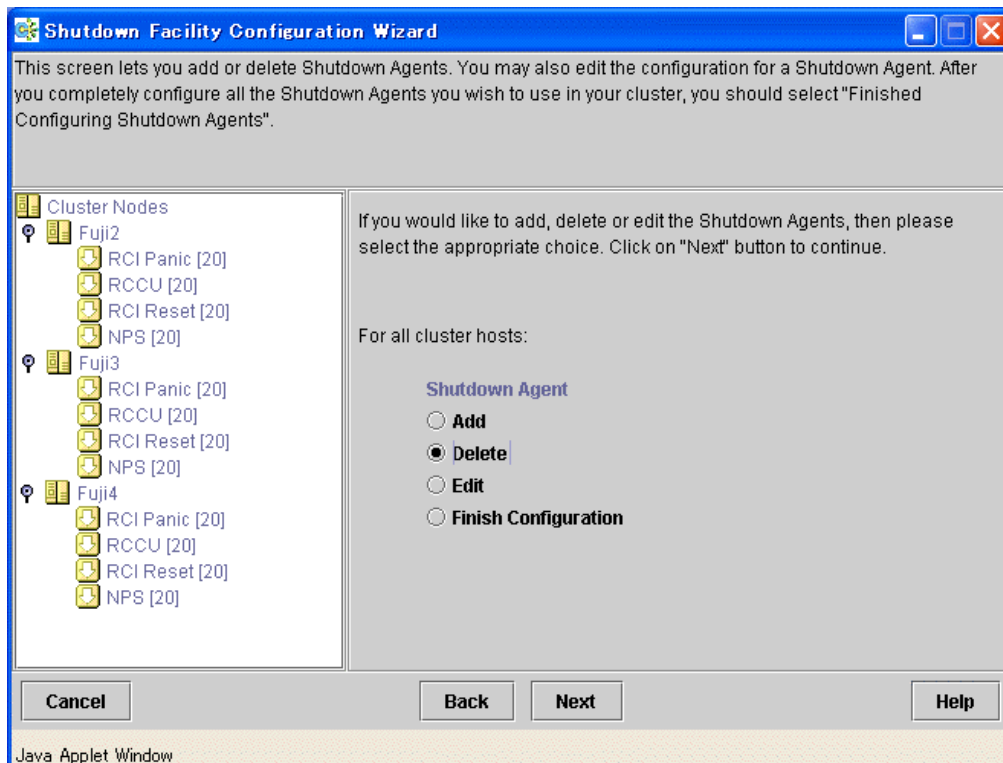
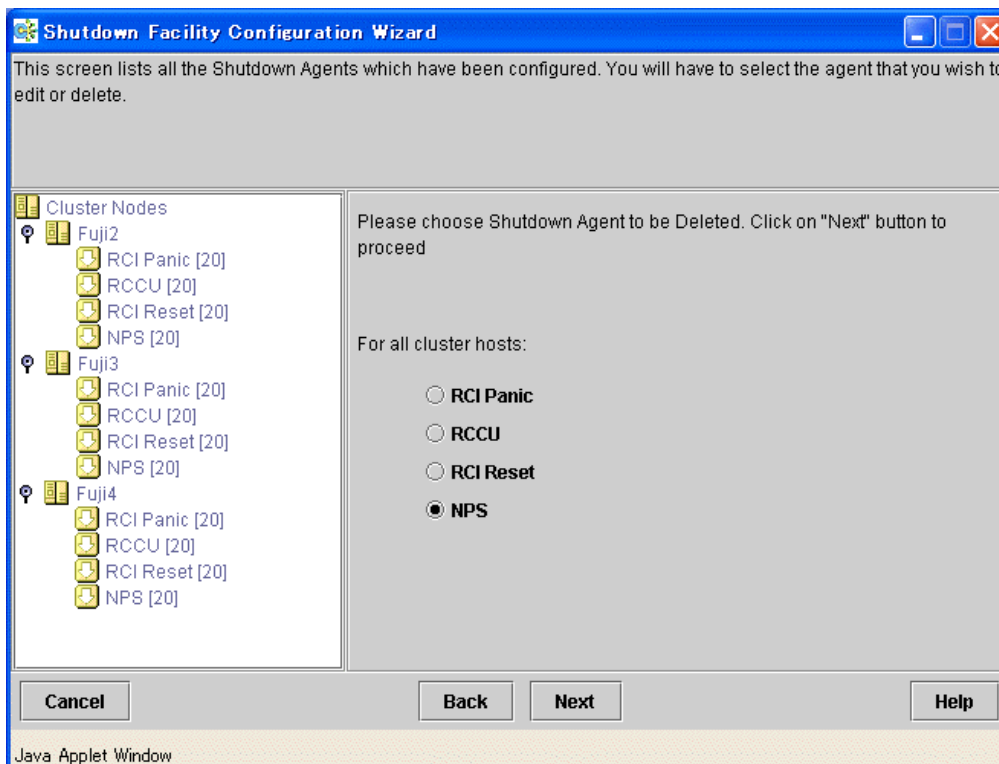


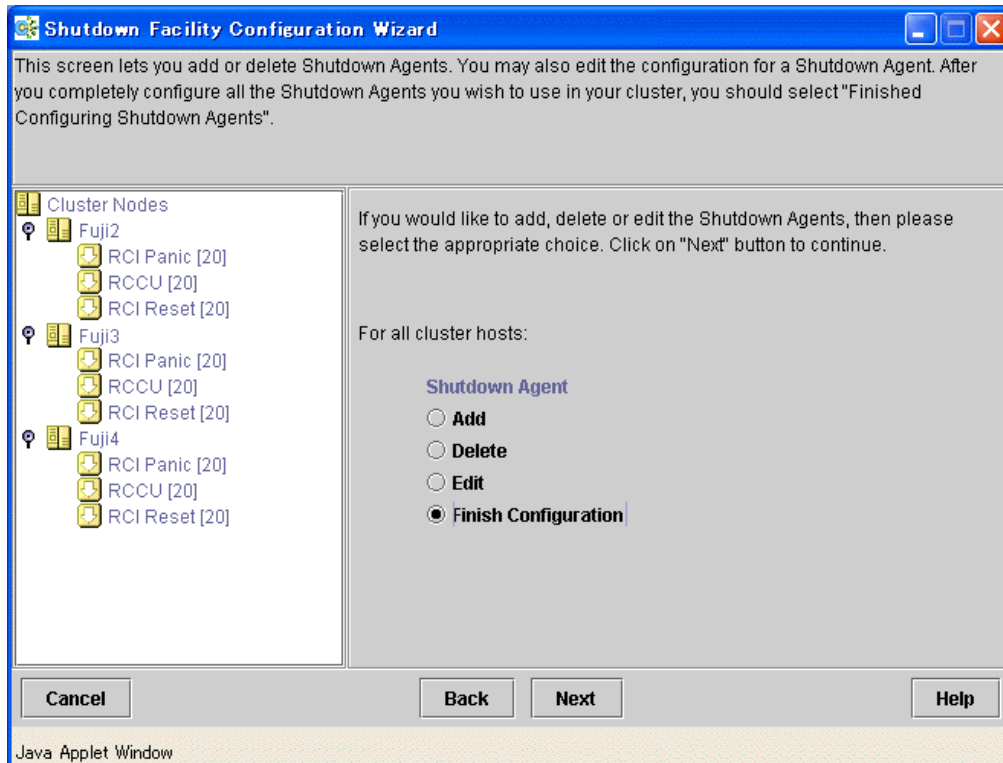
Figure H-17: Selecting the shutdown agent to be deleted



From the configuration list, select the shutdown agent to be deleted and click *Next*.

When the configuration is completed, select *Finished Configuring Shutdown Agent* and click *Next*.

Figure H-18: Selecting Finish Configuration



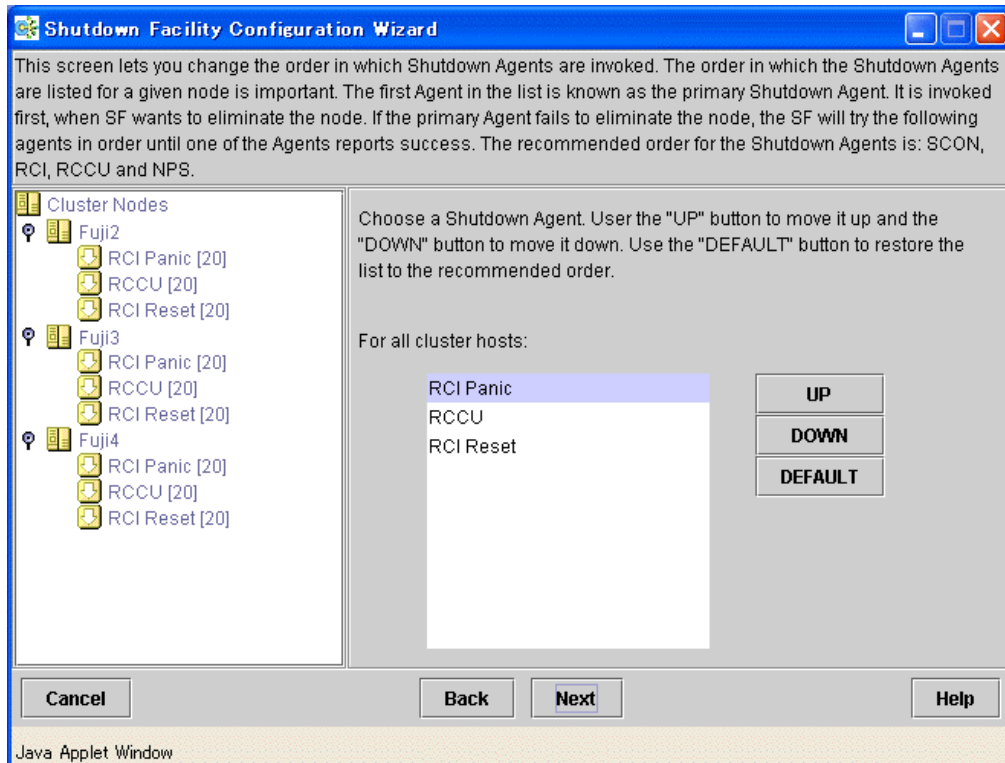
The window shown in Figure H-19 allows you to change the order in which the shutdown agents are invoked. When SF forcibly terminates a node, it invokes the shutdown agents in order from the first agent in the list. This agent is called the primary shutdown agent, and it is invoked first when SF wants to forcibly stop the node. If the primary shutdown agent fails to stop the node, SF will invoke the following agents in order until one of the agents is successful.

To set the shutdown agents in the recommended order, press the *Default* button. The order in which the shutdown agents are invoked will be set to *RCI Panic*, *RCCU*, and *RCI Reset*. This order is determined by the following policy:

- Priority is given to the forced termination method that allows information for troubleshooting to be collected so that the cause of the node failure can be investigated.

- Priority is given to the forced termination method that has fewer hardware faults.

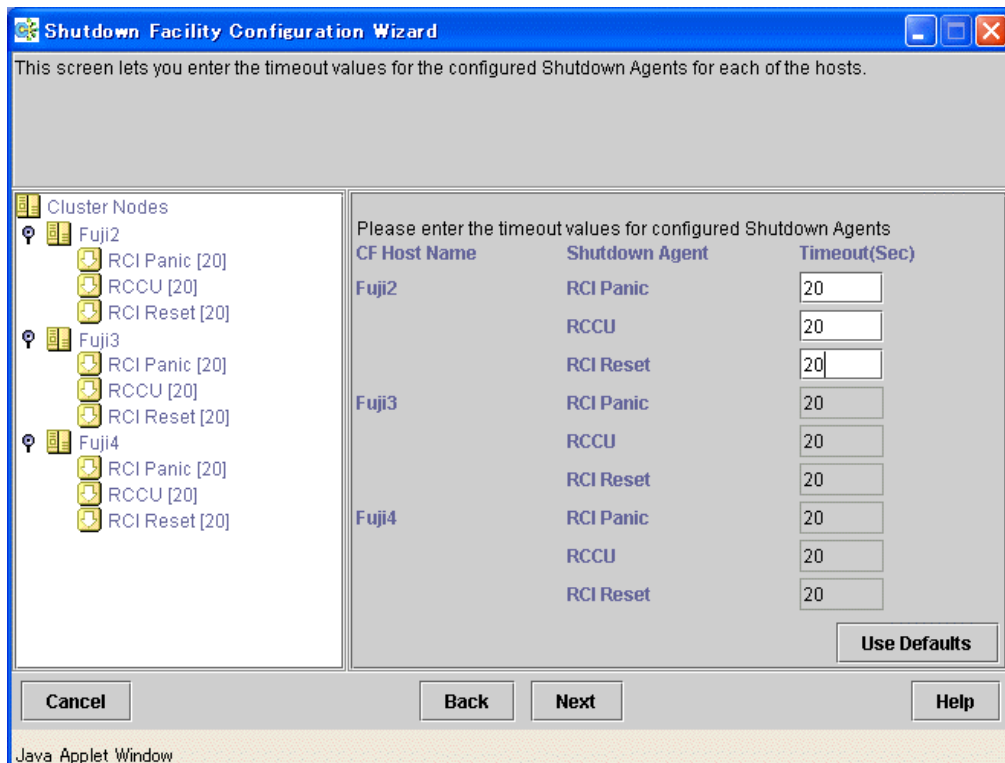
Figure H-19: Invoking sequence of the shutdown agents



Click Next. The screen shown in Figure H-20 will appear.

This screen lets you enter the timeout value for each shutdown agent configured for each node. The default value is 20 seconds.

Figure H-20: Setting the timeout value



Set the timeout value to complete the detailed configuration of the shutdown agent, and Click Next. When the input window shown in Figure H-5 appears, enter the node weight and administrative LAN IP address of each host according to the explanation displayed on the window.

To change the configuration, select Back and change the configuration.

Glossary

AC

See *Access Client*.

Access Client

GFS kernel module on each node that communicates with the Meta Data Server and provides simultaneous access to a shared file system.

See also *Meta Data Server*.

Administrative LAN

In PRIMECLUSTER configurations, an Administrative LAN is a private local area network (LAN) on which machines such as the System Console and Cluster Console reside. Because normal users do not have access to the Administrative LAN, it provides an extra level of security. The use of an Administrative LAN is optional.

See also *public LAN*.

API

See *Application Program Interface*.

application (RMS)

A resource categorized as userApplication used to group resources into a logical collection.

Application Program Interface

A shared boundary between a service provider and the application that uses that service.

application template (RMS)

A predefined group of object definition value choices used by RMS Application Wizards to create object definitions for a specific type of application.

Application wizards

See *RMS Application Wizards*.

attribute (RMS)

The part of an object definition that specifies how the base monitor acts and reacts for a particular object type during normal operations.

automatic configuration (GDS)

Function that automatically recognizes the physical connection configuration of shared disk units and registers the units to the resource database.

automatic power control

This function is provided by the Enhanced Support Facility (ESF), and it automatically switches the PRIMEPOWER power on and off.

automatic switchover (RMS)

The procedure by which RMS automatically switches control of userApplication over to another host after specified conditions are detected.

See also *directed switchover*, *failover*, *switchover*, and *symmetrical switchover*.

availability

Availability describes the need of most enterprises to operate applications via the Internet 24 hours a day, 7 days a week. The relationship of the actual to the planned usage time determines the availability of a system.

base cluster foundation (CF)

This PRIMECLUSTER module resides on top of the basic OS and provides internal interfaces for the CF (Cluster Foundation) functions that the PRIMECLUSTER services use in the layer above.

See also *Cluster Foundation*.

BM (base monitor)(RMS)

The RMS module that maintains the availability of resources. The base monitor is supported by daemons and detectors. Each host being monitored has its own copy of the base monitor

Cache Fusion

The improved interprocess communication interface in Oracle 9i that allows logical disk blocks (buffers) to be cached in the local memory of each node. Thus, instead of having to flush a block to disk when an update is required, the block can be copied to another node by passing a message on the interconnect, thereby removing the physical I/O overhead.

ccbr.conf

The environment setting file that is used backup and restore operations, and is placed in the "/opt/SMAW/ccbr" directory. This file is used in the "\$CCBRHOME" variable setting. For details, see the manual pages for the "cfbackup(1M)" and "cfrestore(1M)" commands and the comments in the "ccbr.conf" file.

ccbr.gen

The file that stores the generation number and is placed in the "/opt/SMAW/ccbr" directory. A value of 0 or higher is stored in this file. For details, see the manual pages for the "cfbackup(1M)" and "cfrestore(1M)" commands.

CCBRHOME variable

The variable that identifies the directory in which backup data is stored. The initial value is the "/var/spool/pcl4.1/ccbr" directory. This variable can be set only in the "ccbr.conf" file.

CF

See Cluster Foundation.

child (RMS)

A resource defined in the configuration file that has at least one parent. A child can have multiple parents, and can either have children itself (making it also a parent) or no children (making it a leaf object).

See also *resource*, *object*, *parent*, and *leaf object*.

class (GDS)

See *disk class*.

cluster

A set of computers that work together as a single computing source. Specifically, a cluster performs a distributed form of parallel computing.

See also *RMS configuration*.

Cluster Foundation

The set of PRIMECLUSTER modules that provides basic clustering communication services.

See also *base cluster foundation*.

cluster interconnect (CF)

The set of private network connections used exclusively for PRIMECLUSTER communications.

Cluster Join Services (CF)

This PRIMECLUSTER module handles the forming of a new cluster and the addition of nodes.

Cluster Resource Management facility

Facility that manages hardware units that are shared among multiple nodes.

concatenated virtual disk

Concatenated virtual disks consist of two or more pieces on one or more disk drives. They correspond to the sum of their parts. Unlike simple virtual disks where the disk is subdivided into small pieces, the individual disks or partitions are combined to form a single large logical disk. (Applies to transitioning users of existing Fujitsu Siemens products only.)

See also *mirror virtual disk*, *simple virtual disk*, *striped virtual disk*, *virtual disk*.

concatenation (GDS)

The linking of multiple physical disks. This setup allows multiple disks to be used as one virtual disk that has a large capacity.

configuration file (RMS)

The RMS configuration file that defines the monitored resources and establishes the interdependencies between them. The default name of this file is `config.us`.

console

See *single console*.

custom detector (RMS)

See *detector*.

custom type (RMS)

See *generic type*.

daemon

A continuous process that performs a specific function repeatedly.

database node (SIS)

Nodes that maintain the configuration, dynamic data, and statistics in a SIS configuration.

See also *gateway node*, *service node*, *Scalable Internet Services*.

detector (RMS)

A process that monitors the state of a specific object type and reports a change in the resource state to the base monitor.

directed switchover (RMS)

The RMS procedure by which an administrator switches control of userApplication over to another host.

See also *automatic switchover*, *failover*, *switchover*, and *symmetrical switchover*.

disk class (GDS)

Collection of SDX objects. The shared type disk class is also a resource unit that can be used by the PRIMECLUSTER system. A disk class is sometimes simply called a "class."

disk group (GDS)

A collection of disks or low-order groups that become the unit for mirroring, striping, or concatenation. Disk and low-order groups that belong to the same disk group are mutually mirrored, striped, or concatenated according to the type attribute (mirror, stripe, or concatenation) of that disk group.

A disk group is sometimes simply called a "group."

DOWN (CF)

A node state that indicates that the node is unavailable (marked as down). A LEFTCLUSTER node must be marked as DOWN before it can rejoin a cluster.

See also *UP*, *LEFTCLUSTER*, *node state*.

ENS (CF)

See *Event Notification Services*.

environment variable (RMS)

Variables or parameters that are defined globally.

error detection (RMS)

The process of detecting an error. For RMS, this includes initiating a log entry, sending a message to a log file, or making an appropriate recovery response.

Ethernet

LAN standard that is standardized by IEEE 802.3. Currently, except for special uses, nearly all LANs are Ethernets. Originally the expression Ethernet was a LAN standard name for a 10 megabyte per second type LAN, but now it also used as a general term that includes high-speed Ethernets and gigabyte Ethernets.

Event Notification Services (CF)

This PRIMECLUSTER module provides an atomic-broadcast facility for events.

failover (RMS, SIS)

The process by which a user application automatically transfers processes and data inherited from an operating system to a standby system because some failure has occurred.

With SIS, this process switches a failed node to a backup node. With RMS, this process is known as switchover.

See also *automatic switchover, directed switchover, switchover, symmetrical switchover*.

Fast switching mode

One of the LAN duplexing modes presented by GLS.

This mode uses a multiplexed LAN simultaneously to provide enhanced communication scalability between Solaris OE servers and high-speed switchover if a LAN failure occurs.

fault tolerant network

A network with the ability to withstand faults (fault tolerant). Fault tolerant is the ability to maintain and continue normal operation even if a fault occurs in part of the computer system. A fault tolerant network is therefore a network that can continue normal communication even if a flat occurs in part of the network system.

gateway node (SIS)

Gateway nodes have an external network interface. All incoming packets are received by this node and forwarded to the selected service node, depending on the scheduling algorithm for the Service.

See also *service node, database node, Scalable Internet Services*.

See *disk group*.

GDS

See *Global Disk Services*.

generation number

Data generation management is enabled in the PRIMECLUSTER backup and restore operations. The current generation number is added as part of the backup and restore data name. Integers of 0 or higher are used as generation numbers, and the generation number is incremented each time backup is successful. The generation number is stored in the "cbr.gen" file and can be specified as an optional argument in the "cfbackup(1M)" and "cfrestore(1M)" commands.

For details, see the manual pages for the "cfbackup(1M)" and "cfrestore(1M)" commands.

generic type (RMS)

An object type which has generic properties. A generic type is used to customize RMS for monitoring resources that cannot be assigned to one of the supplied object types.

See also *object type*.

GFS

See *Global File Services*.

GFS local file system

A local file system that features high-speed file access and file system switchover after a system failure. High-speed file access is available through the serial block allocation to file data, and file system switchover is assured through a file system consistency recovery function.

A GFS local file system is used by one node or by two nodes, in which case the file system is used as a switchover file system.

GFS shared file system

A shared file system that allows simultaneous access from multiple Solaris OE systems that are connected to shared disk units, while maintaining data consistency, and allows processing performed by a node to be continued by other nodes even if the first node fails.

A GFS shared file system can be mounted and used concurrently from multiple nodes.

Global Disk Services

This optional product provides volume management that improves the availability and manageability of information stored on the disk unit of the Storage Area Network (SAN).

Global File Services

This optional product provides direct, simultaneous accessing of the file system on the shared storage unit from two or more nodes within a cluster.

Global Link Services

This PRIMECLUSTER optional module provides network high availability solutions by multiplying a network route.

GLS

See *Global Link Services*.

graph (RMS)

See *system graph*.

graphical user interface

A computer interface with windows, icons, toolbars, and pull-down menus that is designed to be simpler to use than the command-line interface.

group (GDS)**GUI**

See *graphical user interface*.

high availability

This concept applies to the use of redundant resources to avoid single points of failure.

highest-order group (GDS)

Group that does not belong to another group. A volume can be created in the highest-order group.

hub

Star-type wiring device used for LAN or fibre channels.

installation server

System having a Solaris CD image on the disk or CD-ROM drive to distribute the Solaris CD image to other systems over the network.

interconnect (CF)

See *cluster interconnect*.

Internet Protocol address

A numeric address that can be assigned to computers or applications.

See also *IP aliasing*.

internode communication facility

Communication function between cluster nodes that are used by PRIMECLUSTER CF. Since this facility is designed especially for communication between cluster nodes, the overhead is less than that of TCP/IP, and datagram communication services that also guarantee the message arrival sequence can be carried out.

IP address

See *Internet Protocol address*.

IP aliasing

This enables several IP addresses (aliases) to be allocated to one physical network interface. With IP aliasing, the user can continue communicating with the same IP address, even though the application is now running on another host.

See also *Internet Protocol address*.

IP address

See *Internet Protocol address*.

IP aliasing

This enables several IP addresses (aliases) to be allocated to one physical network interface. With IP aliasing, the user can continue communicating with the same IP address, even though the application is now running on another host.

See also *Internet Protocol address*.

IP address

See *Internet Protocol address*.

IP aliasing

This enables several IP addresses (aliases) to be allocated to one physical network interface. With IP aliasing, the user can continue communicating with the same IP address, even though the application is now running on another host.

See also *Internet Protocol address*.

IP address

See *Internet Protocol address*.

IP aliasing

This enables several IP addresses (aliases) to be allocated to one physical network interface. With IP aliasing, the user can continue communicating with the same IP address, even though the application is now running on another host.

See also *Internet Protocol address*.

IP address

See *Internet Protocol address*.

IP aliasing

This enables several IP addresses (aliases) to be allocated to one physical network interface. With IP aliasing, the user can continue communicating with the same IP address, even though the application is now running on another host.

See also *Internet Protocol address*.

IP address

See *Internet Protocol address*.

IP aliasing

This enables several IP addresses (aliases) to be allocated to one physical network interface. With IP aliasing, the user can continue communicating with the same IP address, even though the application is now running on another host.

See also *Internet Protocol address*.

IP address

See *Internet Protocol address*.

IP aliasing

This enables several IP addresses (aliases) to be allocated to one physical network interface. With IP aliasing, the user can continue communicating with the same IP address, even though the application is now running on another host.

See also *Internet Protocol address*.

IP address

See *Internet Protocol address*.

IP aliasing

This enables several IP addresses (aliases) to be allocated to one physical network interface. With IP aliasing, the user can continue communicating with the same IP address, even though the application is now running on another host.

See also *Internet Protocol address*.

IP address

See *Internet Protocol address*.

IP aliasing

This enables several IP addresses (aliases) to be allocated to one physical network interface. With IP aliasing, the user can continue communicating with the same IP address, even though the application is now running on another host.

See also *Internet Protocol address*.

IP address

See *Internet Protocol address*.

IP aliasing

This enables several IP addresses (aliases) to be allocated to one physical network interface. With IP aliasing, the user can continue communicating with the same IP address, even though the application is now running on another host.

See also *Internet Protocol address*.

IP address

See *Internet Protocol address*.

IP aliasing

This enables several IP addresses (aliases) to be allocated to one physical network interface. With IP aliasing, the user can continue communicating with the same IP address, even though the application is now running on another host.

See also *Internet Protocol address*.

IP address

See *Internet Protocol address*.

IP aliasing

This enables several IP addresses (aliases) to be allocated to one physical network interface. With IP aliasing, the user can continue communicating with the same IP address, even though the application is now running on another host.

See also *Internet Protocol address*.

IP address

See *Internet Protocol address*.

IP aliasing

This enables several IP addresses (aliases) to be allocated to one physical network interface. With IP aliasing, the user can continue communicating with the same IP address, even though the application is now running on another host.

See also *Internet Protocol address*.

IP address

See *Internet Protocol address*.

IP aliasing

This enables several IP addresses (aliases) to be allocated to one physical network interface. With IP aliasing, the user can continue communicating with the same IP address, even though the application is now running on another host.

See also *Internet Protocol address*.

IP address

See *Internet Protocol address*.

IP aliasing

This enables several IP addresses (aliases) to be allocated to one physical network interface. With IP aliasing, the user can continue communicating with the same IP address, even though the application is now running on another host.

See also *Internet Protocol address*.

IP address

See *Internet Protocol address*.

IP aliasing

This enables several IP addresses (aliases) to be allocated to one physical network interface. With IP aliasing, the user can continue communicating with the same IP address, even though the application is now running on another host.

See also *Internet Protocol address*.

IP address

See *Internet Protocol address*.

IP aliasing

This enables several IP addresses (aliases) to be allocated to one physical network interface. With IP aliasing, the user can continue communicating with the same IP address, even though the application is now running on another host.

See also *Internet Protocol address*.

IP address

See *Internet Protocol address*.

IP aliasing

This enables several IP addresses (aliases) to be allocated to one physical network interface. With IP aliasing, the user can continue communicating with the same IP address, even though the application is now running on another host.

See also *Internet Protocol address*.

IP address

See *Internet Protocol address*.

IP aliasing

This enables several IP addresses (aliases) to be allocated to one physical network interface. With IP aliasing, the user can continue communicating with the same IP address, even though the application is now running on another host.

See also *Internet Protocol address*.

IP address

See *Internet Protocol address*.

IP aliasing

This enables several IP addresses (aliases) to be allocated to one physical network interface. With IP aliasing, the user can continue communicating with the same IP address, even though the application is now running on another host.

See also *Internet Protocol address*.

IP address

See *Internet Protocol address*.

IP aliasing

This enables several IP addresses (aliases) to be allocated to one physical network interface. With IP aliasing, the user can continue communicating with the same IP address, even though the application is now running on another host.

See also *Internet Protocol address*.

IP address

See *Internet Protocol address*.

IP aliasing

This enables several IP addresses (aliases) to be allocated to one physical network interface. With IP aliasing, the user can continue communicating with the same IP address, even though the application is now running on another host.

See also *Internet Protocol address*.

IP address

See *Internet Protocol address*.

IP aliasing

This enables several IP addresses (aliases) to be allocated to one physical network interface. With IP aliasing, the user can continue communicating with the same IP address, even though the application is now running on another host.

See also *Internet Protocol address*.

IP address

See *Internet Protocol address*.

IP aliasing

This enables several IP addresses (aliases) to be allocated to one physical network interface. With IP aliasing, the user can continue communicating with the same IP address, even though the application is now running on another host.

See also *Internet Protocol address*.

IP address

See *Internet Protocol address*.

IP aliasing

This enables several IP addresses (aliases) to be allocated to one physical network interface. With IP aliasing, the user can continue communicating with the same IP address, even though the application is now running on another host.

See also *Internet Protocol address*.

IP address

See *Internet Protocol address*.

IP aliasing

This enables several IP addresses (aliases) to be allocated to one physical network interface. With IP aliasing, the user can continue communicating with the same IP address, even though the application is now running on another host.

See also *Internet Protocol address*.

IP address

See *Internet Protocol address*.

IP aliasing

This enables several IP addresses (aliases) to be allocated to one physical network interface. With IP aliasing, the user can continue communicating with the same IP address, even though the application is now running on another host.

See also *Internet Protocol address*.

IP address

See *Internet Protocol address*.

IP aliasing

This enables several IP addresses (aliases) to be allocated to one physical network interface. With IP aliasing, the user can continue communicating with the same IP address, even though the application is now running on another host.

See also *Internet Protocol address*.

IP address

See *Internet Protocol address*.

IP aliasing

This enables several IP addresses (aliases) to be allocated to one physical network interface. With IP aliasing, the user can continue communicating with the same IP address, even though the application is now running on another host.

See also *Internet Protocol address*.

IP address

See *Internet Protocol address*.

IP aliasing

This enables several IP addresses (aliases) to be allocated to one physical network interface. With IP aliasing, the user can continue communicating with the same IP address, even though the application is now running on another host.

See also *Internet Protocol address*.

IP address

See *Internet Protocol address*.

IP aliasing

This enables several IP addresses (aliases) to be allocated to one physical network interface. With IP aliasing, the user can continue communicating with the same IP address, even though the application is now running on another host.

See also *Internet Protocol address*.

IP address

See *Internet Protocol address*.

IP aliasing

This enables several IP addresses (aliases) to be allocated to one physical network interface. With IP aliasing, the user can continue communicating with the same IP address, even though the application is now running on another host.

See also *Internet Protocol address*.

IP address

See *Internet Protocol address*.

IP aliasing

This enables several IP addresses (aliases) to be allocated to one physical network interface. With IP aliasing, the user can continue communicating with the same IP address, even though the application is now running on another host.

See also *Internet Protocol address*.

IP address

See *Internet Protocol address*.

IP aliasing

This enables several IP addresses (aliases) to be allocated to one physical network interface. With IP aliasing, the user can continue communicating with the same IP address, even though the application is now running on another host.

See also *Internet Protocol address*.

IP address

See *Internet Protocol address*.

IP aliasing

This enables several IP addresses (aliases) to be allocated to one physical network interface. With IP aliasing, the user can continue communicating with the same IP address, even though the application is now running on another host.

See also *Internet Protocol address*.

IP address

See *Internet Protocol address*.

IP aliasing

This enables several IP addresses (aliases) to be allocated to one physical network interface. With IP aliasing, the user can continue communicating with the same IP address, even though the application is now running on another host.

See also *Internet Protocol address*.

IP address

See *Internet Protocol address*.

IP aliasing

This enables several IP addresses (aliases) to be allocated to one physical network interface. With IP aliasing, the user can continue communicating with the same IP address, even though the application is now running on another host.

See also *Internet Protocol address*.

IP address

See *Internet Protocol address*.

IP aliasing

This enables several IP addresses (aliases) to be allocated to one physical network interface. With IP aliasing, the user can continue communicating with the same IP address, even though the application is now running on another host.

See also *Internet Protocol address*.

IP address

See *Internet Protocol address*.

IP aliasing

This enables several IP addresses (aliases) to be allocated to one physical network interface. With IP aliasing, the user can continue communicating with the same IP address, even though the application is now running on another host.

See also *Internet Protocol address*.

IP address

See *Internet Protocol address*.

IP aliasing

This enables several IP addresses (aliases) to be allocated to one physical network interface. With IP aliasing, the user can continue communicating with the same IP address, even though the application is now running on another host.

See also *Internet Protocol address*.

IP address

See *Internet Protocol address*.

IP aliasing

This enables several IP addresses (aliases) to be allocated to one physical network interface. With IP aliasing, the user can continue communicating with the same IP address, even though the application is now running on another host.

See also *Internet Protocol address*.

IP address

See *Internet Protocol address*.

IP aliasing

This enables several IP addresses (aliases) to be allocated to one physical network interface. With IP aliasing, the user can continue communicating with the same IP address, even though the application is now running on another host.

See also *Internet Protocol address*.

IP address

See *Internet Protocol address*.

IP aliasing

This enables several IP addresses (aliases) to be allocated to one physical network interface. With IP aliasing, the user can continue communicating with the same IP address, even though the application is now running on another host.

See also *Internet Protocol address*.

IP address

See *Internet Protocol address*.

IP aliasing

This enables several IP addresses (aliases) to be allocated to one physical network interface. With IP aliasing, the user can continue communicating with the same IP address, even though the application is now running on another host.

See also *Internet Protocol address*.

IP address

See *Internet Protocol address*.

IP aliasing

This enables several IP addresses (aliases) to be allocated to one physical network interface. With IP aliasing, the user can continue communicating with the same IP address, even though the application is now running on another host.

See also *Internet Protocol address*.

IP address

See *Internet Protocol address*.

IP aliasing

This enables several IP addresses (aliases) to be allocated to one physical network interface. With IP aliasing, the user can continue communicating with the same IP address, even though the application is now running on another host.

See also *Internet Protocol address*.

IP address

See *Internet Protocol address*.

IP aliasing

This enables several IP addresses (aliases) to be allocated to one physical network interface. With IP aliasing, the user can continue communicating with the same IP address, even though the application is now running on another host.

See also *Internet Protocol address*.

IP address

See *Internet Protocol address*.

IP aliasing

This enables several IP addresses (aliases) to be allocated to one physical network interface. With IP aliasing, the user can continue communicating with the same IP address, even though the application is now running on another host.

See also *Internet Protocol address*.

IP address

See *Internet Protocol address*.

IP aliasing

This enables several IP addresses (aliases) to be allocated to one physical network interface. With IP aliasing, the user can continue communicating with the same IP address, even though the application is now running on another host.

See also *Internet Protocol address*.

IP address

See *Internet Protocol address*.

IP aliasing

This enables several IP addresses (aliases) to be allocated to one physical network interface. With IP aliasing, the user can continue communicating with the same IP address, even though the application is now running on another host.

See also *Internet Protocol address*.

IP address

See *Internet Protocol address*.

IP aliasing

This enables several IP addresses (aliases) to be allocated to one physical network interface. With IP aliasing, the user can continue communicating with the same IP address, even though the application is now running on another host.

See also *Internet Protocol address*.

IP address

See *Internet Protocol address*.

IP aliasing

This enables several IP addresses (aliases) to be allocated to one physical network interface. With IP aliasing, the user can continue communicating with the same IP address, even though the application is now running on another host.

See also *Internet Protocol address*.

IP address

See *Internet Protocol address*.

IP aliasing

This enables several IP addresses (aliases) to be allocated to one physical network interface. With IP aliasing, the user can continue communicating with the same IP address, even though the application is now running on another host.

See also *Internet Protocol address*.

IP address

See *Internet Protocol address*.

IP aliasing

This enables several IP addresses (aliases) to be allocated to one physical network interface. With IP aliasing, the user can continue communicating with the same IP address, even though the application is now running on another host.

See also *Internet Protocol address*.

IP address

See *Internet Protocol address*.

IP aliasing

This enables several IP addresses (aliases) to be allocated to one physical network interface. With IP aliasing, the user can continue communicating with the same IP address, even though the application is now running on another host.

See also *Internet Protocol address*.

IP address

See *Internet Protocol address*.

IP aliasing

This enables several IP addresses (aliases) to be allocated to one physical network interface. With IP aliasing, the user can continue communicating with the same IP address, even though the application is now running on another host.

See also *Internet Protocol address*.

IP address

See *Internet Protocol address*.

IP aliasing

This enables several IP addresses (aliases) to be allocated to one physical network interface. With IP aliasing, the user can continue communicating with the same IP address, even though the application is now running on another host.

See also *Internet Protocol address*.

IP address

See *Internet Protocol address*.

IP aliasing

This enables several IP addresses (aliases) to be allocated to one physical network interface. With IP aliasing, the user can continue communicating with the same IP address, even though the application is now running on another host.

See also *Internet Protocol address*.

IP address

See *Internet Protocol address*.

IP aliasing

This enables several IP addresses (aliases) to be allocated to one physical network interface. With IP aliasing, the user can continue communicating with the same IP address, even though the application is now running on another host.

See also *Internet Protocol address*.

IP address

See *Internet Protocol address*.

IP aliasing

This enables several IP addresses (aliases) to be allocated to one physical network interface. With IP aliasing, the user can continue communicating with the same IP address, even though the application is now running on another host.

See also *Internet Protocol address*.

IP address

See *Internet Protocol address*.

IP aliasing

This enables several IP addresses (aliases) to be allocated to one physical network interface. With IP aliasing, the user can continue communicating with the same IP address, even though the application is now running on another host.

See also *Internet Protocol address*.

IP address

See *Internet Protocol address*.

IP aliasing

This enables several IP addresses (aliases) to be allocated to one physical network interface. With IP aliasing, the user can continue communicating with the same IP address, even though the application is now running on another host.

See also *Internet Protocol address*.

IP address

See *Internet Protocol address*.

IP aliasing

This enables several IP addresses (aliases) to be allocated to one physical network interface. With IP aliasing, the user can continue communicating with the same IP address, even though the application is now running on another host.

See also *Internet Protocol address*.

IP address

See *Internet Protocol address*.

IP aliasing

This enables several IP addresses (aliases) to be allocated to one physical network interface. With IP aliasing, the user can continue communicating with the same IP address, even though the application is now running on another host.

See also *Internet Protocol address*.

IP address

See *Internet Protocol address*.

IP aliasing

This enables several IP addresses (aliases) to be allocated to one physical network interface. With IP aliasing, the user can continue communicating with the same IP address, even though the application is now running on another host.

See also *Internet Protocol address*.

IP address

See *Internet Protocol address*.

IP aliasing

This enables several IP addresses (aliases) to be allocated to one physical network interface. With IP aliasing, the user can continue communicating with the same IP address, even though the application is now running on another host.

See also *Internet Protocol address*.

IP address

See *Internet Protocol address*.

IP aliasing

This enables several IP addresses (aliases) to be allocated to one physical network interface. With IP aliasing, the user can continue communicating with the same IP address, even though the application is now running on another host.

See also *Internet Protocol address*.

IP address

See *Internet Protocol address*.

IP aliasing

This enables several IP addresses (aliases) to be allocated to one physical network interface. With IP aliasing, the user can continue communicating with the same IP address, even though the application is now running on another host.

See also *Internet Protocol address*.

IP address

See *Internet Protocol address*.

IP aliasing

This enables several IP addresses (aliases) to be allocated to one physical network interface. With IP aliasing, the user can continue communicating with the same IP address, even though the application is now running on another host.

See also *Internet Protocol address*.

IP address

See *Internet Protocol address*.

IP aliasing

This enables several IP addresses (aliases) to be allocated to one physical network interface. With IP aliasing, the user can continue communicating with the same IP address, even though the application is now running on another host.

See also *Internet Protocol address*.

IP address

See *Internet Protocol address*.

IP aliasing

This enables several IP addresses (aliases) to be allocated to one physical network interface. With IP aliasing, the user can continue communicating with the same IP address, even though the application is now running on another host.

See also *Internet Protocol address*.

IP address

See *Internet Protocol address*.

IP aliasing

This enables several IP addresses (aliases) to be allocated to one physical network interface. With IP aliasing, the user can continue communicating with the same IP address, even though the application is now running on another host.

See also *Internet Protocol address*.

IP address

See *Internet Protocol address*.

IP aliasing

This enables several IP addresses (aliases) to be allocated to one physical network interface. With IP aliasing, the user can continue communicating with the same IP address, even though the application is now running on another host.

See also *Internet Protocol address*.

IP address

See *Internet Protocol address*.

IP aliasing

This enables several IP addresses (aliases) to be allocated to one physical network interface. With IP aliasing, the user can continue communicating with the same IP address, even though the application is now running on another host.

See also *Internet Protocol address*.

IP address

See *Internet Protocol address*.

IP aliasing

This enables several IP addresses (aliases) to be allocated to one physical network interface. With IP aliasing, the user can continue communicating with the same IP address, even though the application is now running on another host.

See also *Internet Protocol address*.

JOIN (CF)

See *Cluster Join Services*.

keyword (reserved words)

A word that has special meaning in a programming language. For example, in the configuration file, the keyword `node` identifies the kind of definition that follows.

LAN

See *public LAN*.

latency (RMS)

Time interval from when a data transmission request is issued until the actual response is received.

leaf object (RMS)

A bottom object in a system graph. In the configuration file, this object definition is at the beginning of the file. A leaf object does not have children.

LEFTCLUSTER (CF)

A node state that indicates that the node cannot communicate with other nodes in the cluster. That is, the node has left the cluster. The purpose for the intermediate LEFTCLUSTER state is to avoid the network partition problem.

See also *UP*, *DOWN*, *network partition*, *node state*.

line switching unit

This device connects external lines to more than one node and switches the connected nodes by the RCI.

link (RMS)

Designates a child or parent relationship between specific resources.

local area network

See *public LAN*.

local host

The host from which a command or process is initiated.

See also *remote host*.

local MAC address

MAC address that the system administrator of a local area network (LAN) system guarantees to be unique within that system.

log file

The file that contains a record of significant system events or messages. The base monitor, wizards, and detectors can have their own log files.

logical volume (GDS)

General term for a virtual disk device that the user can access directly. The user can access a logical volume in the same way as accessing a physical disk slice (partition). A logical volume is sometimes simply called a "volume." low-order group (GDS)

Group that belongs to another group. A volume cannot be created in a low-order group.

MAC address

Address that identifies the office or node that is used by the MAC sublayer of a local area network (LAN).

MDS

See Meta Data Server.

message

A set of data transmitted from one software process to another process, device, or file.

message queue

A designated memory area which acts as a holding place for messages.

Meta Data Server

GFS daemon that centrally manages the control information of a file system (meta-data).

mirrored disk (RCFS)

A set of disks that contain the same data. If one disk fails, the remaining disks of the set are still available, preventing an interruption in data availability. (Applies to transitioning users of existing Fujitsu Siemens products only.)

See also *mirrored piece*.

mirrored piece (RCFS)

Physical pieces that together comprise a mirrored virtual disk. These pieces include mirrored

disks and data disks. (Applies to transitioning users of existing Fujitsu Siemens products only.)
See also *mirrored disk*.

mirrored volume (GDS)

A volume that is created in a mirror group. Data redundancy is created by mirroring.

mirror group (GDS)

A disk group of the mirror type. This a collection of mutually mirrored disks or low-order groups.

mirroring (GDS)

A setup that maintains redundancy by writing the same data to multiple slices. Even if an error occurs in some of the slices, this setup allows access to the volume to continue as long as a normal slice remains.

mirror virtual disk (VM)

Mirror virtual disks consist of two or more physical devices, and all output operations are performed simultaneously on all of the devices. (Applies to transitioning users of existing Fujitsu Siemens products only.)

See also *concatenated virtual disk*, *simple virtual disk*, *striped virtual disk*, and *virtual disk*.

mixed model cluster

A cluster system that is built from different PRIMEPOWER models. For example, one node is a PRIMEPOWER 1000 machine, and another node is a PRIMEPOWER 200 machine.

The models are divided into two groups, which are represented by the PRIMEPOWER 200, 400, and 600 machines and the PRIMEPOWER 800, 1000, and 2000 machines.

monitoring agent

Component that monitors the state of a remote cluster node and immediately detects if that node goes down. This component is separate from the SA function.

mount point

The point in the directory tree where a file system is attached.

multihosting

Same disk via multiple controllers. (Applies to transitioning users of existing Fujitsu Siemens products only.)

native operating system

The part of an operating system that is always active and translates system calls into activities.

network adapter

A LAN network adapter.

network interface card

See *network adapter*.

network partition (CF)

This condition exists when two or more nodes in a cluster cannot communicate over the interconnect; however, with applications still running, the nodes can continue to read and write to a shared device, compromising data integrity.

NIC switching mode

One of the LAN duplexing modes presented by GLS. The duplexed NIC is used exclusively, and LAN monitoring between the Solaris OE server and the switching HUB, and switchover if an error is detected are implemented.

node

A host which is a member of a cluster. A computer node is a computer.

node state (CF)

Every node in a cluster maintains a local state for every other node in that cluster. The node state of every node in the cluster must be either UP, DOWN, or LEFTCLUSTER.

See also *UP*, *DOWN*, *LEFTCLUSTER*.

object (RMS)

In the configuration file or a system graph, this is a representation of a physical or virtual resource.

See also *leaf object*, *object definition*, *node state*, *object type*.

object definition (RMS)

An entry in the configuration file that identifies a resource to be monitored by RMS. Attributes included in the definition specify properties of the corresponding resource. The keyword associated with an object definition is object.

See also *attribute*, *object type*.

object type (RMS)

A category of similar resources monitored as a group, such as disk drives. Each object type has specific properties, or attributes, which limit or define what monitoring or action can occur. When a resource is associated with a particular object type, attributes associated with that object type are applied to the resource.

See also *generic type*.

online maintenance

The capability of adding, removing, replacing, or recovering devices without shutting or powering off the host.

operating system dependent (CF)

This module provides an interface between the native operating system and the abstract, OS-independent interface that all PRIMECLUSTER modules depend upon.

OPS

See *Oracle Parallel Server*.

Oracle Parallel Server

Oracle Parallel Server allows access to all data in the database to users and applications in a clustered or MPP (massively parallel processing) platform.

OSD (CF)

See *operating system dependent*.

parent (RMS)

An object in the configuration file or system graph that has at least one child.

See also *child*, *configuration file*, and *system graph*.

patrol diagnosis

A function that periodically diagnoses hardware faults.

physical IP address

IP address that is assigned directly to the interface (for example, hme0) of a network interface card. See also *logical IP address*. For information about the logical interface, see the explanation of logical interface in *ifconfig(1M)*.

primary host (RMS)

The default host on which a user application comes online when RMS is started. This is always the hostname of the first child listed in the userApplication object definition.

PRIMECLUSTER services (CF)

Service modules that provide services and internal interfaces for clustered applications.

private network address

Private network addresses are a reserved range of IP addresses specified by RFC1918. They may be used internally by any organization but, because different organizations can use the same addresses, they should never be made visible to the public internet.

private resource (RMS)

A resource accessible only by a single host and not accessible to other RMS hosts.

See also *resource*, *shared resource*.

public LAN

The local area network (LAN) by which normal users access a machine.

See also *Administrative LAN*.

queue

See *message queue*.

quorum

State in which integrity is maintained among the nodes that configure the cluster system. Specifically, the CF state in all nodes that configure the cluster system is either UP or DOWN (there is no LEFCLUSTER node).

RC2000

Software (Java application) that provides functions for operating the operating system console of each node.

redundancy

This is the capability of one object to assume the resource load of any other object in a cluster, and the capability of RAID hardware and/or RAID software to replicate data stored on secondary storage devices.

Reliant Monitor Service (RMS)

The package that maintains high availability of user-specified resources by providing monitoring and switchover capabilities.

remote console connection unit

Device that converts an RS232C interface and a LAN interface. This device allows another device (personal computer) that is connected to the LAN to use the TTY console functions through the Telnet function.

remote host

A host that is accessed through a telecommunications line or LAN.

See also *local host*.

remote node

See *remote host*.

reporting message (RMS)

A message that a detector uses to report the state of a particular resource to the base monitor.

resource (RMS)

A hardware or software element (private or shared) that provides a function, such as a mirrored disk, mirrored disk pieces, or a database server. A local resource is monitored only by the local host.

See also *private resource*, *shared resource*.

resource database (RMS)

Database that manages information on hardware units that are shared among multiple nodes.

The resource database is managed by the cluster resource management facility.

resource definition (RMS)

See *object definition*.

resource label (RMS)

The name of the resource as displayed in a system graph.

resource state (RMS)

Current state of a resource.

RMS

See *Reliant Monitor Services*.

RMS Application Wizards

RMS Application Wizards add new menu items to the RMS Wizard Tools for a specific application.

See also *RMS Wizard Tools*, *Reliant Monitor Services*.

RMS command

Commands that enable RMS resources to be administered from the command line.

RMS configuration

A configuration in which two or more nodes are connected to shared resources. Each node has its own copy of operating system and RMS software, as well as its own applications.

RMS wizard

Software tool that creates confirmation definitions for RMS operation. The RMS wizard consists of the RMS Wizard Tools and the RMS Application Wizards.

See also *RMS Wizard Tools*, *RMS Application Wizards*.

RMS Wizard Tools

A software package composed of various configuration and administration tools used to create and manage applications in an RMS configuration.

See also *RMS Application Wizards*, *Reliant Monitor Services*.

route

In the PRIMECLUSTER Concept Guide, this term refers to the individual network paths of the redundant cluster interfaces that connect the nodes to each other.

SAN

See *Storage Area Network*.

scalability

The ability of a computing system to dynamically handle any increase in work load. Scalability is especially important for Internet-based applications where growth caused by Internet usage presents a scalable challenge.

Scalable Internet Service (SIS)

Scalable Internet Services is a TCP connection load balancer, and dynamically balances network access loads across cluster nodes while maintaining normal client/server sessions for each connection.

SCON

See *single console*.

scope (GDS)

The range of nodes that can share objects in the shared type disk class.

script (RMS)

A shell program executed by the base monitor in response to a state transition in a resource. The script may cause the state of a resource to change.

SDX disk (GDS)

General term for disks that GDS manages. Depending on its use, a SDX disk may be called a single disk, a keep disk, a spare disk, or an undefined disk. An SDS disk is sometimes simply called a "disk."

SDX object (GDS)

General term for resources that GDS manages. The resources include classes, groups, SDX disks, and volumes.

service node (SIS)

Service nodes provide one or more TCP services (such as FTP, Telnet, and HTTP) and receive client requests forwarded by the gateway nodes.

See also *database node*, *gateway node*, and *Scalable Internet Services*.

shared disk connection confirmation

Function that checks whether that all shared disk units are turned on and all cable connections are correct when a node is started.

shared resource

A resource, such as a disk drive, that is accessible to more than one node.

See also *private resource*, *resource*.

Shutdown Facility

A facility that forcibly stops a node in which a failure has occurred. When PRIMECLUSTER decides that system has reach a state in which the quorum is not maintained, it uses the Shutdown Facility (SF) to return the cluster system to the quorum state.

shutdown request

Instruction that forcibly stops the specified node so that the quorum is restored.

simple virtual disk

Simple virtual disks define either an area within a physical disk partition or an entire partition.

See also *concatenated virtual disk*, *striped virtual disk*, and *virtual disk*.

single console

The workstation that acts as the single point of administration for hosts being monitored by RMS.

The single console software, SCON, is run from the single console.

single disk (GDS)

SDX disk that does not belong to a group and can be used to create a single volume.

single volume (GDS)

A volume that is created in a single disk that not belong to a group. There is no data redundancy.

SIS

See *Scalable Internet Services*.

spare disk (GDS)

A spare disk for restoring the mirroring state in place of a failed disk.

state

See *resource state*.

state transition procedure

The state transition procedure receives a state transition instruction from the cluster control and controls activation and deactivation of the resource (start and stop of the application).

Storage Area Network

The high-speed network that connects multiple, external storage units and storage units with

multiple computers. The connections are generally fiber channels.

striped group (GDS)

A disk group of the stripe type. This is a collection of disks or low-order groups that become striping units.

striped virtual disk

Striped virtual disks consist of two or more pieces. These can be physical partitions or further virtual disks (typically a mirror disk). Sequential I/O operations on the virtual disk can be converted to I/O operations on two or more physical disks. This corresponds to RAID Level 0 (RAID0).

See also *concatenated virtual disk*, *mirror virtual disk*, *simple virtual disk*, *virtual disk*.

striped volume (GDS)

A volume that is created in a striped group. Striping allows the I/O load to be distributed among multiple disks. There is no data redundancy.

stripe width (GDS)

The size in which data is divided when striping takes place.

striping (GDS)

Dividing data into fixed-size segments, and cyclically distributing and writing the data segments to multiple slices. This method distributes I/O data to multiple physical disks and issues I/O data at the same time.

switching mode

LAN duplexing mode presented by GLS.

There is a total of six switching mode types: fast switching mode, NIC switching mode, GS/SURE linking mode, multipath mode, and multilink Ethernet mode:

switchover

The process by which a user application transfers processes and data inherited from an operating node to a standby node, based on a user request.

switchover (RMS)

The process by which RMS switches control of userApplication over from one monitored host to another.

See also *automatic switchover*, *directed switchover*, *failover*, and *symmetrical switchover*.

symmetrical switchover (RMS)

This means that every RMS host is able to take on resources from any other RMS host.

See also *automatic switchover*, *directed switchover*, *failover*, and *switchover*.

synchronized power control

When the power of one node is turned in the cluster system configured with PRIMEPOWER, this function turns on all other powered-off nodes and disk array unit that are connected to nodes through RCI cables.

system disk (GDS)

The disk in which the operating Solaris OE is installed. This term refers to the entire disk, including slices that are currently operating as one of the following file systems or swap area:

/, */usr*, */var*, or swap area

system graph (RMS)

A visual representation (a map) of monitored resources used to develop or interpret the configuration file.

See also *configuration file*.

template

See *application template*.

type

See *object type*.

UP (CF)

A node state that indicates that the node can communicate with other nodes in the cluster.

See also *DOWN*, *LEFTCLUSTER*, *node state*.

user group

A group that limits the environment setup, operation management, and other operations presented by Web-Based Admin View and the Cluster Admin GUI. There are four user groups: *wvroot*, *clroot*, *cladmin*, and *clmon*. Each user ID is registered in an appropriate user group by the operation system administrator of the management server.

virtual disk

With virtual disks, a pseudo device driver is inserted between the highest level of the Solaris logical Input/Output (I/O) system and the physical device driver. This pseudo device driver then maps all logical I/O requests on physical disks.

See also *concatenated virtual disk*, *mirror virtual disk*, *simple virtual disk*, *striped virtual disk*.

virtual interface (VIP)

Virtual IP address or host name that SIS uses to make multiple nodes of the cluster appear as a single-system image.

volume (GDS)

See *logical volume (GDS)*.

watchdog timer monitoring

Timer value that measures operating system hangs and boot failures.

Web-Based Admin View

This is a common base enabling use of the Graphic User Interface of PRIMECLUSTER. This interface is in Java.

Wizard (RMS)

An interactive software tool that creates a specific type of application

Abbreviations

AC	Access Client
API	application program interface
BM	base monitor
CF	Cluster Foundation or Cluster Framework
CIM	Cluster Integrity Monitor
CIP	Cluster Interconnect Protocol
CLI	command-line interface
CRM	Cluster Resource Management
DLPI	Data Link Provider Interface
EE	Enterprise Edition
ENS	Event Notification Services
GDS	Global Disk Services
GFS	Global File Services
GLS	Global Link Services
GUI	graphical user interface
HA	high availability
ICF	Internode Communication Facility
I/F	Interface
I/O	input/output

JOIN	cluster join services module
LAN	local area network
MA	Monitoring Agents
MDS	Meta Data Server
MIB	Management Information Base
NIC	network interface card
NSM	Node State Monitor
OPS	Oracle Parallel Server
OSD	operating system dependent
PAS	Parallel Application Services
PS	Parallel Server
RAO	RMS-Add on
RCI	Remote Cabinet Interface
RMS	Reliant Monitor Services
SA	Shutdown Agent
SAN	Storage Area Network
SC	Scalability Cluster
SCON	single console software
SD	Shutdown Daemon
SF	Shutdown Facility
SIS	Scalable Internet Services

VIP Virtual Interface Provider

WK Wizard Kit

WT Wizard Tools

Index

1	
1:1 standby	19
2	
2-tier model.....	25
3	
3-tier model.....	27
A	
Activating Gds Resources	318
Adding a user log group	354
Adding an archive log file	321
Application building procedure and manual reference locations.....	82
Assigning Users to Manage the Cluster	42
Associating resources to a cluster service instance.....	485
attributes.....	126
Attributes	179
Automatic configuration	71
Automatic Configuration of Shared Disks	86
B	
Backing Up and Restoring a PRIMECLUSTER System.....	267
Backing Up the PRIMECLUSTER Operation Environment.....	269
Bringing faulted cluster application to Online state	204
Build flow	3
Building a cluster	59
Building Cluster Applications	81
C	
Cascade Cascade (using one cluster application)	22
Cascade (using two or more cluster applications)	23
CE(FE for North America) Instruction Worksheet	376
CF.....	54
CF main window	190
Change userApplication and Resource	55
Changing a CIP Address	238
Changing a node name	241
Changing a Procedure Resource	480
Changing an IP Address on the Public LAN.....	235
Changing environment variables	243
Changing PRIMECLUSTER operation attributes	244
Changing resources	224
Changing settings for the shared device connection confirmation feature.....	239
Changing System Files.....	340
Changing the cluster application configuration ...	220
Changing the cluster configuration	220
Changing the Operation Attributes of a Cluster Application	221
Changing the operation attributes of a userApplication	242
Changing the operation configuration.....	219
Changing the operation environment for patrol diagnosis.....	240
Changing the RMS Configuration Name	182
Changing the Scalable Log Environment	354
Check script.....	110, 115
Checking the cluster worksheet.....	61
Checking the Operation.....	339
Clear fault.....	10
Clearing the Wait state of a node	204
Clients	25
Cluster Admin.....	53
Cluster Admin functions.....	54
Cluster Application Configuration Worksheets ...	386
Cluster Application Exclusive Worksheet	405
Cluster application operations	203
Cluster Application Worksheet.....	404
Cluster Application Worksheets.....	395
Cluster Building Worksheet	409
Cluster Configuration Worksheet.....	384
Cluster Installation Environment Worksheet.....	380
Cluster nodes	25
Cluster Resource Management Facility Message	493
Cluster states	192
Cmdline Resource Worksheet.....	395
Common.....	51
Concurrent viewing of node and cluster application states	206
Configuration Global Settings Worksheet.....	406
Configuration information or object attributes	200
Confirming Web-Based Admin View Startup	45
Corrective Action for failed resources.....	213
Corrective Action for faulted hardware	214
Corrective Action when patrol diagnosis detects a fault.....	214
Corrective Action when the resource state is Faulted.....	212
Create Resource	55
Create userApplication	55
Creating Gds resources.....	128
Creating a Cluster Application	325
Creating a log file for a user log group.....	322
Creating a log group management file.....	320

Creating a log management file.....	320
Creating a temporary log file.....	320
Creating an archive log file.....	321
Creating an RDB dictionary.....	321
Creating an RDB directory for user log group.....	322
Creating cluster applications.....	166
Creating Cmdline resources.....	107
Creating Fsystem resources.....	123
Creating Gls resources.....	134
Creating ISV resources.....	166
Creating line switching unit resources.....	158
Creating Procedure Resources.....	146
Creating process monitoring resources.....	151
Creating raw devices.....	316
Creating RDB environment.....	320
Creating takeover network resources.....	138
CRM.....	54
CRM Main Window.....	191

D

Deactivating Gds Resources.....	322
Delete userApplication and Resource.....	55
Deleting a cluster application.....	245
Deleting a Cluster Service.....	488
Deleting a Procedure Resource.....	481
Deleting a resource.....	246
Deleting a user log group.....	354
Deleting a userApplication.....	245
Detailed resource information.....	195
Detecting a Failed Resource.....	427
Determining the cluster system operation mode... 19	
Determining the Web-Based Admin View operation mode.....	25
Development.....	8
Disk class.....	129
Disk unit setup.....	35
Displayed resource types.....	191
Displaying environment variables.....	210

E

Editing environment setting files.....	317
Editing RDB configuration parameter files.....	316
Enouncement of hot standby.....	322
Environment variables.....	102
Executing Automatic Configuration.....	86
Executing the fjsnap Command.....	425
Exiting the screen.....	57
Expanding the Operation Configuration.....	253

F

Failed Resource and Operator Intervention Messages (CLI).....	448
--	-----

Failed Resource and Operator Intervention Messages (GUI).....	446
Failed Resource Message.....	428
Failover Maintenance and Management.....	340
Failure detection and cause identification if a failure occurs.....	212
Fault Resource List.....	431
File system setup.....	96
Flag.....	135, 143
Flags.....	118
Fsystem Resource Worksheet.....	397

G

GDS configuration setup.....	86
GDS Configuration Worksheet.....	392, 412
Gds Resource Worksheet.....	398
GDS Setup Worksheets.....	390
GFS Local File System.....	98
GFS Local File System Setup Worksheet ...	386, 411
Global Cluster Services menu functions.....	53
GLS Configuration Worksheet.....	387
Gls Resource Worksheet.....	399
GLS setup.....	83
GLS Setup Worksheet.....	411

I

Identifying faulted hardware.....	214
Initial cluster setup.....	63
Initial Configuration Setup.....	69
Initial GDS setup.....	86
Initial GFS setup.....	98
Initial GLS setup.....	83
Initial setup of the cluster resource management facility.....	68
Initial setup of the operation management server.	45
Initial setup of Web-Based Admin View.....	45
Installation.....	5
Installation and environment setup of applications	39
Installation and setup of related software.....	35
Installation procedure and manual reference sections.....	7
Installation script.....	34
Interstage Application Server Enterprise Edition	299

K

Kernel parameter check and setup.....	35
Kernel Parameter Worksheet.....	381

L

Line Switching Unit Resource Worksheet.....	403
Live priority.....	65

<i>M</i>	
Management server.....	25
Manual.....	51
Manual pages.....	419
Manual series.....	474
Messages.....	433
Messages related to CF.....	433
Messages Related to CRM View.....	439
Messages Related to Line Switching Unit ..	434, 439
Messages Related to RMS.....	436
MISC.....	51
Monitoring Cluster Control Messages.....	211
Monitoring the PRIMECLUSTER system.....	205
Monitoring the state of a cluster application.....	205
Monitoring the state of a node.....	205
Mount point.....	123
Mount points.....	125
Multipath disk.....	37
Mutual standby.....	21
<i>N</i>	
N:1 standby.....	20
Network setup.....	35
Node states.....	192
Notes on script creation.....	101
Notes on Worksheet Creation.....	374
NTP setup.....	35
<i>O</i>	
One Shot Installer.....	34
Operating the PRIMECLUSTER system.....	202
Operation and Maintenance.....	13
Operation attribute types.....	242
Operation menu functions.....	50
Operation Mode Change.....	14
Operations.....	189, 193
Other resource states.....	193
Overall Design Worksheet.....	374
<i>P</i>	
Patrol Diagnosis Messages.....	456
planning.....	4
Preparations.....	61
Preparations for starting the Web-Based Admin	
View screen.....	42
Preparing the client environment.....	43
PRIMECLUSTER.....	50
PRIMECLUSTER Enterprise Edition.....	16
PRIMECLUSTER function selection.....	17
PRIMECLUSTER HA Server.....	16
PRIMECLUSTER Installation.....	34
PRIMECLUSTER Product List.....	277
PRIMECLUSTER product selection.....	16
PRIMECLUSTER Products.....	275
PRIMECLUSTER System Design Worksheets ..	373
PRIMECLUSTER Wizard for NetWorker.....	281
PRIMECLUSTER Wizard for Oracle.....	293
Procedure Resource Messages.....	466
Procedure Resource Worksheet.....	401
Process Monitoring Function.....	151
Process Monitoring Messages.....	469
Process Monitoring Resource Worksheet.....	402
<i>R</i>	
Registering a cluster service.....	483
Registering a procedure resource.....	479
Registering SynfinityCluster-compatible	
resources.....	483
Registering, changing, and deleting stage	
transition procedure resources for	
SynfinityCluster compatibility.....	479
Registrating RDB resources.....	323
Replacement test.....	11
Resource association.....	121
Resource Fault History.....	53, 429
Resource icons.....	191
Resource states.....	192
Resource type.....	108
Resources.....	106
Restoring the PRIMECLUSTER Operation	
Environment.....	270
RMS.....	54
Editing global settings in Configuration.....	176
RMS graphs.....	209
RMS Main Window.....	197
RMS Operation.....	202
RMS tree.....	197
<i>S</i>	
Sample scripts.....	101
SCF dump.....	426
Script files.....	111
Set Dependency Between userApplications.....	56
Set Shared Information in the Configuration.....	56
Setting environment variables.....	318
Setting exclusive relationships between cluster	
applications.....	172
Setting the failover range of a cluster application ..	29
Setting the Web-Based Admin View Language....	46
Setting up CF and CIP.....	63
Setting up cluster applications.....	104
Setting up dependency relationships between	
cluster applications.....	171
Setting Up Disk Units.....	36

Setting Up Exclusive Relationships Between Cluster Applications	336	Symfoware Server Hot Standby Option.....	309
Setting up fault resource identification and operator intervention request	79	SysNode.....	109
Setting up Online/Offline scripts	101	System configuration modification	217
Setting Up Patrol Diagnosis.....	183	System Design	18
Setting up power supply linkage	76	System Design examples	407
Setting Up Resources.....	106	System Disk Mirror Setup Worksheet.....	391, 412
Setting up shared disk connection confirmation ...	77	System dump	426
Setting up shared disks	91	Systemwalker CentricMGR	357
Setting Up Symfoware and the Cluster System Environment.....	316	Systemwalker OperationMGR	363
Setting up system disk mirroring.....	87	Systemwalker WebMGR	369
Setting up the application environment.....	100		
Setting up the browser.....	47	<i>T</i>	
Setting up the Java Plug-in.....	47	Takeover IP address.....	134
Setting Up the Network.....	36	Takeover Network Resource Worksheet	400
Setting up the operating system console.....	61	Terminology	473
Setting up the shutdown facility	65	Test.....	9
Setting up Web-Based Admin View when GLS is used	85	Troubleshooting.....	425
Shared Disk Connection Confirmation Messages.....	436, 454		
Shared disks.....	131	<i>U</i>	
Shared resource states	193	User groups.....	42
SIS.....	54	userApplication Configuration Wizard	53, 105, 107, 166, 172, 176, 325, 336
Site Preparation.....	15	userApplication Configuration Wizard functions ...	55
Softtek AdvancedCopy Manager	305	userApplication Configuration Wizard GUI messages	458
Software Installation	33	Using SynfinityCluster Products in PRIMECLUSTER.....	473
Standby Operation.....	19		
Start script	110, 111	<i>V</i>	
Starting a cluster application.....	203	Viewing application logs	208
Starting a Cluster Application	338	Viewing detailed resource information	209
Starting RMS	202	Viewing logs created by the PRIMECLUSTER system	207
Starting the Web-Based Admin View screen ..	41, 48	Viewing switchlogs	208
Startup test	10	Viewing the PRIMECLUSTER system operation management screens	190
Stop	11	Volume setup.....	91
Stop script.....	110, 113		
Stopping a cluster application.....	203	<i>W</i>	
Stopping RMS	202	Web-Based Admin View screen	50
Supplement on Cluster Application and Resource Deletion.....	248	What Are the PRIMECLUSTER Operation Modes.....	278
Switching a cluster application.....	203	Work process continuity	12
Switchlogs and application logs.....	200	Worksheet purpose	373
Switchover	10		